Benjamin Strekha

# Group Theory and Linear Representation Theory

– Notes –

November 30, 2023

# Preface

These notes are about group theory and its applications to the sciences, particularly physics and chemistry. Many excellent textbooks on group theory already exist. However, I do think these notes have something to offer. I think group theory is an extremely important and useful tool that any physicist (theorist or experimentalist) could use productively. However, I remember being frustrated when learning group theory because no book seemed to have quite what I wanted. I wanted a book that didn't shy away from proofs but was also not quite written for aspiring theoretical mathematicians. It wasn't once or twice that I read statements like "$SU(2)$ is a double cover of $SO(3)$" in physics textbooks, only to have "double cover" never explained and any statements involving it never proven. Or, in classical mechanics contexts, that a rigid motion of an object can be written as a translation followed by a rotation about some axis through the object (this is Chasles' theorem). I always found this frustrating. We will explicitly and clearly prove that any rotation in $\mathbb{R}^3$, in other words any $R \in SO(3)$, is a rotation about some axis. Likewise, we will guide through problems many aspects of the "double cover" claims and prove or, at the very least, see plausible outlines of the proofs of those claims.

After covering the traditional group theory topics that are covered in Part I of these notes, an overwhelming number of abstract algebra books switch gears to rings, fields, Galois theory, etc... We won't do this. Instead, we will switch to representation theory of finite groups in Part II and then go to applications in physics settings. My goal is to get to applications as fast as possible while still being rigorous and proving as many claims as possible. Hopefully this approach and style is useful to some.

Large parts of Part I, II are heavily influenced by the fine lectures given in Fine Hall by Dr. Mark McConnell for MATH 340 in the Fall 2019 semester at Princeton University. Those parts were then fleshed out a bit more during the Fall 2020 semester. I also learned and borrowed a lot from Serre's "Linear Representation of Finite Groups," Zee's "Group Theory in a Nutshell for Physicists," and parts of Dummit and Foote's "Abstract Algebra."

Princeton, NJ *Benjamin Strekha*

September 2020

# Contents

Part I Theory of Groups

Part II Linear Representations of Finite Groups

Part III Applications

# Part I
# Theory of Groups

The first part covers the general terminology of group theory and proves many of the theorems of group theory taught to undergraduates in the USA. Before applying group theory to interesting applications in physics or cryptography, one must first invest some time to learn the fundamentals. This is quite similar to learning the fundamentals of piano practice before trying to learn Piano Concerto No. 2 in C minor by Sergei Rachmaninoff. Do not rush through the first part. Read and understand the theorems. Work through as many exercises as possible to reinforce the concepts introduced in the chapters. The more exciting stuff in later parts builds on previously introduced concepts, so there is no point in rushing.

# Chapter 1
# Introduction to Abstract Algebra

**Abstract** This chapter introduces groups abstractly and then provides some examples.

## 1.1 What is a Group?

**Definition 1.1** Let $G$ be a set. A binary operation, which we will label by $\diamond$, is a map $\diamond : G \times G \to G$. Denote the image of $(x, y) \in G \times G$ by $x \diamond y$ instead of $\diamond(x, y)$.

**Definition 1.2** A binary operation $\diamond : G \times G \to G$ is associative if $x \diamond (y \diamond z) = (x \diamond y) \diamond z$ for any $x, y, z \in G$.

**Definition 1.3** Let $G$ be a set and let $\diamond : G \times G \to G$ be a binary operation. We say $x, y \in G$ commute if $x \diamond y = y \diamond x$.

**Definition 1.4** Let $G$ be a set and let $\diamond : G \times G \to G$ be a binary operation. We say that $G$ with this binary operation is a group if

- $\diamond$ is associative.
- There exists an element $e \in G$ called the identity element such that $x \diamond e = e \diamond x = x$ for any $x \in G$.
- For any $x \in G$ there exists a $y \in G$ such that $x \diamond y = y \diamond x = e$. We say that $y$ is the inverse of $x$.

If $x \diamond y = y \diamond x$ for $\forall x, y \in G$ we say that $G$ is an abelian (or commutative) group. Otherwise, we say that $G$ is a non-abelian (or noncommutative) group. If $G$ is a finite set, we say that it is a finite group. Note that the existence of the identity element ensures that a group is not an empty set.

Note: We do not need to explicitly state that $G$ must be closed under the binary operation since the definition of the binary operator $\diamond : G \times G \to G$ already implies closure. The condition of closure under the binary operation will, however, need to be stipulated separately for subgroups.

Note: Writing $x \diamond y$ can get tedious and some groups have a binary operation that we normally think of as multiplication. Therefore, often one uses the multiplicative notation where $x \diamond y$ is written as $xy$ and the inverse of $x$ is denoted as $x^{-1}$. In general, $x^n$ for $n \in \mathbb{Z}$ will mean

$$x^n = \begin{cases} \overbrace{x \cdots x}^{n \text{ terms}} & \text{if } n > 0, \\ e & \text{if } n = 0, \\ \underbrace{x^{-1} \cdots x^{-1}}_{|n| \text{ terms}} & \text{if } n < 0. \end{cases} \tag{1.1}$$

Also note that one needs to write $x^{-1}y$ or $yx^{-1}$, since it usually matters. For abelian groups, $x^{-1}y = yx^{-1}$ and sometimes even for non-abelian groups two elements can commute. However, in general we cannot use notation such as $\frac{y}{x}$. If the group is non-abelian, should one interpret $\frac{x}{y}$ as $xy^{-1}$ or $y^{-1}x$?

Note: Writing $x \diamond y$ can get tedious and some groups have a binary operation that we normally think of as addition. When this is the case, one can write $x + y$ instead of $x \diamond y$ and $-x$ for the inverse of $x$. Also, often the identity element for additive groups is written as 0 instead of $e$. Instead of writing $x^n$, we write $nx$ where we mean

$$nx = \begin{cases} \overbrace{x + \cdots + x}^{n \text{ terms}} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ \underbrace{(-x) + \cdots + (-x)}_{|n| \text{ terms}} & \text{if } n < 0. \end{cases} \tag{1.2}$$

In additive notation, we will sometimes write $x - y$, which we define to mean $x + (-y)$. The additive notation is almost always used for abelian groups, so $x + (-y)$ or $(-y) + x$ will be the same and leave no ambuguity.

Later on, we will often omit $\diamond$, unless a clear distinction or emphasis is needed. Instead, we will usually use the multiplicative notation in lemmas, corollaries, theorems, and proofs unless the groups we deal with have a natural addition operation already associated with the elements. For clarity, if a group $G$ has a binary operation $\diamond$ and identity element $e$ we will write the group as

$$(G, \diamond, e) \qquad \text{or} \qquad (G, \diamond).$$

This notation makes it clear what the set is ($G$), what the group binary operation is ($\diamond$), and what element in $G$ is the identity element ($e$). Before continuing with examples, we note that one can deduce properties of groups using only the group axioms.

**Proposition 1.1** *Let G be a group. Then*

*i) The identity element e of a group G is unique.*

*ii) The inverse of an element $x \in G$ is unique.*
*iii) The inverse of the inverse of an element is that element. That is, $(x^{-1})^{-1} = x$ for all $x \in G$.*
*iv) $(xy)^{-1} = y^{-1}x^{-1}$ for any $x, y \in G$.*
*v) For any $x_1, x_2, \ldots, x_n \in G$ the value of $x_1 \cdot x_2 \cdots x_n$ is independent of how the expression is parenthesized. This is called the general associative law.*

***Proof*** We use multiplicative notation here (as will often, but not always, be the case throughout this text).

i) Suppose that $e, e'$ were both identity elements in $G$. Then

$$\begin{aligned} e' &= e \cdot e' && \text{since } e \text{ is an identity element} \\ &= e && \text{since } e' \text{ is an identity element} \end{aligned} \tag{1.3}$$

ii) Assume that $y$ and $y'$ are inverses of $x$. Then

$$\begin{aligned} y' &= e \cdot y' \\ &= (y \cdot x) \cdot y' \\ &= y \cdot (x \cdot y') \quad \text{(by associativity)} \\ &= y \cdot e \\ &= y. \end{aligned} \tag{1.4}$$

Thus, $y = y'$ so the inverse is unique.

iii) Since $x^{-1} \cdot x = x \cdot x^{-1}$, this means that $x$ is an inverse of $x^{-1}$. Since we proved that inverses are unique, this means that $x$ is the inverse of $x^{-1}$. That is, $(x^{-1})^{-1} = x$.

iv) The reader is asked to prove this in Problem 1.1. (Do it now!)

v) This holds trivially for $n = 1, n = 2$ and it holds for $n = 3$ by the group axioms. This establishes a base case which can be used in (strong) mathematical induction. We will show all parenthesizations are equivalent by showing that they all equal

$$((\ldots(x_1 \cdot x_2) \cdot x_3) \ldots) \cdot x_n, \tag{1.5}$$

which is called the left-associated expression. Let $n > 3$ and assume that the theorem holds for all $1 \leq m < n$. Note that no matter how we parenthesize the expression, there will always be an outermost multiplication:

$$a \cdot b \tag{1.6}$$

where $a = x_1 \cdots x_m$ and $b = x_{m+1} \cdots x_n$ for some integer $0 < m < n$. We don't know how these $a, b$ are parenthesized, but by assumption those parenthesizations can be written/reinterpreted as left-associated expressions. Then we note the following:

- If $b$ consists of only one term (that is, $m = n - 1$), then the expression for $a \cdot b$ is a left-associated expression.

- If $b$ has more then one term, then we note that we can rewrite $a \cdot b$ as

  $$a \cdot b = a \cdot (c \cdot x_n) \tag{1.7}$$

  where $c = x_{m+1} \cdots x_{n-1}$ is a left-associated expression (make sure that you see why this is true). Applying associativity then gives

  $$a \cdot b = (a \cdot c) \cdot x_n, \tag{1.8}$$

  and so the expression $a \cdot c$ can be rewritten/reinterpreted as a left-associated expression so that the final expression for $a \cdot b$ is left-associated.

This completes the induction and the proof. □

*Example 1.1* The set of all integers $\mathbb{Z}$ forms a group under addition (in the usual sense of addition). This is because

- Addition is associative.
- The integer 0 acts like the identity element since $0 + x = x + 0 = x$ for any $x \in \mathbb{Z}$.
- Every nonzero integer $x \in \mathbb{Z}$ has an integer, which we label as $-x$, such that $x + (-x) = (-x) + x = 0$. (Zero is its own inverse.)

This group can be succinctly denoted as $(\mathbb{Z}, +, 0)$.

**Definition 1.5** Let $G$ be a finite group. The number of elements in $G$ is called the order or cardinality of the group. We write $|G|$ for the order of the group.

**Definition 1.6** Let $G$ be a group and let $x \in G$. We define the order of $x \in G$ to be the smallest positive integer $n$ such that $x^n = e$. If no such positive integer $n$ exists, we say that $x$ has infinite order. We write $|x|$ for the order of the element $x \in G$.

Note: Do not confuse these notations for absolute values.

*Example 1.2* The group $(\mathbb{Z}, +, 0)$ is infinite. Every nonidentity element has infinite order. For example, adding 1 to itself any number of times always increases, never going to 0, which is the identity element of this group. Thus, 1 has infinite order.

Note: In the above example, don't think that $1^2 = 1$, so 1 has finite order. Do not confuse multiplicative notation in definitions and theorems with the actual action of multiplication that you learned in prior courses. The group binary operation in the above example is addition, not multiplication.

Let's consider a few more examples of groups.

*Example 1.3* The set $\{1, -1, i, -i\}$ where $i = \sqrt{-1}$ is a group under complex multiplication. The inverse of $-1$ is $-1$, and $i, -i$ are inverses of each other. This is a finite group. $-1$ has order 2, while $i$ and $-i$ have order 4.

*Example 1.4* The set of all positive rational numbers, denoted $\mathbb{Q}^+$, $\mathbb{Q} - \{0\}$, or $\mathbb{Q} \backslash \{0\}$ is a group under multiplication. The number 1 acts as the identity element, and every rational number $r \in \mathbb{Q}^+$ has an inverse $r^{-1}$ which is also a positive rational number.

*Example 1.5* Let $C$ be the set of all complex number of modulus 1 is a group under multiplication. That is,

$$C = \{z \mid z \in \mathbb{C}, |z| = 1\}, \tag{1.9}$$

where $|z|$ means the complex modulus of $z$. Do not confuse $C$ with $\mathbb{C}$. See Figure 1.1 for a visualization of the set $C$.

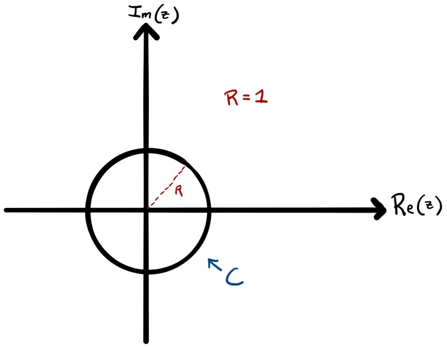


Fig. 1.1: The set $C$ is a unit circle in the complex plane, centered at the origin.

*Example 1.6* The set of all 2-by-2 matrices form a group under component-wise addition. That is,

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}. \tag{1.10}$$

The identity element of this set is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ (*not* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$! Don't be confused by this!). The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

See Problem 1.4 to practice using the binary notation $\diamond$ and to check your understanding of the group axioms. 1.4.

### 1.1.1 The Cayley Table. Once and Only Once.

A convenient way to gather information about a *finite* group is using a Cayley table, or multiplication table (since multiplicative notation is very common). Suppose that the group $G$ has $n$ elements. Label the elements of $G$ as follows:

$$g_1, g_2, \ldots, g_n. \tag{1.11}$$

Construct an $n$-by-$n$ table where the $(i, j)$ entry (the $i^{th}$ row and $j^{th}$ column) is the element $g_i g_j$ (in multiplicative notation. In general, the $(i, j)$ entry is $g_i \diamond g_j$.). See Table 1.1.

Table 1.1: Cayley table for a generic finite group.

| $\diamond$ | $\cdots$ | $g_j$ | $\cdots$ |
|---|---|---|---|
| $\vdots$ | $\ddots$ | | |
| $g_i$ | | $g_i g_j$ | |
| $\vdots$ | | | $\ddots$ |

A nice property of such a table is that each group element appears only once in each row and each column. This is because every element in the group has an inverse. That is, suppose that in row $i$ there were two columns $j, k$ such that $g_i g_j = g_i g_k$. Since we are dealing with a group, $g_i$ has an inverse $g_i^{-1}$, so

$$g_i g_j = g_i g_k, \tag{1.12}$$

$$g_i^{-1} g_i g_j = g_i^{-1} g_i g_k, \tag{1.13}$$

$$g_j = g_k. \tag{1.14}$$

Thus, $j = k$ so the columns are actually the same. Of course, a similar argument can be repeated to show that each element appears only once in any given column. A useful mnemonic for this property is to think of this as the "once and only once rule."

*Example 1.7* Consider the group in Example 1.3. That is, consider the set $\{1, -1, i, -i\}$ where $i = \sqrt{-1}$ and the binary operation is multiplication. The Cayley table for this group is shown in Table 1.2.

Table 1.2: Cayley table for the group in Example 1.7

| $\cdot$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

### 1.1.2 The Dihedral Group

**Definition 1.7** A regular $n$-gon is the plane figure with $n$ equal sides and $n$ equal interior angles.

See Figure 1.2 for some examples of $n$-gons.

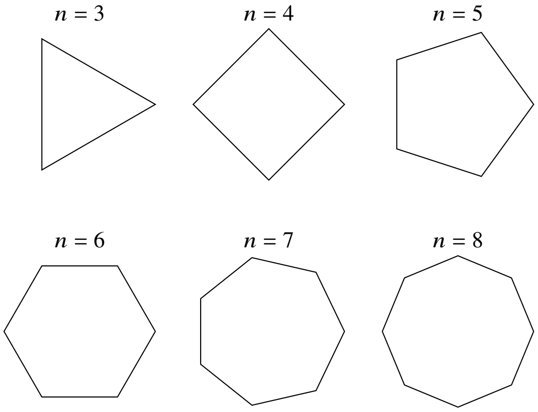


Fig. 1.2: Examples of regular $n$-gons.

**Definition 1.8** The dihedral group $D_n$ is the group of symmetries of the regular $n$-gon in the plane, including rotations and reflections.

Important remark: Some books denote the group of symmetries of a regular $n$-gon as $D_{2n}$. As we will see below, the size of the symmetry group of rotations and reflections for an $n$-gon is $2n$. Thus, the books that write $D_{2n}$ choose to let the subscript denote the order of the group. *In this book, we will choose the subscript to denote the number of edges of the shape*. Thus, for us $|D_n| = 2n$ instead of $|D_{2n}| = 2n$. If you read about dihedral groups online or in other books, make sure you figure out which notation is used to avoid confusion.

Let $r$ be counter-clockwise ↺ rotation by $2\pi/n$ radians. Let $s$ be reflection across a line that goes through the center of the $n$-gon and through a vertex (a horizontal line through through each of the examples provided in Figure 1.2 would work as a chose for $s$).

*Example 1.8* Consider the 6-gon. There are 6 distinct rotations that leave the 6-gon invariant. These are rotations by $k \cdot 2\pi/6$ for $k = 0, 1, \ldots, 5$. There are also 6 lines for which reflection across the line leaves the 6-gon invariant. See Figure 1.3. Therefore, we count 6 rotations and 6 reflections for a total of 12 symmetries of the 6-gon.

*Example 1.9* Consider the 5-gon. There are 5 distinct rotations that leave the 5-gon invariant. These are rotations by $k \cdot 2\pi/5$ for $k = 0, 1, \ldots, 4$. There are also 5 lines for

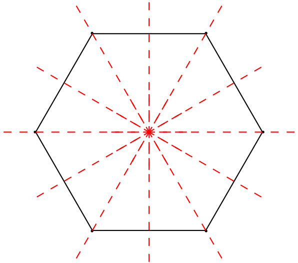


Fig. 1.3: Lines for which reflection across the line is a symmetry. There are 6 such lines for a 6-gon.

which reflection across the line leaves the 5-gon invariant. See Figure 1.4. Therefore, we count 5 rotations and 5 reflections for a total of 10 symmetries of the 5-gon.

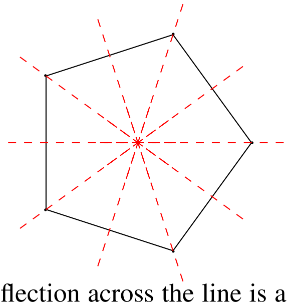


Fig. 1.4: Lines for which reflection across the line is a symmetry. There are 5 such lines for a 5-gon.

Notice that for the 5-gon, all the lines of reflection pass through one vertex and the middle of the opposing edge. Compare this to the 6-gon in Example 1.8. Therefore, there were lines of reflection that passes through two opposing vertices or through the middles of two opposing edges. Convince yourself that this is a general observation. An $n$-gon with $n \geq 3$ odd has only one "type" of line of reflection but if $n \geq 3$ is even then it has two "types" of lines of reflections.

Plane regions can be given either a counter-clockwise ↺ or a clockwise ↻ orientation. In $\mathbb{R}^3$, there are two orientations, which can be distinguished by the right-hand rule and the left-hand rule. A transformation can be orientation-preserving or orientation-reversing. We will see later in Chapter 12 that in $\mathbb{R}^n$ a linear transformation $A$ is orientation-preserving if $\det A > 0$ and orientation-reversing if $\det A < 0$. Orientation-preserving transformations of $\mathbb{R}^n$ are called rotations. Orientation-reversing transformations of $\mathbb{R}^n$ are reflections, or products of reflections.

**Proposition 1.2** *Every element of $D_n$ is either $r^k$ or $r^k s$ for $k = 0, \ldots, n-1$.*

***Proof*** There are exactly $n$ rotations of $D_n$

$$e = r^0, r, \ldots, r^{n-1}. \tag{1.15}$$

These are orientation-preserving transformations. Let $t$ be any orientation-reversing element of $D_n$. Then $ts$ is orientation-preserving. There must exist a $k \in \{0, \dots, \text{n-1}\}$ such that $ts = r^k$. By the group axioms, $s$ has an inverse $s^{-1}$ so

$$t = te = t(ss^{-1}) = (ts)s^{-1} = r^k s^{-1}. \tag{1.16}$$

Finally, it is clear that reflecting twice is the same as the identity: $s^2 = e$. This means that $s^{-1} = s$. Thus, $t = r^k s$. Since $t$ was an arbitrary orientation-reversing element of $D_n$, we have proven our claim. □

Thus, we see that $D_n = \{\underbrace{e, r, r^2, \dots, r^{n-1}}_{n \text{ rotations}}, \underbrace{s, rs, r^2 s, \dots, r^{n-1}s}_{n \text{ reflections}}\}$.

Thus, $|D_n| = 2n$ in our notation. Let's build some computational techniques to use when dealing with $D_n$ for $n \geq 3$. We note that $r^n = e, s^2 = e$. We claim that $rs = sr^{-1}$ and $sr = r^{-1}s$.

**Proposition 1.3** *In $D_n$ for any $n \geq 3$, $rs = sr^{-1}$.*

***Proof*** WLOG, let $s$ be reflection across the horizontal axis (so we center our coordinate system at the center of the $n$-gon). Let $r$ be counter-clockwise ↺ rotation by $2\pi/n$. Let $\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Let $\mathbf{v} = \mathbf{e}_1$ and let $\mathbf{w} = \begin{bmatrix} \cos(2\pi/n) \\ \sin(2\pi/n) \end{bmatrix}$. Since $n > 2$, $\{\mathbf{v}, \mathbf{w}\}$ is a basis for $\mathbb{R}^2$. If suffices to show that $rs$ and $sr^{-1}$ act on the same on $\mathbf{v}$ and on $\mathbf{w}$ (do you see why?). Let $\mathbf{u} = \begin{bmatrix} \cos(-2\pi/n) \\ \sin(-2\pi/n) \end{bmatrix}$. See Figure 1.5 for a visualization of these vectors.

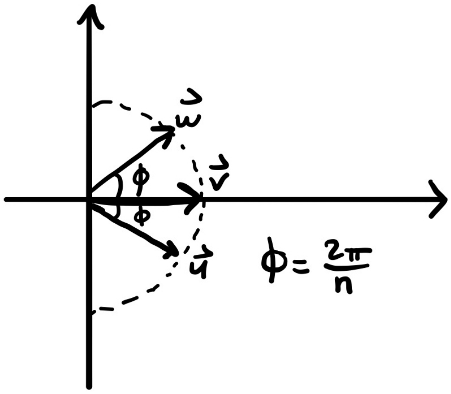


Fig. 1.5: A visualization of the vectors $\mathbf{u}, \mathbf{v}, \mathbf{w}$ used in the proof. With this figure it is easy to see, for example, that $\mathbf{w} \overset{s}{\longmapsto} \mathbf{u}$.

Note that

$$\mathbf{v} \overset{s}{\longmapsto} \mathbf{v} \overset{r}{\longmapsto} \mathbf{w} \tag{1.17}$$

$$\mathbf{v} \overset{r^{-1}}{\longmapsto} \mathbf{u} \overset{s}{\longmapsto} \mathbf{w} \tag{1.18}$$

so $sr$ and $r^{-1}s$ act the same on $\mathbf{v}$. Note that

$$\mathbf{w} \overset{s}{\longmapsto} \mathbf{u} \overset{r}{\longmapsto} \mathbf{v} \tag{1.19}$$

$$\mathbf{w} \overset{r^{-1}}{\longmapsto} \mathbf{v} \overset{s}{\longmapsto} \mathbf{v} \tag{1.20}$$

so $sr$ and $r^{-1}s$ act the same on $\mathbf{w}$. As a side note, we found that in the basis $\{\mathbf{v}, \mathbf{w}\}$ the matrix representing $rs$ and $sr^{-1}$ is $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Since $sr, r^{-1}s$ act the same on $\mathbf{v}, \mathbf{w}$ we conclude that $rs = sr^{-1}$ for the dihedral group for $n \geq 3$ (why?). □

**Proposition 1.4** *In $D_n$ for any $n \geq 3$, $sr = r^{-1}s$.*

***Proof*** Instead of doing this geometrically, we now use associativity of group elements and Proposition 1.3.

$$sr = (sr)e = (sr)(s^2) = s(rs)s = s(sr^{-1})s = s^2(r^{-1}s) = r^{-1}s. \tag{1.21}$$

Perhaps even simpler, we note that one can multiply both sides of $rs = sr^{-1}$ by $r^{-1}$ from the left and $r$ from the right,

$$r^{-1}(rs)r = r^{-1}(sr^{-1})r \tag{1.22}$$

$$(r^{-1}r)(sr) = (r^{-1}s)(r^{-1}r) \tag{1.23}$$

$$sr = r^{-1}s. \tag{1.24}$$

This leads to the following observation: Any expression in $D_n$ in powers of $r, s$ can be reduced by moving $r$ across $s$ (left or right). When you move $r$ past $s$ (left or right), change $r$ to $r^{-1}$. Of course, we already knew this from Proposition 1.2 but now we have the computational tools to do the reductions.

**Proposition 1.5** $r^a sr^b = r^{a-b}s$.

***Proof*** Consider $r^a sr^b$. Without loss of generality, assume $a, b > 0$. Then

$$r^a sr^b = r^a s \underbrace{r \cdots r}_{\text{b terms}} = r^a r^{-1} s \underbrace{r \cdots r}_{\text{b−1 terms}} = \cdots = r^a r^{-b} s. \tag{1.25}$$

*Example 1.10* Consider the following product of $s, r$ in $D_n$ for $n \geq 3$.

$$\begin{aligned} r^5 sr^3 s &= r^5 r^{-3} ss \\ &= r^{5-3} s^2 \\ &= r^2. \end{aligned} \tag{1.26}$$

### 1.1.3 The Infinite Dihedral Group

Consider the real line. Define $t : \mathbb{R} \to \mathbb{R}$ as a translation to the right by one unit. That is, $t(x) = x + 1$ for all $x \in \mathbb{R}$. Define $s : \mathbb{R} \to \mathbb{R}$ to be reflection across the origin. That is, $s(x) = -x$ for all $x \in \mathbb{R}$. Let $D_\infty$ be the set of functions

$$\cdots, t^{-2}, t^{-1}, e, t, t^2, \cdots \tag{1.27}$$

$$\cdots, t^{-2}s, t^{-1}s, s, ts, t^2 s, \cdots \tag{1.28}$$

where $e$ is the identity map and the binary operation is function composition. Note that $(s \circ t)(x) = s(x+1) = -x - 1$ for all $x \in \mathbb{R}$ and $(t^{-1} \circ s)(x) = t^{-1}(-x) = -x - 1$ for any $x \in \mathbb{R}$. Thus, $t^{-1} \circ s = s \circ t$. Clearly $s^2 = e$ while $t^n \neq e$ for any $n \in \mathbb{Z}$. We call $D_\infty$ the infinite dihedral group, for obvious reasons.

Remark: The infinite dihedral group hints that groups can be quite abstract and widely applicable. Notice that the binary operation above is function composition, and not multiplication or addition. While often the binary operation of interest is related to multiplication or addition of some sort that we are used to, do keep mind that we can think of any set of objects as have a group structure as long as there is a binary operation defined on those objects which satisfies the group axioms.

## 1.2 What is a Ring?

Sometimes we want to consider two binary operations instead of one. Let's call the binary operations addition and multiplication.

**Definition 1.9** A ring $(R, +, \cdot, 0)$ is a set with two binary operations $R \times R \to R$, which we call addition and multiplication, such that

- Addition is commutative: $x + y = y + x$ for any $x, y \in R$.
- Addition is associative: $(x + y) + z = x + (y + z)$ for any $x, y, z \in R$.
- There exists an element in $R$, denote it 0, such that $x + 0 = 0 + x = x$ for any $x \in R$.
- For any $x \in R$, there exists a $y \in R$ such that $x + y = y + x = 0$. Such a $y$ is often denote $-x$.
- $x(yz) = (xy)z$ for any $x, y, z \in R$.
- $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for any $x, y, z \in R$.

Remark: The first four properties imply that $R$ is an abelian group under addition. That is, $(R, +, 0)$ is an abelian group (verify this). However, the multiplication is *not* necessarily abelian. Even more, $R$ does not necessarily have a multiplicative identity! If it does, we call such an element an identity (or a multiplicative identity), often denoted 1. Actually, the multiplicative identity is unique so it is not an identity of the ring but *the* identity of the ring. Also, *even if* $R$ has an identity, every element in $R$ is not guaranteed to have a multiplicative inverse.

**Definition 1.10** Let $R$ be a ring with an identity. If $x \in R$ has a multiplicative inverse, then we say that $x$ is a unit of the ring. That is, $x$ is a unit if there exists $y \in R$ such that $xy = yx = 1$. Often, such a $y$ is denoted as $x^{-1}$.

**Definition 1.11** Let $R$ be a ring with identity. The set of units in $R$ is denoted $R^{\times}$. $(R^{\times}, \cdot, 1)$ is a group, called the group of units of $R$.

Though we will focus on groups, we mention a particular type of ring that the reader should be aware of.

**Definition 1.12** A field is a commutative ring $F$ with identity such that every $x \in F$, $x \neq 0$, has a multiplicative inverse.

For any field $F$, $F^{\times} = F - \{0\}$.

*Example 1.11* $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields. $\mathbb{Z}$ is not a field since most elements do not have inverses.

*Example 1.12* $\mathbb{Z}^{\times} = \{1, -1\}$ is a group under multiplication. Any other element in $\mathbb{Z}$ is not a unit. For example, $2 \in \mathbb{Z}$ requires $2 \cdot y = 1$. While $y = \frac{1}{2} \in \mathbb{R}$ would work, $\frac{1}{2} \notin \mathbb{Z}$ so 2 is not a unit.

*Example 1.13* $\mathbb{Q}^{\times} = \mathbb{Z} - \{0\}$. Every element of $\mathbb{Q}$ has a multiplicative inverse which also belongs to $\mathbb{Q}$, except for 0.

0 is never a unit. This is because $0 \cdot x = x \cdot 0 = 0$ for all $x$.

**Proposition 1.6** *In any ring $R$, for any $x \in R$ we have* $0 \cdot x = x \cdot 0 = 0$.

***Proof*** $0 = 0 + 0$. Hence $0 \cdot x = (0 + 0) \cdot x$. Multplication distributes:

$$0 \cdot x = 0 \cdot x + 0 \cdot x. \tag{1.29}$$

Whatever $0 \cdot x \in R$ is, it has an additive inverse $y$. Add $y$ to both sides:

$$0 \cdot x + y = (0 \cdot x + 0 \cdot x) + y. \tag{1.30}$$

Addition is associative, so this is the same as

$$\begin{aligned} 0 \cdot x + y &= 0 \cdot x(0 \cdot x + y) && (1.31) \\ 0 &= 0 \cdot x + 0 && (1.32) \\ 0 &= 0 \cdot x. && (1.33) \end{aligned}$$

A similar proof shows $x \cdot 0 = 0$. □

Note: We will assume that $1 \neq 0$. Suppose that $1 = 0$, then every $x \in R$ is 0 since

$$x = 1 \cdot x = 0 \cdot x = 0. \tag{1.34}$$

While this is a legitimate ring, call it the zero ring $R = \{0\}$, it is not too interesting and there is not much to study about it.

**Definition 1.13** A ring $R$ is commutative if $x \cdot y = y \cdot x$ for all $x, y \in R$.

**Definition 1.14** Let $R$ be a commutative ring and let $a, b \in R$ with $a \neq 0$. We say that $a$ divides $b$ if there exists $c \in R$ such that $c = ab$. If $a$ does not divide $b$, then we write $a \nmid b$.

Compare such a definition to division in the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$. The resemblance should be clear.

*Example 1.14* $\mathbb{Z}$ under ordinary addition and multiplication is a commutative ring with an identity. The only units in $\mathbb{Z}$ are +1 and -1.

*Example 1.15* $\mathbb{Z}$ with $+_n$ (addition modulo $n$) and $\cdot_n$ (multiplication modulo $n$) is a commutative ring with identity (the identity being the number 1). The set of units is labeled $\mathbb{Z}_n^\times$.

*Example 1.16* $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}, \mathbb{R}$, and $\mathbb{C}$ are commuative rings with identity.

*Example 1.17* Let $\mathbb{Z}[x]$ be the set of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication. Then $\mathbb{Z}[x]$ is a ring with identity. The polynomial 1 is the identity of $\mathbb{Z}[x]$.

*Example 1.18* Consider the set of all 2-by-2 matrices with entries in $\mathbb{Z}$. This is a noncommutative ring with identity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

*Example 1.19* The set $2\mathbb{Z}$ (set of even integers) is a ring under ordinary addition and multiplication. However, it has no identity. It is commutative.

**Definition 1.15** Let $R$ be a commutative ring. Let $M_n(R)$ be the set of $n$-by-$n$ matrices with entries in $R$. $M_n(R)$ is a ring where addition is the component-wise addition and multiplication is matrix multiplication. The zero element of $M_n(R)$ is the matrix with all $0 \in R$. If $R$ has an identity element, then $M_n(R)$ has an identity element, which is the matrix with $0 \in R$ on the off-diagonals and $1 \in R$ along the diagonal. Even if $R$ is commutative, $M_n(R)$ is not necessarily commutative.

**Definition 1.16** Let $GL_n(R)$ be the set of $n$-by-$n$ invertible matrices with entries in a commutative ring with identity $R$. This is the general linear group.

Actually, if $R$ is a commutative ring with identity then $GL_n(R)$ is the group of units of $M_n(R)$:

$$GL_n(R) = M_n(R)^\times. \tag{1.35}$$

## 1.3 Subgroups

**Definition 1.17** Let $G$ be a group. A subset $H \subseteq G$ is called a subgroup of $G$ if $H$ is a group under the same group multiplication as $G$. If $H$ is a subgroup of $G$, write $H \leq G$. If $H \subset G$ is a proper subset of $G$ and is a subgroup, write $H < G$.

To check that $H$ is a subgroup of $G$, check:

0. $H$ is nonempty.
1. $H$ is closed under the binary operation of $G$. That is, if $x, y \in H$ then $xy \in H$.
2. $H$ is closed under inverses. That is, if $x \in H$ then $x^{-1} \in H$.

In order to be a subgroup (or a group, for that matter), the set must be nonempty (it must at least contain an identity element). Although this is often left implicit, we explicitly state this as step 0 for clarity. This is called the two-step test for a subgroup. There is also a one-step test.

**Theorem 1.1** *The Subgroup Criterion - A nonempty subset H of G is a subgroup of G if and only if*

*0.* $H \neq \emptyset$.
*1. If* $x, y \in H$, *then* $xy^{-1} \in H$ *as well.*

***Proof*** $\Rightarrow$ If $H$ is a subgroup then $e \in H$ and $xy^{-1} \in H$ for $\forall x, y \in H$ since it it closed under inverses and group multiplication.
$\Leftarrow$ Since $H \neq \emptyset$, pick $x \in H$. Then $x(x)^{-1} = e \in H$ by 1). Also, $e(x)^{-1} = x^{-1} \in H$ by 1). Therefore, for any $x, y \in H$, we have $x, x^{-1}, y, y^{-1} \in H$. By 1), this means $x(y^{-1})^{-1} = xy \in H$. Since $e \in H$ and we have closure under inverses and group multiplication, so $H \leq G$. □

*Example 1.20* $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0)$. Here, the binary operation is addition in the "usual" sense. The addition of two integers is an integer. The negative of an integer is also an integer and the additive inverse of that integer. 0 acts as the group identity element when the binary operation is addition of numbers in the usual sense.

*Example 1.21* $(\mathbb{Q}^{\times}, \cdot, 0) \leq (\mathbb{R}^{\times}, \cdot, 0) \leq (\mathbb{C}^{\times}, \cdot, 0)$. Here, the binary operation is multiplication in the "usual" sense. The multiplication of two rational numbers is a rational number. The inverse of a rational number is a rational number. 1 acts as the group identity element when the binary operation is multiplication of numbers in the usual sense.

*Example 1.22* In $D_n$, the orientation-preserving symmetries (rotations) are a subgroup of $D_n$. For example, $\{e, r, r^2, r^3\} \leq D_4$.

**Definition 1.18** Let $R$ be a commutative ring with 1 (with identity). Define

$$SL_n(R) = \{A \in GL_n(R) \mid \det(A) = 1\}.$$

We call this the special linear group.

**Proposition 1.7** $SL_n(R) \leq GL_n(R)$.

***Proof*** $SL_n(R)$ is nonempty since $I \in SL_n(R)$. Pick $A, B \in SL_n(R)$ and note that

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\det(B)^{-1} = 1 \cdot 1 = 1. \tag{1.36}$$

Thus, $AB^{-1} \in SL_n(R)$. By Theorem 1.1, $SL_n(R) \leq GL_n(R)$. □

**Theorem 1.2** *Let $G$ be a group. Suppose $H_1 \leq G$ and $H_2 \leq G$. Then $H_1 \cap H_2 \leq G$.*

***Proof*** Since $H_1 \leq G$ and $H_2 \leq G$, we know $e \in H_1$ and $e \in H_2$. Therefore, $e \in H_1 \cap H_2$ so $H_1 \cap H_2$ is nonempty. Let $x, y \in H_1 \cap H_2$. Then $x, y \in H_1$ and $x, y \in H_2$. Since $H_1$ and $H_2$ are subgroup of $G$, $xy^{-1} \in H_1$ and $xy^{-1} \in H_2$ and, thus, $xy^{-1} \in H_1 \cap H_2$. □

Note: More generally, if you have a family of subgroups of $G$ (infinite or finite) then their intersection is still a subgroup of $G$.

**Definition 1.19** Let $G$ be a group and $S \subseteq G$ be any (nonempty) subset. A word in $S$ is an expression $s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k}$ where $s_i \in S, n_i \in \mathbb{Z}$ for all $i = 1, 2, \ldots, k$ and $k$ is finite. Let $\langle S \rangle$ be the set of all these words. ($e$ is the empty word.)

*Example 1.23* We know that $D_n = \langle r, s \rangle$ since every element of $D_n$ is $r^k$ or $r^k s$ for some $k = 0, 1, \cdots, n-1$ by Proposition 1.2.

Remark: This is not unique. We also have $D_n = \langle r, rs \rangle$. This is because $r^{-1}(rs) = s \in \langle r, rs \rangle$ so any word in terms of $r, s$ is also a word in terms of $r, rs$ and vice-versa.

*Example 1.24* Consider the Gaussian integers $\{a + bi \mid a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$. This set is an (additive) subgroup of $(\mathbb{C}, +, 0)$ and is equal to $\langle 1, i \rangle$. See Figure 1.6.

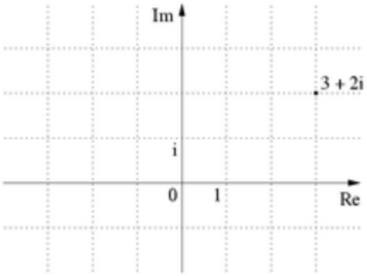


Fig. 1.6: Gaussian integers are located at the vertices of the squares outlined by the dotted lines.

**Theorem 1.3** *$\langle S \rangle$ is a group.*

***Proof*** $\langle S\rangle$ is nonempty since $e \in \langle S\rangle$. Closure is clear since a product of finite number of elements is also finite. Also, $(s_1^{n_1}s_2^{n_2}\cdots s_k^{n_k})^{-1} = s_k^{-n_k}s_{k-1}^{-n_{k-1}}\cdots s_1^{-n_1}$ which is also a word in S. □

**Definition 1.20** $\langle S\rangle$ is called the subgroup of $G$ generated by $S$.

**Theorem 1.4** *Let $G$ be a group. Let $S \subseteq G$ be some subset. Let $C$ be the collection of all subgroups $H \leq G$ such that $S \subseteq H$. Then*

$$\langle S\rangle = \underbrace{\bigcap_{H\in C} H}_{\textit{Called the smallest subgroup of G that contains S.}} .$$

***Proof*** There are several things to check here.

- $\bigcap_{H\in C} H$ is a subgroup since it is the intersection of subgroups. (See Theorem 1.2.)
- If we call $\bigcap_{H\in C} H$ the smallest subgroup of $G$ that contains $H$, then this should make sense in English. It does because suppose $K \leq G$ and $S \subseteq K$. Then $K \in C$ so that $\bigcap_{H\in C} H \leq K$ since $\bigcap_{H\in C} H$ can only contain elements that are also contained in $K$. This holds for arbitrary $K \leq G$ with $S \subseteq K$.
- Need to check that $\langle S\rangle = \bigcap_{H\in C} H$. Note that $\langle S\rangle \in C$ so that $\bigcap_{H\in C} H \subseteq \langle S\rangle$. Now pick any $H \in C$. Since $S \in H$ and $H$ is a subgroup of $G$, $H$ contains every word in $S$. That is, $\langle S\rangle \subseteq H$ for any $H \in C$. Therefore, $\langle S\rangle \subseteq \bigcap_{H\in C} H$.

What this shows is that the subgroup generated by $S \subseteq G$ and the intersection of all the subgroups of $G$ that contain $S$ are the same notions. □

**Definition 1.21** A group $G$ is cyclic if it is generated by one element. That is, $G$ is cyclic if there exists some element $x \in G$ such that $G = \langle x\rangle$.

*Example 1.25* $(\mathbb{Z}, +, 0)$ is cyclic with generator 1. However, we note that $-1$ is also a generator so we see that generators are not, in general, unique. (They are unique in some cases, like for $\mathbb{Z}_2$.)

*Example 1.26* $(\mathbb{Z}_7^\times, \cdot, 1)$ is cyclic and generated by 3. That is, $\mathbb{Z}_7^\times = \langle 3\rangle$. (Verify this!)

Let's set up some notation. $\mathbb{Z}_n$ without the $^\times$ means $(\mathbb{Z}_n, +, 0)$ or the ring. $\mathbb{Z}_n^\times$ is the multiplicative group of units.

## 1.4 Ordering

Let us consider sets with an ordering relation.

**Definition 1.22** Let $\mathbb{N}$ = the set of natural numbers = $\{x \in \mathbb{Z} \mid x \geq 0\}$.

**Definition 1.23** Let $S \subseteq \mathbb{N}$. We say that an element $s \in S$ is a least element of $S$ if for any other element $t \in S$, $s \le t$.

*Example 1.27* Let $S = \{x \in \mathbb{N} \mid x \ge 10 \text{ and } x \text{ is odd}\}$. Then 11 is the least element of $S$.

**Definition 1.24** A set with $<$ is well-ordered if every nonempty subset of it has a least element.

*Example 1.28* $\mathbb{Z}$ is ordered but not well-ordered. For example, the subset of all negative elements of $\mathbb{Z}$ has no least element. There are many subsets of $\mathbb{Z}$ that have no least element.

Axiom for us: $\mathbb{N}$ is well-ordered. Actually, induction can be proved from well-ordering and vice-versa, depending on which one is taken as the axiom. Since it is a useful mathematical proof technique, we remind the reader what mathematical induction is. Mathematical induction says that if we are given statements $S(n)$ such that for every integer $n \ge 1$ integer

i) $S(1)$ is true (called the base case),
ii) $S(n)$ is true implies that $S(n+1)$ is true,

then $S(n)$ is true for every $n \ge 1$. Here is a classic example.

*Example 1.29* What is the sum of the first 100 positive integers? We can do even better and prove a formula for general $n$:

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{1.37}$$

for any $n \in \mathbb{Z}^+$. We note that the formula holds for $n = 1$ (always start by proving a base case). Suppose that the formula holds for $n$. Then

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2}, \end{aligned} \tag{1.38}$$

so the formula also holds for $n+1$. By mathematical induction, the formula holds for all integers $n \ge 1$. Using this, we find that the sum of the first 100 positive integers is $\frac{100 \cdot 101}{2} = 50 \cdot 101 = 5050$.

*Example 1.30* $\{x \mid x \in \mathbb{Q}, x \geq 0\}$ is not well ordered. Suppose it was and let $y \in \mathbb{Q}$ be the least element. But $\frac{y}{2} \in \mathbb{Q}$ and $\frac{y}{2} < y$, contradicting our choice of $y$. Therefore, $\mathbb{Q}$ is not well-ordered.

Knowing that $\mathbb{N}$ is well ordered, we can prove another theorem.

**Theorem 1.5** *Every subgroup of* $(\mathbb{Z}, +, 0)$ *is a cyclic subgroup.*

***Proof*** Since $(\mathbb{Z}, +, 0)$ has addition as the binary operation, it is natural to use the additive notation here. Let $H$ be a subgroup of $(\mathbb{Z}, +, 0)$. If $H = \{0\}$, then $H$ is clearly cyclic. Suppose $H \neq \{0\}$. Pick $x \in H$ with $x \neq 0$. Since $x \in H$, then $-x \in H$ since $H$ is a subgroup and hence closed under inverses. One of $-x, x$ is positive. Thus, there is at least one positive integer in $H$. Pick the smallest positive integer in $H$, call it $n$. This is possible by the well-ordering of $\mathbb{N}$. We want to show that $H = \langle n \rangle$. For any $a \in H$, we can use the division algorithm to write $a = qn + r$ where $0 \leq r < n$ (and $qn$ means do the additive operation $q$ times). Since $H$ is a subgroup, we also have $qn \in H$, $-qn \in H$, and $a - qn \in H$. But $a - qn = r$. Thus, $r \in H$. But $0 \leq r < n$ and we get a contradiction for the choice of $n$ (the smallest positive integer in $H$) unless $r = 0$. Thus, $a \in H$ is $a = qn$. But $a \in H$ was arbitrary. Therefore, $H = \langle n \rangle$, a cyclic subgroup of $G$. □

Using the above, one can show that any subgroup of a cyclic group is cyclic.

**Theorem 1.6** *Let $G$ be a cyclic group. Then every subgroup $K \leq G$ is cyclic.*

***Proof*** Let $x$ be a generator of $G$, so $G = \langle x \rangle$. Every element of $G$ or $K$ can be written as $x^n$ for some $n \in \mathbb{Z}$. Let

$$H = \{n \in \mathbb{Z} \mid x^n \in K\}. \tag{1.39}$$

We alert the reader that we are using multiplicative notation for $G$ and $K$ but additive notation for $H$. $H$ is a subgroup of $(\mathbb{Z}, +, 0)$ since

$$\begin{aligned} n, m \in H &\Rightarrow x^n, x^m \in K && (1.40)\\ &\Rightarrow x^{n-m} \in K \quad \text{(closure under inverses and multiplication)} && (1.41)\\ &\Rightarrow n - m \in H \quad \text{(definition of } H\text{)}. && (1.42) \end{aligned}$$

By Theorem 1.5, $H$ is cyclic, say $H = \langle a \rangle$. Therefore, $K$ is cyclic, with $K = \langle x^a \rangle$. □

**Theorem 1.7** *Let $G$ be a group and let $g$ be an element of order $n$ in $G$. If $g^k = e$, then $n$ divides $k$.*

***Proof*** By the division algorithm, $k = qn + r$ for some integers $q, r$ with $0 \leq r < n$. Therefore, $e = g^k = g^{qn+r} = (g^n)^q g^r = g^r$, which contradicts that $|g| = n > r$ if $r > 0$. Thus, $r = 0$ so $k = qn$, and so $n$ divides $k$. □

**Theorem 1.8** *Let $g$ be an element of order $n$. Let $k$ be a positive integer. Then $\langle g^k \rangle = \langle g^{gcd(n,k)} \rangle$ and $|g^k| = \frac{n}{gcd(n,k)}$.*

***Proof*** Define $d = \gcd(d, k)$ to clean up the notation. Then $k = dr$ for some positive integer $r$. Since $g^k = (g^d)^r$, this means $\langle g^k \rangle \subseteq \langle g^d \rangle$. Also, there exist integers $s, t$ such that $d = ns + kt$. So, $g^d = g^{ns+kt} = g^{ns}g^{kt} = (g^n)^s(g^k)^t = (g^k)^t \in \langle g^k \rangle$. Thus, $\langle g^d \rangle \subseteq \langle g^k \rangle$. Combining both subset inequalities, we conclude $\langle g^k \rangle = \langle g^{\gcd(n,k)} \rangle$.

Now let $d$ be any divisor of $n$ and not just a gcd. Consider the element $g^d$. This has order equal to $|g^d| = n/d$ for any divisor of $n$. To see this, note that $(g^d)^{n/d} = g^n = e$ so the order satisfies $|g^d| \leq n/d$. Now we need to show the inequality in the other direction. Suppose $b$ is a positive integer less than $n/d$. Then $(g^d)^b = g^{db} \neq e$ because otherwise, since $db < n$, this would contradict that $|g| = n$ ($n$ must be the smallest such positive power where $g^n = e$). Thus, $|g^d| \geq n/d$. Combining the two inequalities yields $|g^d| = n/d$. □

## Problems

**1.1** Let $x, y$ be any element of a group $G$.

a) Prove that $(xy)^{-1} = y^{-1}x^{-1}$.
b) Prove or disprove: $(xy)^{-1} = x^{-1}y^{-1}$ in general.

**1.2** Let $G$ be a group. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = e$ for $\forall x, y \in G$.

**1.3** Let $G$ be a group. Show that $g$ and $g^{-1}$ have the same order for $\forall g \in G$.

**1.4** Consider $(\mathbb{R} - \{-1\}, \diamond)$ where the binary operation

$$\diamond : (\mathbb{R} - \{-1\}) \times (\mathbb{R} - \{-1\}) \longrightarrow (\mathbb{R} - \{-1\})$$

is defined by

$$x \diamond y = xy + x + y$$

for all $x, y \in \mathbb{R} - \{-1\}$. The right-hand side means the "usual" multiplication and addition in $\mathbb{R}$.

a) Show that $(\mathbb{R} - \{-1\}, \diamond)$ is an abelian group. What is the identity element?
b) Solve for $x$:

$$2 \diamond x \diamond x = 11.$$

**1.5** Let $G$ be a group. Let $x, y \in G$ be arbitrary. Show that $|x| = |yxy^{-1}|$. Conclude that $|xy| = |yx|$ for $\forall x, y \in G$.

**1.6** Let $G$ be a group. Let $x, y \in G$. Suppose that $x, y, xy$ each have order 2. Prove that $xy = yx$.

**1.7** Let $G$ be a group. Prove that if $g^2 = e$ for $\forall g \in G$ then $G$ is abelian.

**1.8** Let $G$ be a group and let $x, y \in G$ be commuting elements. That is, $xy = yx$. Prove that $(xy)^n = x^n y^n$ for any $n \in \mathbb{Z}$.

**1.9** a) Let $x \in G$ be arbitrary. Suppose that $|x| = n$ and that $x^k = e$. Prove that $n$ divides $k$.

b) Let $x \in G$ be such that $x^2 \neq e$ and $x^6 = e$. Prove that $x^4 \neq e$ and $x^5 \neq e$. What can be said about the order of $x$?

**1.10** a) Let $n$ be an integer. Prove that

$$(x \cdot y \pmod{n}) \cdot z \pmod{n} = x \cdot (y \cdot z \pmod{n}) \pmod{n}.$$

b) Let $p$ be a prime number and let $x$ be an integer which satisfies $1 \leq x \leq p - 1$. Show that none of $x, 2x, \cdots, (p-1)x$ is a multiple of $p$. Deduce the existence of an integer $z$ such that $1 \leq z \leq p-1$ and $xz = 1 \pmod{p}$.

c) Using the previous parts, convince yourself that when $n$ is a prime, the numbers $\{1, 2, \cdots, n-1\}$ with a binary operation of multiplication modulo $n$ forms a group.

d) What goes wrong when $n$ is not a prime number?

**1.11** An element $x$ of a group satisfies $x^2 = e$ if and only if $x = x^{-1}$. Show that a finite group of even order has an odd number of elements of order 2.

**1.12** Recall that $GL_n(\mathbb{R})$ is the group of $n \times n$ invertible matrices $A$ such that both $A$ and $A^{-1}$ have entries in $\mathbb{R}$.

a) Show that $GL_1(\mathbb{R})$ is abelian.

b) Show that $GL_n(\mathbb{R})$ is non-abelian for any $n \geq 2$.

c) In linear algebra, $A$ and $SAS^{-1}$ are similar matrices. In group theory, we say $SAS^{-1}$ is a conjugate of $A$. The conjugacy class of $A$ is $\{SAS^{-1}$ |S is invertible$\}$. Let $\lambda_1, \cdots, \lambda_n$ be distinct nonzero real numbers. Let $D$ be the $n \times n$ matrix with $\lambda_1, \cdots, \lambda_n$ down the diagonal and 0 everywhere else. Think back to your linear algebra course, then fill in the blank: the conjugacy class of $D$ in $GL_n(\mathbb{R})$ is exactly the set of matrices whose characteristic polynomial ________.

**1.13** Which elements of the infinite dihedral group have finite order? Do these elements form a subgroup of $D_\infty$?

**1.14** Let $G$ be a group.

a) Let $H = \{g \in G \mid g$ has finite order$\}$. If $G$ is abelian, show that $H$ is a subgroup of $G$. It is called the <u>torsion subgroup</u> of $G$.

b) Define $H$ as before, but suppose that $G$ is not abelian. Show by example that $H$ may not be a subgroup. (Hint: Consider $D_\infty$ and Problem 1.13.)

**1.15** a) In $D_4$, let $h$ be the reflection in a horizontal line, and let $d$ be the reflection in one of the corner-to-corner diagonals. What is $\langle h, d \rangle$?

b) Find a subgroup $H = \langle r_1, r_2 \rangle$ where $r_1$ and $r_2$ are reflections and $|H| = 4$.

**1.16** Show that $(\mathbb{Q}, +, 0)$ is not cyclic. Even better, show that it cannot be generated by a finite number of elements.

**1.17** What is the sum of the square of the first $n$ natural numbers? That is, find the expression in

$$\sum_{k=1}^{n} k^2 = [\text{some expression involving } n].$$

(Hint: Work out the sum for $n = 1, 2, 3, \dots$ until you see a pattern. Guess a formula that agrees with your work. Use induction to prove that it holds for all positive integers $n$.)

**1.18** Suppose $a, b \in \mathbb{Z}$ are not both zero.

a) Let $H = \{\lambda a + \mu b \mid \lambda, \mu \in \mathbb{Z}\}$. Show that $H$ is a subgroup of $(\mathbb{Z}, +, 0)$.
b) Let $d$ be the smallest positive integer in $H$. Then $d = \gcd(a, b)$ is the greatest common divisor of $a$ and $b$. (Consequently, the greatest common divisor of two integers $a, b$ can always be written as a linear combination $\gcd(a, b) = \lambda a + \mu b$ with integer coefficients.)

**1.19** Suppose $G$is a group and $a, b \in G$ have the property that $b^6 = e$ and $ab = b^4 a$. Show that the order of $b$ is at most 3 and that $ab = ba$. (Hint: consider $aba^{-1}$.)

**1.20** a) Prove that no group is the union of two proper subgroups.
b) Can a group be the union of three proper subgroups?

# Chapter 2
# The Euclidean Algorithm and the Chinese Remainder Theorem

**Abstract** Before proceeding with group theory, we go over some properties of numbers to help us consider more sophisticated groups.

## 2.1 The Euclidean Algorithm

**Definition 2.1** Let $a, b \in \mathbb{Z}$, with $b \neq 0$. We say $b$ is a divisor (or a factor) of $a$ if $\exists c \in \mathbb{Z}$ such that $b \cdot c = a$. In this case, we write $b \mid a$ (read "b divides a"). If $b$ is not a divisor (or a factor) of $a$, we write $b \nmid a$ (read "b does not divide a").

*Example 2.1* We have $5 \mid 60$ since $5 \cdot 12 = 60$.

**Definition 2.2** Let $b, c \in \mathbb{Z}$. A common divisor (also called a common factor) of $b, c$ is an $x \in \mathbb{Z}$ such that $x \mid b$ and $x \mid c$. The greatest common divisor (gcd) (also called the highest common factor (hcf)) is the greatest of the common divisors.

*Example 2.2* Let $b = 2019$ and $c = 249$. Then $249 = 3 \cdot 83$ and $2019 = 3 \cdot 673$. But 83 is prime and $83 \nmid 2019$. Thus, $\gcd(b, c) = 3$.

However, this approach is not practical all the time. If $b, c$ are large then finding the prime factorization is too hard. Also, one can do even better than just finding $\gcd(b, c)$. If $d = \gcd(b, c)$ then one can find $s, t \in \mathbb{Z}$ such that $d = sb + tc$. This is the idea of the Euclidean algorithm. Idea: Input $b, c \in \mathbb{Z}$ not both zero and get as outputs $d \in \mathbb{Z}$ with $d > 0$ and $s, t \in \mathbb{Z}$ such that $d = \gcd(b, c)$ and $d = sb + tc$. Before proving the Euclidean algorithm, we will need the following lemma.

**Lemma 2.1** *If $b = cq + r$ then the set of common divisors of $b, c$ equals the set of common divisors of $c, r$.*

***Proof*** $\Rightarrow$ Let $x$ be a common divisor of $b, c$. This means there $\exists y, z \in \mathbb{Z}$ such that $xy = b$ and $xz = c$. Therefore $r = b - cq = xy - xzq = x(y - zq)$. But $y - zq \in \mathbb{Z}$ so $x \mid r$.

$\Leftarrow$ Let $x$ be a common divisor of $b, r$. This means there $\exists x, z \in \mathbb{Z}$ such that $xy = r$ and $xz = c$. Therefore $b = cq + r = xzq + xy = x(zq + y)$. But $zq + y \in \mathbb{Z}$ so $x \mid b$.□

**Corollary 2.1** *If* $b = cq + r$, *then* $\gcd(b, c) = \gcd(c, r)$.

***Proof*** By Lemma 2.1, $b, c$ and $c, r$ have the same set of common divisors and, therefore, also the same greatest common divisor. □

**Theorem 2.1** *The* <u>*Euclidean algorithm*</u> *relies on iterating the division algorithm. Initially,* $b = cq_1 + r_1$ *where without loss of generality we let* $c \neq 0$ *and* $c > 0$. *Divide* $b$ *by* $c$. *This gives a remainder* $r_1$. *Divide* $c$ *by* $r_1$. *This gives a remainder* $r_2$. *Diving* $r_1$ *by* $r_2$ *and get a remainder* $r_3$. *Keep diving* $r_k$ *by* $r_{k+1}$ *until the remainder* $r_{N+1}$ *is 0. This is more clear when written as follows:*

$$\begin{aligned}
b &= q_1 c + r_1 & 0 &\le r_1 < c \\
c &= q_2 r_1 + r_2 & 0 &\le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &\le r_3 < r_2 \\
&\vdots & &\vdots \\
r_{N-2} &= q_N r_{N-1} + r_N & 0 &\le r_N < r_{N-1} \\
r_{N-1} &= q_{N+1} r_N + 0. & &
\end{aligned}$$

$r_N$ *is the greatest common divisor* $d = \gcd(b, c)$ *we seek.*

***Proof*** Using the lemma, we know that

$$\begin{aligned}
\gcd(b, c) &= \gcd(c, r_1) \\
\gcd(c, r_1) &= \gcd(r_1, r_2) \\
\gcd(r_1, r_2) &= \gcd(r_2, r_3) \\
&\vdots \\
\gcd(r_{N-2}, r_{N-1}) &= \gcd(r_{N-1}, r_N) \\
\gcd(r_{N-1}, r_N) &= \gcd(r_N, 0) \\
&= r_N
\end{aligned} \tag{2.1}$$

This works because $N < \infty$ since each remainder $r_k$ is strictly less than the previous remainder $r_{k-1}$, so the algorithm eventually terminates. □

**Proposition 2.1** *Given* $b, c \in \mathbb{Z}$ *and* $d = \gcd(b, c)$, *then there exist* $s, t \in \mathbb{Z}$ *such that* $d = sb + tc$. *We sometimes says that* $d$ *is a* $\mathbb{Z}$*-linear combination of* $b, c$.

***Proof*** This is really just a consequence of Theorem 2.1. One just needs to backsolve. Using the notation of Theorem 2.1, we have

$$d = r_N = r_{N-2} - q_N r_{N-1}. \tag{2.2}$$

But, we also have

$$r_{N-1} = r_{N-3} - q_{N-1}r_{N-2}, \tag{2.3}$$

so we have

$$d = r_N = r_{N-2} - q_N(r_{N-3} - q_{N-1}r_{N-2}). \tag{2.4}$$

But $r_{N-3} = r_{N-4} - q_{N-2}r_{N_3}$ and so on. Eventually we can get rid of all the remainders until we are left with an expression involving $b$ and $c$. This will end up looking something like

$$d = (\#)b + (\#)c,$$

where the numbers multiplying $b, c$ are some combinations of $q_1$, $q_2$,$\cdots$, $q_N$, $r_1$, $r_2$,$\cdots$, $r_N$ in such a way that still belongs to $\mathbb{Z}$ (this is because we only add, subtract, and multiply numbers in $\mathbb{Z}$ so the result is still in $\mathbb{Z}$). These are the $s, t$ that we claimed exist. □

*Example 2.3* Let $b = 96$ and $c = 44$

$$\begin{align} 96 &= 2 \cdot 44 + 8 \tag{2.5}\\ 44 &= 5 \cdot 8 + 4 \tag{2.6}\\ 8 &= 2 \cdot 4 + 0. \tag{2.7}\end{align}$$

Thus, we have $4 = \gcd(96, 44)$ since it is the last nonzero remainder. Backsolving, we have

$$\begin{align} 4 &= \underline{44} - 5 \cdot \underline{8} \tag{2.8}\\ &= \underline{44} - 5 \cdot (\underline{96} - 2 \cdot \underline{44})\\ &= -5 \cdot \underline{96} + 11 \cdot \underline{44}\\ &\equiv s \cdot b + t \cdot c, \end{align}$$

so we see that $s = -5$ and $t = 11$. Indeed, use your favorite calculator (or work it out manually) to verify that

$$4 = (-5 \cdot 96) + (11 \cdot 44). \tag{2.9}$$

*Example 2.4* Let $b = 2019$ and $c = 249$

$$\begin{align} 2019 &= 8 \cdot 249 + 27 \tag{2.10}\\ 249 &= 9 \cdot 27 + 6 \tag{2.11}\\ 27 &= 4 \cdot 6 + 3 \tag{2.12}\\ 6 &= 2 \cdot 3 + 0. \tag{2.13}\end{align}$$

Thus, we have $3 = \gcd(2019, 249)$ since it is the last nonzero remainder. Backsolving, we have

$$\begin{aligned}
3 &= \underline{27} - 4 \cdot \underline{6} \qquad (2.14)\\
&= \underline{27} - 4 \cdot (\underline{249} - 9 \cdot \underline{27})\\
&= \underline{27} - 4 \cdot \underline{249} + 36 \cdot \underline{27}\\
&= 37 \cdot \underline{27} - 4 \cdot \underline{249}\\
&= 37 \cdot (\underline{2019} - 8 \cdot \underline{249}) - 4 \cdot \underline{249}\\
&= 37 \cdot \underline{2019} - (37 \cdot 8) \cdot \underline{249} - 4 \cdot \underline{249}\\
&= 37 \cdot \underline{2019} - 300 \cdot \underline{249}\\
&\equiv s \cdot b + t \cdot c,
\end{aligned}$$

so we see that $s = 37$ and $t = -300$. Indeed, use your favorite calculator (or work it out manually) to verify that

$$3 = (37 \cdot 2019) + (-300 \cdot 249). \qquad (2.15)$$

Comment: We underline some numbers (the remainders that appeared in the Euclidean division algorithm, actually) in the work only as a guide for our eyes so we know what it is that we are trying to keep and what can be multiplied out and simplified. Work out Problem 2.1 and/or Problem 2.2 to try this yourself.

In closing, we mention some useful tips for later chapters for proving theorems or solving problems. In Chapter 6 we prove that $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn$. The division algorithm, the Euclidean algorithm, $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn$, and properties of modular addition and modular multiplication are very useful when dealing with groups such as $\mathbb{Z}_n, \mathbb{Z}_{mn}, \mathbb{Z}_m \times \mathbb{Z}_n$ (we didn't cover what $\mathbb{Z}_m \times \mathbb{Z}_n$ means, yet. This is done is Chapter 6). Train yourself to recognize trigger words or phrases so that your brain searches your neural network for the things just mentioned whenever you read something similar to the following:

- "Let $m$ and $n$ be positive integers such that $m$ is a factor of $n$. Show that $\mathbb{Z}_n$ . . . [some statement involving $m, n$, or $m$ and $n$]." In such cases, consider using the division algorithm, and maybe take mod $n$ or mod $m$ of equations you write down to see if that somehow lead to the proof/solution.
- "Let $m$ and $n$ be relatively prime. Show that $\mathbb{Z}_m \times \mathbb{Z}_n$ . . . [some statement involving $m, n$, or $m$ and $n$]." In such cases, note that relatively prime means $\gcd(m, n) = 1$ which, by Proposition 2.1, means that there exist integers $s, t$ such that $1 = sm + tn$. You might then consider taking mod $n$ or mod $m$ of this and see if its somehow useful. The problem might also state another assumption that, in conjunction with $1 = sm + tn$, completes the proof/solution or provides a part of the proof/solution.
- "Show that any element in [some statement involving some combinations of $\mathbb{Z}_n, \mathbb{Z}_m$] can be written as . . . [some statement involving $m, n$, or $m$ and $n$]."

## Problems

**2.1** a) Find the greatest common divisor $d$ of 1819 and 3587. Also, find $s, t \in \mathbb{Z}$ such that

$$d = 1819s + 3587t.$$

Compute this by hand, showing all your work.

b) Find the order of the subgroup $\langle 1819 \rangle$ in $(\mathbb{Z}_{3587}, +, 0)$.

**2.2** a) Find the greatest common divisor $d$ of 1665 and 2019. Also, find $s, t \in \mathbb{Z}$ such that

$$d = 1665s + 2019t.$$

Compute by hand, showing all your work.

b) Find the order of the subgroup $\langle 1665 \rangle$ in $(\mathbb{Z}_{2019}, +, 0)$.

**2.3** Find the multiplicative inverse of 19 (mod 287). Please check your work.

**2.4** Solve the equation $61x + 5 = 7 \pmod{127}$. Please check your work.

# Chapter 3
# Permutations

**Abstract** This chapter is about permutations, a convenient notation for permutations, and some general properties of permutations that will be useful throughout the text.

## 3.1 Permutations

**Definition 3.1** A function $f : X \longrightarrow Y$ is invertible if there exists a function $g : Y \longrightarrow X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. We say that $g$ is the inverse of $f$ and often write $g$ as $f^{-1}$.

**Definition 3.2** A function $f : X \longrightarrow Y$ is injective if, whenever $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$ then $x_1 = x_2$.

**Definition 3.3** A function $f : X \longrightarrow Y$ is surjective if for any $y \in Y$ there exists at least one $x \in X$ such that $f(x) = y$.

**Definition 3.4** A function $f : X \longrightarrow Y$ is bijective if it is injective and surjective.

It is proven in standard books/courses that a function is invertible if and only if it is bijective.

Let $X$ be a set.

**Definition 3.5** A permutation of $X$ is a bijective function from $X$ to $X$.

**Proposition 3.1** *Let $S_X$ be the set of all permutations of $X$. Then $S_X$ is a group when the binary operation is function composition. We call $S_X$ the symmetric group on $X$.*

***Proof*** The identity map is bijective and so belongs to $S_X$. Bijective functions have inverses, and those inverses are bijective as well. Function composition is associative. Hence, $S_X$ is indeed a group. □

**Definition 3.6** Suppose that $X$ is a set of $n$ objects. For example, suppose $X = \{1, 2, \ldots, n\}$. Instead of defining $X$, mentioning that $|X| = n$, and writing $S_X$ it is common practice to write $S_n$.

Any set $X$ with $n$ objects has a bijection with the set $\{1, 2, \ldots, n\}$ so one can, without loss of generality, think of permutations of $n$ objects in terms of permutations of the numbers $1, 2, \ldots, n$ and use the $S_n$ notation. That said, in some settings with abstract sets $X$ it is more clear to just use $X$ and $S_X$.

**Proposition 3.2** *The order of $S_n$ is $n!$.*

***Proof*** We must count how many bijective functions exist on a set of $n$ elements. Let $\sigma$ be a permutation, and let us count how many different ways we can define $\sigma$. Let us define $\sigma(1)$ first. We are free to assign $\sigma(1)$ any value from $n$ elements. Pick a value and fix $\sigma(1)$ to that value. Let us now define $\sigma(2)$. Since $\sigma(1)$ is already defined and $\sigma$ must be injective (it is bijective and, in particular, injective), we only have $n - 1$ values to choose from to assign to $\sigma(2)$. Proceeding all the way to $\sigma(n)$, we see that there are $n \cdot (n - 1) \cdots 2 \cdot 1 = n!$ ways to define a bijective function from a set of $n$ elements to itself. Therefore, $|S_n| = n!$. □

The set $S_X$ is a collection of bijective functions. When $X$ is finite, the bijective functions are then not continuous functions but are instead defined explicitly by how they act on the elements of $X$. For example, suppose that $X = \{1, 2, 3\}$. Consider $\sigma$ defined by

$$\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2. \tag{3.1}$$

This is 1-to-1 and onto, so $\sigma \in S_X$. It is easy in this specific case to write out $\sigma(x)$ for all $x \in X$, but what if $X$ consists of 1000 elements? What if $|X| = 1000$ but $\sigma$ only permutes a few elements in $X$? It seems like a more efficient notation is needed to describe $\sigma \in S_X$. A convenient notation is the cycle notation, introduced by Cauchy.

## 3.2 Cycle Notation

**Definition 3.7** A $k$-cycle is a string of integers which are cyclically permuted amongst each other and where the integers not in the string are left fixed. A $k$-cycle is written as $(a_1 \ a_2 \ \cdots \ a_k)$.

**Definition 3.8** A 2-cycle is also called a transposition.

This notation is easier to explain with examples.

*Example 3.1* Consider $S_3$ and $\sigma \in S_3$ defined by

$$\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2. \tag{3.2}$$

This can also be denoted as $\sigma = (1\ 3\ 2)$. This can be read as "$\sigma$ sends 1 to 3, sends 3 to 2, and sends 2 to 1."

*Example 3.2* Consider $S_4$ and $\sigma \in S_4$ defined by

$$\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 3, \sigma(4) = 1. \tag{3.3}$$

This can be denoted as $\sigma = (1\ 2\ 4)$. This can be read as "sigma sends 1 to 2, sends 2 to 4, and sends 4 to 1." One can write $\sigma = (1\ 2\ 4)(3)$, which would be read as "$\sigma$ sends 1 to 2, sends 2 to 4, and sends 4 to 1. $\sigma$ sends 3 to 3." However, elements that are fixed are usually omitted and it is understood that omitted elements are fixed.

*Example 3.3* Consider $S_8$ and suppose that

$$\begin{aligned}&\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2,\\&\sigma(5) = 8, \sigma(6) = 5, \sigma(7) = 7, \sigma(8) = 6.\end{aligned} \tag{3.4}$$

This is written in cycle notation as $\sigma = (1\ 3\ 4\ 2)(5\ 8\ 6)$. Again, the 7 may be omitted in this notation since $\sigma(7) = 7$.

Note: It is important to remember the compositions of permutations are read from *right to left*. Likewise, products of cycles should be read from *right to left*.

*Example 3.4* Consider $S_8$ and suppose that

$$\sigma = (1\ 7\ 8\ 5\ 4\ 6)(2\ 3). \tag{3.5}$$

What would this look like written out explicitly in function form? Convince yourself that the cycle notation above is the same as:

$$\begin{aligned}&\sigma(1) = 7, \sigma(2) = 3, \sigma(3) = 2, \sigma(4) = 6,\\&\sigma(5) = 4, \sigma(6) = 1, \sigma(7) = 8, \sigma(8) = 5.\end{aligned} \tag{3.6}$$

**Definition 3.9** Two cycles are said to be disjoint if they do not have any elements/numbers in common.

*Example 3.5* Consider $S_6$ and suppose $\alpha = (1\ 2\ 4)$ and $\beta = (5\ 4\ 6)$. They are not disjoint cycles since 4 appears in $\alpha$ and in $\beta$.

In previous examples, we considered products of cycles that were disjoint. What if they are not disjoint?

*Example 3.6* Consider $S_5$ and suppose $\alpha = (1\ 2\ 4)$ and $\beta = (1\ 2\ 4\ 5)$. What is $\alpha\beta$? The composition of permutations should be read *right to left*. Then $\alpha\beta$ is written as

$$\alpha\beta = (1\ 2\ 4)(1\ 2\ 4\ 5) = (1\ 4\ 5\ 2). \tag{3.7}$$

Why? Consider the number 1. We want $(\alpha\beta)(1) = \alpha(\beta(1))$. Act on it by $\beta = (1\ 2\ 4\ 5)$. But $\beta = (1\ 2\ 4\ 5)$ sends 1 to 2. Then $\beta(1) = 2$ is plugged into $\alpha$. But $\alpha$ sends 2 to 4. Therefore, $\alpha\beta(1) = 4$. Then we ask what $\alpha\beta$ does to 4. Act on 4 by $\beta$. $\beta = (1\ 4\ 5\ 2)$ sends 4 to 5. Then $\alpha$ acts on $\beta(4) = 5$. But $\alpha = (1\ 2\ 4)$ does nothing to 5. Therefore, $(\alpha\beta)(4) = 5$. Continuing the argument gives the expression for $\alpha\beta$ above.

**Theorem 3.1** *Every permutation in $S_n$ can be written as a product of disjoint cycles.*

***Proof*** This follows from bijectivity and from the fact that $X$ is finite. Let $X = \{1, 2, \cdots, n\}$. Pick an $\alpha \in S_n$. Pick $a_1 \in X$ and define $a_2 \equiv \alpha(a_1), a_3 \equiv \alpha^2(a_2)$, $\cdots \alpha_{n+1} \equiv \alpha^n(a_1)$. Since $X$ is finite, $a_1, a_2, \cdots, a_{n+1}$ cannot all be distinct (after all, $X$ has only $n$ elements). Suppose $\alpha^j(a_1) = \alpha^k(a_1)$ (that is, $a_{j+1} = a_{k+1}$) and take, WLOG, $k \geq j$. Since $\alpha$ is bijective and, in particular injective, $\alpha^{-1}$ exists so $\alpha^j(a_1) = \alpha^k(a_1)$ implies $a_1 = \alpha^{k-j}(a_1) = a_{k-j+1}$. We can then write

$$\alpha = (a_1\ a_2\ \cdots a_{k-j}) \cdots \tag{3.8}$$

where we write $\cdots$ at the end because it is possible that $k - j \neq n$. That is, it is possible that $\alpha$ is not an $n$-cycle. If it is not an $n$ cycle, pick $b_1 \in X$ that is not one of $a_1, a_2, \cdots, a_{k-j}$. Now define $b_2 \equiv \alpha(b_1), b_3 \equiv \alpha^2(b_1), \cdots b_{n+1} \equiv \alpha^n(b_1)$. By the same argument, there exists some $k', j'$ where, WLOG, $k' \geq j'$ and $b_1 = \alpha^{k'-j'}(b_1) = b_{k'-j'+1}$. This means that $\alpha$ now looks like

$$\alpha = (a_1\ a_2\ \cdots a_{k-j})(b_1\ b_2\ \cdots b_{k'-j'}) \cdots . \tag{3.9}$$

Proceed this way until all the numbers $\{1, 2, \cdots, n\}$ appear in a cycle. In the end, drop the 1-cycles. This then gives a disjoint cycle decomposition of $\alpha$. □

**Theorem 3.2** *Disjoint cycles commute. That is, let $\alpha = (a_1\ a_2\ \cdots\ a_r)$ and $\beta = (b_1\ b_2\ \cdots\ b_s)$ where no number in $\{a_1, a_2, \cdots, a_r\}$ is equal to any number in $\{b_1, b_2, \cdots, b_s\}$, then $\alpha\beta = \beta\alpha$.*

***Proof*** The theorem should be intuitively clear. Suppose $\alpha, \beta$ are disjoint. We expect that it shouldn't matter if you move objects specified by $\alpha$ and then move objects specified by $\beta$, or if you choose to move objects specified by $\beta$ and then move objects specified by $\alpha$ if none of the objects they specified are the same. That is, $\alpha\beta = \beta\alpha$. We include a formal proof of this intuition.

To show that two functions are equal, one must show that they agree on all inputs to the functions. Therefore, we must show that $\alpha\beta(x) = \beta\alpha(x)$ for any $x \in X = \{1, 2, \cdots, n\}$. There are three cases to consider.

- Suppose $x \in \{a_1, a_2, \cdots, a_r\}$. Then $x = a_k$ for some $k \in \{1, 2, \cdots, r\}$. Then

$$\alpha\beta(x) = \alpha\beta(a_k) = \alpha(a_k) = a_{k+1} \tag{3.10}$$
$$\beta\alpha(x) = \beta\alpha(a_k) = \beta(a_{k+1}) = a_{k+1} \tag{3.11}$$

  If $k = r$, then $a_{k+1} = a_{r+1}$ is interpreted to be $a_{r+1} = a_1$. That is, the subscript should really be understood with modular meaning. Therefore, $\alpha\beta(x) = \beta\alpha(x)$ for $x \in \{a_1, a_2, \cdots, a_r\}$.
- Suppose $x \in \{b_1, b_2, \cdots, b_s\}$. Then $x = b_k$ for some $k \in \{1, 2, \cdots, s\}$. Then

$$\alpha\beta(x) = \alpha\beta(b_k) = \alpha(b_{k+1}) = b_{k+1} \tag{3.12}$$
$$\beta\alpha(x) = \beta\alpha(b_k) = \beta(b_k) = b_{k+1} \tag{3.13}$$

If $k = s$, then $b_{k+1} = b_{s+1}$ is interpreted to be $b_{s+1} = a_1$. That is, the subscript should really be understood with modular meaning. Therefore, $\alpha\beta(x) = \beta\alpha(x)$ for $x \in \{b_1, b_2, \cdots, b_s\}$.

- If $x \notin \{a_1, a_2, \cdots, a_r\}$ and $x \notin \{b_1, b_2, \cdots, b_s\}$, then

$$\alpha\beta(x) = \alpha(x) = x \tag{3.14}$$

$$\beta\alpha(x) = \beta(x) = x. \tag{3.15}$$

Combining the three cases, we see that $\alpha\beta(x) = \beta\alpha(x)$ for any $x \in X$. Therefore, as claimed, disjoint cycles commute. □

*Example 3.7* Non-disjoint cycles usually don't commute. Consider $S_3$ and the elements $(1\ 2\ 3)$ and $(1\ 2)$.

$$(1\ 2\ 3)(1\ 2) = (1\ 3) \tag{3.16}$$

$$(1\ 2)(1\ 2\ 3) = (2\ 3) \tag{3.17}$$

Therefore, $(1\ 2\ 3)(1\ 2) \neq (1\ 2)(1\ 2\ 3)$.

Actually, convince yourself that the above example proves that $S_n$ is non-abelian for $n \geq 3$. If $n = 2$, then $S_n = S_2 = \{e, (1\ 2)\}$ which is clearly abelian. If $n = 1$, then $S_n = S_1 = \{e\}$ is just the trivial group, which is also clearly abelian.

**Theorem 3.3** *Let $\alpha \in S_n$ be a $k$-cycle. Then $|\alpha| = k$.*

***Proof*** Left to reader. □

**Theorem 3.4** *Let $\alpha = (a_1\ a_2\ \cdots\ a_k)$ be a $k$-cycle in $S_n$. Then*

$$\alpha^{-1} = (a_k\ a_{k-1}\ \cdots\ a_1).$$

***Proof*** Note that

$$(a_1\ a_2\ \cdots\ a_k)(a_k\ a_{k-1}\ \cdots\ a_1) = e \tag{3.18}$$

and

$$(a_k\ a_{k-1}\ \cdots\ a_1)(a_1\ a_2\ \cdots\ a_k) = e. \tag{3.19}$$

**Corollary 3.1** *For any $\alpha \in S_n$, we may decompose it into a product of disjoint cycles $\alpha = \alpha_1 \cdots \alpha_m$. Then $\alpha^{-1} = \alpha_m^{-1} \cdots \alpha_1^{-1}$ and we can apply the previous theorem to each disjoint cycle individually to find a disjoint cycle decomposition of $\alpha^{-1}$.*

Remark: Note that cycles are the same under a cyclic "rotation":

$$(a_1\ a_2\ \cdots\ a_k) = (a_k\ a_1\ \cdots\ a_{k-1}) = \cdots = (a_2\ a_3 \cdots a_1). \tag{3.20}$$

*Example 3.8* Let $\alpha = (1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$.

$$\begin{tikzcd}
1 \arrow[r] & 2 \arrow[d] \\
& 3 \arrow[ul]
\end{tikzcd}$$

Then $\alpha^{-1} = (3\ 2\ 1) = (1\ 3\ 2) = (2\ 1\ 3)$.

$$\begin{tikzcd}
1 \arrow[dr] & 2 \arrow[l] \\
& 3 \arrow[u]
\end{tikzcd}$$

*Example 3.9* Let $\alpha = (1\ 5\ 2\ 9)(6\ 8\ 4)(3\ 7)$.

$$\begin{tikzcd}
1 \arrow[r] & 5 \arrow[d] & 6 \arrow[r] & 8 \arrow[d] & 3 \arrow[d, bend right] \\
9 \arrow[u] & 2 \arrow[l] & & 4 \arrow[ul] & 7 \arrow[u, bend right]
\end{tikzcd}$$

Then $\alpha^{-1} = (7\ 3)(4\ 8\ 6)(9\ 2\ 5\ 1)$.

$$\begin{tikzcd}
1 \arrow[d] & 5 \arrow[l] & 6 \arrow[dr] & 8 \arrow[l] & 3 \arrow[d, bend left] \\
9 \arrow[r] & 2 \arrow[u] & & 4 \arrow[u] & 7 \arrow[u, bend left]
\end{tikzcd}$$

**Theorem 3.5** *Let $\alpha = (a_1\ a_2\ \cdots\ a_k)$ be a $k$-cycle in $S_n$. For any $\beta \in S_n$, $\beta\alpha\beta^{-1}$ is the cycle where each $a_i$ is replaced by $\beta(a_i)$ for $i = 1, 2, \cdots, k$. That is,*

$$\beta\alpha\beta^{-1} = \beta(a_1\ a_2\ \cdots\ a_k)\beta^{-1} = (\beta(a_1)\ \beta(a_2)\ \cdots\ \beta(a_k)).$$

***Proof*** Pick an $x \in \{1, 2, \cdots, n\}$.

- Consider the case where there is some $a_i$ such that $x = \beta(a_i)$. Then

$$\beta\alpha\beta^{-1}(\beta(a_i)) = \beta\alpha(a_i) = \beta(a_{i+1}), \tag{3.21}$$

where the subscript has a modulo interpretation.
- Consider the case where there is no $a_i$ such that $x = \beta(a_i)$. Since $\beta$ is a bijection, there exists some $y$ such that $x = \beta(y)$ but where, in this case, $y \notin \{a_1, a_2, \cdots, a_k\}$. Then

$$\beta\alpha\beta^{-1}(\beta(y)) = \beta\alpha(y) = \beta(y) = x. \tag{3.22}$$

This shows that if $\cdots a_i\ a_{i+1} \cdots$ appears somewhere in the cycle of $\alpha$ then $\cdots \beta(a_i)\ \beta(a_{i+1}) \cdots$ appears in the cycle decomposition of $\beta\alpha\beta^{-1}$. □

**Corollary 3.2** *If $\sigma$ is a product of cycles $\sigma = \alpha_1\alpha_2 \cdots \alpha_m$ then*

$$\beta\sigma\beta^{-1} = \beta\alpha_1\beta^{-1}\beta\alpha_2\beta^{-1} \cdots \beta\alpha_m\beta^{-1},$$

*so we can apply the previous theorem to each $\alpha_i$ for $i = 1, \cdots, m$. Therefore, once one has $\sigma$, all one has to do to get $\beta\sigma\beta^{-1}$ is replace each $x$ in the cycle decomposition of $\sigma$ by $\beta(x)$.*

*Example 3.10* Let $\sigma = (1\ 5\ 2\ 6\ 3)(4\ 7\ 8)$ and $\beta = (1\ 3\ 5)(2\ 4\ 6)$. Then

$$\beta\sigma\beta^{-1} = (3\ 1\ 4\ 2\ 5)(6\ 7\ 8). \tag{3.23}$$

Another notation is a two-line notation:

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

where an element in the top row is center to the element in the bottom row directly beneath it.

*Example 3.11* Consider $\sigma = (1\ 5\ 2\ 6\ 3)(4\ 7\ 8)$ and $\sigma \in S_8$. In the two-line notation this is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 7 & 2 & 3 & 8 & 4 \end{pmatrix}. \tag{3.24}$$

One can prove Corollary 3.2 using the two-line notation. Take any two permutations $\sigma, \beta \in S_n$. Then

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & \cdots & n \\ \beta(1) & \cdots & \beta(n) \end{pmatrix}. \tag{3.25}$$

Note that

$$\beta = \begin{pmatrix} 1 & \cdots & n \\ \beta(1) & \cdots & \beta(n) \end{pmatrix} = \begin{pmatrix} \sigma(1) & \cdots & \sigma(n) \\ \beta(\sigma(1)) & \cdots & \beta(\sigma(n)) \end{pmatrix}, \tag{3.26}$$

$$\beta^{-1} = \begin{pmatrix} \beta(1) & \cdots & \beta(n) \\ 1 & \cdots & n \end{pmatrix}. \tag{3.27}$$

Therefore,

$$\begin{aligned} \beta\sigma\beta^{-1} &= \begin{pmatrix} 1 & \cdots & n \\ \beta(1) & \cdots & \beta(n) \end{pmatrix} \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \begin{pmatrix} \beta(1) & \cdots & \beta(n) \\ 1 & \cdots & n \end{pmatrix} \\ &= \begin{pmatrix} \sigma(1) & \cdots & \sigma(n) \\ \beta(\sigma(1)) & \cdots & \beta(\sigma(n)) \end{pmatrix} \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \begin{pmatrix} \beta(1) & \cdots & \beta(n) \\ 1 & \cdots & n \end{pmatrix} \\ &= \begin{pmatrix} \beta(1) & \cdots & \beta(n) \\ \beta(\sigma(1)) & \cdots & \beta(\sigma(n)) \end{pmatrix}. \end{aligned} \tag{3.28}$$

**Theorem 3.6** *Let $\alpha \in S_n$. Write $\alpha$ as a product of disjoint cycles $\alpha = \alpha_1\alpha_2 \cdots \alpha_k$. Then $|\alpha| = \mathrm{lcm}(|\alpha_1|, |\alpha_2|, \cdots, |\alpha_k|)$.*

***Proof*** This is Problem 3.1. □

*Example 3.12* True or false: $S_5$ has an element of order 6. The answer is true. Consider $\alpha = (1\ 2\ 3)(4\ 5)$. Then $|\alpha| = \text{lcm}(3, 2) = 6$.

Suppose that one didn't know Theorem 3.6. Then

$$\begin{aligned}\alpha^k &= ((1\ 2\ 3)(4\ 5))^k \\ &= (1\ 2\ 3)^k(4\ 5)^k \quad \text{(disjoint cycles commute)}\end{aligned} \tag{3.29}$$

For $\alpha^k = e$ to hold, we need $(1\ 2\ 3)^k = e$ and $(4\ 5)^k = e$ to hold simultaneously. This holds if and only if the order of $(1\ 2\ 3)$ divides $k$ and the order of $(4\ 5)$ divides $k$ (why?). The least such positive $k$ for which this is true is 6.

Remark: As a friendly reminder, it is not enough (in any group, not just $S_n$) to demonstrate that $x^n = e$ and then conclude that $|x| = n$. This is because the order of an element $x$ in a group $G$ is defined as the *least* positive integer $n$ for which $x^n = e$. As a silly example, $(1\ 2)^4 = e$ but we know that $(1\ 2)$ has order 2, not order 4. To have an air-tight argument you must show that $x^n = e$ and argue that $n$ is the least such positive integer.

**Proposition 3.3** *$S_n$ has $\frac{n(n-1)}{2}$ distinct transpositions.*

***Proof*** A transposition looks like $(a_1\ a_2)$ for some $a_1, a_2$ with $a_1 \neq a_2$. Let us fix $a_1$ first. There are $n$ choices for $a_1$. Once $a_1$ is chosen, $a_2$ is left with $n - 1$ options. It seems like the total is $n(n-1)$. However, $(a_1\ a_2) = (a_2\ a_1)$ so we must divide by 2 to count only the distinct transpositions. Thus, there are $\frac{n(n-1)}{2}$ distinct transpositions in $S_n$. □

Reminder: More generally, it is true that

$$(a_1\ a_2\ \cdots\ a_k) = (a_k\ a_1\ \cdots\ a_{k-1}) = \cdots = (a_2\ a_3 \cdots a_1). \tag{3.30}$$

When counting how many distinct $k$-cycles there are in $S_n$, it is important to keep this in mind so as to not overcount. See Problem 3.8.

**Lemma 3.1** *Let $\alpha \in S_n$ be a $k$-cycle for some $k \in \{1, 2, \cdots, n\}$. Then $\alpha = (a_1\ a_2\ \cdots\ a_k)$. We claim that*

$$(a_1\ a_2 \cdots a_k) = (a_1\ a_2)(a_2\ a_3 \cdots a_k).$$

***Proof*** Check if the left side agrees with the right side. It does. □

**Theorem 3.7** *Any $k$-cycle can be written as a product of $k - 1$ transpositions.*

***Proof*** Use induction/iteration of Lemma 3.1. That is, if $\alpha = (a_1\ a_2\ \cdots\ a_k)$, then the lemma allows us to conclude that

$$\begin{aligned}\alpha = (a_1\ a_2\ \cdots\ a_k) &= (a_1\ a_2)(a_2\ a_3\ \cdots\ a_k) \\ &= (a_1\ a_2)(a_2\ a_3)(a_3\ a_4\ \cdots\ a_k) \\ &\ \ \vdots \\ &= (a_1\ a_2)(a_2\ a_3) \cdots (a_{k-1}\ a_k).\end{aligned} \tag{3.31}$$

Actually, a lemma similar to Lemma 3.1 can be used to prove that

$$\begin{aligned} \alpha = (a_1\ a_2\ \cdots\ a_k) &= (a_1\ a_k)(a_1 \cdots a_{k-2}\ a_{k-1}) \\ &= (a_1\ a_k)(a_1 a_{k-1})(a_1 \cdots a_{k-2}\ a_{k-3}) \\ &\vdots \\ &= (a_1\ a_k)\cdots(a_1\ a_3)(a_1\ a_2). \end{aligned} \tag{3.32}$$

In either case, we have written the $k$-cycle $\alpha$ as product of $k-1$ transpositions. □

The proof is clear, but let us suppose that you were given the equality

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)\cdots(a_1\ a_3)(a_1\ a_2) \tag{3.33}$$

and asked to verify that it is true. The way to do this is to remember that, although English is read from left to right, some stuff in math such a function composition and group multiplication is read from right to left (in most math books, that is. You might run into a book that tries to insist that function composition and the permutation notation be read from left to right just like English text. While I understand the notion of not tying oneself down to a particular notation or convention, I personally recommend not confusing oneself and to walk away from such a book.) Thus, read the transpositions on the right-hand side of the expression and convince yourself that it does the same thing as the left-hand side. For example, consider $a_1$. The left-hand size maps $a_1$ to $a_2$. The right-hand side, reading from right to left, maps $a_1$ to $a_2$ and then ... does nothing else since no other transposition involves $a_2$. Thus, the right-hand side also maps $a_1$ to $a_2$. What about $a_2$? The left-hand size maps $a_2$ to $a_3$. The right-hand size, reading from right to left, maps $a_2$ to $a_1$ and then maps $a_1$ to $a_3$ and then ... does nothing else since no other transposition involves $a_3$. Thus, the end result is that the right-hand size also maps $a_1$ to $a_3$. Continuing this line of reasoning validates the equality.

Essentially, imagine you have a staircase with $k$ steps and you want to move objects on those steps. The statement is sort of like saying that if you want to move something, for example yourself, from step $a_j$ to $a_{j+1}$ you could jump from step $a_j$ to $a_{j+1}$ or first jump from step $a_j$ to step $a_1$ and then jump to $a_{j+1}$. In a permutation, the intermediate steps might differ as the objects are permuted, but the final result is the same permutation of the objects.

**Corollary 3.3** *The transpositions generate $S_n$.*

***Proof*** By Theorem 3.1, any element in $S_n$ can be written as a product of disjoint cycles. By Theorem 3.7, each of the cycles in the disjoint cycle decomposition can be written as a product of transpositions. □

**Theorem 3.8** *The transpositions* $(1\ 2), (1\ 3), \cdots, (1\ n)$ *(so a total of* $n-1$ *transpositions) generate $S_n$.*

***Proof*** Note that $(a\ b) = (1\ a)(1\ b)(1\ a)^{-1}$, according to Theorem 3.5. Therefore, starting from the $n-1$ transpositions in the statement of this theorem, we can make all $\frac{n(n-1)}{2}$ transpositions in $S_n$ and then apply Corollary 3.3. □

**Theorem 3.9** $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ *generate* $S_n$.

***Proof*** The idea is to make all the transpositions that appear in Theorem 3.8 from the ones in the statement of this theorem. This can be done since

$$(1\ 2) = (1\ 2) \tag{3.34}$$
$$(1\ 3) = (1\ 2)(2\ 3)(1\ 2)^{-1} \tag{3.35}$$
$$(1\ 4) = (1\ 3)(3\ 4)(1\ 3)^{-1} \tag{3.36}$$
$$\vdots \tag{3.37}$$
$$(1\ n) = (1\ n-1)(n-1\ n)(1\ n-1)^{-1}, \tag{3.38}$$

where we have used Theorem 3.5 to go from the right side to the left side. □

**Theorem 3.10** $S_n$ *is generated by two elements. For example, it suffices to use* $(1\ 2)$ *and* $(1\ 2\ \cdots\ n)$.

***Proof*** Define $\beta \equiv (1\ 2\ \cdots\ n)$. Note that

$$(1\ 2) = (1\ 2) \tag{3.39}$$
$$\beta(1\ 2)\beta^{-1} = (2\ 3) \tag{3.40}$$
$$\beta^2(1\ 2)\beta^{-2} = (3\ 4) \tag{3.41}$$
$$\vdots \tag{3.42}$$
$$\beta^{(n-1)}(1\ 2)\beta^{-(n-1)} = (n-1\ n), \tag{3.43}$$

where we have used Theorem 3.5 to go from the left side to the right side. Theorem 3.9 then gives the necessary conclusion. □

### 3.2.1 Cycle Structure

**Definition 3.10** For $\alpha \in S_n$, the cycle structure (or cycle type, or cycle shape) of $\alpha$ is a list of the number of 1-cycles, 2-cycles, $\cdots$, $n$-cycles in the disjoint cycle decomposition for $\alpha$.

**Definition 3.11** We say that two elements $\alpha, \beta \in S_n$ have the same cycle structure if $\alpha$ and $\beta$ have the same number of 1-cycles, ..., and the same number of $n$-cycles.

We will often denote a particular cycle structure by using • as a stand-in for a number in the disjoint cycle decomposition of the group element. We will drop

1-cycles in this informal notation in order to avoid writing $(\bullet)$ a potentially large number of times.

*Example 3.13* In $S_n$ for $n \geq 5, (\bullet \bullet \bullet)(\bullet\bullet)$ stands for any permutation with $(n - 5)$ 1-cycles, one 2-cycle, and one 3-cycle with all cycles disjoint. For example, $(1\ 2\ 3)(4\ 5) \in S_n$ for any $n \geq 5$ has cycle structure $(\bullet \bullet \bullet)(\bullet\bullet)$.

Note that when talking about cycle structure, we refer to a disjoint cycle decomposition. This means that $(\bullet\bullet\bullet)(\bullet\bullet)$ means the same things as $(\bullet\bullet)(\bullet\bullet\bullet)$ in the context of cycle structures. Outside the context of cycle structures (and disjoint cycles), then $(\bullet \bullet \bullet)$ and $(\bullet\bullet)$ might share numbers and it matters, in general, whether one writes the 3-cycle first or not. We will almost always (maybe even always?) use this bullet notation only when referring to cycle structures so that the positioning won't matter.

**Theorem 3.11** *Suppose $\alpha, \beta \in S_n$ have the same cycle structure. Then there exists a $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$.*

***Proof*** Write out $\alpha$ and $\beta$ individually as a product of disjoint cycles. Order the cycles from left to right in nondecreasing length. That is, list all of the 1-cycles first (if any), then the 2-cycles (if any), $\cdots$, then the $n$-cycle (if any). Write $\alpha$ on top of $\beta$. Define $\sigma$ to be the map that sends the number in $\alpha$ to the number below it in $\beta$. Then $\sigma$ is a permutation and $\sigma\alpha\sigma^{-1} = \beta$. □

*Example 3.14* Let $\alpha = (1\ 4\ 2\ 7\ 9)(3\ 5\ 8)$ and $\beta = (1\ 5\ 9\ 2\ 3)(4\ 6\ 7)$. Then $\alpha$ and $\beta$ has the same cycle structure. The first step is to write out their cycle decomposition fully, including any 1-cycles. Then we order the cycles by nondecreasing lengths. Then stack them on top of each other. The result is:

$$\alpha = (6)(3\ 5\ 8)(1\ 4\ 2\ 7\ 9) \tag{3.44}$$

$$\beta = (8)(4\ 6\ 7)(1\ 5\ 9\ 2\ 3) \tag{3.45}$$

Thus, we want to define $\sigma$ as $\sigma(6) = 8, \sigma(3) = 4, \sigma(5) = 6, \sigma(8) = 7, \sigma(1) = 1, \sigma(4) = 5, \sigma(2) = 9, \sigma(7) = 2, \sigma(9) = 3$. That is, $\sigma = (1)(2\,9\,3\,4\,5\,6\,8\,7)$. Dropping the 1-cycle, the answer can also be written as $\sigma = (2\ 9\ 3\ 4\ 5\ 6\ 8\ 7)$. Actually, the $\sigma$ such that $\sigma\alpha\sigma^{-1} = \beta$ is often not unique. For example, instead of writing

$$\alpha = (6)(3\ 5\ 8)(1\ 4\ 2\ 7\ 9) \tag{3.46}$$

$$\beta = (8)(4\ 6\ 7)(1\ 5\ 9\ 2\ 3) \tag{3.47}$$

we can clearly write

$$\alpha = (6)(5\ 8\ 3)(1\ 4\ 2\ 7\ 9) \tag{3.48}$$

$$\beta = (8)(4\ 6\ 7)(1\ 5\ 9\ 2\ 3) \tag{3.49}$$

which would give $\sigma = (1)(2\ 9\ 3\ 7)(4\ 5)(6\ 8)$.

Note: It is important in the above to actually list the 1-cycles of the permutations. We often drop the 1-cycles when writing the final permutation, but the intermediate steps require that we write things out fully. For example, suppose we wrote

$$\alpha = (3\ 5\ 8)(1\ 4\ 2\ 7\ 9) \tag{3.50}$$

$$\beta = (4\ 6\ 7)(1\ 5\ 9\ 2\ 3) \tag{3.51}$$

with the 1-cycles missing. This would give $\sigma(3) = 4, \sigma(5) = 6, \sigma(8) = 7, \sigma(1) = 1$, $\sigma(4) = 5, \sigma(2) = 9, \sigma(7) = 2, \sigma(9) = 3$. That is, $\sigma = (1)(2\ 9\ 3\ 4\ 5\ 6 \cdots$ . Uh-oh. Where does 6 get mapped to? It seems like we cannot close the cycle. This is because we have omitted the 1-cycles, but if we write them out we see that we can send 6 to 8 and then the cycle closes.

## 3.3 The Alternating Group $A_n$

Consider the following polynomial

$$P(x_1, \cdots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j). \tag{3.52}$$

*Example 3.15* Let $n = 3$. Then

$$P(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3). \tag{3.53}$$

*Example 3.16* Let $n = 4$. Then

$$P(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4). \tag{3.54}$$

Next, we define a way for any $\sigma \in S_n$ to act on the polynomial $P$ (we leave the arguments implicit). Define

$$\sigma P \equiv \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}). \tag{3.55}$$

*Example 3.17* Let $n = 3$. Consider $\sigma = (1\ 3) \in S_3$. Then

$$\begin{aligned} \sigma P &= (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)}) \\ &= (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) \\ &= [-(x_1 - x_2)][-(x_1 - x_3)][-(x_2 - x_3)] \\ &= -P. \end{aligned} \tag{3.56}$$

*Example 3.18* Let $n = 4$. Consider $\sigma = (1\ 4\ 2) \in S_4$. Then

$$\begin{aligned}\sigma P &= \{(x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(1)} - x_{\sigma(4)}) \\ &\quad \cdot (x_{\sigma(2)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(4)})(x_{\sigma(3)} - x_{\sigma(4)})\} \\ &= (x_4 - x_1)(x_4 - x_3)(x_4 - x_2)(x_1 - x_3)(x_1 - x_2)(x_3 - x_2) \\ &= (x_1 - x_2)(x_1 - x_3)[-(x_1 - x_4)][-(x_2 - x_3)][-(x_2 - x_4)][-(x_3 - x_4)] \\ &= +P.\end{aligned} \tag{3.57}$$

More generally, $\sigma P$ will return either $+P$ or $-P$ for any $\sigma \in S_n$.

**Definition 3.12** For any $\sigma \in S_n$, we say that $\sigma$ is an even permutation if $\sigma P = +P$ and an odd permutation if $\sigma P = -P$. Writing $\sigma P = \epsilon P$ where $\epsilon \in \{1, -1\}$, we call $\epsilon$ the sign of $\sigma$.

**Theorem 3.12** *The sign of any transposition in $S_n$ is -1.*

***Proof*** Note that $P$ has only one term involving $\pm(x_1 - x_2)$. To be precise, that term is $(x_1 - x_2)$. Therefore, $(1\ 2)P = -P$, so the sign of $(1\ 2)$ is -1. Also, note that $(a\ b)(a\ b)P = +P$ since if $(a\ b)P = \epsilon P$, we have $(a\ b)^2 P = \epsilon^2 P = +P$. This observation together with the fact that $(1\ a) = (2\ a)(1\ 2)(2\ a)^{-1} = (2\ a)(1\ 2)(2\ a)$ for any $2 < a \leq n$ leads us to conclude that $(1\ a)P = -P$. Then, since $(a\ b) = (1\ a)(1\ b)(1\ a)^{-1} = (1\ a)(1\ b)(1\ a)$, we conclude that $(a\ b)P = -P$. Therefore, all transpositions have sign -1. □

Any product of an even number of transpositions will have a sign of $(-1)^{\text{even}} = +1$ while any product of an odd number of transpositions will have a sign of $(-1)^{\text{odd}} = -1$. Also, Theorem 3.7 tells us that any $k$-cycle $(a_1\ a_2\ \cdots\ a_k)$ can be written as a product of $k - 1$ transpositions:

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3) \cdots (a_{k-1}\ a_k). \tag{3.58}$$

Therefore, a $k$-cycle is an even permutation when $k$ is odd and an odd permutation when $k$ is even.

**Theorem 3.13** *Define $A_n$ to be the subset of $S_n$ consisting of the even permutations of $S_n$. Then $A_n$ with the same binary operation as $S_n$ forms a subgroup of $S_n$, called the alternating group $A_n$ of degree $n$.*

***Proof*** Note that $eP = +P$ so $e \in A_n$. Therefore, $A_n$ is nonempty. Let $\alpha, \beta \in S_n$ be even permutations. Taking the disjoint cycle decomposition of $\beta$ and reversing the order of each cycle gives $\beta^{-1}$ (see Corollary 3.1), which will clearly also be an even permutation. Therefore, $\alpha\beta^{-1}$ is an even permutation so $\alpha\beta^{-1} \in A_n$. By Theorem 1.1, $A_n$ is a subgroup of $S_n$. □

**Theorem 3.14** $|A_n| = \frac{n!}{2}$ *for* $n > 1$ *and* $|A_n| = 1$ *for* $n = 1$.

***Proof*** If $n = 1$, then $S_n$ contains only $e$. Since $e$ is an even permutation, $A_n$ also only contains $e$. Let us consider the case $n > 1$. Let $N_{even}$ be the number of even permutations in $S_n$. Let $N_{odd}$ be the number of odd permutations in $S_n$.

- List all of the even elements of $S_n$:

$$\alpha_1, \cdots, \alpha_{N_{even}}. \tag{3.59}$$

Note that $(1\ 2)\alpha_i$ is an odd permutation for any $i = 1, 2, \cdots, N_{even}$. Also, note that $(1\ 2)\alpha_i = (1\ 2)\alpha_j$ implies that $i = j$ since $S_n$ is a group so the inverse of $(1\ 2)$ exists (namely, $(1\ 2)^{-1} = (1\ 2)$). Therefore, we see that

$$(1\ 2)\alpha_1, \cdots, (1\ 2)\alpha_{N_{even}} \tag{3.60}$$

are $N_{even}$ distinct odd permutations. Thus, $N_{odd} \geq N_{even}$.

- List all of the odd elements of $S_n$:

$$\beta_1, \cdots, \beta_{N_{odd}}. \tag{3.61}$$

Note that $(1\ 2)\beta_i$ is an even permutation for any $i = 1, 2 \cdots, N_{odd}$. Also, note that $(1\ 2)\beta_i = (1\ 2)\beta_j$ implies that $i = j$ since $S_n$ is a group so the inverse of $(1\ 2)$ exists (namely, $(1\ 2)^{-1} = (1\ 2)$). Therefore, we see that

$$(1\ 2)\beta_1, \cdots, (1\ 2)\beta_{N_{odd}} \tag{3.62}$$

are $N_{odd}$ distinct even permutations. Thus, $N_{even} \geq N_{odd}$.

Combine the two inequalities to conclude that $N_{even} = N_{odd}$. Since $|S_n| = N_{even} + N_{odd}$, we conclude that $N_{even} = \frac{|S_n|}{2}$. That is, $|A_n| = \frac{n!}{2}$. □

Actually, let's present the proof slightly more generally.

***Proof*** Fix $\sigma$ to be any odd permutation (this requires $n \geq 2$). For example, could choose $\sigma = (1\ 2)$ as above. Let $B_n$ be the set of odd permutations in $S_n$. Define $f : A_n \longrightarrow B_n$ by $\alpha \mapsto \sigma\alpha$. This is well-defined since if $\alpha$ is even then $\sigma\alpha$ is odd. Define $g : B_n \longrightarrow A_n$ to $\beta \mapsto \sigma^{-1}\beta$. This is well-defined since $\sigma^{-1}$ is odd. Observe that $f \circ g = \text{id}_{B_n}$ and $g \circ f = \text{id}_{A_n}$. Since there exist bijections between the sets $A_n$ and $B_n$ we conclude that $|A_n|$ and $|B_n|$ are equal. Therefore,

$$|S_n| = |A_n| + |B_n| = |A_n| + |A_n| = 2|A_n| \tag{3.63}$$

$$|A_n| = \frac{|S_n|}{2}. \tag{3.64}$$

Using a similar argument, one can prove the following proposition.

**Proposition 3.4** *Let $H$ be a subgroup of $S_n$ such that $H \not\subseteq A_n$. Then $H$ has an equal number of even and odd permutations.*

***Proof*** This is assigned as Problem 3.10. □

We have seen several ways to generate $S_n$. For example, we saw that transpositions (the 2-cycles) generate $S_n$. One can find analogous theorems for $A_n$.

**Theorem 3.15** *The 3-cycles generate $A_n$ for $n \geq 3$.*

***Proof*** Any 3-cycle is an even permutation, so it certainly belongs to $A_n$. Pick any element $\alpha \in A_n$. Write $\alpha$ as a product of disjoint cycles. Then use Theorem 3.8 to write each cycle in the cycle decomposition of $\alpha$ as a product of terms of the form $(1\ a)$, where $1 < a \leq n$. This expresses $\alpha$ as a product of an *even* number of transpositions of the form $(1\ a)$. Read the transposition decomposition of $\alpha$ from right to left and pair off adjacent transpositions. Each pairing will look like $(1\ a)(1\ b)$ for some $a$ and some $b$. But $(1\ a)(1\ b) = (1\ b\ a)$, which is a 3-cycle. The fact that there is an even number of transpositions means that no transposition is left unpaired. Therefore, any $\alpha \in A_n$ can be written as a product of 3-cycles. □

*Example 3.19* Consider the alternating group $A_4$. The twelve elements of $A_4$ are

$$\begin{array}{cccc} e, & (1\,2)(3\,4), & (1\,3)(2\,4), & (1\,4)(2\,3), \\ (1\,2\,3), & (1\,2\,4), & (1\,3\,4), & (2\,3\,4), \\ (1\,3\,2), & (1\,4\,2), & (1\,4\,3), & (2\,4\,3). \end{array} \tag{3.65}$$

$A_4$ has an identity element, three elements with cycle structure $(\bullet\bullet)(\bullet\bullet)$, and eight elements with cycle structure $(\bullet\bullet\bullet)$.

There are many more facts that one can prove about $S_n$ and $A_n$. Consider the following.

**Proposition 3.5** *The set of 3-cycles of the form* $(1\ k\ k+1)$ *(entries read mod n and distinct) generates* $A_n$. *(The case* $n = 1$ *is trivial.)*

***Proof*** This is Problem 3.14. □

**Proposition 3.6** *The set of 3-cycles of the form* $(k\ k+1\ k+2)$ *(entries read mod n) generates* $A_n$ *when* $n \geq 3$. *(The case* $n = 1$ *is trivial.)*

***Proof*** This is Problem 3.15. □

**Proposition 3.7** *When n is odd (and greater than or equal to 3), then* $(1\ 2\ 3)$ *and* $(1\ 2\ \ldots\ n)$ *together generate* $A_n$. *When n is even (and greater than equal to 4), then* $(1\ 2\ 3)$ *and* $(2\ 3\ \ldots\ n)$ *together generate* $A_n$.

***Proof*** This is Problem 3.16. □

You are strongly encouraged to prove the above propositions as practice and as a way to test your understanding of the material.

## Problems

**3.1** Prove Theorem 3.6. That is, let $\alpha \in S_n$. Write $\alpha$ as a product of disjoint cycles $\alpha = \alpha_1\alpha_2\cdots\alpha_k$. Prove that $|\alpha| = \mathrm{lcm}(|\alpha_1|, |\alpha_2|, \cdots, |\alpha_k|)$. In words, the order of an element $\alpha$ in $S_n$ is equal to the least common multiple of the orders of the disjoint cycles that appear in a disjoint cycle decomposition of $\alpha$.

**3.2** What are the orders of the following elements?

a) (4 2 7)(1 3 5 9)
b) (1 3 2)(5 6 9 8 7)
c) (1 3 2)(5 6 9 8 2)

**3.3** Let $X = \{1, 2, 3, \cdots\}$. Prove that $S_X$ is an infinite group. (Do not say $\infty! = \infty$.)

**3.4** Compute $\sigma P(x_1, x_2, x_3, x_4)$ explicitly using the definition of $\sigma P$ when

a) $\sigma = (1\ 2\ 4)$.
b) $\sigma = (1\ 2)(3\ 2\ 4)$.

**3.5** Let $\alpha, \beta \in S_n$. Argue that $\operatorname{sgn}(\alpha\beta\alpha^{-1}) = \operatorname{sgn}(\beta)$.

**3.6** Let $\alpha$ be the $k$-cycle $(1\ 2\ \cdots\ k)$. Show that $\alpha^j$ is a $k$-cycle if and only if $\gcd(j, k) = 1$.

**3.7** Consider the group $A_6$.

a) How many elements of order 2 are there in $A_6$?
b) How many elements of order 3 are there in $A_6$?

**3.8** Consider the group $S_n$. Let $1 \leq k \leq n$. How many (distinct) $k$-cycles are there in $S_n$?

**3.9** How many elements in $S_8$ have the same cycle structure as $(1\ 2\ 3)(4\ 5\ 6)(7\ 8)$?

**3.10** Let $H$ be a subgroup of $S_n$ such that $H \nsubseteq A_n$. Prove that $H$ has an equal number of even and odd permutations. (Needless to say, the problem statement forces $n > 1$.)

**3.11** Show that for $x \in S_7$, the equation $x^2 = (4\ 5\ 6\ 7)$ has no solutions, but the equation $x^3 = (4\ 5\ 6\ 7)$ has at least two solutions.

**3.12** a) For any $k$-cycle $\alpha \in S_n$, find, with proof, the cycle shape of $\alpha^3$. (Example: the cube of a 6-cycle has cycle shape $(\bullet\bullet)(\bullet\bullet)(\bullet\bullet)$.)
b) Find all solutions $\sigma \in S_7$ of the equation $\sigma^3 = (1\ 4\ 5\ 7)$.

**3.13** a) Find the smallest $n$ so that $S_n$ contains an element of order 21. Why is it the smallest?
b) For this $n$, how many elements of order 21 does $S_n$ have?

**3.14** Prove Proposition 3.5.

**3.15** Prove Proposition 3.6.

**3.16** Prove Proposition 3.7.

**3.17** Show that for $n \geq 4$ every element of $S_n$ can be written as a product of two permutations, each of which has order 2.

**3.18** Let $\alpha, \beta \in S_n$ be such that $\alpha\beta = \beta\alpha$. Prove that $\beta$ permutes those integers which are fixed by $\alpha$. Prove that if $\alpha$ is an $n$-cycle then $\beta$ must be a power of $\alpha$.

**3.19** How many permutations in $S_n$ have 1 in the same cycle with either 2 or 3, but not both?

# Chapter 4
# Homomorphisms and Isomorphisms

**Abstract** The theme of this chapter is this: We should study both mathematical objects and the functions/maps/morphisms between them.

## 4.1 Homomorphisms

**Definition 4.1** Let $G$ be a group with binary operation $\diamond : G \times G \longrightarrow G$. Let $G'$ be a group with binary operation $\star : G' \times G' \longrightarrow G'$. A homomorphism $\phi : G \longrightarrow G'$ is a function that satisfies $\phi(x \diamond y) = \phi(x) \star \phi(y)$ for $\forall x, y \in G$.

Note: We often use multiplicative notation when proving theorems and write $\phi(xy) = \phi(x)\phi(y)$, where it is understood that $xy$ is the group operation of $G$ and $\phi(x)\phi(y)$ is the group operation of $G'$. For example, it is possible that the binary operation $\diamond$ is multiplication in one of the usual ways (for example, regular multiplication or modular multiplication) but the binary operation $\star$ is addition in one of the usual ways (for example, regular addition or modular arithmetic). See Propositions 4.1 and 4.2 for a perfect example of this. Perhaps a table would be insightful. See Table 4.1.

Table 4.1: Homomorphism $\phi : G \longrightarrow G'$ for common binary operation notations.

| $G$ binary operation $\diamond$ | $G'$ binary operation $\star$ | $\phi(x \diamond y) = \phi(x) \star \phi(y)$ |
|---|---|---|
| multiplicative | multiplicative | $\phi(xy) = \phi(x)\phi(y)$ |
| multiplicative | additive | $\phi(xy) = \phi(x) + \phi(y)$ |
| additive | multiplicative | $\phi(x + y) = \phi(x)\phi(y)$ |
| additive | additive | $\phi(x + y) = \phi(x) + \phi(y)$ |

*Example 4.1* $\det : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^{\times}, \cdot, 1)$ is a homomorphism since

$$\det(AB) = \det(A)\det(B) \tag{4.1}$$

for $\forall A, B \in GL_n(\mathbb{R})$.

**Definition 4.2** Let $\phi : G \to G'$ be a homomorphism. The kernel of $\phi$, denoted $\ker\phi$, is the set

$$\ker\phi = \{g \in G \mid \phi(g) = e'\}.$$

**Theorem 4.1** *Let $\phi : G \to G'$ be a homomorphism. Then*

*i) $\phi(e) = e'$. (Note: We write $e \in G$ and $e' \in G'$ to emphasize that, in general, the identity elements belong to different groups.)*
*ii) $\phi(x^{-1}) = \phi(x)^{-1}$ for any $x \in G$.*
*iii) $\phi(x^n) = \phi(x)^n$ for any $n \in \mathbb{Z}^+$ and any $x \in G$.*
*iv) $\phi(x^n) = \phi(x)^n$ for any $n \in \mathbb{Z}$ and any $x \in G$.*
*v) $\ker\phi$ is a subgroup of $G$.*
*vi) $\operatorname{im}\phi$ is a subgroup of $G'$.*

***Proof*** i)

$$\begin{aligned} \phi(e) = \phi(ee) &= \phi(e)\phi(e) \\ \phi(e) &= \phi(e)\phi(e) \\ \phi(e)\phi(e)^{-1} &= \phi(e)\phi(e)\phi(e)^{-1} \\ e' &= \phi(e) \end{aligned}$$

ii)

$$\begin{aligned} \phi(e) = \phi(xx^{-1}) &= \phi(x)\phi(x^{-1}) \\ e' &= \phi(x)\phi(x^{-1}) \\ \phi(x)^{-1}e' &= \phi(x)^{-1}\phi(x)\phi(x^{-1}) \\ \phi(x)^{-1} &= \phi(x^{-1}) \end{aligned}$$

iii) $\phi(x^2) = \phi(xx) = \phi(x)\phi(x) = \phi(x)^2$ establishes the base case. Now we use induction. Assume $\phi(x^n) = \phi(x)^n$ holds. Then $\phi(x^{n+1}) = \phi(x^n x) = \phi(x^n)\phi(x) = \phi(x)^n\phi(x) = \phi(x)^{n+1}$.
iv) This follows from part iii) combined with part ii). (The case $n = 0$ is obvious.)
v) Note that $\phi(e) = e'$ so $\ker\phi$ is non-empty. Suppose $x, y \in \ker\phi$. Then

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = e'(e')^{-1} = e'. \tag{4.2}$$

Therefore, $xy^{-1} \in \ker\phi$. By Theorem 1.1, $\ker\phi$ is a subgroup of $G$.
vi) $e \in G$ so $G$ is nonempty. Part i) shows that $\phi(e) = e' \in G'$ so $\operatorname{im}\phi$ is nonempty. Let $x', y' \in \operatorname{im}\phi$. There there exist $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. By part ii), $y'^{-1} = \phi(y)^{-1} = \phi(y^{-1})$. Therefore, $x'y'^{-1} = \phi(x)\phi(y^{-1}) =$

$\phi(xy^{-1})$. But $xy^{-1} \in G$ since $G$ is a group. Therefore, $x'y'^{-1} \in \operatorname{im}\phi$. By Theorem 1.1, $\operatorname{im}\phi$ is a subgroup of $G'$. □

A comment about notation might be appropriate here. Here, $\phi(x)^{-1}$ means the inverse (in multiplicative notation) of $\phi(x)$. In particular, it is not the inverse map of $\phi$ applied to $g$.

While homomorphisms have some nice properties such as those in the proposition above, homomorphisms lose some information.

*Example 4.2* det is surjective on $(\mathbb{R}^\times, \cdot, 1)$ but not injective. For example,

$$\det \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} = x = \det \begin{bmatrix} 1 & 0 \\ 0 & x \end{bmatrix} \tag{4.3}$$

for $\forall x \in \mathbb{R}^\times$.

*Example 4.3* Consider $\det : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^\times, \cdot, 1)$. Note that $GL_n(\mathbb{R})$ is non-abelian for $n \geq 2$ but $(\mathbb{R}^\times, \cdot, 1)$ is abelian. Thus, homomorphisms may "lose" information about the "abelianess" or "non-abelianess" of groups.

A way to contain more information about groups is to consider isomorphisms.

## 4.2 Isomorphisms

**Definition 4.3** Let $G$ and $G'$ be groups. An isomorphism $\phi : G \longrightarrow G'$ is a bijective homomorphism. If $\phi : G \longrightarrow G'$ is an isomorphism, we say that $G$ and $G'$ are isomorphic and write $G \cong G'$.

For some intuition on what this means, see Figure 4.1.

**Proposition 4.1** *Any infinite cyclic group is isomorphic to* $(\mathbb{Z}, +, 0)$.

***Proof*** Let $G$ be an infinite cyclic group. Let $x \in G$ be a generator of $G$. Define $\phi : \mathbb{Z} \longrightarrow G$ by $\phi(n) = x^n$. $\phi$ is a homomorphism since $\phi(n+m) = x^{n+m} = x^n x^m = \phi(n)\phi(m)$. It is surjective because $G$ is cyclic so for $\forall y \in G$ there $\exists m \in \mathbb{Z}$ such that $y = x^m$. Assume $\phi$ were not injective. Pick $n, m \in \mathbb{Z}$ such that $\phi(n) = \phi(m)$. This means $x^n = x^m$, which holds if and only if $e = x^{n-m}$. If $n - m \neq 0$ then $e = x^{n-m}$ which implies that $G$ is generated by an element with a finite order (the order being at most $|n-m|$), a contradiction. Thus, $\phi$ is injective and hence $\phi$ is an isomorphism. □

What the above shows is that all infinite cyclic groups are "the same." To be clear, the notion of "the same" is formalized by the idea of an isomorphism. This means that all infinite cyclic groups are really all just the same group "in disguise" due to a different labeling of its elements and binary operation. This is just a choice. If one wanted to count and distinguish using other methods and definitions, one could. The definitions mentioned are time-tested and have proved to be useful.

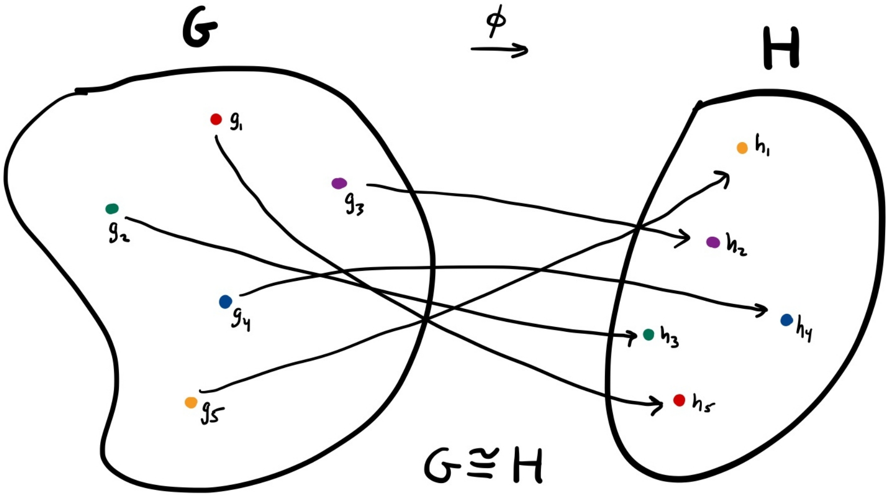


Fig. 4.1: Two groups $G$ and $H$ might appear to be different but a one-to-one and onto "relabeling" by a homomorphism $\phi$ (that is, $\phi$ is an isomorphism) shows that they are really "the same" group.

**Proposition 4.2** *Any finite cyclic group of order n is isomorphic to* $(\mathbb{Z}_n, +, 0)$.

***Proof*** Let $G$ be a cyclic group with $|G| = n$. Pick $x \in G$ with $x \neq e$. Then $G = \langle x \rangle$. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(x^a) = a \pmod{n}$. $\phi$ is clearly bijective. It is also a homomorphism since

$$\begin{aligned} \phi(x^a x^b) = \phi(x^{a+b}) &= a +_n b \\ &= (a \pmod{n}) +_n (b \pmod{n}) \\ &= \phi(x^a) +_n \phi(x^b) \end{aligned} \tag{4.4}$$

(Note that the binary operation for $(\mathbb{Z}_n, +_n, 0)$ involves modular arithmetic so we write $\phi(x^a x^b) = \phi(x^a) +_n \phi(x^b)$ instead of $\phi(x^a x^b) = \phi(x^a)\phi(x^b)$.) □

*Example 4.4* $\mathbb{Q}$ and $\mathbb{Q}^+$ are not isomorphic. Suppose there exists an isomorphism $\phi : \mathbb{Q} \to \mathbb{Q}^+$. Then, since $\phi$ is surjective, there exists an $x \in \mathbb{Q}$ such that $\phi(x) = 2$. Since $\phi$ is a homomorphism, we know that

$$\phi(x/2)\phi(x/2) = \phi(x/2 + x/2) = \phi(x) = 2. \tag{4.5}$$

By assumption, $\phi(x/2) \in \mathbb{Q}^+$. However, there exists no positive rational number equal to $\sqrt{2}$ since $\sqrt{2}$ is irrational. Therefore, there exists no isomorphism between $\mathbb{Q}$ and $\mathbb{Q}^+$.

**Proposition 4.3** *Let* $\phi : G \to G'$ *be an isomorphism of groups. Then* $\phi^{-1} : G' \to G$ *is also an isomorphism of groups.*

***Proof*** $\phi^{-1}$ is clearly bijective. We need to show that $\phi^{-1}$ is a homomorphism. Pick $x', y' \in G'$. Since $\phi$ is bijective, there $\exists x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. Then

$$\phi^{-1}(x'y') = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy. \tag{4.6}$$

Also,

$$\phi^{-1}(x')\phi^{-1}(y') = \phi^{-1}(\phi(x))\phi^{-1}(\phi(y)) = xy. \tag{4.7}$$

Thus, $\phi^{-1}(x'y') = \phi^{-1}(x')\phi^{-1}(y')$ for arbitrary $x', y' \in G'$. □

**Proposition 4.4** *Let $\phi : G \longrightarrow G'$ and $\chi : G' \longrightarrow G''$ be isomorphism. Then $\chi \circ \phi : G \longrightarrow G''$ is an isomorphism. In other words, if $G \cong G'$ and $G' \cong G''$, then $G \cong G''$.*

***Proof*** Recall from previous math experience that the composition of bijective functions is still bijective. We must prove $\chi \circ \phi$ is a homomorphism as well. Let $x, y \in G$ be arbitrary. Note that

$$\begin{aligned}(\chi \circ \phi)(x)(\chi \circ \phi)(y) &= \chi(\phi(x))\chi(\phi(y)) \\ &= \chi(\phi(x)\phi(y)) \\ &= \chi(\phi(xy)) \\ &= (\chi \circ \phi)(xy).\end{aligned} \tag{4.8}$$

Since $x, y \in G$ were arbitrary, this completes the proof. □

Note: $G \cong G$ since the identity map id : $G \longrightarrow G$ defined by $\mathrm{id}(x) = x$ for any $x \in G$ is an isomorphism. This together with Proposition 4.3 and 4.4 shows that being isomorphic is an equivalence relation.

There are a few properties of groups preserved by isomorphisms.

**Theorem 4.2** *Let $\phi : G \longrightarrow G'$ be an isomorphism. Then*

*i) $G$ is abelian if and only if $G'$ is abelian.*
*ii) A subset $H$ is a subgroup of $G$ if and only if $\phi(H)$ is a subgroup of $G'$.*
*iii) $|x| = |\phi(x)|$ for $\forall x \in G$.*

***Proof*** i) Let $x', y' \in G$ be arbitrary. Since $\phi$ is bijective, there exist $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. Note that

$$x'y' = \phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x) = y'x' \tag{4.9}$$

holds if and only if $G$ and $G'$ are abelian. $x', y'$ were arbitrary.

ii) Let $H \subseteq G$. Let $\phi(H) = \{\phi(h) \mid h \in H\}$. Pick $x, y \in H$. Note that

$$\phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \tag{4.10}$$

so that $xy^{-1} \in H$ if and only if $\phi(x)\phi(y)^{-1} \in \phi(H)$.

iii) Let $x \in G$. Consider $H \equiv \langle x \rangle$. Then

$$\begin{aligned}\phi(H) &= \{\phi(h) \mid h \in H\} \\ &= \{\phi(x^n) \mid n \in \{0, \cdots, |x|\}\} \\ &= \{\phi(x)^n \mid n \in \{0, \cdots, |x|\}\}.\end{aligned} \tag{4.11}$$

In particular, $\phi(H) = \langle \phi(x) \rangle$. Since $\phi$ is bijective, $H$ and $\phi(H)$ must have the same number of elements. Therefore, $|\langle x \rangle| = |\langle \phi(x) \rangle|$. That is, $|x| = |\phi(x)|$. □

Note: Theorem 4.2 is useful as a way of checking/proving that certain groups are *not* isomorphic. For example, $S_3 \ncong \mathbb{Z}_6$ since $S_3$ has no element of order 6 whereas $\mathbb{Z}_6$ does. Also, $S_3$ is non-abelian whereas $\mathbb{Z}_6$ is abelian.

**Proposition 4.5** *For cyclic groups of the same order, you can define an isomorphism by sending any generator of one group to any generator of the other group.*

***Proof*** Left to reader. □

### 4.2.1 Automorphisms

You might be tempted to think of isomorphisms $G \longrightarrow G'$ as being defined between differently labeled sets and with different binary operations. However, one can also define an isomorphism from $G$ to $G$.

**Definition 4.4** An isomorphism $\phi : G \longrightarrow G$ is called an automorphism of $G$.

Every group is isomorphic to itself since the identity map id : $G \longrightarrow G$ is an isomorphism. The point is that the identity map isn't necessarily the only isomorphism from $G$ to $G$.

*Example 4.5* Let $G = (\mathbb{Z}_3, +, 0)$. Let the elements of $G$ be $0, 1, 2$. Verify that $\phi_1, \phi_2$ defined by

$$\begin{aligned}&\phi_1(0) = 0, \phi_1(1) = 1, \phi_1(2) = 2, \\ &\phi_2(0) = 0, \phi_2(1) = 2, \phi_2(2) = 1,\end{aligned} \tag{4.12}$$

are both automorphisms of $G$. Of course, $\phi_1$ is the identity isomorphism, but $\phi_2$ is an automorphism distinct from the identity map.

*Example 4.6* Let $G$ be any group. Then $\phi : G \longrightarrow G$ defined by $\phi(x) = gxg^{-1}$ for any $x \in G$ is an automorphism of $G$. Problem 4.1 asks you to verify this.

*Example 4.7* Let $G$ be an abelian group. Then $\phi : G \longrightarrow G$ defined by $\phi(x) = x^{-1}$ is an automorphism of $G$. Problem 4.3 asks you to verify this and also show that if $\phi(x) = x^{-1}$ is an automorphism for some group $G$ then $G$ is abelian.

**Definition 4.5** An inner automorphism is any automorphism that arises from conjugation. That is, an inner automorphism $\phi : G \longrightarrow G$ is equal to $\phi(x) = gxg^{-1}$ for all $x \in G$ for some fixed $g \in G$.

A composition of two automorphisms for a group $G$ is an automorphism of $G$. Automorphisms, being isomorphisms, have inverses which are also automorphisms. The identity map is an automorphism. Convince yourself that the set of all automorphisms where the binary operation is function composition forms a group.

**Definition 4.6** The automorphism group of $G$, written $\text{Aut}(G)$, is the set of all automorphisms of $G$ where the binary operation is function composition.

*Example 4.8* An automorphism, being an isomorphism, must preserve the order of each element (see Theorem 4.2). Consider an automorphism of $S_3$. Then any automorphism must map $\{(1\ 2), (1\ 3), (2\ 3)\}$ to itself. That is, an automorphism of $S_3$ permutes $(1\ 2), (1\ 3), (2\ 3)$. Conversely, every permutation of $(1\ 2), (1\ 3), (2\ 3)$ corresponds to an automorphism of $S_3$. Similar arguments apply to the 3-cycles in $S_3$. Therefore, $\text{Aut}(S_3) \cong S_3$.

Problems 4.10 and 4.11 walk you through the derivation of $\text{Aut}(G)$ when $G = (\mathbb{Z}, +, 0)$ and $G = (\mathbb{Z}_n, +_n, 0)$, respectively.

### 4.2.2 Up to an isomorphism

You may sometimes see the expression "up to an isomorphism" thrown around. In a group theory setting, all this means is that there exists an isomorphism between the two objects in discussion. Isomorphisms in group theory are the precise way to say that two groups are "the same." For example, consider the group $(C, \cdot, 1)$ in Example 1.5. Notice that $\langle -1 \rangle \leq C$. Sometimes you might see statements like "$C$ contains $\mathbb{Z}_2$, up to an isomorphism" or even more briefly/sloppily, "$C$ contains $\mathbb{Z}_2$." Such brief statements which leave the discussion of isomorphisms implicit is common among physicists and physics books.

### 4.2.3 Cayley's Theorem

Some groups act on spaces, for example on solids embedded in $\mathbb{R}^3$. However, every group $G$ acts on itself. Recall that for any set $X$, $S_X$ is the group of permutations on $X$, where the binary operation is function composition.

**Theorem 4.3** *Cayley's theorem - Any group $G$ is isomorphic to a subgroup of $S_G$.*

***Proof*** For $\forall g \in G$, consider the function $L_g$ defined by $L_g(x) = gx$ for $\forall x \in G$, called left translation. It is injective, since $L_g(x) = L_g(y)$ implies $gx = gy$ which implies $x = y$, since $G$ is a group and hence contains $g^{-1}$. It is surjective since for $\forall x \in G$ we have $L_g(g^{-1}x) = x$. Thus, $L_g : G \longrightarrow G$ is bijective and so $L_g \in S_G$. Note that $L_{g^{-1}} \in S_G$ is the inverse of $L_g \in S_G$. Define $\phi : G \longrightarrow S_G$ by $\phi(g) = L_g$. We claim that $\phi$ is an isomorphism. It is a homomorphism because

$$\phi(g_1 g_2) = L_{g_1 g_2} = L_{g_1} \circ L_{g_2} = \phi(g_1) \circ \phi(g_2). \tag{4.13}$$

Injectivity of $\phi$ is clear. Thus, $G \cong \operatorname{im}\phi \cong$ subgroup of $S_G$ (surjectivity of $\phi$ is true by definition. $\phi$ clearly maps onto its image, as does any function.). □

Remark: On a first read, the above proof may seem abstract. As a reminder, in the proof that $\phi : G \longrightarrow S_G$ is a homomorphism it is important to remember that the left-hand and right-hand sides have, in general, different binary operations. On the left-hand side, the binary operation is that of the group $G$. On the right-hand side, the binary operation is that of the group $S_G$, which for us is function composition.

Note: Nowhere in the proof did we assume that $G$ is a finite group. The same proof applies to finite or infinite groups.

## Problems

**4.1** a) Let $G$ be a group. For any $g \in G$, define a function $\phi_g : G \longrightarrow G$ by $\phi_g(x) = gxg^{-1}$ for $\forall x \in G$. Show that $\phi_g$ is an isomorphism. Use Theorem 4.2, to conclude that $|g| = |gxg^{-1}|$. This also solves Problem 1.5.

b) Let $G = A_4$ and $g = (1\ 2\ 3)$. Work out $\phi_g(x)$ for all $x \in A_4$. Corollary 3.2 might be helpful.

**4.2** Let $G$ be a group. Show that $\phi : G \longrightarrow G$ defined by $\phi(x) = x^2$ is a homomorphism if and only if $G$ is abelian.

**4.3** Let $G$ be a group. Show that $\phi : G \longrightarrow G$ defined by $\phi(x) = x^{-1}$ is an isomorphism if and only if $G$ is abelian.

**4.4** Show that the subgroup of $S_4$ generated by $(1\ 2\ 3\ 4)$ and $(2\ 4)$ is isomorphic to $D_4$.

**4.5** Prove that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$.

**4.6** Prove that $D_{12}$ and $S_4$ are not isomorphic.

**4.7** Prove that $D_4$ and $Q_8$ are not isomorphic.

**4.8** How many distinct isomorphisms are there from $S_3$ to $D_3$?

**4.9** Show that every automorphism $\phi$ of the rational numbers $\mathbb{Q}$ under addition has the form $\phi(x) = x\phi(1)$.

**4.10** Let $G$ be the infinite cyclic group $(\mathbb{Z}, +, 0)$.

a) Show that there are two isomorphisms $G \longrightarrow G$, the identity function $\phi_1(a) = a$ and the function $\phi_{-1}(a) = -a$ for all $a \in G$.
b) Show that these are the only isomorphisms $G \longrightarrow G$.
c) Show that, under function composition, $\phi_k \circ \phi_l = \phi_{kl}$. Deduce that the automorphisms of $G = (\mathbb{Z}, +, 0)$ form a group isomorphic to $(\mathbb{Z}^\times, \cdot, 1)$ (which is isomorphic to $\mathbb{Z}_2$).

**4.11** Let $G$ be the finite cyclic group $(\mathbb{Z}_n, +_n, 0)$.

a) For each $k \in \mathbb{Z}_n^\times$, show that $\phi_k(a) = k \cdot_n a$ is an isomorphism $G \longrightarrow G$.
b) Show that these are the only isomorphisms $G \longrightarrow G$.
c) Show that, under function composition, $\phi_k \circ \phi_l = \phi_{kl \pmod{n}}$. Deduce that the automorphisms of $G = (\mathbb{Z}_n, +_n, 0)$ form a group isomorphic to $(\mathbb{Z}_n^\times, \cdot_n, 1)$.

**4.12** Carry out the procedure of Cayley's theorem to obtain a subgroup of $S_6$ which is isomorphic to $D_3$.

**4.13** Let $G$ be a finite group, and choose a list $s_1, \ldots, s_k$ of generators of $G$. The Cayley graph for $G$ and the $\{s_i\}$ is built as follows. Draw one vertex for each $x \in G$. Whenever $y = s_i x$, draw an edge from $x$ to $y$, with an arrowhead[1] in the middle of the edge pointing to $y$. The edges have $k$ different colors, one for each $s_i$.

Rationale: The Cayley graph makes Cayley's Theorem visual. $L_{s_i}$ is the permutation of $G$ where each vertex is sent to the vertex one step forward along the $s_i$-colored arrows. $L_g$ for any $g \in G$ is found by expressing $g$ as a product of the generators.

a) Draw the Cayley graph for $D_3$ with generators $r, s$.
b) Draw the Cayley graph for $S_3$ with generators $(1\ 2), (2\ 3)$.
c) Provide a proof or counterexample to the following claim: the Cayley graph only depends on $G$, not on the choice of generators.
d) Draw the Cayley graph for the Klein four-group using two generators.
e) Draw the Cayley graph for $S_4$ with generators $(1\ 2), (2\ 3), (3\ 4)$. (Hints: Since $\langle (1\ 2), (2\ 3) \rangle$ is a subgroup isomorphic to $S_3$, the answer to b) will appear. From $\langle (2\ 3), (3\ 4) \rangle$, the answer to b) will appear in another way. What about $\langle (1\ 2), (3\ 4) \rangle$?)

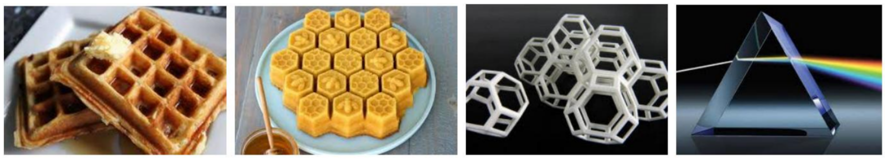


Fig. 4.2: Nice images to accompany Problem 4.13. (Why? What's the connection with the images and the problem?)

[1] A graph with arrowheads on the edges is called a directed graph. When $s_i$ has order 2, we can omit the arrowhead (why?).

**4.14** a) Prove that $\mathbb{Q}$, the group of positive rational numbers under multiplication, is isomorphic to a proper subgroup of itself.

b) Prove that $\mathbb{Q}$, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.

# Chapter 5
# Platonic Solids

**Abstract** This chapter is about Platonic solids and their rotational symmetries.

## 5.1 Platonic Solids and Rotational Symmetries

There are five convex regular solids: the tetrahedron, the cube, the octahedron, the dodecahedron, and the icosahedron. See Figure 5.1. In this chapter, we would like to find the order of the rotational symmetry groups of each of these solids, as well as the symmetry groups (up to isomorphisms).

**Definition 5.1** An <u>$n$-fold axis of symmetry</u> for an object is a line under which rotation by $2\pi/n$ about the line leaves the object invariant.

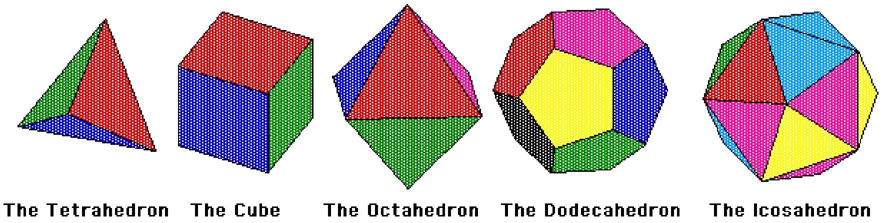


Fig. 5.1: The five Platonic solids. Figure from http://www-groups.mcs.st-andrews.ac.uk/~john/geometry/Lectures/L10.html. (I will need to generate my own figures later.)

### 5.1.1 The Tetrahedron

**Proposition 5.1** *The tetrahedron has 12 rotational symmetries. The group of rotations of a tetrahedron (the tetrahedral group) is isomorphic to $A_4$.*

***Proof*** The tetrahedron has

- four 3-fold axes of symmetry, each of which passes through a vertex and the center of the face opposite to that vertex. These give eight nonidentity group elements, each of which has order 3.
- three 2-fold axes of symmetry, each of which passes through the middle of two opposite edges. These give three nonidentity group elements, each of which has order 2.
- the identity as a symmetry. □

In total, we found $8 + 3 + 1 = 12$ rotational symmetries. We claim that the rotational symmetry group is isomorphic to $A_4$. To see this, label the vertices 1, 2, 3, 4. Note that each rotational symmetry of the tetrahedron corresponds to a permutation of the labeled vertices. In particular, notice that we can always fix one of the vertices and rotate the other three. This corresponds to 3-cycles. All eight 3-cycles are contained in the rotational symmetry group of the tetrahedron. By Theorem 3.15, these eight 3-cycles generate all of $A_4$. Therefore, $A_4$ is "contained" in the rotational symmetry group of the tetrahedron. Using the terminology we have developed in previous chapters, we say that the rotational symmetry group of the tetrahedron contains an isomorphic copy of $A_4$. However, $|A_4| = 12$ and we have found that the tetrahedron has 12 rotational symmetries. Thus, the isomorphic copy of $A_4$ contained by the rotational symmetry group of the tetrahedron is in fact the entire rotational symmetry group. See Figure 5.2 for a visual summary of our findings.

Many molecules with chemical formulas of the form $AB_4$ have a tetrahedral form. See Figure 5.3 for an example.

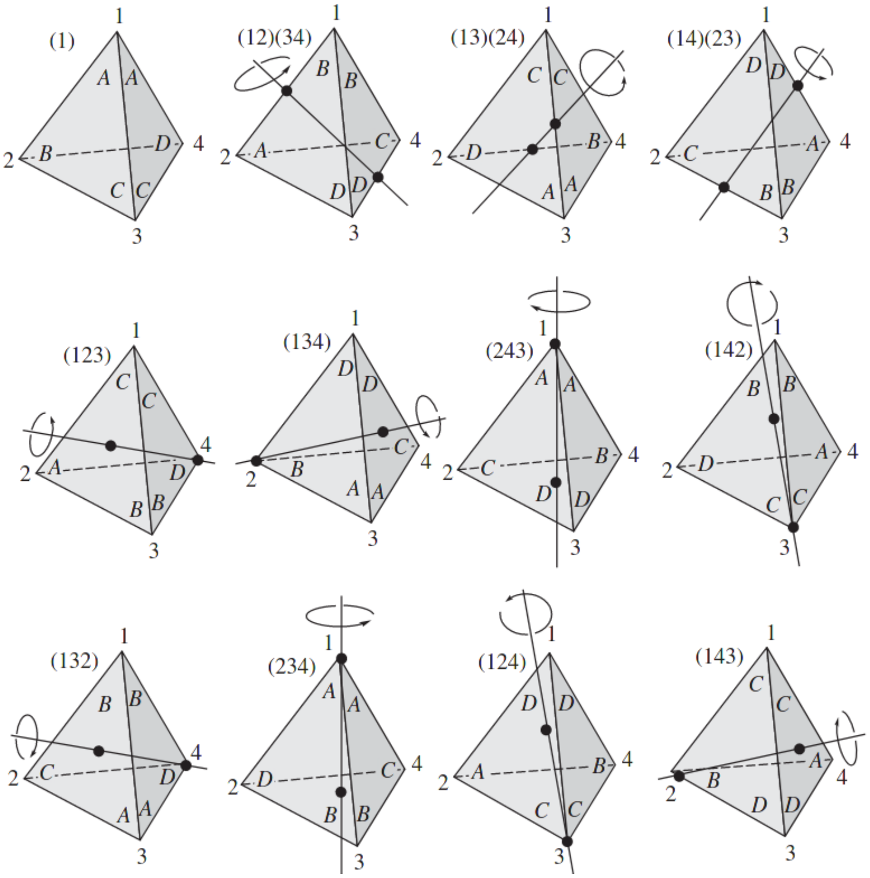
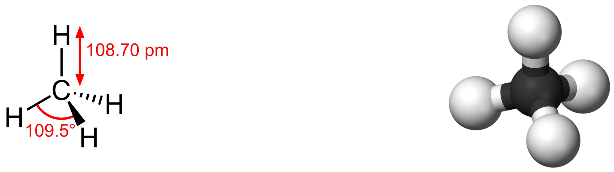


Fig. 5.2: Rotational symmetries of a regular tetrahedron. Figure is from Figure 5.1 in "Abstract Algebra" by Gallian. (I will need to make my own custom images, maybe by using the TikZ package.)



(a) Tetrahedral arrangement in a $CH_4$ molecule.

(b) Ball-and-stick model of $CH_4$.

Fig. 5.3: Models representing a methane ($CH_4$) molecule.

### 5.1.2 The Cube

**Proposition 5.2** *The cube has 24 rotational symmetries. The group of rotations of a cube is isomorphic to $S_4$.*

***Proof*** The cube has

- four 3-fold axes of symmetry, each of which passes through pairs of opposite vertices. These give eight nonidentity rotations, each of order 3.
- three 4-fold axes of symmetry, each of which passes the centroids of opposite faces. These give nine nonidentity rotations, three of which have order 2 and six of which have order 4.
- six 2-fold axes of symmetry, each of which passes through the middles of opposite edges. These give six nonidentity rotations, each of which has order 2.
- the identity as a symmetry.

In total, we found $8 + 9 + 6 + 1 = 24$ rotational symmetries. We claim that the rotational symmetry group is $S_4$. To see this, label the four principle diagonals of the cube 1, 2, 3, 4. Observe that each rotation of the cube corresponds to a permutation of the four principle diagonals, and that this correspondence is one-to-one. Also, the composition of two rotations induces the appropriate permutation of the diagonals. That is, the correspondence between the rotations of the cube and the permutations of the diagonals is a homomorphism. Therefore, the correspondence is injective and a homomorphism. (Verify all these claims.) Note that some rotation of the cube corresponds to the permutation $(1\ 2\ 3\ 4)$ of the principal diagonals and another corresponds to $(1\ 2)$. By Theorem 3.10, $(1\ 2\ 3\ 4)$ and $(1\ 2)$ generate all of $S_4$. Thus, the group of rotational symmetries of the cube contains an isomorphic copy of $S_4$. However, $|S_4| = 24$ and we have found that the group of rotational symmetries of the cube has 24 elements. Thus, the group of rotational symmetries of the cube is in fact isomorphic to $S_4$. □

### 5.1.3 The Octahedron

**Proposition 5.3** *The octahedron has 24 rotational symmetries. The group of rotations of an octahedron is isomorphic to $S_4$.*

***Proof*** The octahedron has

- four 3-fold axes of symmetry, each of which passes through the centroids of opposite vertices. These give eight nonidentity rotations, each of order 3.
- three 4-fold axes of symmetry, each of which passes through pairs of opposite vertices. These give nine nonidentity rotations, three of which have order 2 and six of which have order 4.
- six 2-fold axes of symmetry, each of which passes through the middle of opposite edges. These give six nonidentity rotations, each of which has order 2.

- the identity as a symmetry.

In total, we found $8+9+6+1 = 24$ rotational symmetries. We claim that the symmetry group of rotations of the octahedron is $S_4$. Observe that one can embed four lines in octahedron, each of which goes through the centroid of opposing faces. Label these four lines 1, 2, 3, 4. Observe that each rotation of the octahedron corresponds to a permutation of these four lines and that this correspondence is one-to-one. Also, the composition of two rotations induces the appropriate permutation of the four lines (it is each to the composition of the two permutations corresponding to the two rotations). That is, the correspondence between the rotations of the octahedron and the permutations of the four lines is a homomorphism. (Verify all these claims.) Therefore, the correspondence is injective and a homomorphism. Note that some rotation of the octahedron corresponds to the permutation $(1\ 2\ 3\ 4)$ (label your four lines and find such a rotation) and some other rotation corresponds to the permutation $(1\ 2)$ (using your same labels of the four lines, find the other rotation). By Theorem 3.10, $(1\ 2\ 3\ 4)$ and $(1\ 2)$ generate all of $S_4$. Thus, the group of rotational symmetries of the octahedron contains an isomorphic copy of $S_4$. However, $|S_4| = 24$ and we have found that the group of rotational symmetries of the octahedron has 24 elements. Thus, the group of rotational symmetries of the octahedron is isomorphic to $S_4$. □

### 5.1.4 The Dodecahedron

**Proposition 5.4** *The dodecahedron has 60 rotational symmetries. The group of rotations of a dodecahedron is isomorphic to $A_5$.*

***Proof*** The dodecahedron has

- six 5-fold axes of symmetry, each of which goes through the centroids of opposite faces. These give twenty-four nonidentity rotations, each of which has order 5.
- ten 3-fold axes of symmetry, each of which goes through pairs of opposite vertices. These give twenty nonidentity elements, each of which has order 3.
- fifteen 2-fold axes of symmetry, each of which goes through the middles of opposite edges. These give fifteen nonidentity elements, each of which has order 2.
- the identity as a symmetry.

In total, we found $24 + 20 + 15 + 1 = 60$ rotational symmetries. We claim that the group of rotational symmetries of the dodecahedron is $A_5$. To see this, note that a cube can be embedded inside a dodecahedron. Each edge of the cube is a diagonal across a pentagonal face. There are five diagonals in a pentagonal face. For each of these five diagonals for a particular pentagonal face there is a cube embedded inside the dodecahedron. Every rotation of the dodecahedron corresponds to a permutation of these five cubes. The correspondence between rotations of the dodecahedron and the permutations of the five cubes embedded in the dodecahedron is injective and a homomorphism. (Convince yourself that these claims are true.) Consider rotations about the four 3-fold axes of symmetry which pass through pairs of opposite vertices. These rotations correspond to all the 3-cycles permuting the five embedded cubes. By Theorem 3.15, these 3-cycles generate $A_5$. Thus, the group of rotational symmetries of the dodecahedron contains an isomorphic copy of $A_5$. However, $|A_5| = 60$ and we have found that the group of rotational symmetries of the dodecahedron has 60 elements. Thus, the group of rotational symmetries of the dodecahedron doesn't just contain an isomorphic copy of $A_5$, but *is* isomorphic to $A_5$. □

### 5.1.5 The Icosahedron

**Proposition 5.5** *The icosahedron has 60 rotational symmetries. The group of rotations of an icosahedron is isomorphic to* $A_5$.

***Proof*** The icosahedron has

- six 5-fold axes of symmetry, each of which passes through pairs of opposite vertices. These give twenty-four nonidentity rotations, each of which has order 5.
- ten 3-fold axes of symmetry, each of which goes through the centroids of opposite faces. These give twenty nonidentity elements, each of which has order 3.
- fifteen 2-fold axes of symmetry, each of which goes through the middles of opposite edges. These give fifteen nonidentity elements, each of which has order 2.
- the identity as a symmetry.

In total, we found $24 + 20 + 15 + 1 = 60$ rotational symmetries. We claim that the symmetry group of rotations of the icosahedron is $A_5$. Convince yourself that the icosahedron has tetrahedra "embedded" inside it. In fact, one can embed five of them, with each of the twenty vertices of the icosahedron belonging to one of the embedded tetrahedrons. Label the embedded tetrahedra 1, 2, 3, 4, 5. Each rotation of the icosahedron corresponds to a permutation of the five embedded tetrahedra, i.e. corresponds to an element of $S_5$. Convince yourself that the rotational symmetry group of the icosahedron contains rotations that corresponds to any 3-cycle of $S_5$. By Theorem 3.15, the 3-cycles generate $A_5$ so we conclude that the rotational symmetry group of the icosahedron contains an isomorphic copy of $A_5$. However, $|A_5| = 60$ and we found that the group of rotations of the icosahedron has 60 elements. Therefore, the isomorphic copy of $A_5$ contained by the group of rotations of the icosahedron is in fact isomorphic to the entire group of rotations of the icosahedron.

Another proof is to find a rotation that makes a 3-cycle on the five embedded tetrahedra. A rotation around a vertex gives a 5-cycle. Namely, we can find rotations that corresponds to $(1\ 2\ 3)$ and $(1\ 2\ 3\ 4\ 5)$. By Proposition 3.7, these generate $A_5$.□

## 5.2 Dual Polyhedron

Every convex polyhedron is associated with what is called a dual polyhedron. Each vertex of one convex polyhedron corresponds to a centroid of a face of the other polyhedron, and each edge between vertices of one convex polyhedron corresponds to an edge between pairs of faces of the other. An important observation is the following.

**Proposition 5.6** *The dual polyhedron has the same symmetry group as the original polyhedron.*

The above proposition would have saved some work when calculating the symmetry groups of Platonic solids.

**Proposition 5.7** *The cube and the octahedron are dual to one another. The symmetry group of rotations of both is isomorphic to $S_4$.*

**Proposition 5.8** *The dodecahedron and the icosahedron are dual to one another. The symmetry group of rotations of both is isomorphic to $A_5$.*

## 5.3 Reflections

What about reflections? If you own a cube, you could use it to help visualize the rotations mentioned in this chapter when deriving the symmetry group of the cube. Physically, rotating is no problem. While we can't reflect the cube about a plane that cuts the cube in half, we do note that if this were physically possible then it would map the cube back to a cube. Thus, reflections are also a symmetry of a cube. In the next chapter, we discuss direct products of groups. We will see that to include reflections into the symmetry group in addition to the rotations, we must take the direct product of the rotational group with $\mathbb{Z}_2$ (up to isomorphisms, of course). This discussion appears after Theorem 6.3.

## Problems

**5.1** Let $P$ be a convex polyhedron in $\mathbb{R}^3$, with $V$ vertices, $E$ edges, and $F$ faces. It is proved in topology that the Euler characteristic

$$V - E + F$$

depends only on the boundary of the polyhedron. Topologically, the boundary is the sphere $S^2$.

a) Compute the Euler characteristic of each of the five Platonic solids. (This proves (four times redundantly) that the Euler characteristic is 2.)

A simple polyhedron is one where each vertex is on exactly three edges and three faces. Most polyhedra in nature are simple. If a crystal shaped like an octahedron is washed down a river, its vertices will soon be scraped off (truncated) to look like little squares or quadrilaterals. Each corner of the quadrilateral is on three edges.

b) Let $P$ be a simple polyhedron in which each face is either a pentagon or a hexagon. Show that there must be exactly twelve pentagons.

**5.2** Consider the full symmetry of the cube. Show that all permutations of the principal diagonals can be realized by using only two symmetries of the cube.

# Chapter 6
# (External) Direct Product

**Abstract** We will review a way of making groups by multiplying groups.

## 6.1 Products

**Definition 6.1** In set theory, the Cartesian product of two sets $A$ and $B$, denoted $A \times B$, is the set of all ordered pairs $(a, b)$ where $a \in A$ and $b \in B$. That is,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

One can also take the Cartesian product of the elements of two groups. We would like to turn the resulting set into a group.

**Proposition 6.1** *Let $G$ and $H$ be groups. The (external) direct product $G \times H$ is the set of ordered pairs $\{(g, h)|g \in G, h \in H\}$ equipped with the binary operation $(g, h)(g', h') = (gg', hh')$. This is a group.*

***Proof***
- Associativity holds because it is associative in each "slot" separately, so it holds in total.
- Let $e_G$ be the identity element of $G$ and let $e_H$ be the identity element of $H$. Then $(e_G, e_H)$ is the identity element of $G \times H$.
- Given any $(g, h) \in G \times H$, the inverse is $(g^{-1}, h^{-1})$. □

Remark: To be completely formal, we could say the following. Let $(G, \diamond, e_G)$ and $(H, \star, e_H)$ be groups. Then we could consider the Cartesian product $G \times H$, and define the binary operation $\odot : G \times H \to G \times H$ defined by

$$(g, h) \odot (g', h') = (g \diamond g', h \star h'). \tag{6.1}$$

Then the group could be denoted $(G \times H, \odot, (e_G, e_H))$. While the formality is nice, it gets tedious to write all that out all the time so the theorems are proved using multiplicative notation. It is understood that the multiplicative notation in the theorems and proofs stands for the relevant binary of the relevant group, as specified by the context. For example, $gg'$ is understood to require the binary operation of $G$ and $hh'$ is understood to require the binary operation of $H$. In general, the two groups and binary operations could be different. For example, $G$ could be a group where the binary operation is modular multiplication while $H$ could be a group where the binary operation is addition.

Note: If $G$ and $H$ are finite groups, then the order of $|G \times H| = |G| \cdot |H|$.

**Proposition 6.2** *$G \times H$ is abelian if and only if $G$ and $H$ are abelian.*

***Proof*** Consider $g_1, g_2 \in G$ and $h_1, h_2 \in H$ and note that

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) = (g_2, h_2)(g_1, h_1) \tag{6.2}$$

holds if and only if $G$ and $H$ are abelian. □

*Example 6.1* Consider $\mathbb{Z}_2 \times \mathbb{Z}_2$. This is abelian by Proposition 6.2. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is called the Klein four-group. It has order $2 \cdot 2 = 4$ (hence the name). The elements of the group are the identity $(0, 0)$ and three elements $(1, 0), (0, 1), (1, 1)$ of order 2.

These ideas can be generalized to a finite number of groups $G_1, \ldots, G_n$ by defining

$$G_1 \times \cdots \times G_n \tag{6.3}$$

to be the set of all elements $(g_1, \ldots, g_n)$ with $g_i \in G_i$ for all $i = 1, \ldots, n$ and defining the group binary operation to be the "obvious" one.

**Proposition 6.3** *Let $G$ and $H$ be groups. Then $G \times H \cong H \times G$.*

***Proof*** Define $\phi : G \times H \to H \times G$ by

$$\phi((g, h)) = (h, g) \tag{6.4}$$

for all $(g, h) \in G \times H$. Verify that $\phi$ is an isomorphism. □

**Proposition 6.4** *Let $G$ and $H$ be groups and consider $G \times H$. Define $\tilde{G} \subseteq G \times H$ as $\tilde{G} = \{(g, e_H) \mid g \in G\}$ and $\tilde{H} \subseteq G \times H$ as $\tilde{H} = \{(e_G, h) \mid h \in H\}$. We write $e_G$ and $e_H$ here to emphasize that the groups are, in general, different. Then*

*i) $\tilde{G}$ is isomorphic to $G$.*
*ii) $\tilde{H}$ is isomorphic to $H$.*

***Proof*** i) Define $\phi : \tilde{G} \to G$ by $\phi((g, e_H)) = g$ for every $(g, e_H) \in \tilde{G}$. Verify that $\phi$ is an isomorphism.

ii) Define $\phi : \tilde{H} \to H$ by $\phi((e_G, h)) = h$ for every $(e_G, h) \in \tilde{H}$. Verify that $\phi$ is an isomorphism. □

Consider the Klein four-group. From Example 6.1 we see that the Klein four-group has no element of order 4, so $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not the same as (is not isomorphic to) $\mathbb{Z}_4$. However, a group of the form $\mathbb{Z}_m \times \mathbb{Z}_n$ could very well be (isomorphic to) a cyclic group.

**Proposition 6.5** *$\mathbb{Z}_3 \times \mathbb{Z}_5$ is cyclic. In particular, $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.*

***Proof*** Verify by brute force calculation that $\langle (1,1) \rangle = \mathbb{Z}_3 \times \mathbb{Z}_5$. □

Is there a way to know when $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ without having to find the order of every element and seeing if the order is $mn$? Yes. Before we prove things, we need a lemma.

**Lemma 6.1** *Let $m, n \in \mathbb{Z}$ with $m, n > 0$. Then $\gcd(m,n) \cdot \operatorname{lcm}(m,n) = mn$.*

***Proof*** Recall that the Fundamental Theorem of Arithmetic says that for any $c \in \mathbb{Z}$ with $c > 1$ can be factored uniquely into a product of primes. Consider the prime factorization of

$$m = q_1^{\gamma_1} q_2^{\gamma_2} \dots q_j^{\gamma_j}, \tag{6.5}$$

$$n = r_1^{\delta_1} r_2^{\delta_2} \dots r_k^{\delta_k}. \tag{6.6}$$

Let us consider all the distinct primes that appear in these factorizations and label them $p_1, \dots, p_s$. Then

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, \tag{6.7}$$

$$n = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}, \tag{6.8}$$

where the exponents belong to $\mathbb{N}$. If $p_i$ for some $i = 1, 2, \dots, s$ does not appear in the prime factorization, the exponent is 0. We note that

$$\gcd(m,n) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_s^{\min(\alpha_s,\beta_s)}, \tag{6.9}$$

$$\operatorname{lcm}(m,n) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_s^{\max(\alpha_s,\beta_s)}. \tag{6.10}$$

We note that

$$\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i \tag{6.11}$$

for $i = 1, 2, \dots, s$, proving the claim. □

*Example 6.2* Let $m = 4200$ and $n = 660$. Then $m = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ and $n = 2^2 \cdot 3 \cdot 5 \cdot 11$. Therefore, we see that

$$4200 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 11^0 \tag{6.12}$$

$$660 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1. \tag{6.13}$$

Using Lemma 6.1,

$$\begin{aligned}\gcd(4200,660) &= 2^{\min(3,2)}\cdot 3^{\min(1,1)}\cdot 5^{\min(2,1)}\cdot 7^{\min(1,0)}\cdot 11^{\min(0,1)} && (6.14)\\ &= 2^2\cdot 3^1\cdot 5^1\cdot 7^0\cdot 11^0\\ &= 60\\ \operatorname{lcm}(4200,660) &= 2^{\max(3,2)}\cdot 3^{\max(1,1)}\cdot 5^{\max(2,1)}\cdot 7^{\max(1,0)}\cdot 11^{\max(0,1)} && (6.15)\\ &= 2^3\cdot 3^1\cdot 5^2\cdot 7^1\cdot 11^1\\ &= 46200.\end{aligned}$$

**Theorem 6.1** $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ *if and only if* $\gcd(m,n) = 1$.

***Proof*** Let $l = \operatorname{lcm}(m,n)$. We claim that every element of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order less than or equal to $l$. This is true because $(la \pmod m, lb \pmod n) = (0,0)$ since $m \mid l \Rightarrow m \mid la$ and $n \mid l \Rightarrow n \mid bl$. But $l = mn/\gcd(m,n)$.

- **Case 1**: If $\gcd(m,n) > 1$, then $l < mn$ so every element in $\mathbb{Z}_m \times \mathbb{Z}_n$ has order less than $mn$ so $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic.
- **Case 2**: If $\gcd(m,n) = 1$ then the order of $(1,1)$ is the least $k$ such that $(k,k) = (0,0)$ which means $m \mid k$ and $n \mid k$. Thus, $l \mid k$ and the smallest such (positive) $k$ is $l = mn/\gcd(m,n) = mn$ itself. □

*Example 6.3* Given $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ an isomorphism, how do we find $\phi^{-1}$? That is, given $x \in \mathbb{Z}_m$ and $y \in \mathbb{Z}_n$ what is $k \pmod{mn}$ such that $k \equiv x \pmod m$ and $k \equiv y \pmod n$? If $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, then $\gcd(m,n) = 1$ so $\exists s,t \in \mathbb{Z}$ such that $sm + tn = 1$. Note that $tn \equiv 1 \pmod m, tn \equiv 0 \pmod n$ so $\phi(tn) = (1,0)$. Note that $sm \equiv 0 \pmod m, sm \equiv 1 \pmod n$ so $\phi(sm) = (0,1)$. But for $\forall (x,y) \in \mathbb{Z}_m \times \mathbb{Z}_n$, we have $(x,y) = x(1,0) + y(0,1)$ so

$$\phi(tnx + smy) = x\phi(tn) + y\phi(sm) = x(1,0) + y(0,1) = (x,y). \tag{6.16}$$

Thus, $k \equiv tnx + smy \pmod{mn}$.

*Example 6.4* Using notation as above, if $m = 3, n = 5$ then $(2\cdot 3) + (-1\cdot 5) = 1$ and $sm = 6, tn = 5$. Thus, $k = -5x + 6y \pmod{mn}$.

**Theorem 6.2** *If* $\gcd(m,n) = 1$ *then* $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.

***Proof*** See Problem 6.6. □

Here is a useful theorem for knowing when a group $G$ is isomorphic to an external direct product of two groups. If $H$ and $J$ are subsets of a group $G$, we define $HJ = \{hj \mid h \in H, j \in J\}$.

**Definition 6.2** Let $H$ and $J$ are subgroups of $G$ and suppose

i) $G = HJ$.
ii) $H \cap J = \{e\}$.
iii) $hj = jh$ for any $h \in H$ and $j \in J$.

We say that $G = HJ$ is an internal direct product of $H$ and $J$.

**Theorem 6.3** *If $H$ and $J$ are subgroups of $G$ and*

*i) $G = HJ$.*
*ii) $H \cap J = \{e\}$.*
*iii) $hj = jh$ for any $h \in H$ and $j \in J$.*

*Then $G = HJ \cong H \times J$.*

***Proof*** We claim that $\phi : H{\times}J \longrightarrow HJ$ defined by $\phi((h, j)) = hj$ for any $(h, j) \in H{\times}J$ is an isomorphism.

- It is surjective since any $x \in HJ$ is equal to $x = hj$ for some $h \in H$ and $j \in J$. Then clearly $\phi((h, j)) = hj = x$.
- It is injective since if $\phi((h_1, j_1)) = \phi((h_2, j_2))$ then $h_1 j_1 = h_2 j_2$, which implies that $h_2^{-1} h_1 = j_2 j_1^{-1} \in H \cap J$. However, $H \cap J = \{e\}$ so this implies $h_2^{-1} h_1 = e$ and $j_2 j_1^{-1} = e$.
- $\phi$ is a homomorphism since for any $(h_1, j_1), (h_2, j_2) \in H \times J$

$$\begin{aligned}\phi((h_1, j_1)(h_2, j_2)) &= \phi((h_1 h_2, j_1 j_2)) \\ &= h_1 h_2 j_1 j_2 \\ &= h_1 j_2 h_2 j_2 \\ &= \phi((h_1, j_1))\phi((h_2, j_2))\end{aligned} \tag{6.17}$$

where we have used iii) for the third equality. Therefore, $H \times J \cong HJ = G$. □

The reader might have wondered why the chapter says (external) direct products. In the rest of the text, we will often use the external direct product notation whenever we say "direct product." We will sometimes be pedantic and write "... (external) direct product..." instead of leaving it implied. The above theorem states that internal direct products of two (sub)groups and the external direct products of (isomorphic copies) of those two (sub)groups are the same notions if they have the properties stipulated in the theorem. In such cases, it means we can write "direct product" and not bother mentioning "internal" or "external."

The previous theorem has many uses, as you will find out through problems throughout the text. Here is another use.

*Example 6.5* $O_3 \cong SO_3 \times \mathbb{Z}_2$. This is because $-I_{3\times 3} \notin SO_3$, $\langle -I_{3\times 3}\rangle \cong \mathbb{Z}_2$, and clearly any scalar multiple of the identity commutes with any other matrix. By Theorem 6.3, $O_3 \cong SO_3 \times \mathbb{Z}_2$. Actually, $O_n \cong SO_n \times \mathbb{Z}_2$ for all odd integers $n \geq 3$ since $-I_{n\times n} \notin SO_n$ whenever $n$ is odd so Theorem 6.3 is applicable. What if $n$ is even? See Problem 6.8.

*Example 6.6* Consider a Platonic solid with its center at the origin of $\mathbb{R}^3$. Consider the map $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ defined by $f(\mathbf{r}) = -\mathbf{r}$. Such a map sends all the Platonic solids except for the tetrahedron back to themselves. We say that the Platonic solids except for the tetrahedron have inversion symmetry. A matrix representing this map is $-I_{3\times 3}$. This matrix clearly commutes with any other $3 \times 3$ matrix. Let $H$ be the set of all rotation symmetries of a solid. Let $J$ be the subgroup of the symmetry group generator by the inversion map $f$. We see that every element of $H$ commutes with every element of $J$. Let $G$ be the full symmetry group of a solid. This means we include rotational symmetries as well as inversion symmetry. This means that every symmetry in $G$ can be written as a some element in $HJ$. By Theorem 6.3, $HJ \cong H \times J$. Therefore, the full symmetry group of the solid is $G \cong H \times J \cong H \times \mathbb{Z}_2$.

*Example 6.7* The rotational symmetry group of the cube and octahedron is $S_4$. The full symmetry group is $S_4 \times \mathbb{Z}_2$.

*Example 6.8* The rotational symmetry group of the dodecahedron and icosahedron is $A_5$. The full symmetry group is $A_5 \times \mathbb{Z}_2$.

Inversion is not a symmetry of the tetrahedron, but the reader might wonder if the full symmetry group of the tetrahedron is still $A_4 \times \mathbb{Z}_2$ but one just can't deduce it using Theorem 6.3. It is not. The full symmetry group of the tetrahedron is $S_4$. Let $G = S_4$ and $H = A_4$. WLOG, choose an odd permutation, say $(1\ 2)$, and let $K = \langle (1\ 2) \rangle$. Then $G = HK$, $H \cap K = \{e\}$, but $(1\ 2)$ does *not* commute with every element of $H$. For example,

$$(1\ 2)(2\ 3\ 4) = (2\ 3\ 4\ 1) \tag{6.18}$$

$$(2\ 3\ 4)(1\ 2) = (1\ 3\ 4\ 2). \tag{6.19}$$

Actually, one has what is called a semidirect product $S_4 \cong A_4 \rtimes \mathbb{Z}_2$. We haven't covered semidirect products, so don't worry about this for now.

## Problems

**6.1** a) Use Theorem 6.1 and Proposition 4.5 to show that there is an isomorphism

$$\phi : \mathbb{Z}_{2014962} \longrightarrow \mathbb{Z}_{2019} \times \mathbb{Z}_{998}$$

of additive groups with $\phi(1) = (1, 1)$.

b) Princeton University received its charter in October 1746. Find the $k \in \mathbb{Z}_{2014962}$ such that $\phi(k) = (1746, 10)$. (Hint: Example 6.3 is useful here.)

**6.2** a) Use Theorem 6.1 and Proposition 4.5 to show that there is an isomorphism

$$\phi : \mathbb{Z}_{138195} \longrightarrow \mathbb{Z}_{1665} \times \mathbb{Z}_{83}$$

of additive groups with $\phi(1) = (1, 1)$.

b) Isaac Newton was born on December 25, 1642 (in the old calendar). Find the $k \in \mathbb{Z}_{138195}$ such that $\phi(k) = (12, 1642)$. (Hint: Example 6.3 is useful here.)

**6.3** a) Find the order of the group $\mathbb{Z}_{2015}^{\times}$. (Hint: $31 \mid 2015$.)

b) Find the inverse of 29 in $\mathbb{Z}_{2015}^{\times}$.

**6.4** Prove that $\mathbb{C}$ is isomorphic to $\mathbb{R} \times \mathbb{R}$.

**6.5** Prove that $\mathbb{C} - \{0\}$ is isomorphic to $\mathbb{R}^{+} \times C$, where $C = \{z \in \mathbb{C}^{\times} \mid |z| = 1\}$ by constructing an isomorphism $\phi : \mathbb{C}^{\times} \longrightarrow \mathbb{R}^{+} \times C$.

**6.6** a) Suppose that that $m, n$ are positive integers such that $\gcd(m, n) = 1$. Prove that $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_{m}^{\times} \times \mathbb{Z}_{n}^{\times}$.

b) Use the previous part to argue that $\mathbb{Z}_{20}^{\times}$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$. (No, there is no $^{\times}$ missing on $\mathbb{Z}_4$ or $\mathbb{Z}_2$.)

**6.7** The multiplicative group $\mathbb{C} - \{0\}$ is denoted either $\mathbb{C}^{\times}$ or $\mathbb{C}^{*}$, We know that $C = \{z \in \mathbb{C}^{\times} \mid |z| = 1\}$ is a subgroup of $\mathbb{C}^{\times}$. Draw the the left coset $(24 + 38i)C$ in $\mathbb{C}^{\times}$. Let $\phi : \mathbb{C}^{\times} \longrightarrow \mathbb{R}^{+} \times C$ be the isomorphism from Problem 6.5 and find the subset $\phi((24 + 38i)C) \subset \mathbb{R}^{+} \times C$.

**6.8** What goes wrong when $n$ is even so that one cannot invoke Theorem 6.3? Show that $SO_n \times \mathbb{Z}_2 \ncong O_n$ when $n$ is even.

**6.9** Show that $D_{2n} \cong D_n \times \mathbb{Z}_2$ when $n \geq 3$ and $n$ odd.

# Chapter 7
# Equivalence Relations and Partitions

**Abstract** This chapter reviews a way of breaking up a set into a union of disjoint sets.

## 7.1 Equivalence Relation

**Definition 7.1** Let $S$ be any set. An equivalence relation on $S$ is a relation that satisfies the following conditions for any $x, y, z \in S$:

i) $x \sim x$ (reflexivity).
ii) If $x \sim y$ then $y \sim x$ (symmetry).
iii) If $x \sim y$ and $y \sim z$ then $x \sim z$ (transitivity).

*Example 7.1* Love is *not* an equivalence relation.

**Proposition 7.1** *Let $G$ be a group. Let $H$ be a subgroup of $G$. For $x, y \in G$ define $x \sim y$ if $\exists h \in H$ such that $x = yh$. Such a definition gives an equivalence relation.*

***Proof*** i) For any $x \in G$, $x = xe$ so $x \sim x$.
ii) If $x \sim y$ then $x = yh$ for some $h \in H$. This then means that $y = xh^{-1}$. But $h^{-1} \in H$ since $H$ is a subgroup (closed under inverses). Thus, $y \sim x$.
iii) If $x \sim y$ and $y \sim z$ then $x = yh_1$ and $y = zh_2$ for some $h_1, h_2 \in H$. Therefore, $x = zh_2h_1$. But $h_2h_1 \in H$ since $H$ is a subgroup (closed under group multiplication). □

*Example 7.2* Let $G = (\mathbb{Z}, +, 0)$ and $n > 0$, $H = n\mathbb{Z}$. In this case, the relation $\sim$ is called congruence modulo $n$ and we write $x \equiv y$ (mod n) instead of $x \sim y$. In fact, $x \equiv y$ if and only if $n \mid (x - y)$.

**Definition 7.2** Let $\sim$ be an equivalence relation on $S$. For any $x \in S$, the equivalence class of $x$ is $\{y \in S \mid y \sim x\}$, often denoted $[x]$.

*Example 7.3* For $\equiv$ (mod n), the equivalence classes are $[0], [1], \ldots, [n-1]$.

## 7.2 Cosets

Cosets are important equivalence classes in group theory.

**Definition 7.3** Let $H$ be a subgroup of $G$. The set

$$gH = \{gh \mid h \in H\} \subseteq G$$

is called a left coset of $H$ in $G$. The set

$$Hg = \{hg \mid h \in H\} \subseteq G$$

is called a right coset of $H$ in $G$.

**Definition 7.4** Let $G$ be a group and let $H$ be a subgroup of $G$. We denote the set of all (distinct) left cosets of $H$ in $G$ by $G/H$. We denote the set of all (distinct) right cosets of $H$ in $G$ by $H\backslash G$.

Note that $G/H$ is a set of elements, those elements themselves being sets (namely, the left cosets of $H$ in $G$). Definition 7.3 uses multiplicative notation. Let us restate the definition using the binary operation.

**Definition 7.5** Let $G$ be a group with a binary operation $\diamond : G \times G \longrightarrow G$. Recall that the image of $(x, y) \in G \times G$ is denoted by $x \diamond y$ instead of $\diamond(x, y)$. Let $H$ be a subgroup of $G$. The set

$$g \diamond H = \{g \diamond h \mid h \in H\} \subseteq G$$

is called a left coset of $H$ in $G$. The set

$$H \diamond g = \{h \diamond g \mid h \in H\} \subseteq G$$

is called a right coset of $H$ in $G$.

Why restate the definition this way? This is because many theorems are proven using the multiplicative notation but some examples use additive notation. It is important to note that the binary operation in theorems is not multiplication in the usual or modular sense. The multiplicative notation is just a choice of notation for the binary operation of the group. This is emphasized here to try to dispel some confusion that might arise during first exposure to these ideas.

*Example 7.4* Let $G = (\mathbb{Z}, +, 0)$ and $H = 4\mathbb{Z}$. Then

$$G/H = \mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}. \tag{7.1}$$

Notice that in the additive notation, the left cosets are written as $g + H$ instead of $gH$.

In the above example, notice that one could write $4 + 4\mathbb{Z}$ instead of $4\mathbb{Z}$, or $6 + 4\mathbb{Z}$ instead of $2 + 4\mathbb{Z}$. This leads to the following general observation: for a subgroup $H$ of $G$, $g_1 + H = g_2 + H$ does *not* imply that $g_1 = g_2$. That is, there might be (and usually are) multiple $g \in G$ such that $g + H$ result in the same left coset.

Left cosets are equivalence classes of an equivalence relation. If $H \leq G$ and $x \sim y$ means $x = y \diamond h$ for some $h \in H$ then $[y] = \{y \diamond h \mid h \in H\}$. This is $y \diamond H$, a left coset of $H$ in $G$. Right cosets are equivalence classes of an equivalence relation. If $H \leq G$ and $x \sim y$ means $x = h \diamond y$ for some $h \in H$, then $[y] = \{h \diamond y \mid h \in H\}$. This is $H \diamond y$, a right coset of $H$ in $G$. Let us see another example, this time using multiplicative notation.

*Example 7.5* Let $G = S_3$ and $H = \langle(1\ 2)\rangle = \{e, (1\ 2)\}$. Then

$$eH = \{e, (1\ 2)\}, \tag{7.2}$$

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}, \tag{7.3}$$

$$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}. \tag{7.4}$$

The right cosets partition $S_3$ into disjoint sets $He, H(1\ 3), H(2\ 3)$. However, note that

$$He = \{e, (1\ 2)\}, \tag{7.5}$$

$$H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}, \tag{7.6}$$

$$H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}. \tag{7.7}$$

Therefore, we see that while $eH = He$ (this is always true), $(1\ 3)H \neq H(1\ 3)$ and $(2\ 3)H \neq H(2\ 3)$. Therefore, we see that left cosets are not necessarily equal to right cosets.

Note: It is not necessarily true that, for arbitrary groups $G$ and subgroups $H \leq G$, $yH = Hy$ for $\forall y \in G$ (Example 7.5 is an explicit example demonstrating this). It is true for abelian groups, but for non-abelian groups one needs to be more careful. We will see later (in Chapter 10) that $yH = Hy$ for $\forall y \in G$ when $H$ is (to be defined later) a normal subgroup of $G$, denoted $H \trianglelefteq G$.

Note: Cosets are not usually/necessarily subgroups. For one, a subgroup must contain the identity element. In particular, a coset in $G/H$ is a subgroup if and only if it contains $e$ if and only if it is $eH = H$. (If $e \in xH$, then there exists $h \in H$ such that $e = xh$, so $x^{-1} = h \in H$. Since $H$ is a subgroup, it is closed under inverses and hence contains $(x^{-1})^{-1} = x$. Therefore, $xH = H$ by Theorem 7.1 proved below.)

Important Note: The notation $G/H$ will be used in two ways. It denotes the set of all (distinct) left cosets of $H$ in $G$. These left cosets may also have the structure of a group, as we shall see in Chapter 10. When they have the structure of a group, we also denote them as $G/H$ and call it the quotient group of $G$ by $H$. That is, when you see $G/H$ you can always think of it as the set of all (distinct) left cosets of $H$ in $G$, but don't always assume that it is a quotient group unless $H$ is, as we will see later, a normal subgroup of $G$.

Let us collect some properties of left cosets. We switch back to multiplicative notation when proving general properties of groups. This is for convenience so that one does not have to keep writing $\diamond$. Do note that the results, as usual, can be translated into any binary operation notation by replacing the multiplicative notation with your favorite symbol.

**Theorem 7.1** *Let $G$ be a group (finite or infinite) and let $H$ be a subgroup of $G$. Then, for any $x, y \in G$,*

*i) $x \in xH$.*
*ii) $xH = yH \iff x^{-1}y \in H$.*
*iii) if $xH \neq yH$ then $xH \cap yH = \emptyset$.*

***Proof*** i) Since $H \leq G$, $e \in H$. Therefore, $xH$ contains $xe = x$.

ii) $\Rightarrow$ Suppose that $xH = yH$. This means that there exists $h \in H$ such that $xh = ye$. Therefore, $x^{-1}y = h \in H$.
$\Leftarrow$ Suppose that $x^{-1}y \in H$. This means that there exists $h \in H$ such that $x^{-1}y = h$. Therefore, $yH = xhH \subseteq xH$, where we used $hH \subseteq H$ since $H$ is a subgroup and, hence, closed under multiplication. Likewise, $xH = yh^{-1}H \subseteq yH$ for the same reasons ($h^{-1} \in H$ since $H$ is a subgroup and then closure under multiplication). Therefore, $xH = yH$. One could also note that $hH = H$ for all $h \in H$ since left multiplication is a bijective map when the the domain and range are the same (sub)group, which gives $yH = xhH = xH$.

iii) Suppose that $xH \neq yH$. If $xH \cap yH \neq \emptyset$, then there exists a $z \in xH \cap yH$ such that $z = xh_1$ and $z = yh_2$ for some $h_1, h_2 \in H$. Thus, $x^{-1}y = h_1h_2^{-1} \in H$ since $H$ is a subgroup (and, hence, closed under group binary operation and inverses). By part ii), this would then mean $xH = yH$, a contradiction. Therefore, $xH \cap yH = \emptyset$. □

The second part of the previous theorem implies for $H \leq G$ that if $H = eH = xH$ for some $x \in G$, then $e^{-1}x \in H$. That is, $xH = H$ implies that $x \in H$. This is a useful fact to remember when dealing with expressions involving left cosets.

**Corollary 7.1** *Let $G$ be a group and let $H$ be a subgroup of $G$. Then*

$$G = \bigcup_{g \in G} gH.$$

***Proof*** This follows from the previous theorem since $g \in gH$. Running through all $g \in G$ guarantees that each $g \in G$ shows up in some left coset(s). □

## 7.3 Partitions

**Definition 7.6** Let $S$ be a nonempty set. A partition of $S$ is a collection of subsets $S_i \subseteq S$ such that

i) $S_i \neq \emptyset$ for $\forall i$.
ii) $\cup_i S_i = S$
iii) $S_i \cap S_j = \emptyset$ for $i \neq j$.

**Proposition 7.2** *The equivalence classes of an equivalence relation are a partition of $S$.*

***Proof*** We must show that the equivalence classes of any set $S$ satisfy the above properties in the definition. Label the elements of $S$ by $S = \{x_1, x_2, \cdots\}$.

i) Let $[x_i]$ be the equivalence class determined by $x_i$. Then $x_i \in [x_i]$ so it is nonempty.
ii) Clearly, $\cup_i [x_i] = S$. If we only let $i$ go over elements that determine distinct elements, this will clearly still be true.
iii) Let $[x]$ be an equivalence class determined by $x$ and let $[x']$ be an equivalence class determined by $x'$. We claim that either $[x] \cap [x'] = \emptyset$ or $[x] = [x']$. Suppose $[x] \cap [x'] \neq \emptyset$. Pick $y \in [x] \cap [x']$. Then $y \sim x$ and $y \sim x'$. By symmetry, $x \sim y$. But transitivity, $x \sim y$ and $y \sim x'$ implies $x \sim x'$. Pick any element $a \in [x]$. Then $a \sim x$. By transitivity, $a \sim x$ and $x \sim x'$ implies $a \sim x'$, so $a \in [x']$. Since $a \in [x]$ was arbitrary, we conclude $[x] \subseteq [x']$. By symmetry, $x \sim x'$ implies $x' \sim x$. Now pick $b \in [x']$. Then $b \sim x'$. By transitivity, $b \sim x'$ and $x' \sim x$ implies $b \sim x$, so $b \in [x]$. Since $b \in [x']$ was arbitrary, we conclude $[x'] \subseteq [x]$. Therefore, $[x] = [x']$. □

**Proposition 7.3** *Given a partition $\{S_i\}$ of $S$, define a relation $x \sim y$ on $S$ if and only if $x \in S$ belongs to the same $S_i$ as $y \in S$. That is, $x \sim y$ if and only if $x \in S_i$ and $y \in S_j$ and $i = j$. Then $\sim$ is an equivalence relation. It is called the equivalence relation induced by the partition.*

***Proof*** One must show that the equivalence classes of any set $S$ satisfy the above properties in the definition.

i) Let $x \in S$. Since $S = \cup_i S_i$, there exists some $j$ such that $x \in S_j$. Clearly $x \sim x$ since $x$ does indeed belong to the same set $S_j$ that $x$ belongs to. Thus, $\sim$ is reflexive.
ii) Suppose $x, y$ belong to the same set $S_j$. Then it is clear that $x \sim y$ and $y \sim x$. Thus, $\sim$ is symmetric.
iii) Suppose that $x \sim y$ and $y \sim z$. Then $x, y \in S_i$ for some $i$. Also, $y, z \in S_j$ for some $j$. However, $S_i \cap S_j = \emptyset$ for $i \neq j$ for a partition. Therefore, $y \in S_i$ and $y \in S_j$ implies $i = j$. This then means that $x, z \in S_i$ so $x \sim z$. Thus, $\sim$ is transitive.

This shows that $\sim$ is reflexive, symmetric, and transitive. Hence, it is an equivalence relation, by definition. □

**Corollary 7.2** *If $H \leq G$, then the left cosets of $H$ in $G$ form a partition of $G$.*

Maybe a figure can provide some intuition on the relationship between equivalence classes and partitions. See Figure 7.1.

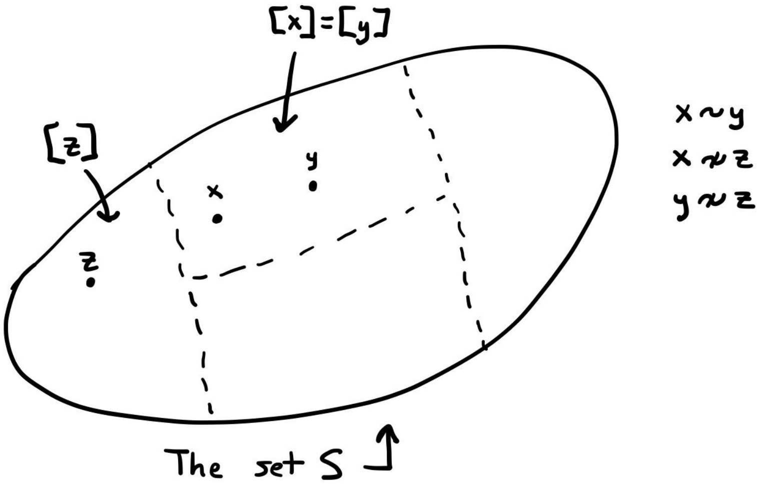


Fig. 7.1: We can mentally collect the points of the set $S$ and bundle them together depending on whether they are equivalent or not under the given equivalence relation. If the equivalence classes are left cosets of a subgroup $H \leq G$, then Corollary 7.3 states that all the left cosets have the same size, as (roughly) in this figure ("size" in this figure being the area). In general, the equivalence classes of an equivalence relation need not all be of the same size.

**Proposition 7.4** *Let $G$ be a group, $H \leq G$, and $g_1, g_2 \in G$. The map $f : g_1H \to g_2H$ defined by $f(x) = g_2g_1^{-1}x$ is a bijection.*

***Proof*** Any element in $g_1H$ is $g_1h$ for some $h \in H$. The maps sends $g_1h$ to $g_2h$. Letting $h$ run through all values in $H$ shows that this maps is surjective. It is injective since if $f(x) = f(y)$ then $g_2g_1^{-1}x = g_2g_1^{-1}y$ and, since $G$ is a group so $g_2g_1^{-1} \in G$ has an inverse, therefore $x = y$. □

**Corollary 7.3** *We can say that any two left cosets of $H \leq G$ have the same number of elements with the understanding that this means there exists a bijection between the two cosets. In particular, if $G$ is a finite group (and so $H$ is a finite subgroup) then $|g_1H| = |g_2H|$ for any $g_1, g_2 \in G$ so that they indeed have the same number of elements in the discrete math sense.*

Remark: To reiterate, when sets are finite the notion of being of the same size is clear. When dealing with infinities, it doesn't make sense to say $\infty = \infty$ and that, therefore, the sizes are the same. For example, $\mathbb{N}$ has infinite size as does $\mathbb{R}$ but $\mathbb{N} \subset \mathbb{R}$. Do they have the "same size"? This requires us to rethink what it means for two sets $S_1$ and $S_2$ to be of the same size. Being able to pair each element in $S_1$ with an element in $S_2$ in a one-to-one and onto way (that is, with a bijection) seems like a good idea. It turns out that there is no bijection between $\mathbb{N}$ and $\mathbb{R}$.[1,2,3] If this stuff is new to the reader leaves the reader asking "if $\mathbb{N}$ has infinite elements, how does it 'run out' of elements to map to elements in $\mathbb{R}$" or something like that, I recommend learning about Cantor's diagonal argument. (The Wikipedia page on Cantor's diagonal argument might be a good place to start.)

**Definition 7.7** The number of cosets of $H$ in $G$ is called the index of $H$ in $G$ and is denoted $[G : H]$.

*Example 7.6* If $G = S_3$ and $H = \langle(1, 2)\rangle$ then $[G : H] = 3$. Note that $|G| = 3! = 6, |H| = 2$ and $[G : H] = 3 = 6 \div 2 = |G| \div |H|$.

## 7.4 Lagrange's Theorem

**Theorem 7.2** *Lagrange's Theorem - Let G be a finite group (this proof does not work if $|G|$ is infinite). Let H be a subgroup of G. Then $|H|$ divides $|G|$. (Important: Note that G is a finite group.)*

***Proof*** Partition $G$ into left cosets of $H$ in $G$. Any two cosets have the same size. Namely, all cosets have the same size $|eH| = |H|$. Thus, $G = k \cdot |H|$ for some $k \in \mathbb{Z}$ (determined by how many cosets are in the partition of $G$). Since $G$ is finite, $k$ is finite. Thus, $|H|$ divides $|G|$. □

Note: We just proved $|G| = [G : H] \cdot |H|$ for finite groups. Rearranging,

$$[G : H] = |G|/|H| \tag{7.8}$$

for *finite* groups $G, H \leq G$. Thus, the notation makes it easy to remember as we can just think of : as meaning /. If $G$ is an infinite group, then $|G|/|H|$ isn't helpful/meaningful. For example, suppose that $G$ is an infinite group and $H \leq G$ is a subgroup which is infinite. What does $\infty/\infty$ mean? In math, expressions such as

$$\infty - \infty, \frac{0}{0}, \frac{\infty}{0}, \frac{\infty}{\infty} \tag{7.9}$$

are called indeterminate forms. (Do you remember learning L'Hopital's rule?)

**Theorem 7.3** *Let G be a finite group and pick any $g \in G$. Then $|g|$ divides $|G|$.*

***Proof*** The order of $g$ is the order of $\langle g\rangle$ and $\langle g\rangle \leq G$. Apply Lagrange's theorem.□

**Proposition 7.5** *Let G be a finite group and pick any $g \in G$. Then $g^{|G|} = e$.*

[1] Fun fact: It turns out that there is a bijection between $\mathbb{N}$ and $\mathbb{Z}$. Colloquially, there are the same number of integers as positive integers.

[2] Fun fact: It turns out that there are the same number of natural numbers as even natural numbers. That is, $|\mathbb{N}| = |2\mathbb{N}|$. To prove this, note that $f : \mathbb{N} \to 2\mathbb{N}$ defined by $f(n) = 2n$ is a bijection.

[3] Fun fact: It turns out that there is a bijection between $\mathbb{Z}$ and $\mathbb{Q}$. Colloquially, there are the same number of integers as rational numbers.

***Proof*** By Theorem 7.3, $|G| = k|g|$ for some $k \in \mathbb{Z}$. Therefore,

$$g^{|G|} = g^{k|g|} = (g^{|g|})^k = e^k = e. \tag{7.10}$$

□

Remark: For finite groups $G$, this proposition puts a bound on $|g|$. This, however, is not a sharp upper bound.

*Example 7.7* For any $g \in S_3, g^6 = e$. This, however, is not a sharp upper bound. For example, $(a\ b)^2 = e, (a\ b\ c)^3 = e$ in $S_3$. $S_3$ has elements of order at most 3, and not $|S_3| = 6$.

Note: It is important to realize what Lagrange's theorem does and does not say. Lagrange's theorem tells us that if $H \leq G$ then $|H|$ divides $|G|$. It is not true, however, that if $m$ divides $|G|$ then there $\exists H \leq G$ with $|H| = m$.

*Example 7.8* If $G = A_4$ then $|G| = 4!/2 = 12$. If $H \leq G$ then we know, by Lagrange's theorem, that the only *potential* values of $H$ are $\{1, 2, 3, 4, 6, 12\}$. However, $A_4$ has no subgroup of order 6 (see the following proposition).

**Proposition 7.6** *$A_4$ has no subgroup of order 6.*

***Proof*** We prove this using simple counting as well as Lagrange's theorem. Suppose that $H \leq A_4$ is a subgroup of order 6. If a 3-cycle belongs to $H$, then its inverse, which is also a 3-cycle, must also belong to $H$ since $H$ is a subgroup. This means that the number of 3-cycles is $H$ is always even.

- There cannot be six 3-cycles, since every subgroup must contain the identity element $e$.
- Suppose that there are four 3-cycles in $H$, label them $\alpha, \alpha^{-1}, \beta, \beta^{-1}$. Together with $e$, this is a total of five elements. However, $H$ is a subgroup so it must be closed under the group binary operation, which means that $\alpha\beta$ and $\alpha\beta^{-1}$ must also belong to $H$. Note that $\alpha\beta$ and $\alpha\beta^{-1}$ are distinct from the previous five elements for otherwise we would have, for example, that $\alpha\beta = \alpha$ which would imply $\beta = e$, a contradiction. Running through all the other options leads to similar contradictions, proving that $\alpha\beta, \alpha\beta^{-1}$ are new and distinct elements. This then means that

$$\{e, \alpha, \alpha^{-1}, \beta, \beta^{-1}, \alpha\beta, \alpha\beta^{-1}\} \subseteq H, \tag{7.11}$$

  which is already more than six elements. Thus, $H$ cannot contain four 3-cycles.
- Suppose that $H$ contains two 3-cycles. Together with the identity, this is a total of three elements. We need three more elements to satisfy $|H| = 6$. We cannot include any more 3-cycles, so that means that the remaining three elements in $A_4$ are the elements with the cycle shape $(\bullet\bullet)(\bullet\bullet)$. There are $(\frac{4\cdot 3}{2}\frac{2\cdot 1}{2})\frac{1}{2!} = 3$ such elements. Namely,

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \tag{7.12}$$

are the only elements of $A_4$ that have the cycle structure $(\bullet\bullet)(\bullet\bullet)$. Thus, these must be the elements that belong to $H$. However, notice that

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \tag{7.13}$$

forms a subgroup of $A_4$ and, more importantly, of $H$. By Lagrange's theorem, 4 divides $|H|$. This leads to a contradiction since, by assumption, $|H| = 6$ which is not divisible by 4. Thus, $H$ cannot contain only two 3-cycles.

This exhausts all the options, proving that $A_4$ cannot have a subgroup $H \leq A_4$ of order 6. □

**Theorem 7.4** *Every group of prime order is cyclic.*

***Proof*** Suppose $|G| = p$ for some prime number $p$. Pick $g \in G$ with $g \neq e$. Then $|g| \neq 1$ ($e$ is the only element with order 1). By Lagrange's theorem, $|g|$ divides $|G| = p$. Therefore, $|g| = p$ and so $G = \langle g \rangle$. □

Lagrange's theorem is extremely restrictive on finite groups of small size.

**Theorem 7.5** *Every group of order 4 is isomorphic to one of* $(\mathbb{Z}_4, +, 0)$ *or the Klein four-group.*

***Proof*** **Case 1**: If $G$ has an element of order 4 then $G$ is cyclic.
**Case 2**: Suppose $G$ does not have an element of order 4. By Lagrange's theorem, the only possible orders for the elements of $G$ are 1 or 2. Let us label the elements of $G$ as $G = e, x, y, z$ where $x, y, z$ have order 2. What is $xy$?

- If $xy = e$, then $y = x^{-1} = x^{-1}e = x^{-1}x^2 = x$, a contradiction.
- If $xy = x$, then $y = e$, a contradiction.
- If $xy = y$, then $x = e$, a contradiction.
- If $xy = z$, then $(xy)^{-1} = z^{-1} \Rightarrow y^{-1}x^{-1} = z^{-1} \Rightarrow yx = z$. This means $G$ is isomorphic to the Klein four-group. □

Using the theorems that we learned so far, we are now able to classify some finite groups, up to isomorphisms. See Table 7.1. We will fill some of the other unknowns as we prove more properties of groups.

## Problems

**7.1** a) Let $G = A_4$ and $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Work out the (distinct) left and right cosets of $H$ in $G$.
b) Let $G = A_4$ and $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Work out the (distinct) left and right cosets of $H$ in $G$.

**7.2** Let $G$ be a group. Show that $G$ cannot have a subgroup $H$ with $|H| = |G| - 1$ if $|G| \neq 2$.

Table 7.1: Classification of some groups, up to isomorphisms.

| \|G\| | How many? | What are they? |
|---|---|---|
| 1 | 1 | {e} |
| 2 | 1 | $\mathbb{Z}_2$ |
| 3 | 1 | $\mathbb{Z}_3$ |
| 4 | 2 | $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$ |
| 5 | 1 | $\mathbb{Z}_5$ |
| 6 | later... | later... |
| 7 | 1 | $\mathbb{Z}_7$ |
| 8 | later... | later... |
| 9 | later... | later... |
| 10 | later... | later... |
| 11 | 1 | $\mathbb{Z}_{11}$ |
| 12 | later... | later... |
| 13 | 1 | $\mathbb{Z}_{13}$ |
| 14 | later... | later... |
| 15 | 1 | $\mathbb{Z}_{15}$ |

**7.3** Let $H$ and $K$ be finite subgroups of a group $G$. Suppose that $\gcd(|H|, |K|) = 1$. Prove that $H \cap K = \{e\}$.

**7.4** a) Suppose $K$ is a proper subgroup of $H$ (denoted $K < H$) and $H$ is a proper subgroup of $G$ (denoted $H < G$). If $|K| = 42$ and $|G| = 420$, what are the possible orders of $H$?

b) Give an example of groups $K, G$ with $|K| = 42$ and $|G| = 420$ and subgroups $H$ of all possible orders which satisfy $K < H < G$.

**7.5** Let $H$ be a subgroup of a finite group $G$. Suppose $g \in G$ and $n$ is the smallest positive integer such that $g^n \in H$. Prove that $n$ divides the order of $g$.

**7.6** Let $H$ be a subgroup of $G$.

a) Show that the function $G \to G$ given by $x \mapsto x^{-1}$ carries the left coset $gH$ to the right coset $Hg^{-1}$ and carries $Hg$ to $g^{-1}H$.

b) Without looking at these notes or your notes, state the definition of the index $[G : H]$ of $H$ in $G$. Explain how part a) shows it doesn't matter whether you use left or right cosets in this definition.

**7.7** a) Let $\alpha$ be a $k$-cycle in $S_n$. Prove that the order of the centralizer of $\alpha$ is $k \cdot (n-k)!$.

b) Find the centralizer of $(1\ 2)(3\ 4)$ in $S_5$. (Hint: Its order is 4.) To which familiar group is it isomorphic to? Explain.

**7.8** Let $G$ be a finite abelian group, with $|G| = n$. Label the elements of $G$ as $g_1, \cdots, g_n$.

a) Let $g_a, g_b \in G$ for some $a, b$. Prove that there exists an element in $G$ with order $\gcd(|g_a|, |g_b|)$. (Hint: Consider solving Problem 1.9, if you haven't done so already.)

b) Let

$$m = \gcd(|g_1|, \ldots, |g_n|).$$

Prove that there exists an element in $G$ with order $m$. (Hint: Recall that if none of $n_1, n_2, n_3$ are zero, then

$$\operatorname{lcm}(n_1, n_2, n_3) = \operatorname{lcm}(\operatorname{lcm}(n_1, n_2), n_3) = \operatorname{lcm}(n_1, \operatorname{lcm}(n_2, n_3)).$$

From this, one can show that if none of $n_1, n_2, \ldots, n_r$ is zero, then

$$\operatorname{lcm}(n_1, n_2, \ldots, n_r) = \operatorname{lcm}(\operatorname{lcm}(n_1, \ldots, n_{r-1}), n_r)$$

and similar expressions as well.)

c) Give an example of a finite non-abelian group where the previous conclusion does not hold.

**7.9** a) Prove that a group of order 63 must have an element of order 3. (Hint: If $g$ has order any multiple of 3, then some power of $g$ has order 3 (why?). If the statement is false, then every has order relatively prime to 3 so...) If you know Cauchy's theorem, then this part is trivial. Solve this problem without using Cauchy's theorem.

b) Can a group of order 55 have exactly 20 elements of order 11?

**7.10** Prove that $A_5$ has no subgroup of order 30. (Hint: Suppose $H \leq A_5$ has order 30. For $\alpha \in A_5$ of order 3, if $\alpha \notin H$, consider $H \cup \alpha H$.)

# Chapter 8
# Cauchy's Theorem

**Abstract** Let $G$ be a group. We saw that if $n$ divides $|G|$ then, in general, we are *not* guaranteed that there exists an element $g \in G$ with $|g| = n$. The story changes if $n$ is prime.

## 8.1 Cauchy's Theorem

In this chapter, we will go over Cauchy's theorem but postpone the proof of the theorem until later (when we cover the Orbit-Stabilizer theorem).

**Theorem 8.1** *Cauchy's theorem - Let G be a finite group. Let p be a prime divisor of $|G|$. Then G has an element of order p.*

***Proof*** Later. Proved in Theorem 11.3 after the introduction and proof of the Orbit-Stabilizer theorem. □

Remark: Cauchy's theorem is a partial converse to Lagrange's Theorem. The Sylow theorems assert a slightly stronger partial (but still not full, as we have seen is not possible) converse to Lagrange's theorem: Let $p$ be a prime factor of $|G|$ for a finite group $G$ and let $k \in \mathbb{Z}$ be the largest positive integer such that $p^k$ divides $|G|$. Then $G$ contains a subgroup $H \leq G$ with $|H| = p^k$.

*Example 8.1* Consider $S_4$. It has order $|S_4| = 4! = 24 = 8 \cdot 3 = 2^3 \cdot 3$. By Cauchy's theorem, we conclude that $S_4$ has at least one element of order 2 and at least one element of order 3. $S_4$ also has elements of order 4 but Cauchy's theorem by itself does not address this. Also note that Cauchy's theorem does not tell how many times a group contains an element of that order, just that it contains at least one element with that order.

Cauchy's theorem lets us classify more groups, up to isomorphisms.

**Theorem 8.2** *Let p be an odd prime (so p is prime and $p \neq 2$). Every group of order $2p$ is isomorphic to either $\mathbb{Z}_{2p}$ or $D_p$.*

***Proof*** Let $G$ be a group of order $2p$, where $p$ is an odd prime. By Cauchy's theorem, $G$ contains an element of order $p$, call it $x$, and an element of order 2, call it $y$. Let $H = \langle x \rangle$, so $|H| = p$. $y \notin H$ since $2 \nmid p$ by assumption. Therefore, $yH \neq H$ and so $G = H \cup yH$. By the same argument, $G = H \cup Hy$. Therefore, $yH = Hy \Rightarrow yHy^{-1} = H$. This means they are equal *as sets* (and not necessarily as ordered sets). That is, for any $h_1 \in H$ there is some $h_2 \in H$ such that $yh_1y^{-1} = h_2$ with $h_1$ not necessarily equal to $h_2$. Applying this to $H = \langle x \rangle$ means that $yxy^{-1} = x^k$ for some $k \in \mathbb{Z}$. The idea/trick is to conjugate $x$ by $y$ twice and use the fact that $y^2 = e$. That is: $y(yxy^{-1})y^{-1} = yx^k y^{-1} = (yxy^{-1}) \cdots (yxy^{-1}) = (x^k)^k = x^{k^2}$. Since $y^2 = e$, this implies $x = x^{k^2}$ and, hence, $k^2 \equiv 1$ (mod p). Thus, $p \mid (k^2 - 1) \Rightarrow p \mid (k-1)(k+1)$ and, since $p$ is prime, this means either $p \mid (k-1)$ or $p \mid (k+1)$.

- **Case 1**: If $k \equiv 1$ (mod p), then $yxy^{-1} = x^k = x \Rightarrow yx = xy$. Thus, $G$ is abelian. In particular, $G \cong \mathbb{Z}_p \times \mathbb{Z}_2$. Since $p$ is an odd prime, $\gcd(2, p) = 1$ so $\mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$. Therefore, $G \cong \mathbb{Z}_{2p}$ is cyclic.
  More systematically and abstractly, one could also solve Problem 8.1 and then use the results here. Since $G$ is a finite abelian group, we know that (see Problem 8.1) $G$ has an element of order $\operatorname{lcm}(2, p) = 2p$ (which is $xy$, as your solution to Problem 8.1 might show). Thus, $G = \langle xy \rangle \cong \mathbb{Z}_{2p}$.
- **Case 2**: If $k \equiv -1$ (mod p), then $x^p = e, y^2 = e$ and $yxy^{-1} = x^k = x^{-1}$. This is isomorphic to $D_p$. □

This theorem lets us fill in our table a bit more.

Table 8.1: Classification of some groups, up to isomorphisms.

| \|G\| | How many? | What are they? |
|---|---|---|
| 1 | 1 | {e} |
| 2 | 1 | $\mathbb{Z}_2$ |
| 3 | 1 | $\mathbb{Z}_3$ |
| 4 | 2 | $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$ |
| 5 | 1 | $\mathbb{Z}_5$ |
| 6 | 2 | $\mathbb{Z}_6, D_3 \cong S_3$ |
| 7 | 1 | $\mathbb{Z}_7$ |
| 8 | later... | later... |
| 9 | later... | later... |
| 10 | 2 | $\mathbb{Z}_{10}, D_5$ |
| 11 | 1 | $\mathbb{Z}_{11}$ |
| 12 | later... | later... |
| 13 | 1 | $\mathbb{Z}_{13}$ |
| 14 | 2 | $\mathbb{Z}_{14}, D_7$ |
| 15 | 1 | $\mathbb{Z}_{15}$ |

## Problems

**8.1** Let $G$ be an abelian group. Show that

a) For any $g_1, g_2 \in G$, there exists an element with order $\mathrm{lcm}(|g_1|, |g_2|)$.
b) Let $|G| = N$. Show that there exists an element in $G$ with order $\mathrm{lcm}(|g_1|, \cdots, |g_N|)$.

**8.2** Give an example of a finite non-abelian group for which the conclusion of Problem 8.1 does not hold.

**8.3** Let $G$ be a finite abelian group whose order is divisible by 10. Prove that $G$ has a cyclic subgroup of order 10.

**8.4** Let $a$ and $b$ be elements of a group $G$ such that $a^5 = e$, $aba^{-1} = b^2$, and $b \neq e$. What is the order of $b$? (Hint: See the idea/trick in Theorem 8.2 for inspiration.)

**8.5** Let $G$ be a group of order $4n + 2$. Use Cauchy's theorem, Cayley's theorem, and Problem 3.10 to show that $G$ contains a subgroup of order $2n + 1$.

**8.6** Let $G$ be a group of order $pqr$, where $p, q$, and $r$ are distinct primes. If $H$ and $K$ are subgroups of $G$ with $|H| = pq$ and $|K| = qr$, prove that $|H \cap K| = q$.

# Chapter 9
# Conjugacy

**Abstract** We saw (in the proof of Cayley's theorem) that a group can act on itself by left translation. A group can also act on itself by conjugation.

## 9.1 Conjugacy

**Definition 9.1** Let $G$ be a group. We say $x \in G$ is conjugate to $y \in G$ if there exists an element $g \in G$ such that $x = gyg^{-1}$.

**Proposition 9.1** *Conjugacy is an equivalence relation.*

***Proof*** i) $x = exe^{-1}$ for $\forall x \in G$. Thus, $x \sim x$ for $\forall x \in G$.

ii) If $x \sim y$ then there $\exists g \in G$ such that $x = gyg^{-1}$. Thus, $y = g^{-1}x(g^{-1})^{-1}$. But $g^{-1} \in G$ since $G$ is a group, so $y \sim x$.

iii) Suppose $x \sim y$ and $y \sim z$. Then there $\exists g_1, g_2 \in G$ such that $x = g_1 y g_1^{-1}$ and $y = g_2 z g_2^{-1}$. Thus, $x = g_1 g_2 z g_2^{-1} g_1^{-1} = (g_1 g_2) z (g_1 g_2)^{-1}$. But $g_1 g_2 \in G$ since $G$ is a group, so $x \sim z$. □

Note: Some books define conjugation slightly different: $x$ is conjugate to $y$ if there exists $g \in G$ such that $gxg^{-1} = y$. By Proposition 9.1, it doesn't really matter.

**Definition 9.2** The equivalence classes for conjugacy are called conjugacy classes of $G$. The conjugacy class of $x$ is $[x] = \{gxg^{-1} \mid g \in G\}$.

Since conjugacy is an equivalence relation and equivalence relations give partitions, this means that the conjugacy classes of a group $G$ are a partition of $G$.

*Example 9.1* Let $G$ be a group. Then $\{e\}$ is always a conjugacy class of $G$ since $geg^{-1} = e$ for any $g \in G$.

*Example 9.2* If $G$ is an abelian group, each conjugacy class has only one element. This is because, for $\forall x \in G$,

$$\begin{aligned}[x] &= \{gxg^{-1} \mid g \in G\} \\ &= \{xgg^{-1} \mid g \in G\} \\ &= \{x \mid g \in G\} \\ &= \{x\}.\end{aligned} \tag{9.1}$$

Each element of $G$ is in a conjugacy class of its own.

### 9.1.1 Conjugacy classes of $S_n$

**Theorem 9.1** *The conjugacy classes of $S_n$ are exactly the permutations with a given cycle structure.*

***Proof*** Corollary 3.2 implies that conjugating an element of $S_n$ does not change the cycle structure. Theorem 3.11 shows that two elements in $S_n$ that have the same cycle structure are conjugate to one another (the theorem even gives a prescription for finding an element that conjugates one into the other). Therefore, elements in $S_n$ are conjugate if and only if they have the same cycle structure. □

*Example 9.3* The conjugacy classes of $S_4$ and the cardinality of those conjugacy classes are listed in Table 9.1.

Table 9.1: Conjugacy classes of $S_4$.

| **Representative Element** | **Cardinality** |
|---|---|
| $e$ | 1 |
| (●●) | $\frac{4\cdot 3}{2} = 6$ |
| (● ● ●) | $\frac{4\cdot 3\cdot 2}{3} = 8$ |
| (●●)(●●) | $(\frac{4\cdot 3}{2}\frac{2\cdot 1}{2})\frac{1}{2!} = 3$ |
| (● ● ●●) | $\frac{4\cdot 3\cdot 2\cdot 1}{4} = 6$ |
| | total = 24 |

There are five (distinct) conjugacy classes in $S_4$. Note that

$$1 + 6 + 8 + 3 + 6 = 24 = |S_4|, \tag{9.2}$$

as a partition of $S_4$ should satisfy.

### 9.1.2 Conjugacy classes of $A_n$

$A_n$ is different from $S_n$. Some $\alpha_1$ and $\alpha_2$ in $A_n$ are not conjugate *even if* they have the same cycle structure. This is because it could be that $g\alpha_1 g^{-1} = \alpha_2$ only has solutions where $g$ an odd permutation, so $g \notin A_n$. Therefore, elements that used to form a single conjugacy class in $S_n$ could split into separate conjugacy classes in $A_n$.

*Example 9.4* The conjugacy classes of $A_4$ are relatively straightforward to evaluate by brute-force. The result is given in Table 9.2.

Table 9.2: Conjugacy classes of $A_4$.

| **Representative Element** | **Conjugacy Class** | **Cardinality** |
|---|---|---|
| $e$ | $\{e\}$ | 1 |
| $(1\,2\,3)$ | $\{(1\,2\,3),(1\,4\,2),(1\,3\,4),(2\,4\,3)\}$ | 4 |
| $(1\,3\,2)$ | $\{(1\,3\,2),(1\,2\,4),(1\,4\,3),(2\,3\,4)\}$ | 4 |
| $(\bullet\bullet)(\bullet\bullet)$ | $\{(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$ | 3 |
| | | total = 12 |

For example, $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are not conjugate. Suppose there were a $g \in A_4$ such that $g(1\ 2\ 3)g^{-1} = (1\ 3\ 2)$. This requires

$$\begin{aligned}(g(1)\ g(2)\ g(3)) &= (1\ 3\ 2) && \Rightarrow g = (2\ 3) && (9.3)\\ &= (3\ 2\ 1) && \Rightarrow g = (1\ 3) && (9.4)\\ &= (2\ 1\ 3) && \Rightarrow g = (1\ 2). && (9.5)\end{aligned}$$

To explain the arrows ⇒, what we mean is that once $g(1)$ is chosen, then $g(2)$ and $g(3)$ are determined.

- If $g(1) = 1$, then $g(2) = 3$ and $g(3) = 2$. That is, $g = (2\ 3)$.
- If $g(1) = 3$, then $g(2) = 2$ and $g(3) = 1$. That is, $g = (1\ 3)$.
- If $g(1) = 2$, then $g(2) = 1$ and $g(3) = 3$. That is, $g = (1\ 2)$.

However, all of these solutions are transpositions. Therefore, when we go from $S_4$ to $A_4$, none of these solutions "carry over." Thus, as claimed, even though $(1\ 2\ 3)$ and $(1\ 3\ 2)$ were conjugate *in* $S_4$ (with the solutions found above) they are not conjugate *in* $A_4$.

Fact: The conjugacy class $(\bullet\bullet\bullet)$ does *not* split in $A_n$ for $n \geq 5$. In fact, $k$-cycles with $1 \leq k \leq (n-2)$ do not split in $A_n$. One only has to worry about $(n-2)$-cycles splitting in $A_n$ (for $n$ even, since if $n$ is odd then the $(n-1)$-cycles are odd permutations and therefore are not in $A_n$). Let's prove this.

**Proposition 9.2** *Any $k$-cycle in $A_n$ is conjugate to any other $k$-cycle in $A_n$ for* $1 \leq k \leq (n-2)$ *(and k odd, of course).*

***Proof*** Let $1 \leq k \leq (n-2)$ with $k$ odd. Let $\alpha, \beta \in A_n$ be arbitrary $k$-cycles. Then $\alpha$ and $\beta$ are conjugate *in* $S_n$. That is, there exists a $g \in S_n$ such that $g\alpha g^{-1} = \beta$. There are two cases to consider.

i) If $g \in A_n$, then $\alpha$ and $\beta$ are conjugate in $A_n$.

ii) If $g$ is an odd permutation, then we can create an even permutation that conjugates $\alpha$ to $\beta$. This is because there exist two integers that do not appear in $\alpha$ (since $1 \leq k \leq (n-2)$). Use those two integers to create a transposition and call it $t$. Then $gt$ is an even permutation so $gt \in A_n$. Also, we have

$$(gt)\alpha(gt)^{-1} = gt\alpha t^{-1}g^{-1} = g\alpha tt^{-1}g^{-1} = g\alpha g^{-1} = \beta, \tag{9.6}$$

where we have used $t\alpha = \alpha t$ since $\alpha$ and $t$ are disjoint. □

## 9.2 Centers

**Definition 9.3** Let $G$ be a group. The center of $G$, denoted $Z(G)$, is the subset $Z(G) = \{x \in G \mid xy = yx \text{ for } \forall y \in G\}$.

**Proposition 9.3** *$Z(G)$ is a subgroup.*

***Proof*** $e \in Z(G)$ so $Z(G)$ is nonempty. Let $x, y \in Z(G)$. Then for any $g \in G$

$$\begin{aligned} gxy^{-1} &= xgy^{-1} && \text{since } x \in Z(G) \\ &= x(yg^{-1})^{-1} \\ &= x(g^{-1}y)^{-1} && \text{since } y \in Z(G) \\ &= xy^{-1}g. \end{aligned} \tag{9.7}$$

Therefore, $xy^{-1} \in Z(G)$. By Theorem 1.1, $Z(G)$ is a subgroup of $G$. □

**Theorem 9.2** *$Z(G)$ is the union of the conjugacy classes of G which have cardinality 1.*

***Proof*** Let $x \in Z(G)$. This means that $gx = xg$ for any $g \in G$. In other words, $gxg^{-1} = x$ for any $g \in G$, so $[x] = \{x\}$. Likewise, if $[x] = \{x\}$ then $gxg^{-1} = x$ for any $g \in G$. This then means $gx = xg$ for any $g \in G$, so $x \in Z(G)$. □

**Proposition 9.4** *$Z(G) = G$ if and only if $G$ is abelian.*

***Proof*** $\Rightarrow$ Suppose $Z(G) = G$. This means that $xy = yx$ for $\forall x, y \in G$. This is, however, precisely what it means for $G$ to be abelian.
$\Leftarrow$ Since $G$ is abelian $[x] = \{gxg^{-1} \mid g \in G\} = \{xgg^{-1} \mid g \in G\} = \{x\}$ for any $x \in G$. Thus, every element in $G$ forms a conjugacy class of size 1. Apply Theorem 9.2 to reach the necessary conclusion. □

*Example 9.5* $Z(S_2) = S_2$ since $S_2 = \{e, (1\ 2)\}$ is abelian.

*Example 9.6* $Z(S_n) = \{e\}$ since the conjugacy classes of $S_n$ are those of a given cycle structure. The only cycle structure that has only 1 element with that cycle structure is the cycle structure with $n$ 1-cycles. That is, only the identity element.

Theorem 9.2 is useful because it means that to find $Z(G)$, one does not necessarily need to check all the possible products of two elements in a group. Instead, one can work out the conjugacy classes and check which ones have only have one element. See Problem 9.2 for practice.

## Problems

**9.1** Show that $A_6$ has exactly one conjugacy class of elements of order two. (Hint: What are the possible cycle structures for elements in $S_6$? What about $A_6$?)

**9.2** a) Work out the conjugacy classes of $D_n$ for $n$ even and $n$ odd.
b) Apply Theorem 9.2 to find $Z(D_n)$ for $n$ even and $n$ odd.

**9.3** Find the center of the following groups:

a) $O_n$ and $SO_n$.
b) $U_n$ and $SU_n$.

(Hint: The idea is to let $A$ be an arbitrary element of the group and ask what are the constraints on $A$ so that $A$ is in the center of the group. To do this, use clever choices of matrices $P$ and enforce $AP = PA$ and compare the two sides to see what the constraints on the entries of $A$ are. The constraints will end up being strict and will force $A$ to be relatively simple.)

**9.4** a) Prove that the 3-cycles in $A_5$ form a single conjugacy class. That is, the 3-cycles which form a single conjugacy class in $S_5$ do *not* split when viewed as elements of $A_5$.
b) The 5-cycles do not form a single conjugacy class. Find two 5-cycles in $A_5$ which are not conjugacy *in* $A_5$ (with proof, of course). We see that the 5-cycles, which form a single conjugacy class in $S_5$ *do* split when the 5-cycles are viewed as elements *in* $A_5$.

**9.5** Let $q = a + bi + cj + dk$ and $q' = a' + b' + c'j + d'k$ be quaternions. Define

$$\begin{aligned} q + q' &= (a + a') + (b + b')i + (c + c')j + (d + d')k, \\ q \cdot q' &= (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i \\ &\quad + (ac' - bd' + ca' + db')j + (ad' + bc' - cb' + da')k. \end{aligned}$$

Prove that $\mathbb{H}$ forms an abelian group under addition and that $\mathbb{H} - \{0\}$ is a group (though not an abelian group) under multiplication. Show that the correspondence

$$a + bi + cj + dk \leftrightarrow (a, b, c, d)$$

is an isomorphism from the additive group $\mathbb{H}$ to $\mathbb{R}^4$.

**9.6** The conjugate of a quaternion $q = a + bi + cj + dk$ is defined to be $q^* = a - bi - cj - dk$, and the length of $q$ is the square root of $q \cdot q^*$. In other words, the length is $\sqrt{a^2 + b^2 + c^2 + d^2}$. Show that the quaternions of unit length form a subgroup of $\mathbb{H} - \{0\}$. We shall denote this group by $S^3$ because it corresponds to the unit sphere if we identify $\mathbb{H}$ with $\mathbb{R}^4$ (see Problem 9.5).

**9.7** Prove that the correspondence

$$a + bi + cj + dk \leftrightarrow \begin{bmatrix} a + ib & , c + id \\ -c + id & , a - ib \end{bmatrix},$$

where $i = \sqrt{-1} \in \mathbb{C}$ on the right hand, defines an isomorphism between $S^3$ and $SU_2$. (Hint: To prove surjectivity, make use of Problem 12.1.)

**9.8** Show that any nonzero quaternion has a multiplicative inverse.

**9.9** Write out the elements of $SU_2$ which correspond to the subgroup $Q$ of $S^3$. Find a subgroup of $S^3$ which is isomorphic to $C$.

**9.10** An element of $\mathbb{H}$ of the form $bi + cj + dk$ is called a pure quaternion. Show that

$$q \cdot (bi + cj + dk) \cdot q^{-1}$$

is a pure quaternion for every $q \in \mathbb{H} - \{0\}$. (Hint: $q \cdot (bi + cj + dk) \cdot q^{-1} = A + Bi + Cj + Dk$ for some $A, B, C, D$. You only need to show that $A$ is 0. You can work in matrix notation as in Problem 9.7, if preferred.)

**9.11** Given $\mathbf{x} = (x_1, x_2, x_3)$ in $\mathbb{R}^3$, let $q(\mathbf{x})$ denote the quaternion $x_1 i + x_2 j + x_3 k$. If $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$ prove that

$$q(\mathbf{x} \times \mathbf{y}) = \mathbf{x} \cdot \mathbf{y} + q(\mathbf{x}) \cdot q(\mathbf{y}).$$

Definition: A division ring is a ring with 1 in which every nonzero element has a multiplicative inverse, but in which multiplication need not be commutative. The quaternions $\mathbb{H}$ are a leading example of a division ring.
Background: A topological group is a group $G$ that is also a topological space (e.g., a metric space); we require that the multiplication function $G \times G \longrightarrow G$ by $(x, y) \mapsto xy$ and the inversion function $G \longrightarrow G$ by $x \mapsto x^{-1}$ be continuous functions. An example of a topological group is $GL_n(\mathbb{R})$, which inherits its topology from viewing the $n^2$ matrix elements as elements of $\mathbb{R}^{n^2}$ with the usual metric.
The sphere $S^n$ can only be a topological group for special $n$:

- $S^0 = \{\pm 1\}$, the sphere of dimension 0 in $\mathbb{R}$.
- $S^1$, the unit circle $C$ in $\mathbb{C}$, is isomorphic to $SO_2$.
- $S^3$, the unit quaternions, is isomorphic to $SU_2$.
- $S^7$, the unit sphere in an 8-dimensional space call the octonions. The octonions are a nonassociative ring.

It is proved in topology that, among spheres, only these four can be topological groups.

**9.12** For paragraphs marker •, you do not have to write anything, but you may use them in later parts.

a) Let $||q|| = \sqrt{q \cdot q^*}$ be the length of a quaternion. Show that the length is multiplicative: $||qr|| = ||q|| \cdot ||r||$.
b) Show that $q \cdot (bi + cj + dk) \cdot q^{-1}$ for $q \in \mathbb{H} - \{0\}$ has the same length as $bi + cj + dk$.
c) Use b) to construct a nontrivial homomorphism $\phi : SU_2 \to O_3$. That is, conjugation preserves the length of pure quaternions.
d) Let $[0, 1]$ be the closed interval from 0 to 1 in $\mathbb{R}$. A path in a space $X$ is a continuous function $p : [0, 1] \to X$. The endpoints of the path are $x_0 = p(0)$ and $x_1 = p(1)$. We say $X$ is path-connected if any two points of $X$ can be joined by a path in $X$. For $n \geq 1$, argue that the sphere $S^n$ is path-connected. (You do not need to be fully rigorous on this part.)

- The determinant is a continuous function on a matrix group. This is because polynomials are continuous, and dividing two continuous function is continuous whenever the denominator is not zero. For complex polynomials in both $z$ and $z^*$, the real and imaginary parts are real polynomials, hence continuous.

e) We know $O_3$ is the disjoint union $SO_3 \cup A \cdot SO_3$ where $A$ is any $A \in O_3$ with $\det A = -1$. Show that no continuous path in $O_3$ can join a point in $SO_3$ to a point in $A \cdot SO_3$. (Hint: What would the determinant do on such a path? In particular, in the intermediate of such a path?) We say $SO_3$ and $A \cdot SO_3$ are in different path-connected components.

- The image of a path-connected space $X$ under a continuous function $f : X \to Y$ is path-connected. Proof: Let $y_0, y_1$ be in the image. Write $f(x_0) = y_0$ and $f(x_1) = y_1$. Let $p$ be a continuous path from $x_0$ to $x_1$. The composition of continuous function is continuous. Thus, $f \circ p$ is a continuous path from $y_0$ to $y_1$.

f) Conclude that the homomorphism $\phi$ really goes $SU_2 \to SO_3$.

- $\phi$ is surjective. One can prove this with more topology. Or, since $n = 2$ is small, one may be able to play with $SU_2$ and prove it directly.

g) Show that the solution set of $\phi(q) = I_{3\times 3}$ contains exactly two points, the quaternions $\pm 1$.
h) Show that for any $B \in SO_3$, the solution set of $\phi(q) = B$ contains exactly two points.

- Parts g) and h) have shown that $SU_2$ is a double cover of $SO_3$. Around any point $\phi(q)$ of $SO_3$, take a small open ball $U$; there are two disjoint small open balls $U_1, U_2$ around $q, -q$, respectively, in $SU_2$, and $\psi$ send each $U_j$ bijectively onto $U$.

- What is the dimension of these balls? $SO_3$ is a 3-dimensional space: it has three degrees of freedom. To see this, put the unit sphere $S^2$ around the origin in $\mathbb{R}^3$. Choose any unit vector $\mathbf{v}$ pointing from the origin to $S^2$- that's two dimensions' worth of choice, since $S^2$ is a 2-dimensional surface. Let $\mathbf{v}$ span the axis of a rotation. Choose an angle $\theta$ between 0 and $2\pi$- that's a third dimension's worth of choice. Rotate around the chosen axis by $\theta$. Since we will prove that every nontrivial element of $SO_3$ is a rotation around an axis, we have accounted for all the dimensions.
- $SU_2$ is also 3-dimensional, because it is a double cover of $SO_3$; the balls $U_1$ and $U_2$ are 3-dimensional, like $U$. The group $U_2$ is 4-dimensional, because it is $SU_2$ times one more dimension, the choice of $\theta$ in $\begin{bmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{bmatrix}$.
- Even more interesting, the map $U_1 \to U$ has the opposite orientation from $U_2 \to U$. Any curve $q(t)$ through the center of $U_1$ corresponds to a curve $-q(t)$ in the opposite direction through the center of $U_2$. Since the dimension is three, the total change of orientation is $(-1)^3 = -1$. $SO_3$ is a nonorientable three-dimensional space, just as the Mobius strip is a nonorientable two-dimensional surface. $SU_2 = S^3$ is orientable, but the double covering map $\phi$ wraps it up in a nonorientable way. $SO_3$ is also called the real projective space of dimension 3. This is more information online about these topics.

# Chapter 10
# Quotient Groups

**Abstract** In chapter 4, we saw how to make groups by "multiplying" groups. In this chapter we will explore how to create groups by "dividing" a group by a (normal) subgroup.

## 10.1 Exploring a Hunch

Let us review some material. Let $H$ be a subgroup of $G$. The set

$$gH = \{gh \mid h \in H\} \subseteq G \tag{10.1}$$

is called a left coset of $H$ in $G$. The set

$$Hg = \{hg \mid h \in H\} \subseteq G \tag{10.2}$$

is called a right coset of $H$ in $G$.

**Definition 10.1** Let $G$ be a group and let $H$ be a subgroup of $G$. We denote the set of all (distinct) left cosets of $H$ in $G$ by $G/H$. We denote the set of all (distinct) right cosets of $H$ in $G$ by $H\backslash G$.

The number of *elements* in $G/H$ is $[G : H]$. Note that $G/H$ is a set of elements, those elements themselves being sets (namely, the left cosets of $H$ in $G$).

Important Note: The notation $G/H$ is used in two ways. It denotes the set of all (distinct) left cosets of $H$ in $G$. These left cosets may also have the structure of a group, as we shall see now. When they have the structure of a group, we also denote them as $G/H$ and call it the quotient group of $G$ by $H$. That is, when you see $G/H$ you can always think of it as the set of all (distinct) left cosets of $H$ in $G$, but don't always assume that it is a quotient group unless $H$ is, as we will now see, a normal subgroup of $G$.

Let $G$ be a (finite or infinite) group and let $H$ be a subgroup of $G$. Recall that a group $G$ is a set with a binary operation $\diamond : G \times G \to G$ which satisfies some conditions (sometimes called the group axioms), as mentioned in Definition 1.4. We have seen that $G/H$ is also a set, albeit a set whose elements are also sets. A natural question that arises is this: is there a binary operation on the set $G/H$, perhaps related to the binary operation of $G$ in some way, which gives the set $G/H$ the structure of a group? That is, suppose that $x \diamond H \in G/H$ and $y \diamond H \in G/H$. Is there a binary operation $\star : (G/H) \times (G/H) \to G/H$ which satisfies the group axioms? If so, is it related to $\diamond : G \times G \to G$? One guess is this: trying composing the two sets. By composing, we mean to define

$$X \diamond Y = \{x \diamond y | x \in X, y \in Y\} \tag{10.3}$$

for any sets $X \subseteq G, Y \subseteq G$. We hope that the following holds:

$$(xH) \diamond (yH) = (x \diamond y) \diamond H, \tag{10.4}$$

for all $xH, yH \in G/H$. If it does, then define $\star : (G/H) \times (G/H) \to G/H$ as

$$(x \diamond H) \star (y \diamond H) = (x \diamond y) \diamond H \tag{10.5}$$

for every $x \diamond H, y \diamond H \in G/H$. The binary operation $\star : (G/H) \times (G/H) \to G/H$ would be a binary operation. It would be associative since $\diamond$ is associative. The coset $e \diamond H = H$ would be the identity element of $G/H$ under the binary operation $\star$ since $(e \diamond H) \star (x \diamond H) = (x \diamond H) \star (e \diamond H) = (e \diamond x) \diamond H = (x \diamond e) \diamond H = x \diamond H$ for any $x \in H$. Also, every $x \diamond H$ would have an inverse since one could pick $y \in G$ such that $x \diamond y = y \diamond x = e$ which would then imply $(x \diamond H) \star (y \diamond H) = (y \diamond H) \star (x \diamond H) = (x \diamond y) \diamond H = (y \diamond x) \diamond H = e \diamond H = H$.

Okay, maybe there are too many $\diamond$ and $\star$ floating around. Let us consider multiplicative notation. In multiplicative notation, this looks like

$$(xH)(yH) = (xy)H \tag{10.6}$$

for any $x, y \in G$. We hope/guess that $(xH)(yH) = (xy)H$ for any $x, y \in G$. If so, then $eH$ is the identity element and $x^{-1}H$ is the inverse of $xH$. In additive notation this looks like

$$(x + H) + (y + H) = (x + y) + H \tag{10.7}$$

for any $x, y \in G$. We hope/guess that $(x + H) + (y + H) = (x + y) + H$. If so, then $0 + H$ is the identity element and $-x + H$ is the inverse of $x + H$.

*Example 10.1* Let $G = D_n$. Let $H = \langle r \rangle$. Then $eH = \{e, r, r^2, \cdots, r^{n-1}\}$ and $sH = \{s, sr, sr^2, \cdots, sr^{n-1}\} = \{s, rs, r^2s, \cdots, r^{n-1}s\}$ (as sets, not as ordered sets) partition $D_n$. Therefore, $G/H = \{eH, sH\}$. We see that (verify this!)

$$\begin{aligned} (eH)(eH) &= (ee)H = eH, \quad (sH)(eH) = (se)H = sH, \\ (eH)(sH) &= (es)H = sH, \quad (sH)(sH) = (ss)H = eH. \end{aligned} \tag{10.8}$$

Thus, the set of left cosets $G/H$ does have the structure of a group. In fact, it is isomorphic to $\mathbb{Z}_2$.

*Example 10.2* Let $G = (\mathbb{Z}, +, 0)$ and $H = 4\mathbb{Z}$. Then

$$G/H = \mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}. \tag{10.9}$$

If these cosets are combined via

$$(x + 4\mathbb{Z}) + (y + 4\mathbb{Z}) = (x + y) + 4\mathbb{Z}, \tag{10.10}$$

then $G/H$ forms a group. More generally, if $n$ is a positive integer then $\mathbb{Z}/n\mathbb{Z}$ consists on $n$ distinct cosets

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots , (n - 1) + n\mathbb{Z} \tag{10.11}$$

which form a group. In fact, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

So far, so good. Was our intuition/guess on how to define $\star : (G/H) \times (G/H) \to G/H$ correct? Are things that straightforward? Actually, not quite.

*Example 10.3* Let $G = S_3$ and $H = \langle(1\ 2)\rangle = \{e, (1\ 2)\}$. Then $G/H$ consists of

$$eH = \{e, (1\ 2)\}, \tag{10.12}$$
$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}, \tag{10.13}$$
$$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}. \tag{10.14}$$

Note that

$$\begin{aligned}(1\ 2)H \cdot (2\ 3)H &= \{e, (1\ 2)\}\{(2\ 3), (1\ 3\ 2)\} \qquad (10.15)\\ &= \{(2\ 3), (1\ 3\ 2), (1\ 2)(2\ 3), (1\ 2)(1\ 3\ 2)\}\\ &= \{(2\ 3), (1\ 3\ 2), (2\ 3\ 1), (1\ 3)\}\end{aligned}$$

while $(1\ 2)(2\ 3) = (1\ 2\ 3)$ and

$$\begin{aligned}(1\ 2\ 3)H &= (1\ 2\ 3)\{e, (1\ 2)\} \qquad (10.16)\\ &= \{(1\ 2\ 3), (1\ 2\ 3)(1\ 2)\}\\ &= \{(1\ 2\ 3), (1\ 3)\}.\end{aligned}$$

Thus, we see that $(1\ 2)H \cdot (2\ 3)H \neq ((1\ 2)(2\ 3))H$, so $G/H$ does not have the group structure that we were hoping for. In fact, $((1\ 2)H(2\ 3))H$ has cardinality 4 so even before calculating $(1\ 2\ 3)H$ we know that the two cannot be equal as $(1\ 2)H(2\ 3)H$ has the wrong size so it can't be a left coset of $H$ in $S_3$.

It seems that the set of left cosets $G/H$ sometimes has the group structure we would like, but not always. Our goal is to understand the reason behind this and see what we can salvage from our intuition into theorems.

## 10.2 Normal Subgroups and Quotient Groups

**Proposition 10.1** *Let $G$ be a (finite or infinite) group and let $H$ be a subgroup of $G$. If $gH = Hg$ for any $g \in G$ then*

$$(xH)(yH) = (xy)H$$

*for any $x, y \in G$.*

***Proof*** We prove this by showing that $(xH)(yH) \subseteq (xy)H$ and $(xy)H \subseteq (xH)(yH)$.

- $(xy)H \subseteq (xH)(yH)$ follows since $(xy)h = (xe)(yh) \in (xH)(yH)$ for any $h \in H$.
- To show that $(xH)(yH) \subseteq (xy)H$, consider $z \in (xH)(yH)$ be arbitrary. Then $z = (xh_1)(yh_2)$ for some $h_1, h_2 \in H$. Then

$$z = x(h_1 y)h_2 = x(yh_3)h_2 = (xy)(h_3 h_2) \tag{10.17}$$

for some $h_3 \in H$. This is because, by assumption, $gH = Hg$ for any $g \in G$. Therefore, $h_1 y \in Hy$ implies $h_1 y \in yH$, so $h_1 y = yh_3$ for some $h_3 \in H$. However, since $H$ is a subgroup, $h_3 h_2 \in H$. Therefore, $z = (xy)(h_3 h_2) \in (xy)H$. Since $z \in (xH)(yH)$ was arbitrary, we conclude that $(xH)(yH) \subseteq (xy)H$. Thus, $(xH)(yH) = (xy)H$. □

**Definition 10.2** Let $H \leq G$. We say $H$ is a normal subgroup of $G$, or a self-conjugate subgroup of $G$, if $gHg^{-1} \subseteq H$ for all $g \in G$. For finite groups, we can think of this as $gHg^{-1} = H$ for all $g \in G$ since conjugation is bijective. If $H \leq G$ is a normal subgroup, we denote this by writing $H \trianglelefteq G$.

Equivalently, $H$ is a normal subgroup of $G$ if $gH = Hg$ for all $g \in G$.

**Proposition 10.2** *Let $H \leq G$. Then $H \trianglelefteq G$ if and only if $xH = Hx$ for all $x \in G$.*

***Proof*** $\Rightarrow$ Suppose $H \trianglelefteq G$. Then $xHx^{-1} = H$ for all $x \in G$. In other words, $xH = Hx$ for all $x \in G$ (since right multiplication is bijective).
$\Leftarrow$ Suppose $xH = Hx$ for all $x \in G$. This means that $xh$ for any $h \in H$ can be written as $xh = \tilde{h}x$ for some $\tilde{h} \in H$ (where the $\tilde{h}$ depends on $h$). That is, for any $x \in G$ and any $h \in H$, there exists a $\tilde{h} \in H$ such that $xhx^{-1} = \tilde{h}$. Thus, $xHx^{-1} \subseteq H$. □

Note: When $H \trianglelefteq G$, it doesn't mean that $ghg^{-1} = h$ for $\forall g \in G$ and $\forall h \in H$. It just means that $ghg^{-1} = \tilde{h} \in H$, where $\tilde{h}$ may or may not be $h$.

We now have terminology to describe an observation.

**Proposition 10.3** *Let $G$ be a group and let $H$ be a normal subgroup of $G$. Then the set of left cosets of $H$ in $G$, denoted $G/H$, form a group where the group binary operation is defined as*

$$(xH)(yH) = (xy)H$$

*for any $xH, yH \in G/H$.*

***Proof*** This follows from our discussions above. If $H \trianglelefteq G$, then $gH = Hg$ for any $g \in G$. By Proposition 10.1, the composition is associative. Also, $x^{-1}H$ is the inverse of $xH$ and $eH$ is the identity element. Therefore, $G/H$ has the structure of a group. If $[G : H]$ is finite, then $|G/H| = [G : H]$. If $G$ is a finite group, then $|G/H| = [G : H] = |G|/|H|$. □

**Definition 10.3** Let $H$ be a normal subgroup of $G$. Then the set $G/H$ with the binary operation $(xH)(yH) = (xy)H$ for any $xH, yH \in G/H$ is called a quotient group or factor group.

Normal subgroups and quotient groups are the big ideas of this chapter. The takeaway from this chapter should be that normal subgroups have a nice feature which lets one "divide" out or "factor" a group into smaller pieces (the pieces being the left cosets comprising $G/H$) and those pieces themselves have a group structure. See Figure 10.1 for some intuition.

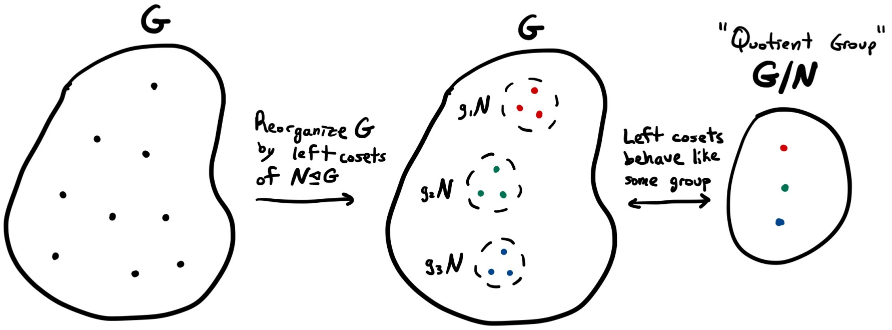

G
Reorganize G by left cosets of N⊴G
G
g₁N
g₂N
g₃N
Left cosets behave like some group
"Quotient Group"
G/N

Fig. 10.1: If $N \trianglelefteq G$, then the left cosets $G/N$ also behave like a group with the binary operation defined as $(xH)(yH) = (xy)H$ for all $xH, yH \in G/H$.

Let us consider some examples of normal subgroups and list some ways to find normal subgroups of a group.

*Example 10.4* Let $SL_n(\mathbb{R})$ be the group of $n \times n$ matrices with determinant 1. Let $GL_n(\mathbb{R})$ be the group of $n \times n$ invertible matrices. Let $A \in SL_n(\mathbb{R})$ be arbitrary. Let $B \in GL_n(\mathbb{R})$ be arbitrary. Then $\det(BAB^{-1}) = \det(B^{-1}BA) = \det(A) = 1$, so $BAB^{-1} \in SL_n(\mathbb{R})$. Therefore, $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.

**Proposition 10.4** *$H \trianglelefteq G$ if and only if $H$ is a union of conjugacy classes of $G$.*

***Proof*** $\Rightarrow$ Suppose that $H$ is a normal subgroup of $G$. Let $h \in H$ be arbitrary. Then $ghg^{-1} \in H$ for any $g \in G$. Equivalently, this means $[h] \subseteq H$ where $[h] \equiv \{ghg^{-1} \mid g \in H\}$ denotes the conjugacy class of $h$. Therefore,

$$H = \bigcup_{h \in H} [h]. \tag{10.18}$$

Therefore, $H$ is a union of conjugacy classes. Note, however, that all the conjugacy classes in the above equation are not necessarily distinct. That doesn't matter. We didn't seek the most efficient expression of $H \trianglelefteq G$ as a union of conjugacy classes of $G$. We just wanted to show that it can be done for any $H \trianglelefteq G$.
$\Leftarrow$ Suppose that $H$ is a union of conjugacy classes of $G$. Then $ghg^{-1} \in [h] \subseteq H$ for any $h \in H$ and any $g \in G$. That is, $ghg^{-1} \in H$ for any $h \in H$ and any $g \in G$. Therefore, $H \trianglelefteq G$. □

Note: Conjugacy classes are usually *not* closed under multiplication.

*Example 10.5* In $S_n$ for $n \geq 4$, $(\bullet \bullet \bullet\bullet)$ is a conjugacy class. However, $(\bullet \bullet \bullet\bullet)^2 = (\bullet\bullet)(\bullet\bullet)$. For example, $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$, which belongs to a different conjugacy class than $(1\ 2\ 3\ 4)$.

**Proposition 10.5** *Let $G$ be an abelian group. Then every subgroup $H \leq G$ is a normal subgroup $H \trianglelefteq G$.*

***Proof*** This is because $ghg^{-1} = gg^{-1}h = h \in H$ for any $h \in H$ and any $g \in G$, so clearly $gHg^{-1} = H$. Or, to connect the discussion to the previous proposition, every conjugacy class of an abelian group has only one element so any subgroup $H \leq G$ is clearly a union of conjugacy classes of $G$. □

A good question to ask is if the converse holds. That is, if every subgroup of a group $G$ is normal, is $G$ an abelian group? The answer is no. Consider the quaternion group $Q_8$. Verify that all the subgroups of $Q_8$ are normal. However, $Q_8$ is a non-abelian group.

**Proposition 10.6** *Let $G$ be an abelian group. Then the center of $G$ (labeled $Z(G)$) is a normal subgroup of $G$.*

***Proof*** Proposition 9.3 shows that $Z(G)$ is a subgroup. It is a normal subgroup because $gzg^{-1} = z \in Z(G)$ for any $z \in Z(G)$ and any $g \in G$, so clearly $gZ(G)g^{-1} = Z(G)$. □

*Example 10.6* Consider $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Then $Z(Q_8) = \{\pm 1\}$. $Q_8/Z(Q_8)$ has four cosets: $eZ(Q_8) = \{\pm 1\}, iZ(Q_8) = \{\pm i\}, jZ(Q_8) = \{\pm j\}, kZ(Q_8) = \{\pm k\}$. Therefore, $Q_8/Z(Q_8)$ is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Notice that $i^2 = -1$, so that $(iZ(Q_8))^2 = (-1)Z(Q_8) = Z(Q_8)$. This means that $Q_8/Z(Q_8)$ has an element of order 2, so $Q_8/Z(Q_8) \ncong \mathbb{Z}_4$. Therefore, $Q_8/Z(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

**Theorem 10.1** *Let $H$ be a subgroup of $G$ with index 2. Then $H \trianglelefteq G$ (actually, $H \triangleleft G$).*

***Proof*** $eH$ is a left coset in $G/H$. Note that for any $x \in H$ we have $xH = Hx$. Consider any $x \notin H$. Then $G = eH \cup xH$. But $G = He \cup Hx = eH \cup Hx$ also. Therefore, $xH = Hx$ for any $x \notin H$. Thus, $xH = Hx$ for all $x \in G$. □

Note: It is not guaranteed that every group $G$ has a subgroup $H$ such that $[G : H] = 2$. All the theorem says is that *if* there exists an $H \leq G$ such that $[G : H] = 2$ then $H \trianglelefteq G$. For example, if $G = \mathbb{Z}_3$ then the only subgroups are $\{e\}$ or $\mathbb{Z}_3$, neither of which have index 2.

*Example 10.7* Let $G = D_n$. Let $H = \langle r \rangle$. Then $G/H = \{eH, sH\}$. Note that $sH \cdot sH = s^2H = eH$ so $G/H$ is a cyclic group of order 2. In other words, $G/H = D_n/\langle r \rangle \cong \mathbb{Z}_2$. Indeed, $\langle r \rangle \trianglelefteq D_n$ for any $n \geq 3$. This is because

$$(r^b)r^a(r^{-b}) = r^a \in \langle r \rangle \tag{10.19}$$

$$(r^b s)r^a(r^b s)^{-1} = (r^b s)r^a sr^{-b} = r^b r^{-a} s^2 r^{-b} = r^{-a} \in \langle r \rangle \tag{10.20}$$

for any $a, b \in \mathbb{Z}$.

*Example 10.8* We collect below some normal subgroups of groups with index 2.

i) $A_n \trianglelefteq S_n$ since $|A_n| = |S_n|/2 \Rightarrow [S_n : A_n] = 2$.
ii) $\langle r \rangle \trianglelefteq D_n$ since $[D_n : \langle r \rangle] = 2$.
iii) $SO_n \trianglelefteq O_n$ since $O_n = SO_n \cup C \cdot SO_n$ where $C \in O_n$ with $\det C = -1$ and, hence, $[O_n : SO_n] = 2$.

There is a generalization of the above theorem.

**Theorem 10.2** *Let $G$ be a finite group and let $p$ be the smallest prime divisor of $|G|$. If $H \leq G$ such that $[G : H] = p$, then $H \trianglelefteq G$.*

***Proof*** Problem 13.9 asks the reader to provide the proof. □

Thus, we see that Theorem 10.1 is a special case of Theorem 10.2 when the smallest prime divisor $p$ of $|G|$ happens to be 2. Let's use this to prove what we already proved in Proposition 7.6: $A_4$ has no subgroup of order 6.

**Proposition 10.7** *$A_4$ has no subgroup of order 6.*

***Proof*** Suppose that $H \leq A_4$ is a subgroup with order 6, $|H| = 6$. Then $[A_4 : H] = 2$, so that $H \triangleleft A_4$. Thus, the quotient group $A_4/H$ is isomorphic to $\mathbb{Z}_2$. Therefore, $\alpha^2 H = (\alpha H)^2 = eH$. By Theorem 7.1, this means that $\alpha^2 \in H$ for any $\alpha \in A_4$. However, working out $\alpha^2$ for every $\alpha \in A_4$ leads to 9 distinct elements, all of which must belong to $H$, a subgroup assumed to be of order 6. Therefore, $A_4$ has no subgroup of order 6.

To see that we get 9 distinct elements in this process, you can explicitly calculate $\alpha^2$ for every $\alpha \in A_4$. A slicker way is to note that $A_4$ consists of the identity, $(\frac{4\cdot 3}{2!}\frac{2\cdot 1}{2!})\frac{1}{2!} = 3$ elements with cycle structure $(\bullet\bullet)(\bullet\bullet)$, and $\frac{4\cdot 3\cdot 2}{3} = 8$ elements with cycle structure structure $(\bullet \bullet \bullet)$. Note that $\alpha^2 = e$ for the identity element and for the three terms that have cycle structure $(\bullet\bullet)(\bullet\bullet)$. Each of the elements with cycle structure $(\bullet \bullet \bullet)$ square to another element with cycle structure $(\bullet \bullet \bullet)$. Thus, $\alpha^2$ with $\alpha$ running through the eight 3-cycles just gives back the eight 3-cycles. Thus, we have $8 + 1 = 9$ distinct results when calculating $\alpha^2$ for $\alpha \in A_4$. □

**Theorem 10.3** *Let $G$ be a group. Let $H \leq G$, $K \trianglelefteq G$. Then $HK \leq G$.*

***Proof*** $HK \leq G$. Note that $HK$ is nonempty since $e \in H$ and $e \in K$, so $e \in HK$. Let $x_1, x_2 \in HK$. Then $x_1 = h_1k_1$ and $x_2 = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$x_1x_2^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = (h_1h_2^{-1})(h_2k_1k_2^{-1}h_2^{-1}) \in HK. \quad (10.21)$$

The last part follows because $H$ is a subgroup so $h_1h_2^{-1} \in H$, $K$ is a subgroup so $k_1k_2^{-1} \in K$ and so, since $K$ is a normal subgroup, $h_2k_1k_2^{-1}h_2^{-1} \in K$. By Theorem 1.1, $HK \leq G$. □

In Problem 10.6, you will show that $HK \leq G$ if $H \trianglelefteq G$ and $K \leq G$. Therefore, $HK \leq G$ as long as one of them is a normal subgroup of $G$. In the same problem, you will show that if $H \trianglelefteq K$ *and* $K \trianglelefteq G$ then $HK$ is not just a subgroup of $G$, but rather a normal subgroup $HK \trianglelefteq G$. If $H$ and $K$ are subgroups of $G$ but neither is a normal subgroup of $G$, then $HK$ is not necessarily a subgroup of $G$. See part a) of Problem 10.6.

## 10.3 Simple groups

**Definition 10.4** A (finite or infinite) group $G$ is called simple if $|G| > 1$ (that is, $G$ is not the trivial group $G = \{e\}$) and the only normal subgroups of $G$ are $G$ and $\{e\}$.

The reader is already aware of some groups that are simple.

**Proposition 10.8** *Let $G$ be a finite group such that $|G|$ is prime. Then $G$ is a simple group.*

***Proof*** By Lagrange's theorem, any group with $|G| = p$ for some prime number $p$ is cyclic (see Theorem 7.4). This means that if $|G|$ is prime then the only subgroups of $G$ are $\{e\}$ or $G$ so that, in particular, the only normal subgroups are $\{e\}$ and $G$. That is, $G$ is simple. □

The rest of the text won't make explicit mention of simple groups, but we mention the terminology and idea to make the reader aware of their existence. In the theory of groups, simple groups play an important role. Simple groups, by definition, cannot be "broken up" into smaller pieces like $\{e\} \neq N \triangleleft G$. Note that for simple groups $N \trianglelefteq G$ implies that $G/N$ is either isomorphic to the trivial group or to $G$. In some sense, simple groups in group theory are like prime numbers in the arithmetic of $\mathbb{Z}$. The analogy is made more precise by a "unique factorization theorem" for finite groups.

**Definition 10.5** Let $G$ be a group. A sequence of subgroups

$$\{e\} = N_0 < N_1 < \cdots < N_{k-1} < N_k = G$$

is called a composition series if $N_i \triangleleft N_{i+1}$ and $N_{i+1}/N_i$ is a simple group for $0 \le i \le k-1$. The quotient groups $N_{i+1}/N_i$ for $0 \le i \le k-1$ are called composition factors of $G$.

Remark: In the above, we do not assume $N_i \trianglelefteq G$ for all $i$. We only require that $N_i \trianglelefteq N_{i+1}$. See Problem 10.2, where you are asked to show that the property of being a normal subgroup is not transitive.

*Example 10.9* The following are composition series for the cyclic group $\mathbb{Z}_6$:

$$\{e\} \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_6, \tag{10.22}$$

$$\{e\} \triangleleft \mathbb{Z}_2 \triangleleft \mathbb{Z}_6. \tag{10.23}$$

*Example 10.10* The following are composition series for $D_4$:

$$\{e\} \triangleleft \langle s\rangle \triangleleft \langle s, r^2\rangle \triangleleft D_4, \tag{10.24}$$

$$\{e\} \triangleleft \langle r^2\rangle \triangleleft \langle r\rangle \triangleleft D_4. \tag{10.25}$$

**Theorem 10.4** *(Jordan-Hölder) Let G be a finite group with $G \neq \{e\}$. Then*

- *$G$ has a composition series.*
- *The composition factors of the composition series are unique. More precisely, if*

  $$\{e\} = N_0 < N_1 < \cdots < N_a = G$$

  *and*

  $$\{e\} = M_0 < M_1 < \cdots < M_b = G$$

  *are composition series for $G$, then $a = b$ and there is some permutation $\sigma$ of $\{1, 2, \dots, a\}$ such that*

  $$M_{\sigma(i)}/M_{\sigma(i)-1} \cong N_i/N_{i-1}, \qquad 1 \le i \le a.$$

***Proof*** We will not explicitly use this theorem throughout the text, so we do not provide a proof. (Proof left to reader, if interested.) □

Before finishing our short discussion on simple groups, we prove that some more of the groups that the reader is familiar with are simple groups.

**Theorem 10.5** *The alternating group $A_n$ is simple for $n \ge 5$.*

***Proof*** There are many ways to prove this. We will use the fact that $A_n$ is generated by 3-cycles (see Theorem 3.15), and then show that a normal subgroup of $A_n$ must contain one 3-cycle and, hence, must contain all the 3-cycles, which would imply that the normal subgroup is $A_n$ itself. This is because all 3-cycles are conjugate in $A_n$ (see Proposition 9.2) so if $\alpha = (\bullet\ \bullet\ \bullet)$ is some 3-cycle is $N$, then letting $g$ run through all elements in $A_n$ means $g\alpha g^{-1} \in N$ (since $N$ is a normal subgroup), so all the 3-cycles are in $N$.

Let $N$ be a nontrivial normal subgroup of $A_n$. We must show that $N$ contains a 3-cycle. Problem 10.7 asks you to fill in this part.

Thus, we see that if $N \trianglelefteq A_n$ for $n \geq 5$ then $N$ is either $\{e\}$ or $A_n$. That is, $A_n$ is a simple group for $n \geq 5$. □

Note that $A_3$ is an abelian simple group while $A_4$ is not a simple group, since

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \triangleleft A_4. \tag{10.26}$$

$A_3$ has three elements, so it is simple (see, for example, Proposition 10.8). $A_2$ is isomorphic to $\mathbb{Z}_2$ and it is easy to see that it is normal.

## Problems

**10.1** Let $G$ be a group, and let $H$ and $J$ both be subgroups of $G$. Prove that $HJ$ is a subgroup of $G$ if and only if $HJ = JH$.

**10.2** Let $G$ be a group. Let $H \trianglelefteq G$ and let $J \trianglelefteq H$. Then $J \leq G$. Give an example where $J \ntrianglelefteq G$. This shows that the property of being a normal subgroup is not transitive.

**10.3** Let $G$ be a group. Let $H \trianglelefteq G$ and let $J \trianglelefteq G$. Suppose $H \cap J = \{e\}$. Show that $hj = jh$ for any $h \in H$ and $j \in J$.

**10.4** Suppose that $G$ contains a normal subgroup $N \trianglelefteq G$ such that $N \cong \mathbb{Z}_2$ and $G/N$ is cyclic of infinite order. Show that $G$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$.

**10.5** Suppose that $G$ contains a normal subgroup $N \trianglelefteq G$ which is cyclic, of infinite order, and $G/N$ is isomorphic to $\mathbb{Z}_2$. Show that $G$ is isomorphic to one of the following: $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}_2$, $D_\infty$.

**10.6** Let $H$ and $K$ be subgroups of $G$. Define $HK = \{hk \mid h \in H, k \in K\}$.

a) Give an example where $HK$ is not a subgroup.
b) If $H$ is a normal subgroup of $G$, prove that $HK$ is a subgroup of $G$.
c) If both $H$ and $K$ are normal in $G$, prove that $HK$ is normal in $G$.

**10.7** a) Find a proper normal subgroup of $A_4$.
b) Consider $A_5$. Work out the commutators

$$(1\ 2\ 3\ 4\ 5)^{-1}(3\ 4\ 5)^{-1}(1\ 2\ 3\ 4\ 5)(3\ 4\ 5),$$
$$(1\ 2)(3\ 4)(3\ 4\ 5)^{-1}(1\ 2)(3\ 4)(3\ 4\ 5).$$

c) Prove that the 3-cycles in $A_5$ form a single conjugacy class. That is, prove that the 3-cycles of $S_5$ do not split into separate conjugacy classes when viewed as elements of $A_5$. Actually, prove that the 3-cycles form a single conjugacy class in $A_n$ for $n \geq 5$.

d) Show that a nontrivial normal subgroup of $A_5$ must contain a 3-cycle. Therefore, the previous part implies that this nontrivial normal subgroup must contain all the 3-cycles. Use Theorem 3.15 to conclude that this subgroup must be all of $A_5$. This proves that $A_5$ is a simple group.

e) Fill in the steps to complete Theorem 10.5, proving that $A_n$ is a simple group for all $n \geq 5$.

# Chapter 11
# Group Actions, Orbits, and Stabilizers

**Abstract** Groups have a natural interpretation of acting on abstract objects. A concrete example is a group acting on an object in 3-D space.

## 11.1 Group Actions, Orbits, and Stabilizers

**Definition 11.1** Let $G$ be a group. Let $X$ be a set. An action of $G$ on $X$ is a homomorphism $\phi : G \longrightarrow S_X$, where $S_X$ is the symmetric group of $X$ (the group of bijective mappings $X \longrightarrow X$ with the binary operation of function composition). Some books write $\phi(g)(x)$, $\phi(g, x)$, or $g \cdot x$ for actions. We will write $\phi_g(x)$, at least for now.

Remark: Since $\phi$ is a dummy variable in our notation which refers to the action $\phi : G \longrightarrow S_X$, $g \cdot x$ is a convenient notation because it saves time and space by not requiring that one always say "let $\phi : G \longrightarrow S_X$ be an action of $G$ on $X$." However, sometimes this causes confusion when learning about group actions for the first time since $g \cdot x$ looks like $gx$ in multiplicative notation, even though that is not what the notation means unless the action is left translation. That is, for left translation $\phi_g(x) = gx$ so $g \cdot x = gx$. However, suppose the action is conjugation. Then $g \cdot x$ means $gxg^{-1}$ so writing $\phi_g(x) = gxg^{-1}$ instead of $g \cdot x = gxg^{-1}$ might cause less confusion for a beginner.

*Example 11.1* Let $X$ be the set of the points in a tetrahedron. Then $D_4$ acts on $X$ in an "obvious" way.

*Example 11.2* Any group $G$ acts on itself by left translation. Define $\phi : G \longrightarrow S_G$ by $\phi : g \mapsto L_g$, where $L_g \in S_G$ is defined by $L_g(x) = gx$ for all $x \in X$. This is what was done in proving Cayley's theorem. It is an action because

$$L_{gh}(x) = ghx = gL_h(x) = L_g \circ L_h(x) \tag{11.1}$$

for all $x \in X$ so $L_{gh} = L_g \circ L_h$. That is $\phi_{gh} = \phi_g \circ \phi_h$.

*Example 11.3* Every group $G$ acts on itself by conjugation. That is, define $\phi_g(x) = gxg^{-1}$ for all $x, g \in G$. It is an action because conjugation is bijective so $\phi_g \in S_G$ and

$$\begin{aligned} \phi_{gh}(x) = (gh)x(gh)^{-1} &= ghxh^{-1}g^{-1} \\ &= g\phi_h(x)g^{-1} = \phi_g \circ \phi_h(x). \end{aligned} \tag{11.2}$$

**Definition 11.2** Let $G$ act on a set $X$. Let $x \in X$. The orbit of x, denoted $\text{Orb}(x)$, is the set $\text{Orb}(x) = \{\phi_g(x) \mid g \in G\}$.

**Definition 11.3** Let $G$ act on a set $X$. Let $x \in X$. The stabilizer of x, denoted $\text{Stab}(x)$, is the set $\text{Stab}(x) = \{g \in G \mid \phi_g(x) = x\}$.

Note: $\text{Orb}(x)$ and $\text{Stab}(x)$ consist of different types of objects if $X \neq G$ (if $G$ is not acting on itself). $\text{Orb}(x)$ consists of (not necessarily all) elements which belong to the set $X$ (which could be points of some object in $\mathbb{R}^3$ or something like that) while $\text{Stab}(x)$ consists of (not necessarily all) elements which belong to the group $G$.

**Proposition 11.1** *Let $G$ act on a set $X$. Let $x \in X$. Then* $\text{Stab}(x)$ *is not just a subset of $G$, but* $\text{Stab}(x) \leq G$.

***Proof*** $\text{Stab}(x)$ is nonempty since $e \in \text{Stab}(x)$. Let $g, h \in \text{Stab}(x)$. Then

$$\phi_h(x) = x \tag{11.3}$$

$$\phi_h^{-1} \circ \phi_h(x) = \phi_h^{-1}(x) \tag{11.4}$$

$$\phi_{h^{-1}} \circ \phi_h(x) = \phi_{h^{-1}}(x) \tag{11.5}$$

$$\phi_e(x) = \phi_{h^{-1}}(x) \tag{11.6}$$

$$x = \phi_{h^{-1}}(x). \tag{11.7}$$

Thus, $h^{-1} \in \text{Stab}(x)$. Therefore,

$$\phi_{gh^{-1}}(x) = \phi_g \circ \phi_{h^{-1}}(x) = \phi_g(x) = x, \tag{11.8}$$

so $gh^{-1} \in \text{Stab}(x)$. By Theorem 1.1, $\text{Stab}(x) \leq G$. □

*Example 11.4* Consider $A_4$ acting on the tetrahedron. If $x$ is a vertex of the tetrahedron, then $\text{Orb}(x)$ = set of all vertices on the tetrahedron and $\text{Stab}(x) \cong$ a rotation group of order 3. A generic point $x$ of the tetrahedron (so not the vertices or middle of edges) has $|\text{Orb}(x)| = 12$ and $\text{Stab}(x) = \{e\}$.

*Example 11.5* In the action of $G$ on itself (so $X = G$) by left translation, there is only one orbit, namely $G$ itself. This is because for any $x \in G$ and any $y \in G$, there exists a $g$, namely $g = yx^{-1}$, such that $\phi_g(x) = (yx^{-1})x = y$. Also, $\text{Stab}(x) = \{e\}$ for $\forall x \in G$ since $\phi_g(x) = x$ means $gx = x \Rightarrow g = e$. ($G$ is a group so $x^{-1}$ exists for all $x \in G$.)

There is a special name for such actions.

**Definition 11.4** An action is transitive if it has only one orbit.

We have shown in Example 11.5 that the action of $G$ on itself by left translation is a transitive action.

*Example 11.6* Let $G$ act on itself by conjugation. Fix $g \in G$ and define

$$\phi_g(x) = gxg^{-1} \tag{11.9}$$

for any $x \in G$. Then

$$\operatorname{Orb}(x) = \{\phi_g(x) \mid g \in G\} = \{gxg^{-1} \mid g \in G\} = [x] \tag{11.10}$$

is the conjugacy class of $x$ in $G$. Also,

$$\operatorname{Stab}(x) = \{g \in G \mid \phi_g(x) = x\} = \{g \in G \mid gxg^{-1} = x\}. \tag{11.11}$$

We see that $\operatorname{Stab}(x)$ is the centralizer of $x$ in $G$.

**Theorem 11.1** *Elements in the same orbit have conjugate stabilizers. In particular, if $\phi_g(x) = y$ then $g\operatorname{Stab}(x)g^{-1} = \operatorname{Stab}(y)$.*

***Proof*** Let $G$ act on $X$. Let $x, y \in X$ be in the same orbit. This means there $\exists g \in G$ such that $\phi_g(x) = y$. Since $\phi$ is a homomorphism, we have $\phi_{g^{-1}}\phi_g(x) = \phi_{g^{-1}}(y) \Rightarrow \phi_{gg^{-1}}(x) = \phi_e(x) = x = \phi_{g^{-1}}(y)$. We want to show that $g\operatorname{Stab}(x)g^{-1} = \operatorname{Stab}(y)$.

- Step 1: We want to show $g\operatorname{Stab}(x)g^{-1} \subseteq \operatorname{Stab}(y)$. Pick any $h \in \operatorname{Stab}(x)$ and note that

$$\begin{aligned}
\phi_{ghg^{-1}}(y) &= \phi_{gh}\phi_{g^{-1}}(y) && \text{since } \phi \text{ is a homomorphism} \\
&= \phi_{gh}(x) \\
&= \phi_g\phi_h(x) && \text{since } \phi \text{ is a homomorphism} \\
&= \phi_g(x) && \text{since } h \in \operatorname{Stab}(x) \\
&= y.
\end{aligned} \tag{11.12}$$

  Thus, $ghg^{-1} \in \operatorname{Stab}(y)$. But $h \in \operatorname{Stab}(x)$ was arbitrary. Thus, $g\operatorname{Stab}(x)g^{-1} \subseteq \operatorname{Stab}(y)$.
- Step 2: We want to show $g\operatorname{Stab}(x)g^{-1} \supseteq \operatorname{Stab}(y)$. Pick any $h \in \operatorname{Stab}(y)$ and note that

$$\begin{aligned}
\phi_{g^{-1}hg}(x) &= \phi_{g^{-1}h}\phi_g(x) && \text{since } \phi \text{ is a homomorphism} \\
&= \phi_{g^{-1}h}(y) \\
&= \phi_{g^{-1}}\phi_h(y) && \text{since } \phi \text{ is a homomorphism} \\
&= \phi_{g^{-1}}(y) && \text{since } h \in \operatorname{Stab}(y) \\
&= x.
\end{aligned} \tag{11.13}$$

Thus, $g^{-1}hg \in \operatorname{Stab}(x)$. But $h \in \operatorname{Stab}(y)$ was arbitrary. Thus, $g^{-1}\operatorname{Stab}(y)g^{-1} \subseteq \operatorname{Stab}(x)$. This is the same as $\operatorname{Stab}(y) \subseteq g\operatorname{Stab}(x)g^{-1}$ (we can move $g$ over to the other side since conjugation is bijective). □

## 11.2 Orbit-Stabilizer Theorem

**Theorem 11.2** *Orbit-Stabilizer Theorem - Let $G$ act on $X$. Let $x \in X$. Then there exists a bijection $f$ from $G/\operatorname{Stab}(x) \to \operatorname{Orb}(x)$ given by $f : g\operatorname{Stab}(x) \mapsto \phi_g(x)$. (Note: Recall $G/\operatorname{Stab}(x)$ is always well-defined as a left coset space, but it is not necessarily a group since it is not always the case that $\operatorname{Stab}(x) \trianglelefteq G$.)*

***Proof*** There are a few things to check.

- $f$ is well-defined. By this we mean that it does not matter which representative $g$ of a coset we choose when mapping $g\operatorname{Stab}(x) \mapsto \phi_g(x)$. Any other coset representative $\tilde{g}$ of $g\operatorname{Stab}(x)$ is equal to $\tilde{g} = gh$ for some $h \in \operatorname{Stab}(x)$. But

$$f(\tilde{g}\operatorname{Stab}(x)) \mapsto \phi_{\tilde{g}}(x) = \phi_{gh}(x) = \phi_g\phi_h(x) = \phi_g(x) = f(g\operatorname{Stab}(x)). \tag{11.14}$$

- $f$ is injective. Suppose $f(g_1\operatorname{Stab}(x)) = f(g_2\operatorname{Stab}(x))$. Then $\phi_{g_1}(x) = \phi_{g_2}(x)$ so $\phi_{g_2^{-1}g_1}(x) = x$ and hence $g_2^{-1}g_1 \in \operatorname{Stab}(x)$. But then

$$g_2\operatorname{Stab}(x) = g_2(g_2^{-1}g_1)\operatorname{Stab}(x) = g_1\operatorname{Stab}(x), \tag{11.15}$$

where the first equality follows from $g_2^{-1}g_1 \in \operatorname{Stab}(x)$.
- $f$ is surjective. Let $y \in \operatorname{Orb}(x)$. Then there $\exists g \in G$ such that $\phi_g(x) = y$. Therefore, $f(g\operatorname{Stab}(x)) = \phi_g(x) = y$.

Thus, $f$ is indeed a bijection between $G/\operatorname{Stab}(x)$ and $\operatorname{Orb}(x)$. □

**Corollary 11.1** *If $G$ is finite, then for $\forall x \in X$, $|\operatorname{Stab}(x)| \cdot |\operatorname{Orb}(x)| = |G|$.*

***Proof***

$$\begin{aligned} |G/\operatorname{Stab}(x)| &= |G|/|\operatorname{Stab}(x)| && \text{by Lagrange's theorem} \\ &= |\operatorname{Orb}(x)| && \text{by Orbit-Stabilizer theorem.} \end{aligned} \tag{11.16}$$

□

With these theorems, we have enough machinery to prove some more theorems.

### 11.2.1 Cauchy's Theorem

**Theorem 11.3** *Cauchy's Theorem - Let $G$ be a finite group. Let $p$ be a prime number that divides $|G|$. Then $G$ contains an element of order $p$.*

***Proof*** Let $X$ be the set of all $p$-tuples $(g_1, \cdots, g_p)$ with $g_1, \cdots, g_p \in G$ such that $g_1 \cdots g_p = e$. The number of elements in $X$ is $|G|^{p-1}$. This is because $g_1, ..., g_{p-1}$ can be arbitrarily chosen from $G$ and then $g_p$ is fixed to be $(g_1 \cdots g_{p-1})^{-1}$. Let $H$ be the group $(\mathbb{Z}_p, +, 0)$. Let $H$ act on $X$ by $\phi((g_1, g_2, \cdots, g_{p-1}, g_p)) = (g_p, g_1, \cdots, g_{p-2}, g_{p-1})$. Every $(g_1, \cdots, g_p)$ has a stabilizer which is a subgroup of $H$ (*not* $G$! Do not confuse the dummy letter/variable labeling the group in Proposition 11.1. Stab$(x)$ is a subgroup of the group "doing the acting," which we called $H$ in this case not $G$). But $|H| = p$ so the stabilizer of any $(g_1, \cdots, g_p)$ in $X$ must be of cardinality 1 or $p$. By the Orbit-Stabilizer theorem, we know $|\operatorname{Orb}((g_1, \cdots, g_p))| \cdot |\operatorname{Stab}((g_1, \cdots, g_p))| = |H| = p$. Thus, the orbits must have size 1 or $p$. Now, recall that the orbits partition $X$. Thus, the orders of all of the orbits must give $|G|^{p-1}$. In particular, note that $|G|^{p-1} = 0 \pmod p$ since $p \mid |G|$ by assumption. Thus, the sum of the orders of all the orbits must also be $0 \pmod p$. But $(e, \cdots, e)$ is clearly in an orbit of its own. If all other orbits had order $p$ then we would get $|G| = 1 \pmod p$, a contradiction. Thus, there must at least another orbit, call it $\operatorname{Orb}((x_1, \cdots, x_p))$, disjoint from $\operatorname{Orb}((e, \cdots, e))$ such that $|\operatorname{Orb}((x_1, \cdots, x_p))| = 1$. Thus, $x_1 = \cdots = x_p$ with $x_1 \cdots x_p = e$, meaning $x_1^p = e$ where $x_1 \neq e$. □

**Definition 11.5** Let $p$ be a prime. A $p$-group is a group of order $p^k$ for some integer $k \geq 0$.

*Example 11.7* $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $D_4$, $Q_8$ are 2-groups.

**Theorem 11.4** *Any $p$-group has a nontrivial center. That is, $Z(G) \neq \{e\}$ if $G$ is a $p$-group.*

***Proof*** Let $G$ be a $p$-group with $|G| = p^k$ for some nonnegative integer $k$. Let $G$ act on itself by conjugation. The orbits are the conjugacy classes. For any $x \in G$, the centralizer is a subgroup of $G$ so, by Lagrange's theorem, has order $p^l$ for $0 \leq l \leq k$. Therefore, by the Orbit-Stabilizer theorem, the conjugacy class of $x$ has size $p^{k-l}$ which is $0 \pmod p$ if $k \neq l$ or $1 \pmod p$ if $k = l$. Since the conjugacy classes partition $G$, their orders must add up to $|G|$. But $|G| \equiv 0 \pmod p$ so the orders of the conjugacy classes must also add up to $0 \pmod p$. Note that $\{e\}$ is a conjugacy class and has order 1. If all other conjugacy classes had order not equal to 1, then we would get $|G| \equiv 1 \pmod p$, a contradiction. Thus, there exists at least one other conjugacy class $\{g\}$ with order 1 which is distinct from $\{e\}$. By Theorem 9.2, $g \in Z(G)$ so the center is nontrivial. □

**Theorem 11.5** *Let $p$ be a prime. Any group of order $p^2$ is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.*

***Proof*** Let $G$ be a group of order $p^2$. Then $Z(G) \neq \{e\}$. Pick $x \in Z(G)$ with $x \neq e$.

- **Case 1**: If $|x| = p^2$, then clearly $G = \langle x \rangle$ and $G \cong \mathbb{Z}_{p^2}$.
- **Case 2**: If $|x| = p$, then consider $\langle x \rangle$. Pick a $y \in G$ such that $y \notin \langle x \rangle$ (this also includes $y \neq e$ since $e \in \langle x \rangle$). Since $x \in Z(G), xy = yx$. Define $\phi : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow G$ by $(i, j) \mapsto x^i y^j$. This is an isomorphism. Thus, $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

*Example 11.8* Any group $G$ such that $|G| = 4 = 2^2$ is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

*Example 11.9* Any group $G$ such that $|G| = 9 = 3^2$ is isomorphic to either $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

We can now fill in our table a bit more. See Table 11.1.

Table 11.1: Classification of some groups, up to isomorphisms.

| **\|G\|** | **How many?** | **What are they?** |
|---|---|---|
| 1 | 1 | {e} |
| 2 | 1 | $\mathbb{Z}_2$ |
| 3 | 1 | $\mathbb{Z}_3$ |
| 4 | 2 | $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$ |
| 5 | 1 | $\mathbb{Z}_5$ |
| 6 | 2 | $\mathbb{Z}_6, D_3 \cong S_3$ |
| 7 | 1 | $\mathbb{Z}_7$ |
| 8 | later... | later... |
| 9 | 2 | $\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$ |
| 10 | 2 | $\mathbb{Z}_{10}, D_5$ |
| 11 | 1 | $\mathbb{Z}_{11}$ |
| 12 | later... | later... |
| 13 | 1 | $\mathbb{Z}_{13}$ |
| 14 | 2 | $\mathbb{Z}_{14}, D_7$ |
| 15 | 1 | $\mathbb{Z}_{15}$ |

Actually, we won't spend much time on what are called the Sylow Theorems. The Sylow Theorems are needed to classify groups of order 12, up to isomorphisms. Here is the answer, which we haven't proved: If $G$ is a group such that $|G| = 12$ then $G$ is isomorphic to one of the following: $\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2, D_6$, the dicyclic group of order 12, and $A_4$.

## 11.3 Ruminations

Let us step back for a second and appreciate what we have accomplished so far. We started with an abstract definition of what a group is, using inspiration/motivation from the symmetries of solid in $\mathbb{R}^3$. Eventually, we were able to show that the requirements that go into a group are strict enough that they put restrictions of what groups exist. In particular, our table above classifies *all* finite discrete groups up to order 15. Therefore, if you think you have a group with order less than or equal to 15 but it doesn't match one of our groups listed (up to isomorphisms) your first reaction should not be "Eureka! I found a new group!" but rather "Aw shucks, where did I make a mistake...". Also, this means that we only really have to work hard to prove a bunch of theorems about the groups listed in Table 11.1. If one finds a group of order 15 or less, then the properties of that group don't have to be rediscovered but can be read off from the theorems corresponding to the group to which it is isomorphic to.

## Problems

**11.1** Let $G$ be a finite group with exactly two conjugacy classes. Show that $G$ has order two.

**11.2** Let $\phi : G \longrightarrow S_X$ be the action of $G$ on a set $X$. Show that every point of some orbit has the same stabilizer if and only if this stabilizer is a normal subgroup of $G$.

**11.3** Discuss the structure of the orbits and the stabilizers in each of the following group actions on $\mathbb{R}^4$ :

a) The usual action of $GL_4(\mathbb{R})$.
b) Identify $\mathbb{R}^4$ with $\mathbb{R}^2 \times \mathbb{R}^2$ and take the product action of $SO_2 \times SO_2$.
c) Think of $\mathbb{R}^4$ as $\mathbb{C} \times \mathbb{C}$ and let $SU_2$ act in the usual way.
d) Identify $\mathbb{R}^4$ with $\mathbb{R}^3 \times \mathbb{R}$ and take the product action of $SO_3 \times \mathbb{Z}$, where $\mathbb{Z}$ acts on $\mathbb{R}$ by addition.

**11.4** Let $X = \{1, 2, 3, 4\}$ and let $G$ be the subgroup of $S_4$ generated by $(1\ 2\ 3\ 4)$ and $(2\ 4)$. Work out the oribts and stabilizers for the diagonal action of $G$ on $X \times X$.

**11.5** The rotational symmetry group of a cube is isomorphic to $S_4$. Consider the subgroup $A_4$ and act on the set of vertices of the cube. Find the orbit and stabilizer of each vertex.

**11.6** In this problem, include 1-cycles in a cycle shape. Let $\beta \in A_n$. Show that the conjugacy class of $\beta$ in $S_n$ splits into two conjugacy classes in $A_n$ if the lengths in the cycle shape of $\beta$ are *all odd* and are *distinct*. Show that, otherwise, the conjugacy class of $\beta$ is $S_n$ is a single conjugacy class in $A_n$. (Hints: Compare the centralizer of $\beta$ in $S_n$, denoted $C_{S_n}(\beta)$, with the centralizer of $\beta$ in $A_n$, denoted $C_{A_n}(\beta)$. Use Problem 3.10.)

**11.7** Let $G$ be a group of order $p^3$, where $p$ is a prime.

a) Show that the center of $G$ cannot have order 1 or order $p^2$.
b) Let $p$ be an arbitrary prime number. Give examples of groups of order $p^3$ whose centers have the two possible orders $p$ or $p^3$.

# Chapter 12
# Matrix Groups

**Abstract** In this chapter, we will cover the most common matrix groups that occur in a physics setting.

## 12.1 Orthogonal Matrices

**Definition 12.1** Let $V$ be a real vector space of dimension $n$. A bilinear form on $V$, denoted $\langle \mathbf{x}, \mathbf{y} \rangle$ for $\mathbf{x}, \mathbf{y} \in V$, is a function $V \times V \longrightarrow \mathbb{R}$ satisfying:

1. $\langle a\mathbf{x}_1 + b\mathbf{x}_2, \mathbf{y} \rangle = a\langle \mathbf{x}_1, \mathbf{y} \rangle + b\langle \mathbf{x}_2, \mathbf{y} \rangle$,
2. $\langle \mathbf{x}, a\mathbf{y}_1 + b\mathbf{y}_2 \rangle = a\langle \mathbf{x}, \mathbf{y}_1 \rangle + b\langle \mathbf{x}, \mathbf{y}_2 \rangle$,

for any $a, b \in \mathbb{R}$.

*Example 12.1* The standard dot product on $\mathbb{R}^n$ is

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{k=1}^{n} x_k y_k . \tag{12.1}$$

*Example 12.2* The Lorentzian product on $\mathbb{R}^4$ is $c^2 t_1 t_2 - x_1 x_2 - y_1 y_2 - z_1 z_2$.

*Example 12.3* The standard $(p, q)$ product is

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{k=1}^{p} x_k y_k - \sum_{k=p+1}^{p+q} x_k y_k . \tag{12.2}$$

**Definition 12.2** A matrix $B$ is symmetric if $B = B^T$.

**Definition 12.3** A matrix $B$ is skew-symmetric if $B = -B^T$.

Note that for any matrix $B$, we have

$$B = \underbrace{\frac{1}{2}(B + B^T)}_{\text{symmetric}} + \underbrace{\frac{1}{2}(B - B^T)}_{\text{skew-symmetric}}, \tag{12.3}$$

so that any matrix $B$ can be written as a sum of symmetric and skew-symmetric matrices.

**Definition 12.4** Let $\langle\ ,\ \rangle$ be a bilinear form. The group that preserves $\langle\ ,\ \rangle$ is

$$\{A \in GL_n(\mathbb{R}) \mid \langle A\mathbf{x}, A\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle \text{ for } \forall \mathbf{x}, \mathbf{y} \in V\}.$$

**Definition 12.5** If $\langle\ ,\ \rangle$ is the standard dot product, then the group preserving it is the orthogonal group, written $O_n(\mathbb{R})$.

Remark: Following the definitions, we can see that

$$O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid A^T A = I_{n\times n}\}. \tag{12.4}$$

Our convention is that vectors are $n$-by-1 matrices, rather that 1-by-$n$ matrices.

If $\mathbf{x}, \mathbf{y}$ are (column) vectors and we consider the standard dot product, then $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}^T \mathbf{y}$. Therefore, $\langle A\mathbf{x}, A\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$ is

$$(A\mathbf{x})^T (A\mathbf{y}) = \mathbf{x}^T \mathbf{y} \tag{12.5}$$

$$\Rightarrow \mathbf{x}^T A^T A\mathbf{y} = \mathbf{x}^T \mathbf{y} \tag{12.6}$$

for all $\mathbf{x}, \mathbf{y} \in V$. Thus, $A^T A = I_{n\times n}$, as claimed. This also gives $A^{-1} = A^T$.

Verify that the definition makes sense and the $O_n(\mathbb{R})$ is indeed a group.

**Definition 12.6** If $\langle\ ,\ \rangle$ is the $(p, q)$ form with $p + q = n$, then the group preserving it is written $O_{p,q}(\mathbb{R})$.

Note:

**Proposition 12.1** *If* $A \in O_n(\mathbb{R})$*, then* $\det A = \pm 1$.

***Proof*** This follows from

$$\det(A^T A) = \det I_{n\times n} \tag{12.7}$$

$$\det A^T \cdot \det A = \det I_{n\times n} \tag{12.8}$$

$$(\det A)^2 = 1. \tag{12.9}$$

□

**Definition 12.7** $SO_n(\mathbb{R})$, the special orthogonal group, is

$$SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det A = 1\}.$$

$SO_n(\mathbb{R})$ is a (normal) subgroup of $O_n(\mathbb{R})$ since det is a homomorphism.

**Corollary 12.1** *$O_n(\mathbb{R})$ is the union of two cosets $SO_n(\mathbb{R}) \cup C \cdot SO_n(\mathbb{R})$ where C is an orthogonal matrix with* $\det C = -1$.

**Proposition 12.2** $SO_2(\mathbb{R}) = \{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mid \theta \in \mathbb{R}\}$.

***Proof*** The requirement that $A \in SO_2(\mathbb{R})$ means that the columns of $A$ are orthogonal, that the columns (considered as vectors) have norm 1, and that the determinant be 1. Write

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \tag{12.10}$$

Then $A \in O_2(\mathbb{R})$ requires

$$a^2 + c^2 = 1 \tag{12.11}$$

$$b^2 + d^2 = 1 \tag{12.12}$$

$$ab + cd = 0. \tag{12.13}$$

Note that $a^2 + b^2 = 1$ with $a, b \in \mathbb{R}$ means that we can parametrize $a, c$ as $a = \cos\phi$ and $c = \sin\phi$ for some $\phi \in \mathbb{R}$. Once $a, c$ are written in this way, we see that the require $ab + cd = 0$ is satisfied for $b = \sin\phi$ and $d = -\cos\phi$ or $b = -\sin\phi$ and $d = \cos\phi$.

- If $b = \sin\phi$ and $d = -\cos\phi$ then

$$A = \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix}. \tag{12.14}$$

  Note that $\det A = -(\cos\phi)^2 - (\sin\phi)^2 = -1$. Matrices such as these do not belong to $SO_2(\mathbb{R})$.
- If $b = -\sin\phi$ and $d = \cos\phi$ then

$$A = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}. \tag{12.15}$$

  Note that $\det A = (\cos\phi)^2 + (\sin\phi)^2 = 1$. □

**Theorem 12.1** *Any element of $SO_3(\mathbb{R})$ is a rotation about some axis. Matrices such as these belong to $SO_2(\mathbb{R})$. (The $I_{3\times3}$ case is trivial, as it rotates by 0 around any axis.)*

***Proof*** Every orthogonal matrix (with all entries in $\mathbb{R}$) is diagonalizable over $\mathbb{C}$. This follows from the spectral theorem in linear algebra. To be the eigenvalues of $A \in SO_3(\mathbb{R})$, one needs to solve for $\lambda$ in the polynomial

$$\det(\lambda I_{3\times3} - A) = 0. \tag{12.16}$$

There are 3 solutions to such an equation, and they are the 3 eigenvalues of $A$. Actually, because $A \in SO_3(\mathbb{R})$ is means that all the coefficients of the characteristic polynomial are real. Recall that if a polynomial has coefficients which are purely real then if there exists a root $\lambda_k$ that has a nonzero imaginary component, then $\lambda_k^*$ (the complex conjugate of $\lambda_k$) is also a root (can you prove this?). We claim that in our case $+1$ is always a root.

- WLOG, suppose that $\lambda_1$ is real while $\lambda_2, \lambda_3$ are complex. Then $\lambda_2 = \lambda_3^*$. But then $\det A = 1$ means

$$\lambda_1 \lambda_2 \lambda_3 = 1 \tag{12.17}$$

$$\lambda_1 |\lambda_2|^2 = 1. \tag{12.18}$$

  However,

$$A\mathbf{v} = \lambda_1 \mathbf{v} \tag{12.19}$$

$$(A\mathbf{v})^T (A\mathbf{v}) = \mathbf{v}^T A^T A\mathbf{v} = \mathbf{v}^T \mathbf{v} \tag{12.20}$$

$$(\lambda_1 \mathbf{v})^T (\lambda_1 \mathbf{v}) = \lambda_1^2 \mathbf{v}^T \mathbf{v} \tag{12.21}$$

  so $\lambda_1^2 = 1$ (being an eigenvector means $\mathbf{v} \neq 0$, by definition, so we can cancel $\mathbf{v}^T \mathbf{v}$ on both sides of $\mathbf{v}^T \mathbf{v} = \lambda_1^2 \mathbf{v}^T \mathbf{v}$). Therefore, $\lambda_1 = \pm 1$. However, $|\lambda_2|^2 > 0$ ($\det A = 1$ means no eigenvalue can be 0) so $\lambda_1 |\lambda_2|^2 = 1$ implies $\lambda_1 = +1$.
- Suppose $\lambda_1, \lambda_2, \lambda_3$ are all real. Then $\det A = 1$ means

$$\lambda_1 \lambda_2 \lambda_3 = 1 \tag{12.22}$$

  which implies that one of the eigenvalues must be $+1$.

Thus, there is always at least one eigenvector, call it $\mathbf{v}$, with eigenvalue $+1$. Normalize the eigenvector $\mathbf{v} \mapsto \mathbf{v}/|\mathbf{v}|$ and choose an orthonormal basis for $\mathbb{R}^3$ where the eigenvector $\mathbf{v}/|\mathbf{v}|$ is the first basis vector. This means that there exists a basis in which $A \in SO_3(\mathbb{R})$ takes the form

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & b_{11} & b_{12} \\ 0 & b_{21} & b_{22} \end{bmatrix}. \tag{12.23}$$

Define

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}. \tag{12.24}$$

Then $\det A = 1$ means that $1 \cdot \det B = 1$ so $\det B = 1$. Since $A \in O_3(\mathbb{R})$, $A = A^T$ which means $b_{12} = b_{21}$. Therefore, $B = B^T$ and $\det B = 1$, so $B \in SO_2(\mathbb{R})$. Thus, we see that $A$ is a rotation around some axis (namely, the axis determined by the eigenvector $\mathbf{v}/|\mathbf{v}|$ passing through the origin). □

**Proposition 12.3** *If $n$ is odd, $O_n(\mathbb{R}) \cong SO_n(\mathbb{R}) \times \mathbb{Z}_2$.*

***Proof*** Already proved in Example 6.5. □

### 12.1.1 Special Relativity

This section is for those who are familiar with special relativity. In special relativity, the assumption about physical reality (which has been experimentally verified numerous times) is that the speed of light is the same in all reference frames. Intuitively, think of it as meaning that it doesn't matter whether you run toward or away from someone shining a flashlight at you. In any case, the observer (you, but could be any object) observes the light moving at the same speed regardless. One of the consequence of this is that the coordinates of an event in two reference frames are related by a linear transformation, different from what one expects based on classical physics. Label the coordinates in one reference without primes and the other with primes. Suppose that we align the coordinates of the reference frames so that the motion between the two frames is in the $x/x'$ direction. In special relativity, it is derived that $(t, x, y, z)$ and $(t', x', y', z')$ are related as follows:

$$t' = \gamma(t - vx/c^2) \tag{12.25}$$

$$x' = \gamma(x - vt) \tag{12.26}$$

$$y' = y \tag{12.27}$$

$$z' = z \tag{12.28}$$

where $\gamma = 1/\sqrt{1 - (v/c)^2}$. In matrix form, this is

$$\begin{bmatrix} t' \\ x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} \gamma & -\gamma v/c^2 & 0 & 0 \\ -\gamma v & \gamma & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} t \\ x \\ y \\ z \end{bmatrix}. \tag{12.29}$$

One thing to notice is that the quantity

$$(ct)^2 - x^2 - y^2 - z^2 = (ct')^2 - x'^2 - y'^2 - z'^2 \tag{12.30}$$

is independent of the reference frame (verify this!). Actually, in quantum field theory one gets tired of writing so many letters. What one does is write $x^\mu$ where one thinks of $x^\mu = (x^0, \mathbf{x})$ as a vector. Here $x^0$ is the time component and $\mathbf{x}$ are the spatial components. $\mathbf{x}$ has $D$ components, so in total there are $d = 1 + D$ dimensions. One might argue that maybe $D$ should be the total dimension and $d$ should be the spatial dimension, but for some reason most quantum field theory books use $D$ for the number of non-temportal dimensions and $d$ is the total dimension of the theory. Note that the physicists' way of referring to spatial component might differ from a mathematicians. If one has a $d$-dimensional space, the mathematician would say one has $d$ spatial dimensions. However, the physicist often means that the spatial components are the non-temporal parts of the $d$-dimensional space. In any case, quantum field theorists often follow the convention of setting $c = 1$. This then means

$$x'^0 = \gamma(x^0 - vx^1) \tag{12.31}$$

$$x'^1 = \gamma(x^1 - bx^0) \tag{12.32}$$

$$x'^2 = x^2 \tag{12.33}$$

$$\vdots = \vdots \tag{12.34}$$

where $\gamma = 1/\sqrt{1 - v^2}$. Next, note that

$$\begin{aligned} \gamma^2 - (\gamma v)^2 &= \frac{1}{1 - v^2} - \frac{v^2}{1 - v^2} \\ &= 1. \end{aligned} \tag{12.35}$$

This means that we can parametrize the $\gamma$ and $\gamma v$ expressions as $\cosh r$ and $\sinh r$ for some $r \in \mathbb{R}$, where $r$ is known as the rapidity. The transformation can then be written as

$$\begin{bmatrix} x'^0 \\ x'^1 \\ x'^2 \\ \vdots \end{bmatrix} = \begin{bmatrix} \cosh r & \sinh r & 0 \dots \\ \sinh r & \cosh r & 0 \dots \\ 0 & 0 & 1 \dots \\ \vdots & \vdots & \vdots \ddots \end{bmatrix} \begin{bmatrix} x^0 \\ x^1 \\ x^2 \\ \vdots \end{bmatrix}. \tag{12.36}$$

This can be written in a matrix-like notation as $x' = Lx$. All Lorentz transformations may be written this way by taking different matrices $L$. However, the matrices cannot be any $d$-by-$d$ matrices, as we shall see.

Any vector that transforms like $x \mapsto Lx$ is called a Lorentz $d$-vector. A feature of such Lorentz vectors is that the quantity $(x^0)^2 - \mathbf{x}^2$ does not change after the transformation. A quantity that doesn't change after a Lorentz transformation is known as a Lorentz scalar. Actually, define

$$\eta = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{12.37}$$

Then we note that

$$(x^0)^2 - \mathbf{x}^2 = x^T \eta x \tag{12.38}$$

where $x = (x^0, \mathbf{x})$. More generally, for any vectors $a$ and $b$ one has that a Lorentz transformation sends

$$\begin{aligned} a^T \eta b \mapsto a' \eta b' &= (La)^T \eta (Lb) \\ &= a^T L^T \eta L b. \end{aligned} \tag{12.39}$$

For this to be a Lorentz scalar for all Lorentz vectors $a$ and $b$, it must be true that $L^T \eta L = \eta$. Thus, the Lorentz transformations are determined by matrices $L$ that satisfy

$$L^T \eta L = \eta. \tag{12.40}$$

The Lorentz transformations comprise a group (check this!).

## 12.2 Unitary Matrices

**Definition 12.8** Let $V$ be a complex ($\mathbb{C}$) vector space of dimension $n$. A sesquilinear form on $V$, denoted $\langle \mathbf{x}, \mathbf{y} \rangle$ for $\mathbf{x}, \mathbf{y} \in V$, is a function $V \times V \to \mathbb{C}$ satisfying:

1. $\langle a\mathbf{x}_1 + b\mathbf{x}_2, \mathbf{y} \rangle = a^* \langle \mathbf{x}_1, \mathbf{y} \rangle + b^* \langle \mathbf{x}_2, \mathbf{y} \rangle$,
2. $\langle \mathbf{x}, a\mathbf{y}_1 + b\mathbf{y}_2 \rangle = a \langle \mathbf{x}, \mathbf{y}_1 \rangle + b \langle \mathbf{x}, \mathbf{y}_2 \rangle$,

for any $a, b \in \mathbb{C}$.

*Example 12.4* The standard dot product on $\mathbb{C}^n$ is

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{k=1}^{n} x_k^* y_k. \tag{12.41}$$

Comment: Mathematicians might be used to

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{k=1}^{n} x_k y_k^*. \tag{12.42}$$

The overwhelming majority of physics textbooks conjugate the left term rather than the right term. One can spend (waste) time arguing over which convention is better, but we won't. In physics, choosing to put the conjugation on the left makes things a bit cleaner since it moves all the operations to the left-hand side. For example, calculating the expectation value of the momentum operator in quantum mechanics becomes

$$\langle \hat{\mathbf{p}} \rangle = \int\int\int d^3x \, \psi^*(\mathbf{x}, t) \, (-i\hbar\nabla) \psi(\mathbf{x}, t) \,, \tag{12.43}$$

and the convention is such that the conjugation is on the left rather than on the operator in the middle or on the wave function on the right. In other math settings, maybe putting the conjugation on the right term makes some expressions appear "cleaner" by resulting in formulas that don't have a conjugation on terms. In the end, things like minus signs or conjugations usually don't go away in formulas and it's a matter of choosing in what definition or formula one wants the minus signs or conjugation terms to appear. The choices differ depending on the field of study.

**Definition 12.9** Let $\langle\, , \rangle$ be a sesquilinear form. The group that preserves $\langle\, , \rangle$ is

$$\{A \in GL_n(\mathbb{C}) \mid \langle A\mathbf{x}, A\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle \text{ for } \forall \mathbf{x}, \mathbf{y} \in V\}.$$

**Definition 12.10** If $\langle\, , \rangle$ is the standard inner product on $\mathbb{C}^n$ then the group preserving it is the unitary group, written $U_n(\mathbb{C})$.

Remark: Following the definitions, we can see that

$$U_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C}) \mid A^{*T}A = I_{n\times n}\}. \tag{12.44}$$

This means that $A^{-1} = A^{*T}$ for any unitary matrix $A$.

**Proposition 12.4** *If $A \in U_n(\mathbb{C})$, then* $|\det A| = 1$.

***Proof*** This follows from

$$\det(A^{*T}A) = \det I_{n\times n} \tag{12.45}$$

$$\det A^{*T} \cdot \det A = \det I_{n\times n} \tag{12.46}$$

$$|\det A|^2 = 1. \tag{12.47}$$

The complex modulus or a complex number is real and greater than or equal to 0. However, $|\det A|$ can't be 0 since $A$ must be invertible. Therefore, $|\det A| > 0$ so we conclude that $|\det A| = 1$. □

**Definition 12.11** $SU_n(\mathbb{C})$, the special unitary group, is

$$SU_n(\mathbb{C}) = \{A \in U_n(\mathbb{C}) \mid \det A = 1\}.$$

Verify that the definition makes sense and that $SU_n(\mathbb{C})$ is indeed a group.

## Problems

**12.1** a) Show that the elements of $U_2$ have the form $\begin{bmatrix} z & w \\ -e^{i\phi}w^* & e^{i\phi}z^* \end{bmatrix}$ where $w, z \in \mathbb{C}$, $\phi \in \mathbb{R}$, and $|w|^2 + |z|^2 = 1$.

b) Which of these matrices belong to $SU_2$?

**12.2** a) Prove that $SO_3(\mathbb{R})$ has a trivial center.

b) Prove that $SU_2$ has a nontrivial center. (Hint: Consider $\begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}$ for an appropriate $z$.)

c) Conclude $SO_3(\mathbb{R}) \ncong SU_2$. Why can we conclude this?

**12.3** Let $B$ be an $n \times n$ matrix with entries in $\mathbb{C}$. Define

$$e^B \equiv \sum_{k=0}^{\infty} \frac{B^k}{k!} = 1 + B + \frac{B^2}{2!} + \frac{B^3}{3!} + \cdots .$$

a) Prove that this series converges.
b) Prove that $\det(e^B) = e^{\mathrm{Tr}(B)}$.

# Chapter 13
# Isomorphism Theorems

**Abstract** In this chapter, we will cover important isomorphism theorems.

## 13.1 The Isomorphism Theorems

Before proceeding, it might be a good time to review Theorem 4.1.

**Proposition 13.1** *Let $\phi : G \to G'$ be a homomorphism.* $\ker\phi$ *is a normal subgroup of $G$.*

***Proof*** Note that $\phi(e) = e'$ so $\ker\phi$ is nonempty. Suppose $x, y \in \ker\phi$. Then

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = e'(e')^{-1} = e'. \tag{13.1}$$

Therefore, $xy^{-1} \in \ker\phi$. By Theorem 1.1, $\ker\phi$ is a subgroup of $G$. It is a normal subgroup because for any $x \in \ker\phi$ and any $g \in G$ we have

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)e'\phi(g)^{-1} = e', \tag{13.2}$$

so $gxg^{-1} \in \ker\phi$. Therefore, $g(\ker\phi)g^{-1} \subseteq \ker\phi$ for any $g \in G$. (Actually, since conjugation is bijective we have $g(\ker\phi)g^{-1} = \ker\phi$.) □

**Proposition 13.2** *Let $\phi : G \to G'$ be a homomorphism. $\phi$ is injective if and only if* $\ker\phi = \{e\}$.

***Proof*** ⇒ We proved $\phi(e) = e'$ for any homomorphism (see Theorem 4.1). If $\phi$ is injective then $\phi(x) \neq e'$ for any $x \in G$ with $x \neq e$. Therefore, $\ker\phi = \{e\}$.
⇐ Suppose $\ker\phi = \{e\}$. Let $x, y \in G$ and suppose $\phi(x) = \phi(y)$. Then

$$\phi(x)\phi(y)^{-1} = e' \tag{13.3}$$

$$\phi(x)\phi(y^{-1}) = e' \tag{13.4}$$

$$\phi(xy^{-1}) = e'. \tag{13.5}$$

Thus, $xy^{-1} \in \ker\phi$, so $xy^{-1} = e \Rightarrow x = y$. Therefore, $\phi$ is injective. □

**Definition 13.1** Let $N \trianglelefteq G$. The homomorphism $\pi : G \longrightarrow G/N$ defined by

$$\pi(g) = gN$$

is called the natural projection (homomorphism) of $G$ onto $G/N$.

**Theorem 13.1** *The Fundamental Theorem of Homomorphisms (or The First Isomorphism Theorem) - Let $\phi : G \longrightarrow G'$ be a homomorphism. Let $K = \ker\phi$. Then $G/K \cong \operatorname{im}\phi$. The isomorphism sends $xK \mapsto \phi(x)$.*

***Proof*** Let $\psi : G/\ker\phi \longrightarrow \operatorname{im}\phi$ be defined by $\psi(xK) = \phi(x)$. Then

- $\psi$ is well-defined, in the sense that this definition is independent of the coset representative used. Suppose $\tilde{x} \in xK$ and consider $\psi(\tilde{x})$. Then, since $\tilde{x} \in xK$, there exists a $k \in K$ such that $\tilde{x} = xk$. Therefore,

$$\psi(\tilde{x}K) = \phi(\tilde{x}) = \phi(xk) = \phi(x)\phi(k) = \phi(x)e' = \phi(x) = \psi(xK). \tag{13.6}$$

- $\psi$ is a homomorphism. Note that

$$\psi(xK)\psi(yK) = \phi(x)\phi(y) = \phi(xy) = \psi(xyK) = \psi(xKyK), \tag{13.7}$$

  where the last equality follows because $K = \ker\phi \trianglelefteq G$.
- $\psi$ is injective. $xK$ is in the kernel of $\psi$ if and only if $\phi(x) = e'$ if and only if $x \in \ker\phi$ if and only if $x \in K$. Therefore, $\ker\psi = eK$. In equations,

$$\begin{aligned} \ker\psi &= \{xK \mid \psi(xK) = e'\} \\ &= \{xK \mid \phi(x) = e'\} \\ &= \{xK \mid x \in \ker\phi \equiv K\} \\ &= eK. \end{aligned} \tag{13.8}$$

  By Proposition 13.2, $\psi$ is injective.
- $\psi$ is surjective by definition. Pick $y \in \operatorname{im}\phi$. Then there exists $x \in G$ such that $\phi(x) = y$. Therefore, $\psi(xK) = \phi(x) = y$.

Therefore, $\psi : G/\ker\phi \longrightarrow \operatorname{im}\phi$ is an explicit isomorphism demonstrating that $G/\ker\phi \cong \operatorname{im}\phi$, as claimed. □

**Corollary 13.1** *Let $\phi : G \longrightarrow G'$ is be a homomorphism. Then $|G : \ker\phi| = |\phi(G)|$.*

**Corollary 13.2** *If $\phi : G \longrightarrow G'$ is a surjective homomorphism then $G/\ker\phi \cong G'$.*

When first learning about the theorem (and the ones that follow later in this chapter), the following are common:

- Visible confusion at the start.

- After coming back at a later time and rereading the proof, the proof makes sense from an algebraic point of view. The manipulations of the symbols make sense. However, while the proof and theorem make sense from sentence to sentence the big idea is still a bit unclear.
- After a few more rereads, seeing a few examples, and working out some simple problems the theorem makes sense.

Before continuing with examples, maybe it's a good time to stop and try to make more sense of the theorem. Let's use pictures to try to visualize what is happening.

- Start with a homomorphism $\phi : G \to G'$. See Figure 13.1.

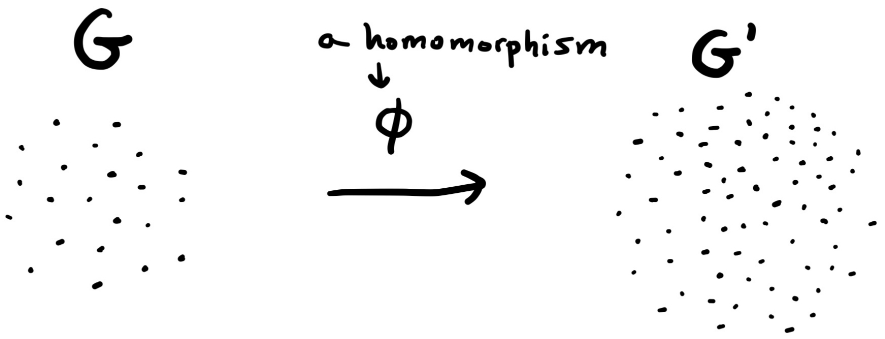


Fig. 13.1: A visualization of two groups $G, G'$ and a homomorphism $\phi : G \to G'$. It is not required that $\operatorname{im}\phi = G'$. This is demonstrated in the figure by using more dots to represent $G'$ than $G$.

- Next, note that $\ker\phi \trianglelefteq G$ (by Proposition 13.1). Let $r_1, r_2, \cdots, r_k$ be representatives of the left cosets of $\ker\phi$ in $G$. WLOG, let $r_1 = e$. What this means is that the distinct left cosets of $\ker\phi$ in $G$ are

$$e\ker\phi = r_1\ker\phi, r_2\ker\phi, \ldots, r_k\ker\phi. \tag{13.9}$$

  Again, recall that this means that they are pairwise disjoint and that their union gives $G$:

$$r_i\ker\phi \cap r_j\ker\phi = \emptyset, \qquad i \neq j \tag{13.10}$$
$$\cup_{i=1}^k r_i\ker\phi = G. \tag{13.11}$$

  Note that elements in the same left coset of $\ker\phi$ in $G$ get mapped to the same element in $G'$ (this is established in the line "$\psi$ is well-defined..." at the start of Theorem 13.1). See Figure 13.2. In the figure, we consider a case where $k = 5$ and $\phi$ is not surjective.
- Pictorially, it seems that if we ignore all the "left over" points in $G'$ (namely, the ones not in the image of $\phi$) then it looks like one can match (all) elements

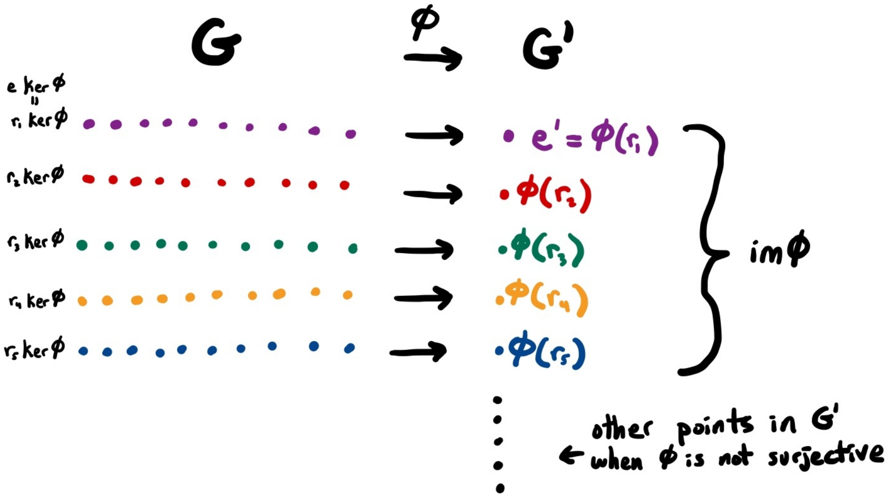


Fig. 13.2: Another visualization of two groups $G, G'$ and a homomorphism $\phi : G \to G'$, where now we use the fact that all elements in a given left coset of $\ker \phi$ in $G$ get mapped to the same element in $G'$. Note also that $\phi$ does not need to be surjective, hence the "left over" dots on the right.

in $G$ with (some) elements in $G'$. The elements of $G'$ that are in $\operatorname{im} \phi$ have the structure of a group ($\operatorname{im} \phi \leq G'$, by Theorem 4.1), and so it seems likely that this group structure is mimicked by the elements in $G$. Unless $\ker \phi = \{e\}$, then the mimicking is not done by individual elements in $G$ but rather by sets of elements in $G$ (namely the left cosets of $\ker \phi$ in $G$). The theorem formalizes all of this and states it in a precise way.

- Let's summarize. Define $\pi : G \to G/\ker \phi$ by $\pi(g) = g \ker \phi$. Define $\psi : G/\ker \phi \to \operatorname{im} \phi$ by $\psi(x \ker \phi) = \phi(x)$. Let $\phi : G \to G'$ be the given homomorphism. Then the First Isomorphism Theorem says that $\psi$ is an isomorphism and that $\phi = \psi \circ \pi$. That is, the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[dr, "\phi"'] & G/\ker \phi \arrow[d, "\psi"] \\
& \operatorname{im} \phi
\end{tikzcd}$$

  See Figure 13.3 for a visualization of this statement.

Hopefully this discussion and the figures have shed some light on what the theorem is about. Here are a few examples that use the First Isomorphism Theorem.

*Example 13.1* Consider $\det : GL_n(\mathbb{F}) \to \mathbb{F}^\times = \mathbb{F} - \{0\}$. det is a homomorphism. $\ker \det = SL_n(\mathbb{F}) = \{A \mid \det A = 1\}$. Thus, $SL_n(\mathbb{F}) \trianglelefteq GL_n(\mathbb{F})$ by Proposition 13.1. The image of det is all of $\mathbb{F}^\times$ since for any $c \in \mathbb{F}^\times$ the identity matrix with one diagonal element replaced with $c$ has a determinant $c$.

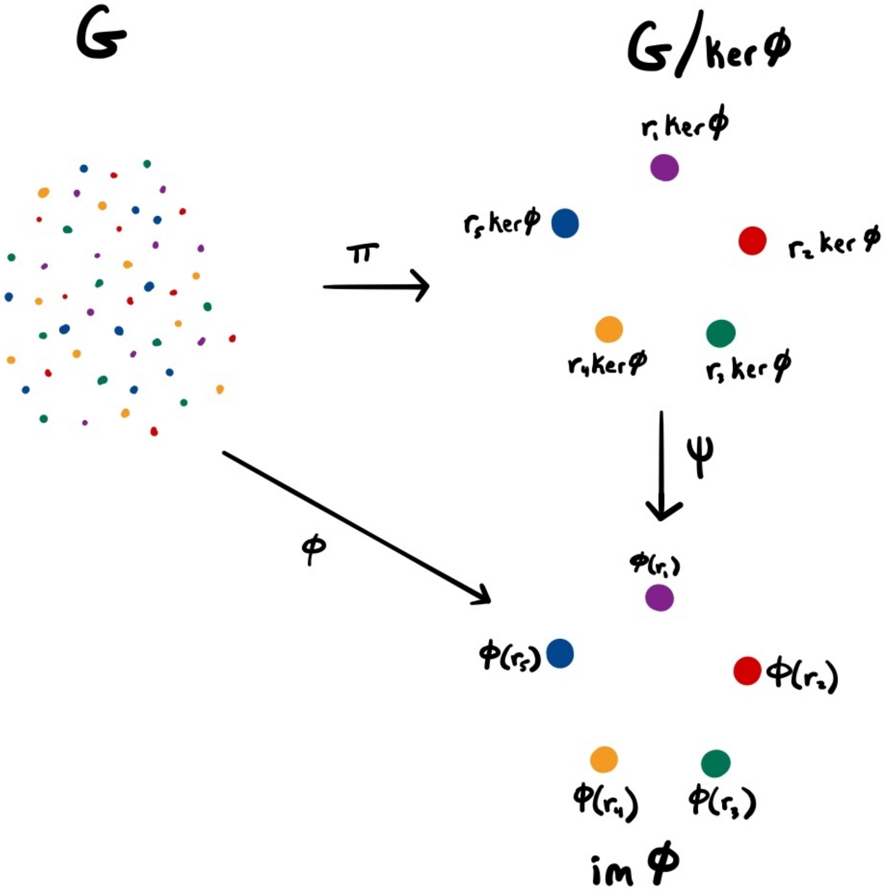


Fig. 13.3: Diagram showing the relationship between $G, \phi, \operatorname{im}\phi \subseteq G', G/\ker\phi, \psi$, $\pi$.

*Example 13.2* The determinant of unitary matrices is in $\mathbb{C}$ of modulus 1. Let $C$ be the set of all complex numbers of modulus one. Then $\det U_n$ maps into $C$. Actually, replacing one diagonal element of the identity matrix by $e^{i\theta}$ with $\theta \in \mathbb{R}$ shows that det maps $U_n$ *onto* $C$. Also, ker det in this case is $SU_n$. Theorem 13.1 and Corollary 13.2 imply

$$U_n/SU_n \cong C. \tag{13.12}$$

*Example 13.3* Let $G = (\mathbb{R}, +, 0)$ and $\phi : \mathbb{R} \to C$ defined by $\phi(t) = e^{2\pi i t}$. This is a homomorphism with $\ker\phi = \mathbb{Z}$. Therefore, $\mathbb{R}/\mathbb{Z} \cong C$.

*Example 13.4* Let $G = S_4$ and $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. (Actually, $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.) $V$ is a normal subgroup because it is a union of conjugacy classes of

$S_4$. That is,

$$V = \{e\} \cup \{(\bullet\bullet)(\bullet\bullet)\}. \tag{13.13}$$

$S_4/V$ must be a group of order $24/4 = 6$. There is no $g \in S_4$ with order 6, so there is no left coset $gV$ with order 6. Therefore, $S_4/V \ncong \mathbb{Z}_6$. Combining this observation with Theorem 8.2, we conclude that $S_4/V \cong D_3 \cong S_3$.

*Example 13.5* Let $G = S_3$ and let $\phi : S_3 \longrightarrow \{\pm 1\} \cong \mathbb{Z}_2$ be defined by $\phi(g) = \text{sgn}(g)$. Then $\phi$ is a homomorphism. Also, $\text{im}\,\phi = \mathbb{Z}_2$ since $S_3$ has even and odd permutations. Note that $\ker\phi = \{g \mid g \in S_3, \phi(g) = +1\} = A_3$. Therefore, $S_3/A_3 \cong \mathbb{Z}_2$. More generally, $S_n/A_n \cong \mathbb{Z}_2$ for any integer $n \geq 3$. That $S_n/A_n \cong \mathbb{Z}_2$ for $n \geq 3$ can also be arrived at by $A_n \trianglelefteq S_n$ (from $[S_n : A_n] = 2$ and Theorem 10.1) along with the fact that $\mathbb{Z}_2$ is the only group of order 2, up to an isomorphism.

**Theorem 13.2** *The Second Isomorphism Theorem (or The Diamond Isomorphism Theorem) - Let $G$ be a group. Let $H \leq G$, $J \trianglelefteq G$. Then $HJ \leq G$, $H \cap J \trianglelefteq H$, and $HJ/J \cong H/(H \cap J)$.*

***Proof*** $HJ \leq G$. Note that $HJ$ is nonempty since $e \in H$ and $e \in J$, so $e \in HJ$. Let $x_1, x_2 \in HJ$. Then $x_1 = h_1 j_1$ and $x_2 = h_2 j_2$ for some $h_1, h_2 \in H$ and $j_1, j_2 \in J$. Then

$$x_1 x_2^{-1} = (h_1 j_1)(h_2 j_2)^{-1} = h_1 j_1 j_2^{-1} h_2^{-1} = (h_1 h_2^{-1})(h_2 j_1 j_2^{-1} h_2^{-1}) \in HJ. \tag{13.14}$$

The last part follows because $H$ is a subgroup so $h_1 h_2^{-1} \in H$, $J$ is a subgroup so $j_1 j_2^{-1} \in J$ and so, since $J$ is a normal subgroup, $h_2 j_1 j_2^{-1} h_2^{-1} \in J$. By Theorem 1.1, $HJ \leq G$.

Now define the map $\phi : H \longrightarrow HJ/J$ by $\phi(x) = xJ$. We then have

- $\phi$ is a homomorphism since

$$\phi(xy) = xyJ = xJyJ = \phi(x)\phi(y) \tag{13.15}$$

  for any $x, y \in H$, where the second equals sign follows because $J \trianglelefteq G$.
- $\phi$ is surjective. Suppose $xJ \in HJ/J$. Then, since $x \in HJ$, there exist $h \in H$,$j \in J$ such that $x = hj$. Then

$$xJ = hjJ = hJ = \phi(h). \tag{13.16}$$

  Therefore, any element in $xJ \in HJ/J$ is the image of some $h \in H$.
- The kernel of $\phi$ consists of

$$\begin{aligned} \ker\phi &= \{h \in H \mid \phi(h) = eJ\} \\ &= \{h \in H \mid hJ = eJ\} \\ &= \{h \in H \mid h \in J\} \\ &= \{h \mid h \in H \text{ and } h \in J\} \\ &= H \cap J. \end{aligned} \tag{13.17}$$

Use Theorem 13.1 to conclude that

$$H/\ker\phi \cong \operatorname{im}\phi \Rightarrow H/(H \cap J) \cong HJ/J. \tag{13.18}$$

**Theorem 13.3** *Third Isomorphism Theorem - Let $H \leq J \leq G$ with $H \trianglelefteq G$, $J \trianglelefteq G$ (and hence also $H \trianglelefteq J$). Then $J/H \trianglelefteq G/H$ and $(G/H)/(J/H) \cong G/J$.*

***Proof*** Define a homomorphism $\phi : G/H \rightarrow G/J$ by $\phi(xH) = xJ$ for all $x \in G$. Then

- $\phi$ is well-defined since $H \leq J$. Suppose $x_1H = x_2H$. Then there exists an $h \in H$ such that $x_1 = x_2h$. But then

$$\phi(x_1H) = \phi(x_2hH) = x_2hJ = x_2J \tag{13.19}$$

  since $H \leq J$ so that $h \in H$ is also in $J$.
- $\phi$ is a homomorphism since $J \trianglelefteq G$ and $H \trianglelefteq G$ so

$$\phi(xH)\phi(yH) = xJyJ = xyJ = \phi(xyH) = \phi(xHyH) \tag{13.20}$$

  for any $x, y \in G$.
- $\phi$ is surjective ($\operatorname{im}\phi = G/J$) since $x \in G$ is arbitrary, so $\phi(xH) = xJ$ gives all cosets of $G/J$ as $x$ runs through all the elements $x \in G$.
- $\ker\phi = J/H$. This is because $xH \in \ker\phi$ if and only if $\phi(xH) = xJ = eJ$ if and only if $x \in J$. In equations,

$$\begin{aligned}\ker\phi &= \{xH \in G/H \mid \phi(xH) = eJ\} \\ &= \{xH \in G/H \mid xJ = eJ\} \\ &= \{xH \in G/H \mid x \in J\} \\ &= J/H.\end{aligned} \tag{13.21}$$

By Theorem 13.1, $(G/H)/\ker\phi \cong \operatorname{im}\phi$. That is, $(G/H)/(J/H) \cong G/J$. □

One way to remember the above theorem is to note that $(G/H)/(J/H) \cong G/J$ looks a bit like the cancellation one does when reducing fractions. For example, $(2/3)/(5/3) = \frac{2}{3}\frac{3}{5} = 2/5$. Warning: Don't take this too literally. It holds under the conditions mentioned in Theorem 13.3, but don't expect it to hold for all cosets.

## Problems

**13.1** Let $\alpha = (1\ 3\ 5\ 7\ 9)(2\ 4\ 6)(8\ 10) \in S_{10}$. Let $f : (\mathbb{Z}, +, 0) \rightarrow \langle\alpha\rangle$ be the homomorphism $m \mapsto \alpha^m$.

a) Find $N$ so that $\ker f = N\mathbb{Z}$.
b) Find all $m \in \mathbb{Z}_N$ such that $f(m)$ is a 5-cycle.

**13.2** Show that $G \times \{e\}$ is a normal subgroup of $G \times H$ and that the quotient group $(G \times H)/(G \times \{e\})$ is isomorphic to $H$.

**13.3** Let $G, H$ be groups. Let $A \trianglelefteq G$ and $B \trianglelefteq H$. Prove that $A \times B \trianglelefteq G \times H$ and that $(G \times H)/(A \times B) \cong (G/A) \times (H/B)$.

**13.4** (Example of the First Isomorphism Theorem)

a) Given numbers $a \in \mathbb{R} - \{0\}$, $b \in \mathbb{R}$ define a function $f(a, b)$ from $\mathbb{R}$ to $\mathbb{R}$ by $f(a, b) = ax + b$. Show that the collection of all such functions forms a group $G$, where the binary operation is function composition. If $H$ consists of those elements of $G$ for which $a = 1$, prove that $H \trianglelefteq G$ and that $G/H \cong \mathbb{R} - \{0\}$.
b) Define the affine general linear group $AGL_1(\mathbb{R})$ to be the subset of $GL_2(\mathbb{R})$ where the matrices have the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$. Show that $AGL_1(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$ and that the group of functions in the previous part is isomorphic to $AGL_1(\mathbb{R})$.

(Hint: $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix} = \begin{bmatrix} ax + b \\ 1 \end{bmatrix}$.)

**13.5** (Example of the Second Isomorphism Theorem) Let $G = S_4$. Let $J$ be the Klein 4-group. That is, let $J = \{e\} \cup \{(\bullet\bullet)(\bullet\bullet)\}$. Since $J$ is the union the $\{e\}$ and $\{(\bullet\bullet)(\bullet\bullet)\}$ conjugacy classes of $S_4$, we have $J \trianglelefteq S_4$ (see Proposition 10.4). Let $H = \langle (1\ 3)(2\ 4) \rangle$, another Klein 4-group.

a) Find $HJ$. To which familiar group is it isomorphic to? Why?
b) Find $H \cap J$. Describe explicitly the isomorphism

$$HJ/J \cong H/(H \cap J).$$

**13.6** Let $\phi : G \longrightarrow G'$ be a surjective homomorphism and let $K$ denote its kernel. If $H'$ is a subgroup of $G'$ define

$$\phi^{-1}(H') = \{g \in G \mid \phi(g) \in H'\}.$$

a) Verify that $\phi^{-1}(H')$ is a subgroup of $G$ which contains $K$.
b) Verify that the correspondence $H' \leftrightarrow \phi^{-1}(H')$ is a bijection between the collection of all subgroups of $G'$ and the collection of all those subgroups of $G$ which contain $K$.

**13.7** (Example of the Third Isomorphism Theorem and Problem 13.6) Let $G = S_4$. Let $J$ be the Klein 4-group. That is, let $J = \{e\} \cup \{(\bullet\bullet)(\bullet\bullet)\}$.

a) Show that there is an isomorphism $f : G/J \xrightarrow{\cong} S_3$.
b) Let $\mathcal{H}$ be the set of all the subgroups $H \leq G$ that satisfy $J \leq H \leq G$. Make a table with one row for each $H$. The row should have two entries: $H$, and $H/J$ expressed as a subgroup of $S_3$ via $f$. Show that the table gives a one-to-one correspondence between $\mathcal{H}$ and all the subgroups of $S_3$. (We say that the $H$'s are the *lifts mod* $J$ of the subgroups of $S_3$.)

c) In the cases where $H \trianglelefteq G$, describe explicitly the isomorphism

$$(G/J)/(H/J) \cong G/H$$

of the Third Isomorphism Theorem.

**13.8** Let $G$ be a group with $|G| = p^n m$, where $p$ is a prime and $m$ is relatively prime to $p$ (in other words, $\gcd(p, m) = 1$). Suppose $G$ has a normal subgroup $J$ of order $p^n$.

a) Give an example of such a $G$ and $J$, with $G$ non-abelian, $n > 1$, and $m > 1$.
b) If $H$ is a subgroup of $G$ of order $p^k$, show that $H \leq J$.

**13.9** a) Show that if a finite group $G$ has a subgroup $H$ of index $n$, then there is a normal subgroup $N \trianglelefteq G$ with $N \trianglelefteq H$ and $[G : N]$ a divisor of $n!$. (Hint: Consider the action of $G$ on $G/H$ by left translations.)
b) Let $p$ be the smallest prime dividing the order of a finite group $G$. Show that any subgroup $H \leq G$ of index $p$ is normal.

This generalizes the theorem that any subgroup of index 2 is a normal subgroup. Note: A subgroup of index $p$ does not necessarily exist. For instance, $A_4$ has no subgroup of index 2. *If* a subgroup of index $p$ exists, then this problem is applicable.

# Chapter 14
# Counting Orbits

**Abstract** In this chapter, we introduce a powerful method for enumeration. In particular, we will see how objects with symmetry can be enumerated by using group theory.

## 14.1 Counting

Consider the following problem:

> How many different ways are there to color the vertices of a square using only two colors?

See Figure 14.1, where we show $2^4$ squares with colored vertices.

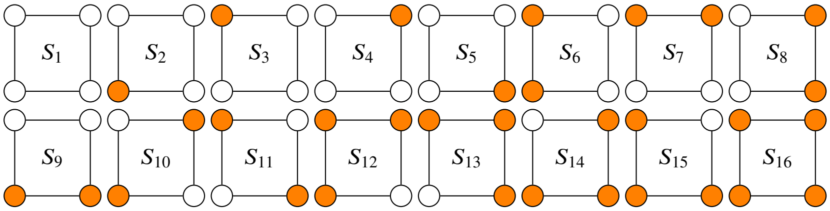


Fig. 14.1: Square vertices colored using two colors (white and orange, in this case).

The answer to our question seems to be that there are $2^4 = 16$ ways to color the vertices of a square using only two colors. However, to really make the question well-defined, we must agree on how to count the colorings. For example, suppose that the squares shown in Figure 14.1 appear as a design pattern on the top sides of tiles made by a company. These tiles will eventually make it to a kitchen floor where the home owner is a mathematician. The mathematician, who was a perspicacious student when taking a course on group theory in his or her undergraduate days, notices the following:

- tiles with the design pattern $S_1$ differ from all the other design patterns.
- tiles with the design patterns $S_2, S_3, S_4, S_5$ can all be rotated into one another.
- tiles with the design patterns $S_6, S_7, S_8, S_9$ can all be rotated into one another.
- tiles with the design patterns $S_{10}, S_{11}$ can all be rotated into one another.
- tiles with the design patterns $S_{12}, S_{13}, S_{14}, S_{15}$ can all be rotated into one another.
- tiles with the design pattern $S_{16}$ differ from all the other design patterns.

The mathematician comes to the conclusion that the company makes 6 distinct tiles, not $2^4 = 16$ distinct tiles. The mathematician's way of counting makes a bit more sense. A manufacturer would likely have a machine that can print one of six designs onto a tile during production, with the understanding that the person laying the tiles will rotate the tiles as wanted and needed.

In sum, we have found that while we initially had $2^4$ squares those $2^4$ squares partitioned into 6 orbits when acted on by the group of rotations of the square. When asking how many different ways one can color something, it makes sense to agree to count any designs as being the same coloring if they belong to the same orbit under the action of the relevant symmetry group.

Before continuing we note that we only considered rotations acting on the tiles. This is because the top of the tile usually has the design, and the bottom of the tile is placed on spread mortar. Essentially, the relevant group when counting tiles is the group of rotations of the tiles, and reflections are not relevant: the symmetry group is isomorphic to $\mathbb{Z}_4$, not $D_4$. Suppose that, instead one was counting a necklace with 4 equispaced beads, each of which can be colored choosing from two colors. In that case, the group would be $D_4$. However, even if reflections are allowed we notice that we are still left with "the same" design patterns as before. In the case of coloring a necklace with four beads using two colors, we conclude that there are 6 distinct designs as well. We alert the reader that this is normally not the case. One needs to be careful in reading a problem statement to know whether to allow reflections or not as this will usually change the number of colorings allowed.

The example we presented is simple enough that a brute force solution is doable. However, this method very quickly becomes tedious and untenable. A more sophisticated and systematic method is desirable. Symmetry groups and orbits seem related to enumeration. Is there a connection?

## 14.2 The Orbit-Counting Theorem

**Definition 14.1** Let a group $G$ act on a set $X$. Label the action by $\phi : G \longrightarrow S_X$. Let $g \in G$. The fixed-point set of $g$, denoted $\text{Fix}(g)$ or $X^g$, is the set

$$\text{Fix}(g) = \{x \in X \mid \phi_g(x) = x\}.$$

**Theorem 14.1** *The Orbit-Counting Theorem - Let G be a finite group acting on a finite set X. Let $N_{orb}$ be the number of orbits. Then*

$$N_{orb} = \frac{1}{|G|} \sum_{g\in G} |\operatorname{Fix}(g)| = \frac{1}{|G|} \sum_{x\in X} |\operatorname{Stab}(x)|.$$

Note: This is sometimes called Burnside's lemma.

***Proof*** Consider the set $F = \{(g,x) \in G \times X \mid \phi_g(x) = x\}$. Count the size of this set in two different ways.

- For a given $g \in G$, a pair $(g,x) \in F$ if and only if $x$ is fixed by $g$. Therefore,

$$|F| = \sum_{g\in G} |\operatorname{Fix}(g)|. \tag{14.1}$$

- For a given $x \in X$, a pair $(g,x) \in F$ if and only if $g$ is in $\operatorname{Stab}(x)$. Therefore,

$$|F| = \sum_{x\in X} |\operatorname{Stab}(x)|. \tag{14.2}$$

By the Orbit-Stabilizer theorem, $|G| = |\operatorname{Stab}(x)| \cdot |\operatorname{Orb}(x)|$. Therefore,

$$|F| = \sum_{x\in X} \frac{|G|}{|\operatorname{Orb}(x)|} = |G| \sum_{x\in X} \frac{1}{|\operatorname{Orb}(x)|} = |G| \sum_{\text{orbits}} 1 = |G| N_{orb}, \tag{14.3}$$

where we used the fact that elements in the same orbits have the same value of $|\operatorname{Orb}(x)|$ so that each distinct orbit contributes 1 in the sum $\sum_{x\in X} \frac{1}{|\operatorname{Orb}(x)|}$. Therefore,

$$N_{orb} = \frac{|F|}{|G|} = \frac{1}{|G|} \sum_{g\in G} |\operatorname{Fix}(g)| = \frac{1}{|G|} \sum_{g\in G} |\operatorname{Stab}(g)|. \tag{14.4}$$

□

**Theorem 14.2** *Let G be a group. If $g_1, g_2 \in G$ are conjugate then $|\operatorname{Fix}(g_1)| = |\operatorname{Fix}(g_2)|$.*

***Proof*** If $g_1, g_2 \in G$ are conjugate, that means there exists an element $g \in G$ such that $g_2 = g g_1 g^{-1}$. Let $x \in \operatorname{Fix}(g_1)$. Let us consider $\phi_g(x)$. Note that $\phi_g(x) \in \operatorname{Fix}(g_2)$ since

$$\phi_{g_2}(\phi_g(x)) = \phi_{g_2 g}(x) = \phi_{g g_1 g^{-1} g}(x) = \phi_{g g_1}(x) = \phi_g(\phi_{g_1}(x)) = \phi_g(x). \tag{14.5}$$

This shows that $|\operatorname{Fix}(g_1)| \le |\operatorname{Fix}(g_2)|$. A similar argument shows that $|\operatorname{Fix}(g_2)| \le |\operatorname{Fix}(g_1)|$. Therefore, $|\operatorname{Fix}(g_1)| = |\operatorname{Fix}(g_2)|$. □

Theorem 14.2 is useful because it means that to calculate $N_{orb}$ using the orbit-counting theorem, one only needs to calculate $|\operatorname{Fix}(g)|$ for one $g$ in each conjugacy class. This leads us to the following Corollary.

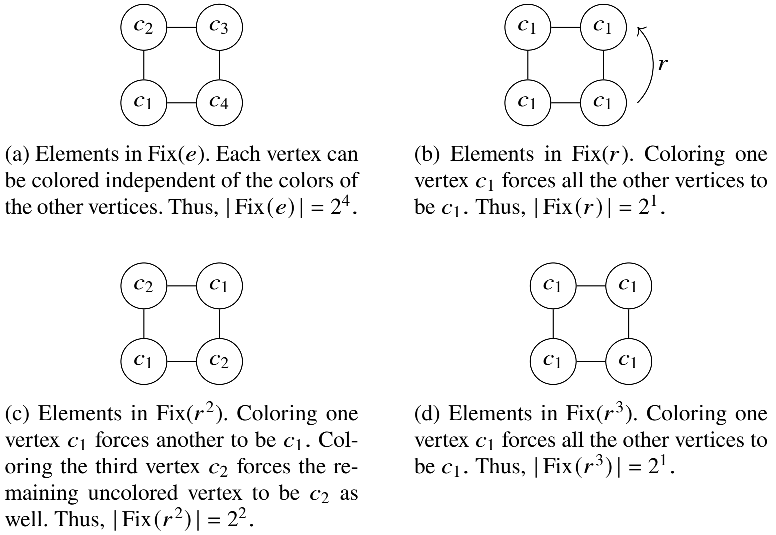
**Corollary 14.1** *Let $r_1, \cdots, r_k$ be representative elements of the conjugacy classes of a finite group $G$. Then*

$$N_{orb} = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)| = \frac{1}{|G|} \sum_{j=1}^{k} |[r_j]| \cdot |\operatorname{Fix}(r_j)|.$$

***Proof*** This follows directly from Theorem 14.1 and Theorem 14.2. □

### 14.2.1 Counting again

Let us redo the problem of counting the number of colorings of the vertices of a square using two colors. Let's first consider the case where only reflections are allowed. The group of rotations of the square is $\{e, r, r^2, r^3\}$ and, since this group is abelian, each element is in its own conjugacy class. We want to find the sizes of $\operatorname{Fix}(e), \operatorname{Fix}(r), \operatorname{Fix}(r^2)$, and $\operatorname{Fix}(r^3)$. See Figure 14.2 for the calculations. The work is summarized in Table 14.1.



(a) Elements in $\operatorname{Fix}(e)$. Each vertex can be colored independent of the colors of the other vertices. Thus, $|\operatorname{Fix}(e)| = 2^4$.

(b) Elements in $\operatorname{Fix}(r)$. Coloring one vertex $c_1$ forces all the other vertices to be $c_1$. Thus, $|\operatorname{Fix}(r)| = 2^1$.

(c) Elements in $\operatorname{Fix}(r^2)$. Coloring one vertex $c_1$ forces another to be $c_1$. Coloring the third vertex $c_2$ forces the remaining uncolored vertex to be $c_2$ as well. Thus, $|\operatorname{Fix}(r^2)| = 2^2$.

(d) Elements in $\operatorname{Fix}(r^3)$. Coloring one vertex $c_1$ forces all the other vertices to be $c_1$. Thus, $|\operatorname{Fix}(r^3)| = 2^1$.

Fig. 14.2: Sketch-work for finding $|\operatorname{Fix}(g)|$ for representative elements $g$ of the conjugacy classes when the symmetry group only includes rotations.

Table 14.1: Information needed for the orbit-counting theorem for a square when the symmetry group is rotations only.

| representative element $g$ | $\lvert [g] \rvert$ | $\lvert \mathrm{Fix}(g) \rvert$ |
|---|---|---|
| $e$ | 1 | $2^4$ |
| $r$ | 1 | $2^1$ |
| $r^2$ | 1 | $2^2$ |
| $r^3$ | 1 | $2^1$ |

The orbit-counting theorem (in the form given in Corollary 14.1) gives

$$\begin{aligned} N_{orb} &= \frac{1}{4}(1 \cdot 2^4 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^1) \\ &= 6. \end{aligned} \tag{14.6}$$

Now let's suppose that reflections are allowed, so the relevant group is $D_4$. The conjugacy classes are

$$\{e\}, \{r, r^3\}, \{r^2\}, \{s, r^2 s\}, \{rs, r^3 s\}. \tag{14.7}$$

See Figure 14.3 for the calculations. The work is summarized in Table 14.1.

Table 14.2: Summary of information needed for the orbit-counting theorem for a square when the symmetry group is rotations and reflections.

| representative element $g$ | $\lvert [g] \rvert$ | $\lvert \mathrm{Fix}(g) \rvert$ |
|---|---|---|
| $e$ | 1 | $2^4$ |
| $r$ | 2 | $2^1$ |
| $r^2$ | 1 | $2^2$ |
| $s$ | 2 | $2^2$ |
| $rs$ | 2 | $2^3$ |

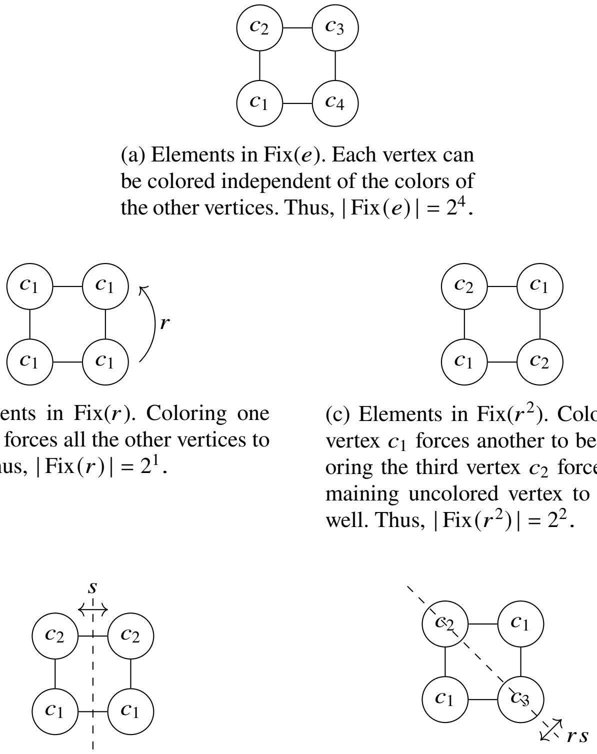
The orbit-counting theorem (in the form given in Corollary 14.1) gives

$$\begin{aligned} N_{orb} &= \frac{1}{8}(1 \cdot 2^4 + 2 \cdot 2^1 + 1 \cdot 2^2 + 2 \cdot 2^2 + 2 \cdot 2^3) \\ &= 6. \end{aligned} \tag{14.8}$$

Before continuing, let us generalize this problem a bit more and consider the following question:

How many different ways are there to color the vertices of a square using $k$ colors?

The beauty of the orbit-counting theorem is that the hard work has already been done to solve this more general question. Our work in Figures 14.2 and 14.3 is all



(a) Elements in Fix($e$). Each vertex can be colored independent of the colors of the other vertices. Thus, $|\operatorname{Fix}(e)| = 2^4$.

(b) Elements in Fix($r$). Coloring one vertex $c_1$ forces all the other vertices to be $c_1$. Thus, $|\operatorname{Fix}(r)| = 2^1$.

(c) Elements in Fix($r^2$). Coloring one vertex $c_1$ forces another to be $c_1$. Coloring the third vertex $c_2$ forces the remaining uncolored vertex to be $c_2$ as well. Thus, $|\operatorname{Fix}(r^2)| = 2^2$.

(d) Elements in Fix($s$). For the square to be fixed by $s$, only vertices on one side of the reflection line can be colored independently. Thus, $|\operatorname{Fix}(s)| = 2^2$.

(e) Elements in Fix($rs$). For the square to be fixed by $rs$, only three vertices can be colored independently. Thus, $|\operatorname{Fix}(rs)| = 2^3$.

Fig. 14.3: Sketch-work for finding $|\mathrm{Fix}(g)|$ for representative elements $g$ of the conjugacy classes when the symmetry group includes rotations and reflections.

that we need to use the orbit counting theorem. Instead of only having 2 colors to choose from, we modify our numbers for $|\operatorname{Fix}(g)|$ by replacing $2^{\text{some power}}$ with $k^{\text{that same power}}$ (convince yourself that this true). If we only consider rotations (by, for example, thinking of square patterns on a tile) then the number of distinct tiles using $k$ colors is equal to the number of orbits which, by the orbit-counting theorem, is

$$\begin{aligned} N_{orb}^{\mathbb{Z}_4} &= \frac{1}{4}(1 \cdot k^4 + 1 \cdot k^1 + 1 \cdot k^2 + 1 \cdot k^2) \\ &= \frac{1}{4}(k^4 + 2k^2 + k). \end{aligned} \tag{14.9}$$

If we consider rotations and reflections (by, for example, thinking of a necklace with four equispaced beads and each bead can be one of $k$ colors) then the number of distinct colors are

$$\begin{aligned}
N_{orb}^{D_4} &= \frac{1}{8}(1 \cdot k^4 + 2 \cdot k^1 + 1 \cdot k^2 + 2 \cdot k^2 + 2 \cdot k^3) \\
&= \frac{1}{8}(k^4 + 2k^3 + 3k^2 + 2k). \qquad (14.10)
\end{aligned}$$

Notice that the number of colorings differs if one considers only rotations ($\mathbb{Z}_4$) or considers rotations and reflections ($D_4$). This makes sense. The number of orbits definitely depends on the symmetry group. For a square and for $k = 2$, we saw that the situation was such that the two answers were the same. This, as we now see, is usually not the case.

## 14.3 Applications of the Orbit-Counting Theorem

Counting the number of colorings of necklaces is nice and all, but there are also more interesting applications of the orbit-counting theorem.

### 14.3.1 Chemistry

Consider a benzene molecule. See Figure 14.4.

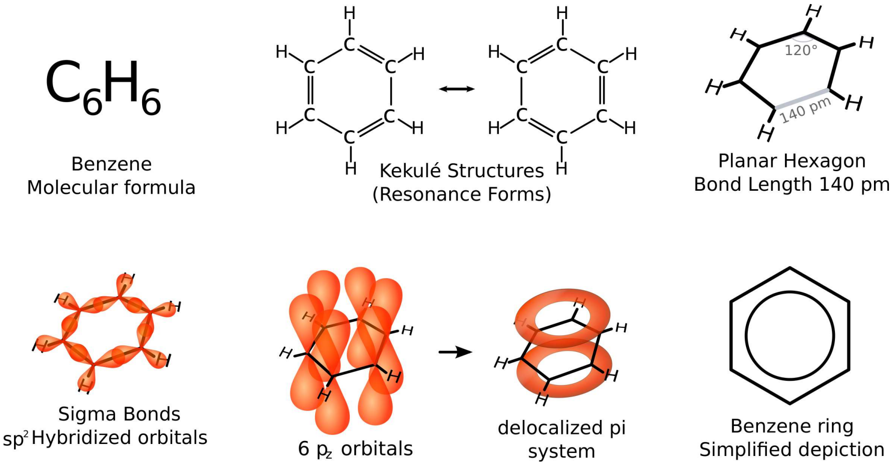
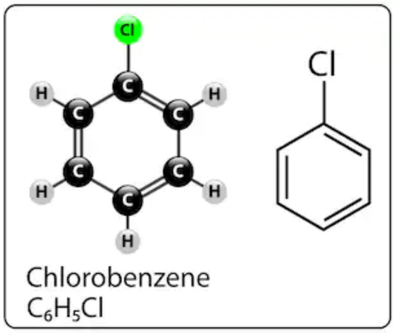


Fig. 14.4: A couple of different ways one can imagine benzene. (From the Wikipedia page on benzene.)

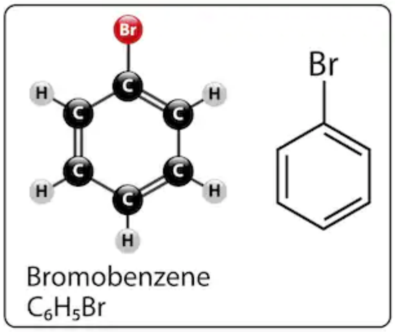
Consider removing a hydrogen atom bonded to a carbon atom and replace it, with say, a chlorine atom. This results in chlorobenzene. See Figure 14.5.



shutterstock.com • 1359286433

Fig. 14.5: One of the hydrogen atoms of benzene is replaced with chlorine. This is chlorobenzene.

Now suppose we also had bromine laying around. If one of benzene's hydrogen atoms were removed and replaced with bromine we would have Bromobenzene. See Figure 14.6.



shutterstock.com • 1358351288

Fig. 14.6: One of the hydrogen atoms of benzene is replaced with bromine. This is bromobenzene.

It should be clear that this problem maps to a problem where one has a necklace of evenly spaced beads and one can color the beads using $k$ colors. If only hydrogen and chlorine are allowed, this corresponds to having $k = 2$ colors to color the necklace. If one has hydrogen, chlorine, and bromide then $k = 3$. One could then work out the number of colorings of the necklace using the relevant $k$ for the number of allowed colors, and conclude that this is also the number of molecules one can get that are derived from benzene. Of course, this assumes that all such possibilities are chemically stable so this method can very well overestimate the number of such possible molecules in any real-world setting. In sum, we see that Burnside's lemma can be used alongside very simple chemistry models to put a bound on the number of derivatives of a given molecule.

## Problems

**14.1** Consider an equilateral triangle. Suppose that each edge is colored using a color from $k$ possible colors. How many colorings of the triangle are possible? Two colorings are considered the same if they map to each other using rotations and/or reflections.

**14.2** Each edge of a cube can be painted by one of $r$ colors.

a) How many different decorated cubes are possible?
b) How many different decorated cubes are possible if the cubes are colored red and blue (so $r = 2$)?

**14.3** Find the number of nonisomorphic graphs on six vertices. Here's how. The complete graph on $n$ vertices, denoted $K_n$, is the graph with $n$ vertices where every pair of vertices is joined by an edge. See Figure 14.7 for the graph $K_6$.

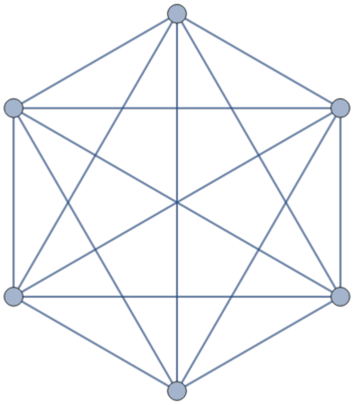


Fig. 14.7: $K_6$, a complete graph with 6 vertices.

To make an arbitrary graph $\Gamma$ on $n$ vertices, color the edges of $K_n$ with two colors: black (for present) and white (for absent). Let $\Gamma$ be the subgraph of $K_n$ where the edges are present. $S_n$ acts on $K_n$ by permuting the vertices and permuting the edges in the corresponding way. Two graphs are said to be isomorphic if and only if $S_n$ carries one to the other. For comparison, $K_4$, there are 11 nonisomorphic graphs on four vertices. 11 is small enough that we can list them. See Figure 14.8.

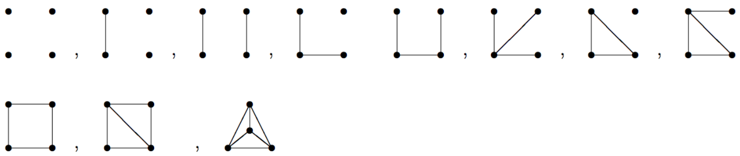


Fig. 14.8: Eleven nonisomorphic graphs with 4 vertices.

**14.4** Let $\phi : G \to S_X$ be an action of $G$ on a set $X$ of $n$ elements. In coloring problems with Burnside's lemma, there tend to be two parts: figuring out the fixed-point set of each $g \in G$, and figuring out how to color the fixed-point set. Pólya's theorem does the first part as one-time work, making it easier to solve the second part for different coloring schemes.
*Definition*: Suppose the disjoint cycle decomposition of $\phi_g$ has $j_1$ 1-cycles, $j_2$ 2-cycles, $\cdots$, and $j_n$ $n$-cycles. (Thus, $1j_1 + 2j_2 + \cdots nj_n = n$.) Call $(j_1, \cdots, j_n)$ the *cycle index* of $g$ for $\phi$.
*Definition*: Introduce $n$ indeterminates $x_1, \cdots, x_n$. The polynomial

$$Z(\phi) = \frac{1}{|G|} \sum_{g \in G} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

(where $(j_1, \cdots, j_n)$ is the cycle index of $g$) is the *cycle index polynomial* of $\phi$.

a) Let $S_4$ act on $\{1, 2, 3, 4\}$ as usual. Show that the cycle index polynomial is

$$\frac{1}{24}(x_1^6 + 6x_1^2 x_2 + 3x_2^2 + 8x_1 x_3 + 6x_4).$$

b) Let $S_4$ act on the six faces of the cube by rotating the cube as usual. Show that the cycle index polynomial is

$$\frac{1}{24}(x_1^6 + 3x_1^2 x_2^2 + 6x_1^2 x_4 + 6x_2^3 + 8x_3^2).$$

c) Let $S_4$ act on the twelve edges of the cube by rotating the cube as usual. Show that the cycle index polynomial is

$$\frac{1}{24}(x_1^{12} + 3x_2^6 + 8x_3^4 + 6x_1^2 x_2^5 + 6x_4^3).$$

d) Prove Pólya's theorem: If each of the $n$ elements of $X$ can be colored with $r$ different colors, then the number of inequivalent coloring for the action $\phi$ is

$$Z(\phi)(r, r, \cdots, r).$$

(In other words, substitute $x_1 = r, x_2 = r, \cdots, x_n = r$ into $Z(\phi)$.)

e) Use Pólya's theorem to solve Emily's problem for any number $r$ of colors.

f) Use Pólya’s theorem to solve Problem 14.2.

**14.5** Determine the number of different necklaces of 16 beads that can be made using 13 white beads and 3 black beads. Two necklaces are considered the same if one can be carried to the other by rotation or reflection. (Assume that necklaces are perfectly circular and the beads are evenly distributed on the circle.)

**14.6** Suppose students in Princeton Astrophysics invent a new card game, whose rules we don’t concern ourselves with. The cards of the game have 11 circles each, arranged with five-fold symmetry as in Figure 14.9.

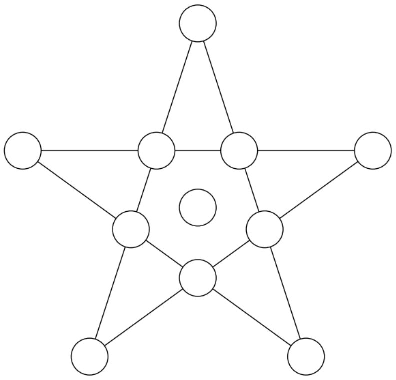


Fig. 14.9: Pattern on the cards for Problem 14.6.

On each card, 3 circles will be colored orange, and the remaining 8 will be colored black, in keeping with the color traditions of Princeton University. Two colorings are considered the same if and only if one can be carried to the other by a rotation or a reflection. How many different colorings are there?

**14.7** Repeat Problem 14.6 but suppose that now we have 10 circles where 3 circles will be colored orange, the remaining 7 will be colored black, and the pattern looks as in Figure 14.10. (For the record: this is the Petersen graph (rather, an isomorphic copy of it).)

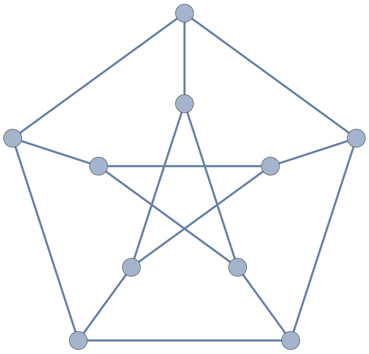


Fig. 14.10: Pattern on the cards for Problem 14.7.

# Chapter 15
# Pop Quiz on Part 1

**Abstract** In this chapter, we present a list of qualitative questions about the content of Part 1 in order to help readers test their understanding of (what we consider) the big takeaway ideas.

## 15.1 Important Questions on Part 1

- What is a group?
- What is a ring?
- What is a field?
- What does Cayley's theorem state? (Can you recall/sketch the main idea(s) of the proof?)
- What does Lagrange's theorem state? (Can you recall/sketch the main idea(s) of the proof?)
- What does Cauchy's theorem state? (Can you recall/sketch the main idea(s) of the proof?)
- What is a conjugacy class? Do you remember what the conjugacy classes of $D_n$ are? (Remember, you need to consider $n$ even and odd separately). What are the conjugacy classes of $Q_8$? What are the conjugacy classes of $S_n$? Are the conjugacy classes of $A_n$ the same as that of $S_n$?
- What is the orbit-counting theorem (often called Burnside's lemma)? (Can you recall/sketch the main idea(s) of the proof?)

If the reader is comfortable with these topics and is able to answer these questions, then Part 2 should be tackle-able.

# Part II
# Linear Representations of Finite Groups

Now that we have built up the necessary terminology and techniques, we can cover representation theory.

# Chapter 16
# Introduction to Representation Theory

**Abstract** A group $G$ can also act on vector spaces by linear maps. This is what linear representation theory is all about.

## 16.1 Linear Representations

**Definition 16.1** Let $V$ be a vector space over the field $\mathbb{C}$. $GL(V)$ is the group of all invertible linear maps $V \to V$. If $V$ has finite dimension $n$ and we fix a basis $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ in $V$, then linear maps represented with respect to this basis can be written as $n \times n$ matrices and $GL(V) \cong GL_n(\mathbb{C})$.

In what follows, we will restrict ourselves to cases where $V$ is finite dimensional and often to the case where $G$ is finite.

**Definition 16.2** Let $G$ be a group. A linear representation of $G$ on $V$ is a homomorphism $\rho : G \to GL(V)$. That is, $\rho_g$ is an invertible linear map from $V \to V$ such that $\rho_g \rho_h = \rho_{gh}$ for $\forall g, h \in G$. If $\dim V = n$, $\rho$ is said to be a representation on $n$-dimensions or of degree $n$.

Note: A quick comment about notation might be appropriate. Notice that $\rho : G \to GL(V)$ takes an element $g \in G$ as input and "spits out" some element in $GL(V)$. That element in $GL(V)$ can itself take in an input (a vector) and "spit out" another vector. Thus, we could write expressions like

$$\rho(g)(\mathbf{v}) = \mathbf{w} \tag{16.1}$$

where $g \in G$ and $\mathbf{v}, \mathbf{w} \in V$. It is understood that what this really means is $(\rho(g))(\mathbf{v})$. I've arbitrarily decided that I like writing $\rho_g(\mathbf{v})$ or $\rho_g \mathbf{v}$ more. Since we will often (mostly?) deal with finite groups, it is possible to think of $\rho_g$ as some $n$-by-$n$ matrix so that $\rho_g \mathbf{v}$ looks like a matrix multiplying a column vector.

Note: Some books, many of them physics books, define the dimension of the representation $\rho$ to be the dimension of the vector space $V$. They will then say things like "$\rho$ is an $n$-dimensional representation."

Note: Since $\rho$ is a homomorphism, we automatically know that $\rho_e = I_{n\times n}$ and that $\rho_{g^{-1}} = (\rho_g)^{-1}$ for $\forall g \in G$. (See Theorem 4.1.)

Note: $\rho$ is not required to be injective. If it is injective, $\rho$ is called a faithful representation.

So far, this might seem rather abstract. Since we will be dealing with cases where $\dim V = n < \infty$, let us think of $\rho_g$ for any $g \in G$ as an $n \times n$ matrix for concreteness. Therefore, a degree-$n$ representation of a group $G$ is just a way of associating to each $g \in G$ an $n \times n$ matrix, call it $\rho_g$, in such a way that the matrices behave somewhat similar to the elements of $G$ under the binary operation of the group. For any $g, h \in G$ we have:

$$\begin{array}{cl} g \;\cdot\; h \;= g \cdot h & (\cdot \text{ means the binary operation of } G) \\ \downarrow & \\ \rho_g \cdot \rho_h = \rho_{gh} & (\cdot \text{ means matrix multiplication}). \end{array} \tag{16.2}$$

That is, the matrix that we associate to $gh$, namely $\rho_{gh}$, is equal to the product of the matrices that we associate to $\rho_g$ and $\rho_h$ individually, namely $\rho_g\rho_h$. We say "the matrices behave somewhat similar..." because $\rho$ is a homomorphism and not necessarily an isomorphism. This means that $\rho_g$ can be equal to $\rho_h$ even when $g \neq h$.

*Example 16.1* Let $G = S_2 \cong \mathbb{Z}_2$. Let us define $\rho : G \to GL_2(\mathbb{C})$ by

$$\rho_e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \rho_{(1\ 2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{16.3}$$

This is clearly a representation of $S_2$, although a bit plain.

*Example 16.2* Let us construct a degree-3 representation $\rho : S_3 \to GL_3(\mathbb{C})$. Let $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ be a basis for $V$. Let $S_3$ act on these 3 basis vectors/objects in the "usual" way. That is, think of $(1\ 2) \in S_3$ as permuting objects 1 and 2 and $(1\ 2\ 3)$ as sending object 1 to object 2, object 2 to object 3, and object 3 to object 1. Let us construct matrices that "act" on the basis in the same way that $S_3$ acts on three objects. This then defines $\rho$ as follows:

$$\begin{gathered} \rho_e = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \rho_{(1\ 2)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \rho_{(1\ 3)} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \\ \rho_{(2\ 3)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \rho_{(1\ 2\ 3)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \rho_{(1\ 3\ 2)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \end{gathered} \tag{16.4}$$

so that, by construction, $\rho_{(1\ 2)}\mathbf{e}_1 = \mathbf{e}_2, \rho_{(1\ 3\ 2)}\mathbf{e}_2 = \mathbf{e}_1$, and so on. Evidently, (by construction, really) the matrices $\rho_g$ will act on the basis elements $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ in the same way that $g$ acts on the set $\{1, 2, 3\}$. We know that $(1\ 2\ 3)(1\ 2) = (1\ 3)$, so we had better have that $\rho_{(1\ 2\ 3)}\rho_{(1\ 2)} = \rho_{(1\ 3)}$. We leave it to the reader to verify that this is indeed the case.

It should be clear that this method can be generalized for any finite group.

**Definition 16.3** Let $G$ be a finite group. Let $G$ act on $X = G$ (that is, let $G$ act on itself) by left translation. Denote this action by $\phi : G \longrightarrow S_G$. Take a complex vector space $V$ with $\dim V = |G|$. Choose a basis of $V$ whose elements are in 1-to-1 correspondence with the elements of $G$: $\mathbf{e}_g$ for $\forall g \in G$. Define $\rho : G \longrightarrow GL(V)$ by $\rho_g(\mathbf{e}_h) = \mathbf{e}_{\phi_g(h)} = \mathbf{e}_{gh}$ for $\forall g, h \in G$. This gives $\rho_g \in GL(V)$ since it maps a basis into a basis (since left translation is bijective). This representation of $G$ is called the regular representation of $G$. This is a degree-$|G|$ representation of $G$.

It should also be clear that this can be generalized even further. ($G$ can now be an infinite group, though a lot of the theorems we prove in this chapter will be for finite groups so let's assume $G$ is still a finite group. The set $X$ must be finite, though, since $\dim V = |X|$ and we restrict ourselves to cases where $\dim V < \infty$.)

**Definition 16.4** Let $G$ be a finite group. Let $G$ act on a finite set $X$ with action $\phi : G \longrightarrow S_X$. Take a complex vector space $V$ with $\dim V = |X|$. Choose a basis of $V$ whose elements are in 1-to-1 correspondence with the elements of $X$: $\mathbf{e}_x$ for $\forall x \in X$. Define $\rho : G \longrightarrow GL(V)$ by $\rho_g(\mathbf{e}_x) = \mathbf{e}_{\phi_g(x)}$ for $\forall g \in G$ and $\forall x \in X$. This gives $\rho_g \in GL(V)$ since it maps a basis into a basis (since $\phi_g \in S_X$ is bijective). This representation of $G$ is called the permutation representation associated with $X$. This is a degree-$|X|$ representation of $G$.

Note: The regular representation is a special case of the permutation representation. The regular representation is the permutation representation where $G$, a finite group, acts on itself by left translation.

Actually, we worked harder in Examples 16.1 and 16.2 than we needed to when looking for a representation.

*Example 16.3* Let $G = S_2 \cong \mathbb{Z}_2$. Let us define $\rho : G \longrightarrow GL_1(\mathbb{C})$ by

$$\rho_e = [1] \text{ and } \rho_{(1\ 2)} = [1] \tag{16.5}$$

By $[1]$, we mean a $1 \times 1$ matrix whose entry is 1. Often people just write $\rho_e = 1$ and $\rho_{(1\ 2)} = 1$ without the $[\ ]$ where it is understood that $\rho_g$ is thought of as a matrix, not a scalar. This is allowed since $GL_1(\mathbb{C}) \cong \mathbb{C}^\times$. This is clearly a representation of $S_2$, although even plainer than Example 16.1.

**Definition 16.5** Let $G$ be a finite group and let $\dim V = 1$. Define $\rho : G \longrightarrow GL(V)$ by $\rho_g = \text{id}$ for $\forall g \in G$ (id is the identity map $\text{id} : V \longrightarrow V$). This is called the trivial representation or unit representation. If we think in terms of matrices, this is $\rho : G \longrightarrow GL_1(\mathbb{C})$ with $\rho_g = [1]$ for $\forall g \in G$, where $[1]$ is the $1 \times 1$ identity matrix.

*Example 16.4* Any degree-1 representation is a homomorphism $\rho : G \longrightarrow GL(V)$ where $V$ is a line (for example, $V \cong \mathbb{C}$ of dim 1, not 2). For $\forall g \in G$, $\rho_g$ acts on $V$ by multiplying by a scalar $c_g$ (the constant depends on the $g \in G$). Since $\rho_g$ is invertible (with inverse $\rho_g^{-1}$) we must have $c_g \neq 0$ for $\forall g \in G$. More concretely, let $G$ be a cyclic group of order $d$, with $G = \langle g \rangle$. Let $\rho$ be any degree-1 representation. Then $\rho_g \in GL_1(\mathbb{C})$. But

$$1 = \rho_e = \rho_{g^d} = (\rho_g)^d. \tag{16.6}$$

Therefore (thinking of $\rho_g \in GL_1(\mathbb{C})$ as a scalar), $\rho_g$ is a $d$-root of unity, so we have $\rho_g = e^{i\phi}$ for some $\phi \in \mathbb{R}$ with $e^{i\phi d} = 1$. The unique solutions are $\rho_g^{(k)} = e^{2\pi ik/d}$ with $k = 0, 1, \ldots, d-1$. Once $\rho_g^{(k)}$ is chosen, $\rho_{g^a}^{(k)}$ is fixed for all $a$ since $\rho_{g^a}^{(k)} = (\rho_g^{(k)})^a = e^{2\pi ika/d}$. When $k = 0$, we recover the trivial representation, so this leaves $d - 1$ nontrivial degree-1 representations.

## 16.2 Unitary Representations

**Definition 16.6** Let $V$ be a vector space with an inner product $\langle\ ,\ \rangle$. A representation $\rho : G \longrightarrow GL(V)$ is said to be a unitary representation if

$$\langle \rho_g \mathbf{v}, \rho_g \mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle$$

for any $g \in G$ and any $\mathbf{v}, \mathbf{w} \in V$.

Recall that if $V$ is a vector space over $\mathbb{C}$ a Hermitian inner product, label it $\langle \mathbf{v}, \mathbf{w} \rangle$, is a sesquilinear form on $V$. That is, it is linear in the first argument but conjugate linear in the second argument.

*Example 16.5* The standard Hermitian inner product on $\mathbb{C}^n$ is

$$[\mathbf{v}, \mathbf{w}] = \sum_{k=1}^{n} v_k \overline{w_k}. \tag{16.7}$$

**Theorem 16.1** *Weyl's Unitary Trick: Let G be a* finite *group. Let $\rho : G \longrightarrow GL(V)$ be a representation. There is a G-invariant Hermitian inner product on V; that is, there is an inner product* ( , ) *such that*

$$(\rho_g \mathbf{v}, \rho_g \mathbf{w}) = (\mathbf{v}, \mathbf{w})$$

*for* $\forall g \in G$ *and* $\forall \mathbf{v}, \mathbf{w} \in V$.

***Proof*** The trick is to use "averaging over $G$." Let $\langle \mathbf{v}, \mathbf{w} \rangle$ be any Hermitian inner product on $V$. Define

$$(\mathbf{v},\mathbf{w}) = \frac{1}{|G|}\sum_{g\in G}\langle \rho_g\mathbf{v}, \rho_g\mathbf{w}\rangle \tag{16.8}$$

for any $\mathbf{v},\mathbf{w}\in V$. (Do you see why we restrict ourselves to finite groups?) This is

i) Linear in $\mathbf{v}$.
ii) Conjugate linear in $\mathbf{w}$.
iii) Positive-definite.
iv) $G$-invariant.

This is because

i) $\rho_g$ is linear in $\mathbf{v}$ and $\langle\ ,\ \rangle$ is linear in the first argument.
ii) $\rho_g$ is linear in $\mathbf{w}$ and $\langle\ ,\ \rangle$ is conjugate linear in the second argument.
iii) Positive-definite since $(\mathbf{v},\mathbf{v}) = \frac{1}{|G|}\sum_{g\in G}\langle \rho_g\mathbf{v}, \rho_g\mathbf{v}\rangle$ is a sum of positive-definite terms (since $\langle\ ,\ \rangle$ is positive definite).
iv) $G$-invariant because see Problem 16.1 and apply it, for any $h\in G$, to

$$\begin{aligned}(\rho_h\mathbf{v},\rho_h\mathbf{w}) &= \frac{1}{|G|}\sum_{g\in G}\langle \rho_h\rho_g\mathbf{v}, \rho_h\rho_g\mathbf{w}\rangle \\ &= \frac{1}{|G|}\sum_{g\in G}\langle \rho_{hg}\mathbf{v}, \rho_{hg}\mathbf{w}\rangle \\ &= \frac{1}{|G|}\sum_{g\in G}\langle \rho_g\mathbf{v}, \rho_g\mathbf{w}\rangle \qquad \text{(by Problem 16.1)} \\ &= (\mathbf{v},\mathbf{w})\end{aligned} \tag{16.9}$$

for any $\mathbf{v},\mathbf{w}\in V$. □

What is "Weyl's Unitary Trick" for? Suppose that $\langle\ ,\ \rangle$ is the standard Hermitian inner product. Then

$$\begin{aligned}(\rho_h\mathbf{v},\rho_h\mathbf{w}) &= \frac{1}{|G|}\sum_{g\in G}\langle \rho_h\rho_g\mathbf{v}, \rho_h\rho_g\mathbf{w}\rangle \\ &= \frac{1}{|G|}\sum_{g\in G}(\rho_h\rho_g\mathbf{v})^T\overline{\rho_h\rho_g\mathbf{w}} \\ &= \frac{1}{|G|}\sum_{g\in G}\mathbf{v}^T\rho_g^T\rho_h^T\overline{\rho_h\rho_g\mathbf{w}} \\ &\overset{!}{=} (\mathbf{v},\mathbf{w}) \\ &= \frac{1}{|G|}\sum_{g\in G}\mathbf{v}^T\rho_g^T\overline{\rho_g\mathbf{w}}\end{aligned} \tag{16.10}$$

for $\forall h\in G$ and $\forall\mathbf{v},\mathbf{w}\in V$ means $\rho_h^T\overline{\rho_h} = I$ for $\forall h\in G$. This is the same as $\overline{\rho_h}^T\rho_h = I$ for $\forall h\in G$, which is indeed the equation for unitary matrices given in introductory courses in linear algebra (which implicitly often use the standard Hermitian inner product).

In short, we can always choose a $G$-invariant Hermitian inner product on $V$ and $\rho_g$ is a unitary matrix for any $g \in G$.

## 16.3 Linear Representations Have Character

**Definition 16.7** Let $A$ be an $n \times n$ matrix. The trace of $A$, denoted $\mathrm{Tr}(A)$, is the sum of the diagonal entries of $A$.

**Proposition 16.1** $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ *for any* $n \times n$ *matrices* $A, B$.

***Proof***

$$\begin{aligned}\mathrm{Tr}(AB) &= \sum_i (AB)_{ii} = \sum_i \sum_j A_{ij} B_{ji} \\ &= \sum_j \sum_i B_{ji} A_{ij} = \sum_j (BA)_{jj} \\ &= \mathrm{Tr}(BA).\end{aligned} \tag{16.11}$$

□

**Corollary 16.1** *Let* $S$ *be an* $n \times n$ *invertible matrix. Then* $\mathrm{Tr}(A) = \mathrm{Tr}(SAS^{-1})$.

***Proof*** $\mathrm{Tr}(SAS^{-1}) = \mathrm{Tr}(S(AS^{-1})) = \mathrm{Tr}((AS^{-1})S) = \mathrm{Tr}(A(S^{-1}S)) = \mathrm{Tr}(A)$. □

**Definition 16.8** Let $\rho : G \to GL(V)$ be a representation. The character $\chi$ of $\rho$ is defined as $\chi(g) = \mathrm{Tr}(\rho_g)$ for $\forall g \in G$.

**Proposition 16.2** *If* $\rho : G \to GL(V)$ *is a degree-n representation, then (bar indicates complex conjugation. Also,* $n = \dim V$ *holds by definition. It is written this way to emphasize the relationship between characters and the dimension of the vector space* $V$*.):*

*i)* $\chi(e) = n = \dim V$.
*ii)* $\chi(g^{-1}) = \overline{\chi(g)}$ *for* $\forall g \in G$.
*iii)* $\chi(hgh^{-1}) = \chi(g)$ *for* $\forall g, h \in G$.
*iv) If G is a finite group, then* $\chi(g)$ *is a sum of* $n = \dim V$ *terms which are each* $|g|^{th}$ *roots of unity for* $\forall g \in G$.
*v) If G is a finite group, then* $|\chi(g)| \leq n = \dim V$ *for* $\forall g \in G$*, with equality if and only if* $\rho_g = \lambda I_{n\times n}$ *for some* $\lambda \in \mathbb{C}$ *with* $|\lambda| = 1$.
*vi) If G is a finite group, then* $\chi(g) = \chi(e) = n = \dim V$ *if and only if* $\rho_g = \rho_e = I_{n\times n}$*. (That is, if and only if* $g \in \ker \rho$*.)*

***Proof*** i) $\rho_e = I_{n\times n} \Rightarrow \chi(e) = \mathrm{Tr}(\rho_e) = \mathrm{Tr}(I_{n\times n}) = n = \dim V$.

ii) Choose a $G$-invariant Hermitian inner product on $V$. Then $\rho_g$ is unitary for any $g \in G$. This means that $\rho_g^T \overline{\rho_g} = I$, which means that $\overline{\rho_g} = (\rho_g^T)^{-1} = ((\rho_g)^{-1})^T$.

$$\overline{\chi(g)} = \overline{\mathrm{Tr}(\rho_g)} = \mathrm{Tr}(\overline{\rho_g}) = \mathrm{Tr}((\rho_g^{-1})^T) = \mathrm{Tr}((\rho_g)^{-1}) = \mathrm{Tr}(\rho_{g^{-1}}) = \chi(g^{-1}). \tag{16.12}$$

iii) $\chi(hgh^{-1}) = \mathrm{Tr}(\rho_{hgh^{-1}}) = \mathrm{Tr}(\rho_h \rho_g \rho_{h^{-1}}) = \mathrm{Tr}(\rho_h \rho_g \rho_h^{-1}) = \mathrm{Tr}(\rho_g) = \chi(g)$ for $\forall g, h \in G$.

iv) Fix $g \in G$. Choose a $G$-invariant Hermitian inner product on $V$. Then $\rho_g$ is unitary, so there exists a basis where $\rho_g$ is diagonal. That is, $\rho_g = \mathrm{diag}[\lambda_1, \cdots, \lambda_n]$. Since $g^{|g|} = e$ (by definition of $|g|$), then

$$I_{n\times n} = \rho_e = \rho_g^{|g|} = (\rho_g)^{|g|} = \mathrm{diag}[\lambda_1^{|g|}, \cdots, \lambda_n^{|g|}]. \tag{16.13}$$

Thus, $\lambda_i$ for $i = 1, \cdots, n$ is a $|g|^{th}$ root of unity so

$$\chi(g) = \mathrm{Tr}(\rho_g) = \sum_{i=1}^{n} \lambda_i \tag{16.14}$$

is a sum of $n$ $|g|^{th}$ roots of unity.

v) This follows from the previous part along with repeated use of the triangle inequality:

$$|\chi(g)| = \left|\sum_{i=1}^{n} \lambda_i\right| \le \sum_{i=1}^{n} |\lambda_i| = n \tag{16.15}$$

since $|\lambda_i| = 1$ for $i = 1, \cdots, n$ since it is a root of unity. Equality holds if and only if all the lambdas are equal $\lambda_i = \lambda$ for $i = 1, \cdots, n$ for some $\lambda \in \mathbb{C}$ with $|\lambda| = 1$. In the case of equality, $\rho_g = \mathrm{diag}[\lambda, \cdots, \lambda] = \lambda I_{n\times n}$.

vi) $\Leftarrow$ If $\rho_g = I_{n\times n}$ then clearly $\chi(g) = n = \chi(e)$.
$\Rightarrow$ If $\chi(g) = \chi(e) = n$, then $|\chi(g)| = n$ so, by the work in the previous parts, $\rho_g = \lambda I_{n\times n}$ for some $\lambda \in \mathbb{C}$ with $|\lambda| = 1$. Then

$$\chi(g) = \mathrm{Tr}(\lambda I_{n\times n}) = \lambda n \overset{!}{=} n \tag{16.16}$$

implies $\lambda = 1$, so $\rho_g = I_{n\times n}$. □

Note: A (conjugacy) class function on a finite group $S$ is a function that takes a constant value on each element in a given conjugacy class. Thus, Proposition 16.2 says that the character $\chi$ of a representation $\rho : G \to GL(V)$ is a class function.

Why is $\chi$ called the character of a group? We will see later that the character $\chi$ characterizes the representation, in the sense that it allows us to distinguish between equivalent and nonequivalent (irreducible, to be defined later) representations. Indeed, we will see later that characters are an orthonormal basis for the space of class functions on $G$.

### 16.3.1 Character of the Regular Representation

Choose a basis of $V$ whose elements are in 1-to-1 correspondence with the elements of a finite group $G$: $\mathbf{e}_g$ for $\forall g \in G$. The regular representation is defined by $\rho_g(\mathbf{e}_h) = \mathbf{e}_{gh}$ for $\forall g, h \in G$. If $g \neq e$, then $\mathbf{e}_{gh} \neq \mathbf{e}_h$ (since $gh = h \Rightarrow g = e$). Therefore, all the diagonal entries of $\rho_g$ are 0 for $g \neq e$. If $g = e$, then $\rho_g = I_{n\times n}$, where $n = \dim V = |G|$ since $\rho_e \mathbf{e}_h = \mathbf{e}_{eh} = \mathbf{e}_h$ for any $h \in G$. Therefore, $\mathrm{Tr}(\rho_g) = 0$ if $g \neq e$ and $\mathrm{Tr}(\rho_g) = n = |G|$ for $g = e$. Let's collect this work into a proposition.

**Proposition 16.3** *Let $G$ be a finite group and let $\chi^{reg}$ be the character of the regular representation of $G$. Then*

$$\chi^{reg}(g) = \begin{cases} |G|, & \text{if } g = e, \\ 0, & \text{if } g \neq e. \end{cases}$$

## 16.4 Equivalent Representations

We want to be able to quantify how many representations a group has. One aspect of this is deciding how to count different representations. Again, let us think of our representations as matrices for concreteness. Let $\rho : G \longrightarrow GL_n(\mathbb{C})$ be a representation and $\rho' : G \longrightarrow GL_n(\mathbb{C})$ be a representation. Suppose there exists an invertible matrix $S$ such that $\rho'_g = S\rho_g S^{-1}$ for every $g \in G$. (Note: It is the same $S$ for every $g \in G$.) Recall from linear algebra that this means that $\rho'_g$ and $\rho_g$ are really the same linear maps just written in different bases, and the matrix $S$ relates the two bases. We agree to not really count $\rho'$ as a new representation. Why not, you may ask? Well, suppose that we worked really hard to find a degree-$n$ representation $\rho_g : G \longrightarrow GL_n(\mathbb{C})$ and then someone comes along, picks any invertible $n \times n$ matrix $S$, and defines $\rho' : G \longrightarrow GL_n(\mathbb{C})$ as $\rho'_g = S\rho_g S^{-1}$ for $\forall g \in G$. Then $\rho'_g$ is a representation as well since

$$\rho'_g \rho'_h = (S\rho_g S^{-1})(S\rho_h S^{-1}) = S\rho_g \rho_h S^{-1} = S\rho_{gh} S^{-1} = \rho'_{gh}. \tag{16.17}$$

This seems like a really cheap way to get a "new" representation from an existing one. Let's not count this as new.

How does one determine whether two given representations $\rho$ and $\rho'$ are equivalent? It seems tedious to look for an invertible matrix $S$ such that $\rho'_g = S\rho_g S^{-1}$ for $\forall g \in G$. For some intuition, suppose that there exists such an invertible matrix $S$. Then

$$\chi'(g) = \mathrm{Tr}(\rho'_g) = \mathrm{Tr}(S\rho_g S^{-1}) = \mathrm{Tr}(\rho_g) = \chi(g). \tag{16.18}$$

From this we conclude that if there $\exists x \in G$ such that $\chi'(x) \neq \chi(x)$ then the two representations $\rho'$ and $\rho$ are *not* equivalent. But what if $\chi'(x) = \chi(x)$ for $\forall x \in G$?

We will see later that their characters are the same if and only if they are "the same"/isomorphic/equivalent representations. Let's start to formalize these notions.

**Definition 16.9** A map of representations from $\rho$ to $\rho'$ (also called a $G$-linear map, or $G$-map, or intertwining operator) is a linear map $\tau : V \longrightarrow V'$ such that we have the commutative diagram

$$\begin{tikzcd}
V \arrow[r, "\rho_g"] \arrow[d, "\tau"'] & V \arrow[d, "\tau"] \\
V' \arrow[r, "\rho'_g"'] & V'
\end{tikzcd}$$

for any $g \in G$. That is, $\rho'_g \circ \tau = \tau \circ \rho_g$ for $\forall g \in G$. (Note: It is the same $\tau$ for every $g \in G$.)

**Proposition 16.4** *If $\tau$ from $\rho$ to $\rho'$ is a $G$-linear isomorphism then $\tau^{-1}$ is also a $G$-linear map.*

***Proof*** We want to show that for the linear map $\tau^{-1} : V' \longrightarrow V$ we have a commutative diagram

$$\begin{tikzcd}
V \arrow[r, "\rho_g"] & V \\
V' \arrow[r, "\rho'_g"'] \arrow[u, "\tau^{-1}"] & V' \arrow[u, "\tau^{-1}"']
\end{tikzcd}$$

for $\forall g \in G$. This commutative diagram holds since

$$\begin{aligned}
\rho'_g \circ \tau &= \tau \circ \rho_g \\
\tau^{-1} \circ \rho'_g \circ \tau \circ \tau^{-1} &= \tau^{-1} \circ \tau \circ \rho_g \circ \tau^{-1} \\
\tau^{-1} \circ \rho'_g &= \rho_g \circ \tau^{-1}.
\end{aligned} \tag{16.19}$$

□

**Corollary 16.2** *Isomorphism of representations is an equivalence relation. That is, the following commutative diagram holds:*

$$\begin{tikzcd}
V \arrow[r, "\rho_g"] \arrow[d, "\tau"'] & V \arrow[d, "\tau"] \\
V' \arrow[r, "\rho'_g"] \arrow[d, "\tau'"'] & V' \arrow[d, "\tau'"] \\
V'' \arrow[r, "\rho''_g"'] & V''
\end{tikzcd}$$

*for any $g \in G$.*

Loosely and informally speaking, the path taken doesn't matter for the "top" square and "bottom" square individually, so from this you can conclude that it doesn't matter what path one takes when the two squares are stacked together.

**Definition 16.10** Let $G$ be a finite group and let $V, V'$ be finite-dimensional vector spaces. Let $\rho : G \longrightarrow GL(V)$ and $\rho' : G \longrightarrow GL(V')$ be representations. We say that the representations $\rho$ and $\rho'$ are isomorphic or equivalent if there exists a $G$-linear map $\tau : V \longrightarrow V'$ which "transforms" $\rho$ to $\rho'$, in the sense of Definition 16.9, and where $\tau$ is also an isomorphism (a bijective function) $V \cong V'$. If there is no such $\tau$, we say that $\rho$ and $\rho'$ are nonisomorphic or inequivalent.

Important Clarifying Note: When we say "where $\tau$ is also an isomorphism $V \cong V'$" we mean in the sense of vector spaces $V \cong V'$ and not in the sense of groups where homomorphism in the group element argument is required (such as $\rho_g\rho_h = \rho_{gh}$). Isomorphism of two vector spaces means there exists a linear bijection between the spaces. The same word "isomorphism" is used but stipulates different constraints on the function. Do not let this confuse you. If you read that a function is an "isomorphism," ask yourself if the input to the function is an element of a group or an element of a vector space to figure out which version of isomorphism is meant.

Note: This more abstract definition in terms of $GL(V)$ and linear maps is just a formal definition of what we have already mentioned before. If we think in terms of matrices, then $\tau$ in this definition is the invertible matrix $S$ considered before.

**Proposition 16.5** *Let $\rho : G \longrightarrow GL(V)$ and $\rho' : G \longrightarrow GL(V')$ be isomorphic representations of the group $G$. Let $\chi$ be the character of $\rho$ and let $\chi'$ be the character of $\rho'$. Then $\chi = \chi'$. That is, $\chi(g) = \chi'(g)$ for any $g \in G$.*

***Proof*** Since $\rho$ and $\rho'$ are isomorphic, there exists a bijective $G$-linear map $\tau$ (consider it as a matrix) from $V$ to $V'$ such that $\rho'_g\tau = \tau\rho_g$ for every $g \in G$. This is the same as $\rho_g = \tau^{-1}\rho'_g\tau$ for every $g \in G$. Therefore,

$$\chi(g) = \mathrm{Tr}(\rho_g) = \mathrm{Tr}(\tau^{-1}\rho'_g\tau) = \mathrm{Tr}(\rho'_g) = \chi'(g) \tag{16.20}$$

for every $g \in G$. □

**Proposition 16.6** *The $d$ degree-1 representations in Example 16.4 are mutually nonisomorphic.*

***Proof*** Assume the contrary. Choose $m \neq n$ and assume there exists an isomorphic $G$-map $\tau : \mathbb{C} \longrightarrow \mathbb{C}$ (strictly speaking, $\tau : GL_1(\mathbb{C}) \longrightarrow GL_1(\mathbb{C})$). In one dimension, we can think of $\tau$ as acting by some scalar $c$ (strictly speaking, a $1 \times 1$ matrix). The commutative diagram says

$$ce^{2\pi im/d} = e^{2\pi in/d}c \Rightarrow e^{2\pi i(m-n)/d} = 1. \tag{16.21}$$

We may divide by $c$ since $\tau = 0$ satisfies the commutative diagram but that is not what we are seeking. We seek solutions with $c \neq 0$ since $\tau = 0$ is not invertible and hence not an isomorphic $G$-map. This then requires $m = n$ since $m, n$ are restricted to $\{0, 1, ..., d-1\}$. A contradiction. Thus, there is no $\tau$ an isomorphism that satisfies the commutative diagram so the $d$ degree-1 representations are mutually not similar. □

Thus, we have found $d$ (distinct) degree-1 representations for cyclic groups of order $d$. We will see later that these are the only irreducible (think for now "smallest distinct") representations of cyclic groups of order $d$.

## 16.5 Character Tables

Now seems as good of a time as any to introduce character tables. Consider the group $\mathbb{Z}_3 = \langle x \rangle$. By Proposition 16.6, we have three distinct degree-1 representations for $\mathbb{Z}_3$ given by (where $\omega = e^{2\pi i/3}$):

$$\begin{array}{lll} \rho_e^{(1)} = 1 & \rho_x^{(1)} = 1 & \rho_{x^2}^{(1)} = 1 \\ \rho_e^{(2)} = 1 & \rho_x^{(2)} = \omega & \rho_{x^2}^{(2)} = \omega^2 \\ \rho_e^{(3)} = 1 & \rho_x^{(3)} = \omega^2 & \rho_{x^2}^{(3)} = \omega. \end{array} \tag{16.22}$$

The characters for these are easy to calculate: the trace of a 1 × 1 matrix is the entry of that matrix! See Table 16.1.

Table 16.1: Character table of $\mathbb{Z}_3 = \langle x \rangle$.

| size | 1 | 1 | 1 |
|---|---|---|---|
| class | $e$ | $x$ | $x^2$ |
| $\chi^{(1)}$ | 1 | 1 | 1 |
| $\chi^{(2)}$ | 1 | $\omega$ | $\omega^2$ |
| $\chi^{(3)}$ | 1 | $\omega^2$ | $\omega$ |

At the very top row, we list the sizes of the (distinct) conjugacy classes. The second row gives a representative element in the (distinct) conjugacy classes. Then the rows for $\chi^{(k)}$ with $k = 1, 2, 3$ label the characters of the representations $\rho^{(k)}$ with $k = 1, 2, 3$, respectively. We only list the character of one element from each conjugacy class because Proposition 16.2 tells us that elements in the same conjugacy class have the same character. We often list the size of the conjugacy class in the first row because it will of use during calculations of inner products on characters (to be discussed later, in particular in Theorem 16.9). The examples and problems will have the reader work out character tables of a number of groups introduced in Part I.

## 16.6 Direct Sums

**Definition 16.11** Let $V$ be a vector space with $V \neq \{\mathbf{0}\}$. Let $W_1$ and $W_2$ be subspaces of $V$. We say that $V$ is a direct sum of $W_1$ and $W_2$ and write $V = W_1 \oplus W_2$ if every $\mathbf{v} \in V$ can be written uniquely as $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2$ with $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$.

**Proposition 16.7** *$V = W_1 \oplus W_2$ if and only if:*

*i) $W_1 \cap W_2 = \{\mathbf{0}\}$*
*ii) $W_1$ and $W_2$ span $V$.*

***Proof*** $\Leftarrow$ Suppose $W_1, W_2$ are subspaces of $V$ satisfies conditions i) and ii). Take any $\mathbf{v} \in V$. Since $W_1$ and $W_2$ span $V$, there exists some $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$ such that $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2$. Suppose $\mathbf{v}$ is also equal to $\mathbf{v} = \mathbf{w}_1' + \mathbf{w}_2'$. Then $\mathbf{w}_1 + \mathbf{w}_2 = \mathbf{w}_1' + \mathbf{w}_2'$, which means that $\mathbf{w}_1 - \mathbf{w}_1' = \mathbf{w}_2' - \mathbf{w}_2$. But $\mathbf{w}_1 - \mathbf{w}_1' \in W_1$ and $\mathbf{w}_2' - \mathbf{w}_2 \in W_2$, so by i) we conclude that $\mathbf{w}_1 - \mathbf{w}_1' = \mathbf{0}$ and $\mathbf{w}_2' - \mathbf{w}_2 = \mathbf{0}$. Therefore, the expression $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2$ with $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$ is unique.
$\Rightarrow$ Suppose $V = W_1 \oplus W_2$. Then every $\mathbf{v} \in V$ can be written uniquely as $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2$ with $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$. In particular, this means that $W_1$ and $W_2$ span $V$. The uniqueness requirement then means that $W_1 \cap W_2 = \{\mathbf{0}\}$. Why? Suppose that $\mathbf{u} \in W_1 \cap W_2$ with $\mathbf{u} \neq \mathbf{0}$. Then $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2 = (\mathbf{w}_1 + \mathbf{u}) + (\mathbf{w}_2 - \mathbf{u})$. However, $\mathbf{w}_1 \neq \mathbf{w}_1 + \mathbf{u}$ and $\mathbf{w}_2 \neq \mathbf{w}_2 - \mathbf{u}$. This contradicts that $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2$ with $\mathbf{w}_1 \in W_1$ and $\mathbf{w}_2 \in W_2$ is unique. □

**Definition 16.12** Let $\rho^{(1)} : G \to GL(V_1)$ be a linear representation of $G$ and let $\rho^{(2)} : G \to GL(V_2)$ be a linear representation of $G$. Define the representation $\rho^{(1)} \oplus \rho^{(2)} : G \to GL(V_1 \oplus V_2)$ by

$$(\rho^{(1)} \oplus \rho^{(2)})_g = \rho_g^{(1)} \oplus \rho_g^{(2)}$$

for any $g \in G$. By this, we mean

$$(\rho^{(1)} \oplus \rho^{(2)})_g(\mathbf{v}_1, \mathbf{v}_2) = (\rho_g^{(1)}\mathbf{v}_1, \rho_g^{(2)}\mathbf{v}_2) \in V_1 \oplus V_2$$

for any $(\mathbf{v}_1, \mathbf{v}_2) \in V_1 \oplus V_2$. We call this the direct sum of the representation $\rho^{(1)}$ and $\rho^{(2)}$.

What does the above definition look like in terms of matrices? Let $n_1 = \dim V_1$ and $n_2 = \dim V_2$. It means that there exists some ordered basis where the first $n_1$ basis vectors span the subspace $V_1$ and the next $n_2$ basis vectors span the subspace $V_2$ such that

$$\rho_g = \begin{array}{cc} \begin{array}{cc} V_1 & V_2 \end{array} & \\ \begin{bmatrix} \rho_g^{(1)} & \mathbf{0} \\ \mathbf{0} & \rho_g^{(2)} \end{bmatrix} & \begin{array}{c} V_1 \\ V_2 \end{array} \end{array} \tag{16.23}$$

in that basis. This is often written as $\rho_g = \rho_g^{(1)} \oplus \rho_g^{(2)}$ since the matrix $\rho_g$, in some suitably chosen basis, looks like the matrices $\rho_g^{(1)}$ and $\rho_g^{(2)}$ stacked together along the "diagonal." Formally, $\rho_g$ is a block diagonal matrix. Also, the $\mathbf{0}$ (the "big zero") in the matrix carries multiple meanings. In the upper right, $\mathbf{0}$ means that you have a $\dim V_1$ by $\dim V_2$ rectangular (square only if $\dim V_1 = \dim V_2$) block of zeros. In the lower left block, $\mathbf{0}$ means you have a $\dim V_2$ by $\dim V_1$ rectangular (square only if $\dim V_1 = \dim V_2$) block of zeros.

*Example 16.6* Define the representations $\rho^{(1)} : \mathbb{Z}_n \longrightarrow GL_1(\mathbb{C})$ as $\rho_m^{(1)} = e^{2\pi i m/n}$ and $\rho^{(2)} : Z_n \longrightarrow GL_1(\mathbb{C})$ as $\rho_m^{(2)} = e^{-2\pi i m/n}$. Then $\rho^{(1)} \oplus \rho^{(2)} : \mathbb{Z}_n \longrightarrow GL_2(\mathbb{C})$ is given by

$$(\rho^{(1)} \oplus \rho^{(2)})_m = \begin{bmatrix} e^{2\pi i m/n} & 0 \\ 0 & e^{-2\pi i m/n} \end{bmatrix}. \tag{16.24}$$

This gives a way of making "new" representations by "stacking" old ones together. This raises a question/idea. Here, we are given two representations and we stack them. Is the converse possible? That is, suppose we are given a representation. Can the given representation be written as a direct sum of some "smaller" representations? This leads to the ideas of reducible/irreducible and decomposable/indecomposable representations.

## 16.7 Indecomposable and Irreducible Representations

**Definition 16.13** Let $\rho : G \longrightarrow GL(V)$ be a representation. A subspace $W \subseteq V$ is called $G$-stable or G-invariant if $\rho_g W \subseteq W$ for $\forall g \in G$. That is, if $\mathbf{w} \in W$ then $\rho_g \mathbf{w} \in W$ for $\forall g \in G$. If $W$ is finite-dimensional then, since $\rho_g$ is invertible, being $G$-stable means $\rho_g W = W$ for $\forall g \in G$. If $W$ is $G$-stable, then $\rho_g$ carries $W$ into $W$ as a linear map. This defines a representation $\rho^W : G \longrightarrow GL(W)$ called the restriction of $\rho$ from $V$ to $W$. We say that $W$ is a subrepresentation of $V$.

*Example 16.7* Let $G = S_3$. Let $V = \mathbb{R}^3$. Let $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ be the standard basis of $\mathbb{R}^3$. Let $G$ act on the basis by permutation. This gives a permutation representation $\rho : G \longrightarrow GL_3(\mathbb{R})$. But the vector $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ and any scalar multiple of this vector is fixed by the action. For example, $(1\ 2) \in S_3$ sends $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ to $\mathbf{e}_2 + \mathbf{e}_1 + \mathbf{e}_3$, which is obviously the same vector. Thus the whole line $W = \{c(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3) \mid c \in \mathbb{R}\}$ is a $G$-stable subspace of $V = \mathbb{R}^3$. Let $\langle\ ,\ \rangle$ be the standard inner product given by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{k=1}^{3} x_k y_k$. This is also preserved by the action. Again, for example, $(1\ 2)$ sends $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3$ to $x_2 y_2 + x_1 y_1 + x_3 y_3 = \langle \mathbf{x}, \mathbf{y} \rangle$. Thus, the plane $W^\perp$ perpendicular to $W$ must also be $G$-stable. $W^\perp = \{(x, y, z) \mid x + y + z = 0\}$ since $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ is perpendicular to the plane. Orthogonally project $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ onto the plane, obtaining $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3$. To do this projection, subtract an appropriate multiple of $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ until each $\mathbf{e}_i$ for $i = 1, 2, 3$ lands in the plane $W^\perp$. Verify that the correct multiple is 1/3.

$$\mathbf{f}_1 = \begin{bmatrix}1\\0\\0\end{bmatrix}_e - \begin{bmatrix}1/3\\1/3\\1/3\end{bmatrix}_e = \begin{bmatrix}2/3\\-1/3\\-1/3\end{bmatrix}_e \tag{16.25}$$

$$\mathbf{f}_2 = \begin{bmatrix}0\\1\\0\end{bmatrix}_e - \begin{bmatrix}1/3\\1/3\\1/3\end{bmatrix}_e = \begin{bmatrix}-1/3\\2/3\\-1/3\end{bmatrix}_e \tag{16.26}$$

$$\mathbf{f}_3 = \begin{bmatrix}0\\0\\1\end{bmatrix}_e - \begin{bmatrix}1/3\\1/3\\1/3\end{bmatrix}_e = \begin{bmatrix}-1/3\\-1/3\\2/3\end{bmatrix}_e \tag{16.27}$$

The reader should verify that $\langle \mathbf{f}_i, \mathbf{f}_j \rangle = -1/3$ for $i \neq j$ and $\langle \mathbf{f}_i, \mathbf{f}_i \rangle = 2/3$ for $i = 1, 2, 3$. Take $\{\mathbf{f}_1, \mathbf{f}_2\}$ as a basis of $W^{\perp}$, and call it the "$f$" basis. Verify that $\mathbf{f}_1 + \mathbf{f}_2 + \mathbf{f}_3 = 0$, so $\mathbf{f}_3 = -\mathbf{f}_1 - \mathbf{f}_2$. In matrix notation, we have:

$$\mathbf{f}_1 = \begin{bmatrix}1\\0\end{bmatrix}_f \; \mathbf{f}_2 = \begin{bmatrix}0\\1\end{bmatrix}_f \; \mathbf{f}_3 = \begin{bmatrix}-1\\-1\end{bmatrix}_f . \tag{16.28}$$

How does $\rho_{(1\ 2)}$ act on $W^{\perp}$ using the $f$-basis? $(1\ 2)$ interchanges $\mathbf{f}_1$ and $\mathbf{f}_2$ but leaves $\mathbf{f}_3$ fixed. What about $\rho_{(1\ 2\ 3)}$? $(1\ 2\ 3)$ sends $\mathbf{f}_1$ to $\mathbf{f}_2$ and $\mathbf{f}_2$ to $\mathbf{f}_3 = -\mathbf{f}_1 - \mathbf{f}_2$. Therefore,

$$\rho^{W^{\perp}}_{(1\ 2)} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}_f , \; \rho^{W^{\perp}}_{(1\ 2\ 3)} = \begin{bmatrix}0 & -1\\1 & -1\end{bmatrix}_f . \tag{16.29}$$

Work out the rest in Problem 16.16. (Recall that $(1\ 2)$ and $(1\ 2\ 3)$ generate $S_3$. See Theorem 3.10.)

**Definition 16.14** Let $\rho : G \longrightarrow GL(V)$ be a representation. We say $\rho$ is irreducible if $V$ has no $G$-stable subspace besides $\{\mathbf{0}\}$ and $V$. This means that there is only one way to write $V$ as a direct sum of $G$-stable subspaces: $V = V \oplus \{\mathbf{0}\}$.

Remark: Any degree-1 representation of a group $G$ is clearly an irreducible representation.

Remark: A common nickname for an irreducible representation is irrep. Instead of saying "consider a degree-2 irreducible representation of..." you could say "consider a degree-2 irrep of..." Of course, there is also the plural form "irreps."

**Definition 16.15** If a representation is not irreducible, we say that it is reducible.

**Definition 16.16** Let $G$ be a group and let $\rho : G \longrightarrow GL(V)$ be a representation of $G$. The representation $\rho$ is said to be completely reducible if $V = V_1 \oplus \cdots \oplus V_k$ where $V_i$ is a $G$-stable subspace and $\rho^{V_i}$ is irreducible for each $i = 1, \cdots, k$.

**Definition 16.17** Let $\rho : G \longrightarrow GL(V)$ be a representation. We say $\rho$ is decomposable if we can write $V = V_1 \oplus V_2$ where $V_1, V_2$ are $G$-stable subspaces with $V_1 \neq \{\mathbf{0}\}$ and $V_2 \neq \{\mathbf{0}\}$.

**Definition 16.18** Let $\rho : G \longrightarrow GL(V)$ be a representation. We say $\rho$ is indecomposable if it is not decomposable.

Why all these terms? These are two different notions, and irreducibility is the finer notion. Theorem 16.4 makes this statement more precise. We will show now that for *finite* groups $G$, every representation of $G$ on a finite-dimensional complex vector space $V$ that is indecomposable is irreducible. The representation theory of finite groups $G$ over $\mathbb{C}$ is completely reducible.

**Theorem 16.2** *Let $\rho : G \longrightarrow GL(V)$ be a unitary representation of the group $G$. Then $\rho$ is either irreducible or decomposable.*

***Proof*** If $\rho$ is irreducible then $\rho$ is obviously either irreducible or decomposable. Suppose that $\rho$ is reducible. This means that there is a $G$-stable subspace $W \subsetneq V$. Its orthogonal complement $W^\perp$ is then also nonzero and $V = W \oplus W^\perp$. Looking at Definition 16.17, we see that if we can show that $W$ and $W^\perp$ are $G$-stable, then $\rho$ is decomposable. $W$ in $G$-stable by assumption. Therefore, let us consider $W^\perp$. Let $\mathbf{w} \in W$ and $\mathbf{w}^\perp \in W^\perp$ be arbitrary. Then, for any $g \in G$,

$$\begin{aligned}(\rho_g \mathbf{w}^\perp, \mathbf{w}) &= (\rho_{g^{-1}}\rho_g \mathbf{w}^\perp, \rho_{g^{-1}}\mathbf{w}) \\ &= (\mathbf{w}^\perp, \rho_{g^{-1}}\mathbf{w}) \\ &= 0.\end{aligned} \tag{16.30}$$

The first equality follows from the unitarity of $\rho$ (so $(\rho_h \mathbf{v}_1, \rho_h \mathbf{v}_2) = (\mathbf{v}_1, \mathbf{v}_2)$ for any $\mathbf{v}_1, \mathbf{v}_2 \in V$ and any $h \in G$), the second because $W$ is $G$-stable so $\rho_{g^{-1}}\mathbf{w} \in W$ and hence $(\mathbf{w}^\perp, \rho_{g^{-1}}\mathbf{w}) = 0$. Therefore, $\rho_g \mathbf{w}^\perp \in W^\perp$ for any $g \in G$ and any $\mathbf{w}^\perp \in W^\perp$. Therefore, $\rho$ is decomposable. □

**Theorem 16.3** *Let $G$ be a finite group and let $\rho : G \longrightarrow GL(V)$ be a representation of $G$. Then $\rho$ is either irreducible or decomposable.*

***Proof*** Since $G$ is finite, Theorem 16.1 and the comments after it let us conclude that we can, WLOG, consider $\rho_g$ as unitary matrices for all $g \in G$. (More formally, there is a change of basis matrix $\tau$ such that $\rho'_g = \tau\rho_g\tau^{-1}$ is unitary for any $g \in G$. We are saying that suppose from the start we are in the basis where $\rho$ is unitary and no change of basis to an equivalent representation is needed.) Theorem 16.2 then tells us that $\rho$ is either irreducible or decomposable. □

Let us build some intuition by thinking in terms of matrices and not abstract linear maps between vector spaces. Let $G$ be a group and let $V$ be a vector space over $\mathbb{C}$ with $\dim V = n$. Let $\rho : G \longrightarrow GL(V) \cong GL_n(\mathbb{C})$ be a representation. The matrices $\rho_g$ for $g \in G$ will, in some generic basis, be some $n \times n$ matrix:

$$\rho_g = \begin{bmatrix} (\rho_g)_{1,1} & (\rho_g)_{1,2} & \cdots & (\rho_g)_{1,n} \\ (\rho_g)_{2,1} & (\rho_g)_{2,2} & \cdots & (\rho_g)_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ (\rho_g)_{n,1} & (\rho_g)_{n,2} & \cdots & (\rho_g)_{n,n} \end{bmatrix} \tag{16.31}$$

where in principle all the entries could be nonzero. Suppose that $V$ has two and only two $G$-invariant subspaces, call them $V_1$ and $V_2$ with $\dim V_1 = n_1, \dim V_2 = n_2$ and

$n = n_1 + n_2$ with $0 < n_1, n_2 < n$. Suppose that $V = V_1 \oplus V_2$. This means that there exists some ordered basis where the first $n_1$ basis vectors span the subspace $V_1$ and the next $n_2$ basis vectors span the subspace $V_2$ such that

$$\rho_g = \begin{array}{cc} \begin{array}{cc} V_1 & V_2 \end{array} & \\ \begin{bmatrix} \rho_g^{(1)} & \mathbf{0} \\ \mathbf{0} & \rho_g^{(2)} \end{bmatrix} & \begin{array}{c} V_1 \\ V_2 \end{array} \end{array} \tag{16.32}$$

in that basis. This is sometimes written as $\rho_g = \rho_g^{(1)} \oplus \rho_g^{(2)}$ since the matrix $\rho_g$, in some suitably chosen basis, looks like the matrices $\rho_g^{(1)}$ and $\rho_g^{(2)}$ stacked together along the "diagonal." Formally, $\rho_g$ is a block diagonal matrix. Also, the $\mathbf{0}$ (the "big zero") in the matrix carries multiple meanings. In the upper right, $\mathbf{0}$ means that you have a $\dim V_1$ by $\dim V_2$ rectangular (square only if $\dim V_1 = \dim V_2$) block of zeros. In the lower left block, $\mathbf{0}$ means you have a $\dim V_2$ by $\dim V_1$ rectangular (square only if $\dim V_1 = \dim V_2$) block of zeros.

If $\rho : G \to GL(V)$ is irreducible, it means that no matter how hard we try, we will not be able to find a basis where $\rho_g$ for $\forall g \in G$ can be written as smaller matrices stacked together. That is, if $\rho : G \to GL(V) \cong GL_n(\mathbb{C})$ is an irreducible representation and, in general, $\rho_g$ is as in Equation 16.31 for the basis we are working in, then there exists no invertible matrix $S$ such that $S\rho_g S^{-1}$ has the form of the matrix in Equation 16.32 for $\forall g \in G$. In some sense, $\rho_g$ is already written as "small" as it can be for all $g \in G$. It is irreducible.

**Theorem 16.4** *(Maschke's Theorem) - Let G be a finite group. Any representation of G on a finite-dimensional complex vector space is completely reducible. That is, every representation of a finite group is a direct sum of irreducible representations.*

***Proof*** Let $G$ be a finite group and let $\rho : G \to GL(V)$ be a representation of $G$. We proceed by induction on $\dim V$. If $\dim V = 1$, then $\rho$ is obviously irreducible. Suppose the theorem is true for $\dim V \leq n$. Let $\rho : G \to GL(V)$ be a representation where $\dim V = n + 1$. If $\rho$ is irreducible, there is nothing to prove. Suppose $\rho$ is reducible. By Theorem 16.3, $\rho$ is decomposable so $V = V_1 \oplus V_2$ where $V_1 \neq \{\mathbf{0}\}$ and $V_2 \neq \{\mathbf{0}\}$ and $V_1, V_2$ are $G$-stable. Since $\dim V_1, \dim V_2 \leq n$ we conclude that $\rho^{V_1}$ and $\rho^{V_2}$ are completely reducible by our induction hypothesis. Therefore, $V_1 = A_1 \oplus \cdots \oplus A_{k_1}$ and $V_2 = B_1 \oplus \cdots \oplus B_{k_2}$ where $A_i, B_j$ are $G$-stable and $\rho^{A_i}, \rho^{B_j}$ are irreducible for $1 \leq i \leq k_1, 1 \leq j \leq k_2$. Then $V = A_1 \oplus \cdots \oplus A_{k_1} \oplus B_1 \oplus \cdots \oplus B_{k_2}$, so the representation $\rho$ can indeed be written as a direct sum of irreducible representations. □

The theorem above is extremely important for *finite* groups. What it means is that we can focus all of our attention on understanding the irreducible representations when dealing with *finite* groups, since any other representation will be a direct sum of the irreducible representations.

Note: If $n > 1$, then the representation $\rho : G \to GL_n(\mathbb{C})$ given by $\rho_g = I_{n\times n}$ for all $g \in G$ is *not* the trivial representation. It is equivalent to a direct sum of $n$ copies of the trivial representation.

*Example 16.8* Let $G = (\mathbb{R}, +, 0)$. $G$ is not a finite group. There is a degree-2 representation $\rho : G \to GL_2(\mathbb{R})$ defined by

$$\rho_u = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}. \tag{16.33}$$

This is a homomorphism since

$$\rho_u \rho_v = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & u+v \\ 0 & 1 \end{bmatrix} = \rho_{u+v}. \tag{16.34}$$

This representation is sometimes called horizontal shears. Why the name? Consider points along the $x = 1$ axis. Any point $(a, 1)$ gets mapped by $\rho_b$ to $(a + b, 1)$, $(a, 2)$ gets mapped to $(a + 2b, 2)$, and $(a, 3)$ gets mapped to $(a + 3b, 3)$, etc.

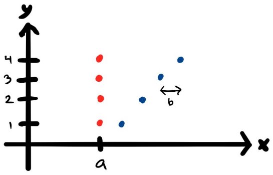


Fig. 16.1: Horizontal shears. The vertical dots each get mapped sideways by a different amount.

What are the $G$-stable subspaces? Convince yourself that only the $x$-axis is $G$-stable. That is, only the subspace $\mathbb{R}\mathbf{e}_1$ is $G$-stable. Any other line through the origin will not get mapped into itself but will instead, due to the shearing action of $\rho$, be rotated around into some other line through the origin. Therefore, $\mathbb{R}^2$ *cannot* be written as a direct sum of two one-dimensional subspaces which are both $G$-stable. Thus, $G$ is *not* irreducible (since the $x$-axis is $G$-stable) but it *is* indecomposable.

Note: The above was over the real scalars so that an intuitive picture could be drawn. The same conclusion applies if we consider it over $\mathbb{C}$. Then $\mathbb{C}\mathbf{e}_1$ is $G$-stable and no other line through the origin is $G$-stable, so $\rho : G \to GL_2(\mathbb{C})$ is not irreducible but it is indecomposable. The whole point of this example is that $G$ is not finite here so the theorems we just proved are not applicable.

Note: An irreducible representation is indecomposable. The horizontal shears example above, however, shows that it is possible to be indecomposable but not irreducible.

### 16.7.1 Determining If Degree-2 and Degree-3 Representations Are Irreducible

In Theorem 16.11, we will show a way to determine if a representation (of any finite degree) is irreducible. However, for a degree-2 or degree-3 representation, one can determine if a representation is irreducible by solving for eigenvectors of $\rho_g$ for each $g \in G$. Of course, this method is only convenient/practical to do by hand if $G$ has a small number of generators.

**Theorem 16.5** *Let $G$ be a finite group and let $\rho : G \to GL(V)$ be a degree-2 representation. Then $\rho$ is irreducible if and only if there does not exist a common eigenvector for $\rho_g$ for all $g \in G$. (Actually, one only needs to consider the generators of $G$.)*

***Proof*** If $\dim V = 2$, then any nonzero proper $G$-invariant subspace W (that is, $\{\mathbf{0}\} \subsetneqq W \subsetneqq V$) must be one-dimensional. Pick any nonzero vector $\mathbf{w} \in W$. Then $W = \mathbb{C}\mathbf{w}$. If $W$ is $G$-stable, we have $\rho_g \mathbf{w} = \lambda_g \mathbf{w}$ for every $g \in G$. The subscript on $\lambda_g$ is there because the proportionality constant (the eigenvalue, actually) is not necessarily the same for all $g \in G$. It follows that $\mathbf{w}$ is an eigenvector for all $g \in G$. The other direction is similar. Suppose there exists a vector $\mathbf{w} \in V$ such that $\rho_g = \lambda_g \mathbf{w}$ for all $g \in G$. Then $W = \mathbb{C}\mathbf{w}$ is a nonzero proper $G$-stable subspace of $V$ and, hence, $\rho$ is reducible. □

*Example 16.9* Consider $\rho : D_4 \to GL_2(\mathbb{C})$ defined by

$$\rho(r^k) = \begin{bmatrix} i^k & 0 \\ 0 & (-i)^k \end{bmatrix}, \ \rho(sr^k) = \begin{bmatrix} 0 & (-i)^k \\ i^k & 0 \end{bmatrix}.$$

Here, $r$ is counterclockwise rotation by $\pi/2$ while $s$ is reflection over the $x$-axis. Then $\mathbf{e}_1$ and $\mathbf{e}_2$ are clearly eigenvectors of $\rho(r^k)$ but not $\rho(sr^k)$. Thus, this degree-2 representation of $D_4$ is irreducible.

**Theorem 16.6** *Let $G$ be a finite group and let $\rho : G \to GL(V)$ be a degree-3 representation. Then $\rho$ is irreducible if and only if there does not exist a common eigenvector for $\rho_g$ for all $g \in G$. (Actually, one only needs to consider the generators of $G$.)*

***Proof*** Left to reader. □

## 16.8 New Representations From Old Ones - Tensor Products

Idea: Once we have a representation, we can create new ones (often not irreducible representations, but representations nonetheless) from the existing one.

**Definition 16.19** Let $V_1, V_2$ be finite dimensional vector spaces over $\mathbb{C}$. Let $\{\mathbf{e}_1, \cdots, \mathbf{e}_m\}$ be a basis of $V_1$ and $\{\mathbf{f}_1, \cdots, \mathbf{f}_n\}$ be a basis for $V_2$. Then the $\underline{\text{tensor product } V_1 \otimes V_2}$ or $V_1 \otimes_{\mathbb{C}} V_2$ is a complex vector space whose basis consists of the formal $m \cdot n$ symbols $\mathbf{e}_i \otimes \mathbf{f}_j$ for $i = 1, \cdots, m$ and $j = 1, \cdots, n$. The tensor product is bilinear in the sense that

$$(\sum_{i=1}^{m} a_i \mathbf{e}_i) \otimes (\sum_{j=1}^{n} b_j \mathbf{f}_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j \mathbf{e}_i \otimes \mathbf{f}_j.$$

1. Distributive: $\mathbf{v}_1 \otimes (\mathbf{w}_1 + \mathbf{w}_2) = \mathbf{v}_1 \otimes \mathbf{w}_1 + \mathbf{v}_1 \otimes \mathbf{w}_2$
2. Distributive: $(\mathbf{v}_1 + \mathbf{v}_2) \otimes \mathbf{w}_1 = \mathbf{v}_1 \otimes \mathbf{w}_1 + \mathbf{v}_2 \otimes \mathbf{w}_1$
3. Associative: $(\mathbf{v}_1 \otimes \mathbf{v}_2) \otimes \mathbf{v}_3 = \mathbf{v}_1 \otimes (\mathbf{v}_2 \otimes \mathbf{v}_3)$

where the vectors are arbitrary vectors from their respective vectors spaces. They are *not* however commutative. That is, $\mathbf{v} \otimes \mathbf{w} \neq \mathbf{w} \otimes \mathbf{v}$ in general. Things do, however, commute with the scalars: $\lambda(\mathbf{v} \otimes \mathbf{w}) = (\lambda \mathbf{v}) \otimes \mathbf{w} = \mathbf{v} \otimes (\lambda \mathbf{w})$.

*Example 16.10* If $m = 2$ and $n = 2$ then

$$(4\mathbf{e}_1 + 3\mathbf{e}_2) \otimes (2\mathbf{f}_1 + 5\mathbf{f}_2) = 8\mathbf{e}_1 \otimes \mathbf{f}_1 + 20\mathbf{e}_1 \otimes \mathbf{f}_2 + 6\mathbf{e}_2 \otimes \mathbf{f}_1 + 15\mathbf{e}_2 \otimes \mathbf{f}_2. \quad (16.35)$$

**Definition 16.20** Let $G$ be a finite group. Let $\rho^{(1)} : G \to GL(V_1)$ and $\rho^{(2)} : G \to GL(V_2)$ be representations. Let us define a representation $\rho^{(\otimes)} : G \to GL(V_1 \otimes V_2)$ by

$$\rho_g^{(\otimes)}(\mathbf{v}_1 \otimes \mathbf{v}_2) = (\rho_g^{(1)}(\mathbf{v}_1)) \otimes (\rho_g^{(2)}(\mathbf{v}_2))$$

for $\forall \mathbf{v}_1 \in V_1, \forall \mathbf{v}_2 \in V_2$, and $\forall g \in G$. We will sometimes write $\rho^{(\otimes)} = \rho^{(1)} \otimes \rho^{(2)}$. Then the previous equation becomes

$$(\rho_g^{(1)} \otimes \rho_g^{(2)})(\mathbf{v}_1 \otimes \mathbf{v}_2) = (\rho_g^{(1)}(\mathbf{v}_1)) \otimes (\rho_g^{(2)}(\mathbf{v}_2)).$$

We can think of the new representation $\rho^{(\otimes)} = \rho^{(1)} \otimes \rho^{(2)}$ as having a $\rho^{(1)}$ part and a $\rho^{(2)}$ part in such a way that when $\rho_g^{(\otimes)}$ acts on $\mathbf{v}_1 \otimes \mathbf{v}_2$, the respective parts of $\rho^{(\otimes)}$ only "see" and act on their respective vectors. We say that $\rho^{(\otimes)}$ is a $\underline{\text{tensor product of the given representations}}$.

Let $\mathbf{v}_1 = \sum_{i=1}^{m} a_i \mathbf{e}_i$ and $\mathbf{v}_2 = \sum_{j=1}^{n} b_j \mathbf{f}_j$. Then

$$\begin{aligned} \rho_g^{(1)}(\mathbf{v}_1) &= \textstyle\sum_{i=1}^{m} a_i \rho_g^{(1)}(\mathbf{e}_i) = \sum_{i,k=1}^{m} a_i \left(\rho_g^{(1)}\right)_{ki} \mathbf{e}_k \\ \rho_g^{(2)}(\mathbf{v}_2) &= \textstyle\sum_{j=1}^{n} b_j \rho_g^{(2)}(\mathbf{f}_j) = \sum_{j,l=1}^{n} b_j \left(\rho_g^{(2)}\right)_{lj} \mathbf{f}_l \end{aligned} \quad (16.36)$$

Therefore,

$$\begin{aligned}\rho_g^{(\otimes)}(\mathbf{v}_1 \otimes \mathbf{v}_2) &= (\rho_g^{(1)} \otimes \rho_g^{(2)})(\mathbf{v}_1 \otimes \mathbf{v}_2) \\ &= (\rho_g^{(1)}(\mathbf{v}_1)) \otimes (\rho_g^{(2)}(\mathbf{v}_2)) \\ &= (\sum_{i,k=1}^{m} a_i \left(\rho_g^{(1)}\right)_{ki} \mathbf{e}_k) \otimes (\sum_{j,l=1}^{n} b_j \left(\rho_g^{(2)}\right)_{lj} \mathbf{f}_l) \\ &= \sum_{i,k=1}^{m} \sum_{j,l=1}^{n} a_i b_j \left(\rho_g^{(1)}\right)_{ki} \left(\rho_g^{(2)}\right)_{lj} \mathbf{e}_k \otimes \mathbf{f}_l.\end{aligned} \tag{16.37}$$

Consider the case when $\mathbf{v}_1 = \mathbf{e}_a$ and $\mathbf{v}_2 = \mathbf{f}_b$. Then this gives

$$\begin{aligned}\rho_g^{(\otimes)}(\mathbf{e}_a \otimes \mathbf{f}_b) &= (\rho_g^{(1)} \otimes \rho_g^{(2)})(\mathbf{e}_a \otimes \mathbf{f}_b) \\ &= \sum_{k=1}^{m} \sum_{l=1}^{n} \left(\rho_g^{(1)}\right)_{ka} \left(\rho_g^{(2)}\right)_{lb} \mathbf{e}_k \otimes \mathbf{f}_l.\end{aligned} \tag{16.38}$$

Thus, we see that we can think of the direct-product matrix as satisfying

$$\left((\rho_g^{(1)} \otimes \rho_g^{(2)})\right)_{kl,ab} = \left(\rho_g^{(1)}\right)_{ka} \left(\rho_g^{(2)}\right)_{lb} \tag{16.39}$$

where the columns and rows are indexed by *pairs* of indices. Therefore, we see again that $\dim V_1 \otimes V_2 = \dim V_1 \cdot \dim V_2$ since that is the number of independent values for the pair of indices. The trace is defined as the sum of the diagonal elements. Therefore,

$$\begin{aligned}\mathrm{Tr}(\rho_g^{(1)} \otimes \rho_g^{(2)}) &= \sum_{k=1}^{m} \sum_{l=1}^{n} \left((\rho_g^{(1)} \otimes \rho_g^{(2)})\right)_{kl,kl} \\ &= \sum_{k=1}^{m} \sum_{l=1}^{n} \left(\rho_g^{(1)}\right)_{kk} \left(\rho_g^{(2)}\right)_{ll} \\ &= \mathrm{Tr}(\rho_g^{(1)})\, \mathrm{Tr}(\rho_g^{(2)}).\end{aligned} \tag{16.40}$$

We have just proved that $\chi^{(\otimes)}(g) = \chi^{(1)}(g)\chi^{(2)}(g)$. That is, the character of the direct product representation can be calculated from the characters of the "original" representations simply by multiplying the characters.

### 16.8.1 Symmetric Square and Alternating Square

Let us consider the case when the two vector spaces are the same $V_1 = V_2$. Relabel the vector space and call it $V \equiv V_1$. Also, consider $\rho^{(1)} = \rho^{(2)}$. Relabel the representation $\rho$. That is, $\rho_g^{(\otimes)} = \rho_g \otimes \rho_g$ for all $g \in G$. Let us use $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ as our basis (so $\dim V = n$).

**Definition 16.21** The symmetric square of $V$, denoted $\mathrm{Sym}^{(2)}(V)$, is the subspace of $V \otimes V$ where all tensors are symmetric under the map $\theta : \mathbf{e}_i \otimes \mathbf{e}_j \mapsto \mathbf{e}_j \otimes \mathbf{e}_i$.

**Definition 16.22** The alternating square of $V$, denoted $\mathrm{Alt}^{(2)}(V)$, is the subspace of $V \otimes V$ where all tensors are skew-symmetric under the map $\theta : \mathbf{e}_i \otimes \mathbf{e}_j \mapsto \mathbf{e}_j \otimes \mathbf{e}_i$. That is, they are invariant under $\mathbf{e}_i \otimes \mathbf{e}_j \mapsto -\mathbf{e}_j \otimes \mathbf{e}_i$.

Comment: Many books write $\mathrm{Alt}^{(2)}(V)$ as $\bigwedge^2 V$. However, there is no standard "fancy" symbol/notation for Sym. Maybe this reflects the fact that skew-symmetry appears more often in math concepts than symmetry. Think about how many formulas you know that involve the determinant compared to the permanent. (Both are important in physics. Think of fermions and bosons.)

In other words, we define an automorphism $\theta$ of $V \otimes V$ by $\theta(\mathbf{e}_i \otimes \mathbf{e}_j) = \mathbf{e}_j \otimes \mathbf{e}_i$. This $\theta$ satisfies $\theta^2 = 1$, so the eigenvectors of this linear map $\theta$ on $V \otimes V$ have eigenvalue 1 or $-1$. $\mathrm{Sym}^{(2)}(V)$ is the eigenspace for eigenvalue 1 while $\mathrm{Alt}^{(2)}(V)$ is the eigenspace for the eigenvalue $-1$. These eigenspaces span $V \otimes V$ and we have, as we will shortly show,

$$V \otimes V = \mathrm{Sym}^{(2)}(V) \oplus \mathrm{Alt}^{(2)}(V). \tag{16.41}$$

Essentially, the observation is that

$$\begin{aligned} \mathbf{v} \otimes \mathbf{w} &= \frac{1}{2}(\mathbf{v} \otimes \mathbf{w} + \mathbf{w} \otimes \mathbf{v}) + \frac{1}{2}(\mathbf{v} \otimes \mathbf{w} - \mathbf{w} \otimes \mathbf{v}) \qquad (16.42) \\ &= \underbrace{\frac{1}{2}(\mathbf{v} \otimes \mathbf{w} + \theta(\mathbf{v} \otimes \mathbf{w}))}_{\text{in } \mathrm{Sym}^{(2)}(V)} + \underbrace{\frac{1}{2}(\mathbf{v} \otimes \mathbf{w} - \theta(\mathbf{v} \otimes \mathbf{w}))}_{\text{in } \mathrm{Alt}^{(2)}(V)} \end{aligned}$$

for any $\mathbf{v} \otimes \mathbf{w} \in V \otimes V$ and that this decomposition satisfies the criteria of direct sum decomposition. To verify that $\mathrm{Sym}^{(2)}(V) \cap \mathrm{Alt}^{(2)}(V) = \{\mathbf{0} \otimes \mathbf{0}\}$, note that any $\mathbf{v} \otimes \mathbf{w} \in \mathrm{Sym}^{(2)}(V) \cap \mathrm{Alt}^{(2)}(V)$ satisfies $\theta(\mathbf{v} \otimes \mathbf{w}) = \mathbf{v} \otimes \mathbf{w}$ and $\theta(\mathbf{v} \otimes \mathbf{w}) = -\mathbf{v} \otimes \mathbf{w}$, which means that $\mathbf{v} \otimes \mathbf{w} = -\mathbf{v} \otimes \mathbf{w}$, so $\mathbf{v} \otimes \mathbf{w} = \mathbf{0} \otimes \mathbf{0}$.

A basis for $\mathrm{Sym}^{(2)}(V)$ is $\{\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i \mid i \le j\}$ and a basis for $\mathrm{Alt}^{(2)}(V)$ is $\{\mathbf{e}_i \otimes \mathbf{e}_j - \mathbf{e}_j \otimes \mathbf{e}_i \mid i < j\}$[1]. Convince yourself that

$$\dim \mathrm{Sym}^{(2)}(V) = \frac{n(n+1)}{2}, \tag{16.43}$$

$$\dim \mathrm{Alt}^{(2)}(V) = \frac{n(n-1)}{2}. \tag{16.44}$$

These subspaces are $G$-stable. To verify this claim, note that

[1] Note that we say *a* basis rather than *the* basis. A choice of basis is just that: a choice. Some authors might introduce factors of $\frac{1}{p!}$ where $p$ is the number of indices in the basis choice for $\mathrm{Alt}^{(2)}(V)$ to make some formulas look nicer when introducing inner products in tensor product spaces.

$$\begin{aligned}
\theta((\rho_g \otimes \rho_g)(\mathbf{v} \otimes \mathbf{w})) &= \theta((\rho_g \otimes \rho_g) \sideset{}{'}\sum_{ij} c_{ij}(\mathbf{e}_i \otimes \mathbf{e}_j + (-1)^s \mathbf{e}_j \otimes \mathbf{e}_i)) \qquad (16.45)\\
&= \theta(\sideset{}{'}\sum_{ij} c_{ij}(\rho_g \mathbf{e}_i \otimes \rho_g \mathbf{e}_j + (-1)^s \rho_g \mathbf{e}_j \otimes \rho_g \mathbf{e}_i))\\
&= \sideset{}{'}\sum_{ij} c_{ij}(\theta(\rho_g \mathbf{e}_i \otimes \rho_g \mathbf{e}_j) + (-1)^s \theta(\rho_g \mathbf{e}_j \otimes \rho_g \mathbf{e}_i))\\
&= \sideset{}{'}\sum_{ij} c_{ij}(\rho_g \mathbf{e}_j \otimes \rho_g \mathbf{e}_i + (-1)^s \rho_g \mathbf{e}_i \otimes \rho_g \mathbf{e}_j)\\
&= (-1)^s \sideset{}{'}\sum_{ij} c_{ij}(\rho_g \mathbf{e}_i \otimes \rho_g \mathbf{e}_j + (-1)^s \rho_g \mathbf{e}_j \otimes \rho_g \mathbf{e}_i)\\
&= (-1)^s \mathbf{v} \otimes \mathbf{w},
\end{aligned}$$

where $s = 1$ if $\mathbf{v} \otimes \mathbf{w} \in \mathrm{Sym}^{(2)}(V)$ and $s = -1$ if $\mathbf{v} \otimes \mathbf{w} \in \mathrm{Alt}^{(2)}(V)$. The prime on the summation is just to serve as a reminder that the sum is restricted to $i \leq j$ for $s = 1$ and $i < j$ for $s = -1$. The restriction of $\rho \otimes \rho$ to these $G$-stable subspaces is called the symmetric square and the alternating square of the $\rho \otimes \rho$ representation. Using the language introduced in Definition 16.13, we say that $\mathrm{Sym}^{(2)}(V)$ is a subrepresentation of $V \otimes V$ and $\mathrm{Alt}^{(2)}(V)$ is a subrepresentation of $V \otimes V$.

## 16.9 New Representations From Old Ones - (External) Direct Product of Two Groups

Recall that in Chapter 6 we discussed how to make groups by multiplying two groups. Review the chapter if needed. In this chapter, we discussed the tensor product of two groups and their representations. We will now discuss the (external) direct product of two groups and their representations.

**Definition 16.23** Let $\rho^{(1)} : G_1 \to GL(V_1)$ be a linear representation of $G_1$ and let $\rho^{(2)} : G_2 \to GL(V_2)$ be a linear representation of $G_2$. Define the representation $\rho^{(1)} \times \rho^{(2)} : G_1 \times G_2 \to GL(V_1 \times V_2)$ by

$$(\rho^{(1)} \times \rho^{(2)})_{g_1, g_2} = \rho^{(1)}_{g_1} \times \rho^{(2)}_{g_2}$$

for any $(g_1, g_2) \in G_1 \times G_2$. By this, we mean

$$(\rho^{(1)} \times \rho^{(2)})_{g_1, g_2}(\mathbf{v}_1, \mathbf{v}_2) = (\rho^{(1)}_{g_1} \mathbf{v}_1, \rho^{(2)}_{g_2} \mathbf{v}_2) \in V_1 \times V_2$$

for any $(\mathbf{v}_1, \mathbf{v}_2) \in V_1 \times V_2$. We call this the direct product of the representation $\rho^{(1)}$ and $\rho^{(2)}$.

Let $\chi^{(\times)}$ be the character of $\rho^{(1)} \times \rho^{(2)}$. Arguments similar to the one given in the section of tensor products give

$$\chi^{(\times)}((g_1, g_2)) = \chi^{(1)}(g_1)\chi^{(2)}(g_2) \tag{16.46}$$

for any $(g_1, g_2) \in G_1 \times G_2$.

## 16.10 New Representations From Old Ones - Lifting

**Theorem 16.7** *Let $G$ and $H$ be finite groups. Let $f : G \longrightarrow H$ be a homomorphism. Let $\tilde{\rho} : H \longrightarrow GL(V)$ be a representation of $H$. Then $\rho \equiv \tilde{\rho} \circ f : G \longrightarrow GL(V)$ is a representation of $G$. That is,*

$$\rho : G \xrightarrow{f} H \xrightarrow{\tilde{\rho}} GL(V)$$

*is a representation.*

***Proof*** We must verify that $\rho \equiv \tilde{\rho} \circ f$ is a homomorphism. Let $g_1, g_2 \in G$ be arbitrary. Then

$$\begin{aligned}(\tilde{\rho} \circ f)(g_1 g_2) &= \tilde{\rho}_{f(g_1 g_2)} \\ &= \tilde{\rho}_{f(g_1) f(g_2)} \\ &= \tilde{\rho}_{f(g_1)} \tilde{\rho}_{f(g_2)} \\ &= (\tilde{\rho} \circ f)(g_1)(\tilde{\rho} \circ f)(g_2).\end{aligned} \tag{16.47}$$

Therefore, $\rho$ is a homomorphism from $G$ to $GL(V)$ and so, by definition, is a representation of $G$. □

**Definition 16.24** Using notation as in the previous theorem, the representation $\rho \equiv \tilde{\rho} \circ f : G \longrightarrow GL(V)$ is said to be the lift or inflation of the representation of $H$.

**Corollary 16.3** *Lifting (or inflating) from a quotient group - Let $N$ be a normal subgroup of a finite group $G$. Consider the quotient group $G/N$ and suppose that one is able to construct a representation for $G/N$. Let $\tilde{\rho} : G/N \longrightarrow GL(V)$ be a representation of $G/N$. Define $f : G \longrightarrow G/N$ by $f(g) = gN$. Then $f : G \longrightarrow G/N$ is a homomorphism. This follows since $f(g_1 g_2) = g_1 g_2 N = g_1 N g_2 N = f(g_1) f(g_2)$, where we have used the fact the $N \trianglelefteq G$. By Theorem 16.7, $\tilde{\rho} \circ f$ is a representation of $G$. We say that the representation of $G/N$ can be lifted to give a representation of $G$.*

*Example 16.11* Recall that $A_n \trianglelefteq S_n$. Also, $[S_n : A_n] = 2$ so $S_n/A_n \cong \mathbb{Z}_2$. For example, $S_n/A_n = \langle (1\ 2)A_n \rangle$. There are two degree-1 representations of $\mathbb{Z}_2$. Then $\tilde{\rho}^{(1)}_{(1\ 2)A_n} = 1$ and $\tilde{\rho}^{(2)}_{(1\ 2)A_n} = -1$ determine the two degree-1 representations of $S_n/A_n$. Let $f : S_n \longrightarrow S_n/A_n$ be the homomorphism defined by $f(x) = xA_n$. Then the compositions $\rho^{(i)} \equiv \tilde{\rho}^{(i)} \circ f : S_n \longrightarrow GL_1(\mathbb{C})$ for $i = 1, 2$

$$\rho^{(i)} : S_n \xrightarrow{f} S_n/A_n \xrightarrow{\tilde{\rho}^{(i)}} GL_1(\mathbb{C}) \tag{16.48}$$

are representations of $S_n$, according to Corollary 16.3. The representation $i = 2$ is called the sign representation of $S_n$, often denoted as sgn. That is, sgn : $S_n \to GL_1(\mathbb{C})$ defined by

$$\operatorname{sgn}(g) = \begin{cases} +1, & \text{if } g \in S_n \text{ is an even permutation.} \\ -1, & \text{if } g \in S_n \text{ is an odd permutation.} \end{cases} \tag{16.49}$$

is a representation of $S_n$. (The case $i = 1$ is the trivial representation of $S_n$.)

*Example 16.12* Let $G = A_4$ and let $V = \{e\} \cup \{(\bullet\bullet)(\bullet\bullet)\}$. That is, $V$ is an isomorphic copy of the Klein 4-group (that is, $\mathbb{Z}_2 \times \mathbb{Z}_2$) inside $A_4$. Also, $V \trianglelefteq A_4$. (See Example 13.4. That example is about $S_4$ but similar considerations apply to $A_4$. See Table 9.2 to see that $V$ is a union of conjugacy classes of $A_4$ and, hence, a normal subgroup of $A_4$.) $|A_4/V| = 12/4 = 3$, so $A_4/V \cong \mathbb{Z}_3$. By Proposition 16.6, we have three distinct degree-1 representations of $A_4/V$ given by (where $\omega = e^{2\pi i/3}$):

$$\begin{array}{lll} \tilde{\rho}^{(1)}_{eV} = 1 & \tilde{\rho}^{(1)}_{(1\ 2\ 3)V} = 1 & \tilde{\rho}^{(1)}_{(1\ 3\ 2)V} = 1 \\ \tilde{\rho}^{(2)}_{e} = 1 & \tilde{\rho}^{(2)}_{(1\ 2\ 3)V} = \omega & \tilde{\rho}^{(2)}_{(1\ 3\ 2)V} = \omega^2 \\ \tilde{\rho}^{(3)}_{e} = 1 & \tilde{\rho}^{(3)}_{(1\ 2\ 3)V} = \omega^2 & \tilde{\rho}^{(3)}_{(1\ 3\ 2)V} = \omega. \end{array} \tag{16.50}$$

Let $f : A_4 \to A_4/V$ be defined by $f(g) = gV$ for every $g \in A_4$. By Corollary 16.3, $\tilde{\rho}^{(i)} \circ f : A_4 \to GL_1(\mathbb{C})$ for $i = 1, 2, 3$ are degree-1 representations of $A_4$.

As demonstrated by the examples above, the observation that a representation can be lifted to give a representation can allow one to fill in parts of a character table, provided the group has normal subgroups that lead to quotient groups whose representations are already known or, at the very least, are a little easier to calculate.

## 16.11 Schur's Lemma

A very powerful and useful lemma in representation theory over $\mathbb{C}$ is Schur's lemma. But first, we need the following proposition.

**Proposition 16.8** *If $\tau : V \to V'$ is a G-linear map then*

*i)* ker $\tau$ *is a G-stable subspace of V.*
*ii)* im $\tau$ *is a G-stable subspace of V′.*

***Proof*** i) Note that ker $\tau$ is nonempty since $\mathbf{0} \in \ker\tau$. (This is because $\tau$ is a linear map. Therefore, $\tau(\mathbf{0}) = \tau(\mathbf{0} + \mathbf{0}) = \tau(\mathbf{0}) + \tau(\mathbf{0})$ and, hence, $\tau(\mathbf{0}) = \mathbf{0}$). Let $\mathbf{v} \in \ker\tau$. We want to show that $\rho_g(\mathbf{v}) \in \ker\tau$. This holds because

$$\tau(\rho_g(\mathbf{v})) = \rho'_g(\tau(\mathbf{v})) = \rho'_g(\mathbf{0}) = \mathbf{0}, \tag{16.51}$$

where the last equality holds because $\rho'_g \in GL(V')$ is also a linear map.

ii) Let $\mathbf{w} \in \operatorname{im}\tau \subseteq V'$. Then $\tau(\mathbf{v}) = \mathbf{w}$ for some $\mathbf{v} \in V$ and

$$\rho'_g \mathbf{w} = \rho'_g \tau(\mathbf{v}) = \tau(\rho_g \mathbf{v}) \in \operatorname{im}\tau. \tag{16.52}$$

We are now ready for Schur's lemma.

**Lemma 16.1** *Schur's Lemma Let $\rho : G \longrightarrow GL(V)$ and $\rho' : G \longrightarrow GL(V')$ be irreducible representations. Let $\tau : V \longrightarrow V'$ be a $G$-linear map.*

*i) If $V \ncong V'$, then $\tau = 0$.*
*ii) If $V \cong V'$, then $\tau$ is a scalar multiple of the identity map.*

***Proof*** i) $\ker\tau$ is a $G$-stable subspace of $V$. Since, by assumption, $V$ is irreducible this means $\ker\tau = \{\mathbf{0}\}$ or $\ker\tau = V$. If $\ker\tau = V$, $\tau \equiv 0$. Suppose $\ker\tau = \{\mathbf{0}\}$. $\operatorname{im}\tau$ is a $G$-stable subspace of $V'$. Since, by assumption, $V'$ is irreducible this means $\operatorname{im}\tau = \{\mathbf{0}\}$ or $\operatorname{im}\tau = V'$. If $\operatorname{im}\tau = \{\mathbf{0}\}$, then $\tau \equiv 0$. If $\operatorname{im}\tau = V'$, then $\tau$ is bijective since $\ker\tau = \{\mathbf{0}\}$ and $\operatorname{im}\tau = V'$. Therefore, $\tau^{-1}$ exists so $V \cong V'$, a contradiction. Therefore, only $\tau \equiv 0$ does not lead to contradictions.

ii) If $\tau \equiv 0$ then it is clearly a scalar multiple of the identity map. Suppose $\tau \neq 0$. Then $\tau$ has at least one nonzero eigenvalue because $\mathbb{C}$ is algebraically closed (hence why we are considering representations over $\mathbb{C}$ and not $\mathbb{R}$ and this version of Schur's lemma is for representations over $\mathbb{C}$). Let $\mathbf{v} \neq 0$ be an eigenvector for this eigenvalue $\lambda$. Consider $\tilde{\tau} \equiv \tau - \lambda \cdot \mathrm{id}$. We clearly have $\tilde{\tau} \circ \rho_g = \rho'_g \circ \tilde{\tau}$ for all $g \in G$. By assumption, $V$ is irreducible so this means $\ker\tilde{\tau} = \{\mathbf{0}\}$ or $\ker\tilde{\tau} = V$. Since $\mathbf{v} \neq 0 \in \ker\tilde{\tau}$, we conclude that $\ker\tilde{\tau} = V \Longrightarrow \tilde{\tau} \equiv 0$ and, hence, $\tau \equiv \lambda \cdot \mathrm{id}$. □

**Definition 16.25** A scalar multiple of the identity map is called a homothety.

Using this terminology, Schur's lemma says that $\tau$ is a homothety. If the representations $\rho$ and $\rho'$ are nonequivalent, then the scalar multiple is 0. In general, it is $\lambda \cdot \mathrm{id}$ for some nonzero $\lambda$.

Note: It is important to remember that Schur's lemma stipulates that the representations must be irreducible, and not just any generic representations.

Note: The proof does not assume that $G$ is finite. It can be infinite. See Problem 16.21.

Let us consider things in terms of matrices. For example, let $G$ be a finite group with $|G| = k$ and $\dim V = n$. Let $\rho : G \longrightarrow GL(V)$ be an *irreducible* representation. Then we have matrices

$$\rho_{g_1}, \rho_{g_2}, \cdots, \rho_{g_k}$$

which multiply in the same way as the group elements in $G$. It is obvious that the identity matrix $I_{n\times n}$ as well as $\lambda I_{n\times n}$ for any $\lambda \in \mathbb{C}$ commutes with all these matrices ($0_{n\times n}$ does too, but we are interested in invertible matrices). However, what Schur's lemma says is that if these collection of matrices are not just any collection of $n \times n$ matrices but, rather, are special in that they are matrices of an *irreducible* representation of some group $G$, then $I_{n\times n}$ and its scalar multiples are the *only* matrices that commute with these matrices.

*Example 16.13* Consider the matrices

$$I_{2\times 2} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}. \tag{16.53}$$

Which matrices commute with $I_{2\times 2}$ and $A$? Let us define

$$B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{16.54}$$

and impose $AB = BA$. This then gives four equations for the four unknowns $a, b, c, d$. Well,

$$AB - BA = \begin{bmatrix} -b + 3c & -3a - 2b + 3d \\ a + 2c - d & b - 3c \end{bmatrix}. \tag{16.55}$$

Demanding that this vanish then gives that $b = 3c$ and $d = a + 2c$. Thus,

$$B = \begin{bmatrix} a & 3c \\ c & a + 2c \end{bmatrix} \text{ with } a, c \in \mathbb{C} \tag{16.56}$$

commutes with $I_{2\times 2}$ and $A$. In particular, choosing $a = c = 1$ gives

$$B = \begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix}, \tag{16.57}$$

which is certainly not proportional to the identity. Thus, we see that it is certainly possible to have a collection of matrices where some nonidentity matrix commutes with every matrix in that collection of matrices.

## 16.12 Orthogonality of Characters of Irreducible Representations

**Proposition 16.9** *Let $G$ be a finite group. Let $\rho : G \to GL(V)$ and $\rho' : G \to GL(V')$ be representations. Let $h : V \to V'$ be any linear map. Then consider the linear map $h^0 : V \to V'$ created from $h$ by "averaging over $G$" defined as*

$$h^0 = \frac{1}{|G|} \sum_{g\in G} \rho'_{g^{-1}} h \rho_g = \frac{1}{|G|} \sum_{g\in G} (\rho'_g)^{-1} h \rho_g.$$

$$\begin{tikzcd}
V \arrow[r, "\rho_g"] \arrow[d, "h^0"'] & V \arrow[d, "h"] \\
V' & V' \arrow[l, "(\rho'_g)^{-1}"]
\end{tikzcd}$$

*Then $h^0$ is $G$-linear.*

***Proof*** $h^0$ is $G$-linear because for any $x \in G$ we have

$$\begin{aligned}
\rho'_{x^{-1}} h^0 \rho_x &= \frac{1}{|G|} \sum_{g \in G} \rho'_{x^{-1}} \rho'_{g^{-1}} h \rho_g \rho_x \qquad (16.58)\\
&= \frac{1}{|G|} \sum_{g \in G} \rho'_{x^{-1}g^{-1}} h \rho_{gx}\\
&= \frac{1}{|G|} \sum_{g \in G} \rho'_{(gx)^{-1}} h \rho_{gx}\\
&= \frac{1}{|G|} \sum_{g \in G} \rho'_{g^{-1}} h \rho_g \qquad \text{(by Problem 16.1)}\\
&= h^0,
\end{aligned}$$

so that $h^0 \rho_x = \rho'_x h^0$. □

**Corollary 16.4** *Let $\rho, \rho'$ be irreducible representations. Then*

*i) If $\rho \not\cong \rho'$ then $h^0 = 0$.*
*ii) If $V = V'$ with* $\dim V = n$ *and $\rho = \rho'$ then $h^0 = \lambda I_{n \times n}$ where $\lambda = \frac{1}{n}$* Tr *$h$.*

***Proof*** i) If $\rho$ and $\rho'$ are irreducible then Schur's lemma requires $h^0 = 0$.
ii) If $\rho$ and $\rho'$ are irreducible then Schur's lemma requires $h^0 = \lambda I_{n \times n}$ for some scalar $\lambda$. Taking the trace of $h^0$ then gives

$$\begin{aligned}
\mathrm{Tr}(h^0) = \mathrm{Tr}(\lambda I_{n \times n}) = \lambda n &= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\rho_g^{-1} h \rho_g) \qquad (16.59)\\
&= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(h) = \mathrm{Tr}(h).
\end{aligned}$$

This gives $\lambda = \frac{1}{n} \mathrm{Tr}(h)$, as claimed. □

What's the idea behind all of this? Well, $h : V \longrightarrow V'$ was an arbitrary linear map. If we apply Schur's lemma and let $h : V \longrightarrow V'$ run through a bunch of simple linear maps, it seems like we will derive a lot of facts about or constraints on the *irreducible* (Why? Hint: What does Schur's lemma require?) representations $\rho$ and $\rho'$. Consider a finite group $G$ and a vector space $V$ over $\mathbb{C}$ with $\dim V = n$ and let $\rho, \rho'$ be irreducible representations. Let's switch from abstract linear maps and choose specific bases so that we may think of $\rho_g$ and $\rho'_g$ as matrices. Then,

i) If $\rho \not\cong \rho'$, $h^0 = 0_{n\times n}$ for any linear map $h : V \longrightarrow V'$. In particular, let us run through all linear maps where $h = \Theta^{(ab)}$ where $\Theta$ is defined to be nonzero only for $\Theta^{(ab)}_{ij} = 1$ if $i = a, j = b$ and $\Theta^{(ab)}_{ij} = 0$ if $i \neq a, j \neq b$. (Basically, we are running through all matrices where one of the entries is 1 and all the other entries are 0. $a$ and $b$ are labels for such matrices.)

$$\begin{aligned}(h^0)_{ij} = (0_{n\times n})_{ij} = 0 &= \frac{1}{|G|}\sum_{g\in G}\sum_k\sum_l (\rho'_{g^{-1}})_{ik}h_{kl}(\rho_g)_{lj} \\ &= \frac{1}{|G|}\sum_{g\in G}(\rho'_{g^{-1}})_{ia}(\rho_g)_{bj}\end{aligned} \tag{16.60}$$

for $a, b$ arbitrary. Let's box it to keep track of the important work.

$$\boxed{0 = \frac{1}{|G|}\sum_{g\in G}(\rho'_{g^{-1}})_{ia}(\rho_g)_{bj}} \tag{16.61}$$

for $a, b$ arbitrary.

ii) If $V = V'$ and $\rho = \rho'$, then $h^0 = \lambda I_{n\times n}$ for some scalar $\lambda$. Consider $h = \Theta^{(ab)}$ for arbitrary $a, b$. Then $\mathrm{Tr}(h) = \mathrm{Tr}(\Theta^{(ab)}) = \delta_{ab}$, where $\delta$ is the Kronecker delta function. Therefore, $\lambda = \frac{1}{n}\,\mathrm{Tr}(h) = \frac{1}{n}\delta_{ab}$ Then,

$$\begin{aligned}(h^0)_{ij} = (\lambda I_{n\times n})_{ij} = \frac{1}{n}\delta_{ab}\delta_{ij} &= \frac{1}{|G|}\sum_{g\in G}\sum_k\sum_l (\rho_{g^{-1}})_{ik}h_{kl}(\rho_g)_{lj} \\ &= \frac{1}{|G|}\sum_{g\in G}(\rho_{g^{-1}})_{ia}(\rho_g)_{bj}\end{aligned} \tag{16.62}$$

where $a, b$ are arbitrary. Let's box it to keep track of the important work.

$$\boxed{\frac{1}{n}\delta_{ab}\delta_{ij} = \frac{1}{|G|}\sum_{g\in G}(\rho_{g^{-1}})_{ia}(\rho_g)_{bj}} \tag{16.63}$$

for $a, b$ arbitrary.

Let's collect this work into a theorem.

**Theorem 16.8** *Schur orthogonality relations - Let $\rho : G \longrightarrow GL(V)$ and $\rho' : G \longrightarrow GL(V')$ be inequivalent irreducible representations. Let $n = \dim V$. Then*

*i)* $0 = \frac{1}{|G|}\sum_{g\in G}(\rho'_{g^{-1}})_{ia}(\rho_g)_{bj}$.

*ii)* $\frac{1}{n}\delta_{ab}\delta_{ij} = \frac{1}{|G|}\sum_{g\in G}(\rho_{g^{-1}})_{ia}(\rho_g)_{bj}$

***Proof*** See the discussion above. □

Here is an idea: There are a lot of indices floating around in the boxed equations. It seems like those formulas hold so much information that we can afford to simplify things a bit and still learn some nontrivial information. In particular, set $a = i$ and $b = j$ and sum over $i, j$ and recall that, by definition, $\mathrm{Tr}(\rho_x) = \chi(x)$ for all $x \in G$.

i) If $\rho \not\cong \rho'$, then

$$0 = \frac{1}{|G|} \sum_{g \in G} \chi'(g^{-1})\chi(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi'(g)}\chi(g), \tag{16.64}$$

where we have used Proposition 16.2.

ii) If $V = V'$ and $\rho = \rho'$, then

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})\chi(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\chi(g), \tag{16.65}$$

where we have used Proposition 16.2.

If we combine all of this together, we see that we have derived a nontrivial result. Before that, a definition.

**Definition 16.26** Let $G$ be a finite group. The inner product $(\phi|\psi)$ on characters of $G$ is defined as

$$(\phi|\psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}.$$

**Theorem 16.9** *Let $G$ be a finite group. Let $\rho : G \to GL(V)$ and $\rho' : G \to GL(V')$ be irreducible representations with $\dim V = n$ and $\dim V' = n'$. Then*

*i) If $\rho \not\cong \rho'$, then $0 = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)} = (\chi|\chi')$.*
*ii) If $V = V'$ and $\rho = \rho'$, then $1 = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = (\chi|\chi)$.*

This theorem says that characters of *irreducible* representations of a finite group $G$ form an orthonormal set under the inner product on characters.

**Definition 16.27** If $\rho : G \to GL(V)$ is an irreducible representation, its character is called an irreducible character.

**Proposition 16.10** *Let $G$ be a finite group. Let $R = \{r_1, \cdots, r_k\}$ be a set of representatives of the conjugacy classes of $G$. That is,*

$$[r_1], \cdots, [r_k]$$

*are the conjugacy classes of $G$. Then*

$$(\phi|\psi) = \frac{1}{|G|} \sum_{r \in R} |[r]| \cdot \phi(r)\overline{\psi(r)}.$$

***Proof*** This follows directly from the fact that characters are class functions (see Proposition 16.2). □

Proposition 16.10 along with the fact that characters are class functions explains why we choose to add a row called "size" to the character table (see Table 16.5 in Problem 16.26 for an example). Writing a row for the size of each conjugacy class later helps one during the evaluation of inner products of characters.

**Proposition 16.11** *If $\phi$ and $\psi$ are characters of a finite group $G$, then $(\phi|\psi) = (\psi|\phi)$.*

***Proof***

$$\begin{aligned}(\phi|\psi) &= \frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)} \qquad (16.66)\\ &= \frac{1}{|G|}\sum_{g\in G}\phi(g)\psi(g^{-1}) \quad \text{(by Proposition 16.2)}\\ &= \frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})\psi(g) \quad \text{(by Problem 16.1)}\\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\phi(g)}\psi(g)\\ &= (\psi|\phi).\end{aligned}$$

□

## 16.13 Characters Characterize Representations

**Theorem 16.10** *Let $\rho : G \to GL(V)$ be a representation of the group $G$ with character $\chi$. Let*

$$V \cong W_1 \oplus \cdots \oplus W_k$$

*where the $W_i$ are irreducible. Let $\rho' : G \to GL(V')$ be an irreducible representation with character $\chi'$. Then the number of $W_i$ that are isomorphic to $V'$ is $(\chi|\chi')$.*

***Proof*** Let $\chi^{(i)}$ be the character of the representation for $W_i$, for $i = 1, \cdots k$ in the decomposition of $V$. Then we have

$$\chi = \chi^{(1)} + \cdots + \chi^{(k)} \qquad (16.67)$$

$$\Rightarrow (\chi|\chi') = \sum_{j=1}^{k}(\chi^{(j)}|\chi') = \sum_{j=1}^{k}\begin{cases}1, & \text{if } V' \cong W_j.\\ 0, & \text{if } V' \ncong W_j.\end{cases} \qquad (16.68)$$

where we have used Theorem 16.9. □

**Corollary 16.5** *Let $\rho : G \to GL(V)$ and $\rho' : G \to GL(V')$ be representations. Then $\rho \cong \rho'$ (also sometimes written as $V \cong V'$) if and only if their characters are equal.*

***Proof*** Decompose $V$ and $V'$ as a direct sum of irreducibles. Let $\chi$ be the character of $\rho$ and $\chi'$ be the character of $\rho'$. Let $\psi : G \to GL(W)$ be any irreducible representation with character $\theta$.
$\Rightarrow$ If $\chi = \chi'$, then $(\chi|\theta) = (\chi'|\theta)$ so by Theorem 16.10, $W$ occurs the same number of times in the decomposition of $V$ and $V'$. $W$ was an arbitrary irreducible representation.
$\Leftarrow$ Let $W$ be an arbitrary irreducible representation and suppose the number of times $W$ occurs in $V$ and $V'$ is the same. We conclude that they are isomorphic (as vector spaces, see the clarifying note after Definition 16.10). □

Note: Theorems such as these are what we mean when we say "characters characterize representations." Knowing the character of a representation lets us know how it is composed of the irreducible representations of that group. Knowing the character of two representations lets us know if they are really "the same" representations or not.

Let's introduce a bit more notation. Let $\rho : G \to GL(V)$ be a representation of the group $G$ with character $\chi$. We will use the following notation:

$$mV = \underbrace{V \oplus \cdots \oplus V}_{m \text{ terms}} \tag{16.69}$$

$$m\rho = \underbrace{\rho \oplus \cdots \oplus \rho}_{m \text{ terms}} . \tag{16.70}$$

Now suppose $\rho : G \to GL(V)$ is an arbitrary representation. Decompose $V$ as a direct sum

$$V \cong W_1 \oplus \cdots \oplus W_k \tag{16.71}$$

where the $W_i$ are isomorphic copies of the vectors spaces of the irreducible representations. Let $N_{irr}$ be the number of (distinct) irreducible representations of $G$. Label these distinct representations (really, the vector spaces they act on) by $W_1, \cdots W_{N_{irr}}$ and label their characters $\chi^{(1)}, \cdots, \chi^{(N_{irr})}$, respectively. Then we can write

$$V \cong m_1 W_1 \oplus \cdots \oplus m_{N_{irr}} W_{N_{irr}}, \tag{16.72}$$

where $m_i \equiv (\chi|\chi^{(i)})$ and where we have used Theorem 16.10. Therefore, the character $\chi$ of $\rho : G \to GL(V)$ is

$$\chi = m_1 \chi^{(1)} + \cdots + m_{N_{irr}} \chi^{(N_{irr})} \tag{16.73}$$

$$\Rightarrow (\chi|\chi) = \sum_{j=1}^{N_{irr}} m_j^2, \tag{16.74}$$

where we have used Theorem 16.9. This equation leads to the following theorem.

**Theorem 16.11** *Let $\rho : G \to GL(V)$ be a representation of the group G with character $\chi$. Then $(\chi|\chi) > 0$ and $(\phi|\phi) = 1$ if and only if $\rho : G \to GL(V)$ is an irreducible representation.*

***Proof*** Using notation as above, we see from

$$(\chi|\chi) = \sum_{j=1}^{N_{irr}} m_j^2 \tag{16.75}$$

that $(\chi|\chi)$ is certainly positive. It is equal to 1 only if one of the $m_j$ is equal to 1 and all the others vanish. In that case, $V \cong W_r$ where $r$ is the index for which $m_r = 1$. □

Note: Theorem 16.11 is very convenient as it gives a criterion for checking whether a given representation is irreducible or not.

**Theorem 16.12** *Let $\rho : G \to GL(V)$ be an irreducible representation with degree n and character $\chi$. Then $\rho$ occurs in the regular representation n times. That is, if $\rho^{reg} : G \to GL(V^{reg})$ is the regular representation, then $V^{reg}$ contains n copies of V (up to vector space isomorphisms) in its decomposition into irreducible representations.*

***Proof*** The character of the regular representation of $G$ is (see Proposition 16.3)

$$\chi^{reg}(g) = \begin{cases} |G|, & \text{if } g = e, \\ 0, & \text{if } g \neq e. \end{cases} \tag{16.76}$$

Use Theorem 16.10 along with

$$(\chi^{reg}|\chi) = \frac{1}{|G|}\sum_g \chi^{reg}(g)\overline{\chi(g)} = \frac{1}{|G|}\chi^{reg}(e)\overline{\chi(e)} = \frac{1}{|G|}|G|\overline{n} = n. \tag{16.77}$$

□

**Corollary 16.6** *Let G be a finite group. Let $N_{irr}$ be the number of irreducible representations of G. Let $n_1, \cdots, n_{N_{irr}}$ be the degrees of these $N_{irr}$ irreducible representations. Then*

*i)* $\sum_{j=1}^{N_{irr}} n_j^2 = |G|$.
*ii)* $\sum_{j=1}^{N_{irr}} n_j \chi^{(j)}(g) = 0$ *for* $g \neq e$.

***Proof*** Let $\chi^{(1)}, \cdots, \chi^{(N_{irr})}$ be the characters of the $N_{irr}$ irreducible representations of $G$. By Theorem 16.12,

$$\chi^{reg} = \sum_{j=1}^{N_{irr}} n_j \chi^{(j)}. \tag{16.78}$$

i) Therefore, $\chi^{reg}(e) = \sum_{j=1}^{N_{irr}} n_j \chi^{(j)}(e) \Rightarrow |G| = \sum_{j=1}^{N_{irr}} n_j^2$, where we used $\chi^{reg}(e) = |G|$ and $\chi^{(j)}(e) = n_j$.

ii) Therefore, $\chi^{reg}(g) = \sum_{j=1}^{N_{irr}} n_j \chi^{(j)}(g) \Rightarrow 0 = \sum_{j=1}^{N_{irr}} n_j \chi^{(j)}(g)$, where we used $\chi^{reg}(g) = 0$ whenever $g \neq e$. □

**Theorem 16.13** *Let $N$ be a normal subgroup of a finite group $G$. Let $[G : N] = k$ and let $r_1, \cdots, r_k$ be coset representatives. That is,*

$$G = r_1 N \cup \cdots \cup r_k N. \tag{16.79}$$

*Let $\tilde{\rho} : G/N \to GL(V)$ be a representation. Let $f : G \to G/N$ be defined by $f(g) = gN$. Let $\rho$ be the lift of the representation $\tilde{\rho}$. That is, $\rho \equiv \tilde{\rho} \circ f : G \to GL(V)$. Then $\rho$ is an irreducible representation of $G$ if and only if $\tilde{\rho}$ is an irreducible representation of $G/N$.*

***Proof*** Let $\chi$ be the character of $\rho$ and let $\tilde{\chi}$ be the character of $\tilde{\rho}$. First, note that $\rho_g = \tilde{\rho}_{gN}$, so $\text{Tr}(\rho_g) = \text{Tr}(\tilde{\rho}_{gN})$. That is, $\chi(g) = \tilde{\chi}(gN)$. In particular, if $g \in r_i N$ for some $i$, then $g = r_i n$ for some $n \in N$. Then

$$\chi(g) = \tilde{\chi}(gN) = \tilde{\chi}(r_i n N) = \tilde{\chi}(r_i N) = \chi(r_i). \tag{16.80}$$

That is, all elements of $G$ in the same coset have the same character. Also,

$$\begin{aligned}(\chi|\chi) &= \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi(g)} \qquad (16.81)\\ &= \frac{1}{|G|}\sum_{i=1,\cdots,k}\sum_{n\in N} \chi(r_i n)\overline{\chi(r_i n)}\\ &= \frac{1}{|G|}\sum_{i=1,\cdots,k}\sum_{n\in N} \chi(r_i)\overline{\chi(r_i)}\\ &= \frac{|N|}{|G|}\sum_{i=1,\cdots,k} \chi(r_i)\overline{\chi(r_i)}\\ &= \frac{1}{[G:N]}\sum_{i=1,\cdots,k} \tilde{\chi}(r_i N)\overline{\tilde{\chi}(r_i N)}\\ &= (\tilde{\chi}|\tilde{\chi}).\end{aligned}$$

Thus, we see that $(\chi|\chi) = 1$ if and only if $(\tilde{\chi}|\tilde{\chi}) = 1$ so, by Theorem 16.11, $\rho$ is irreducible if and only if $\tilde{\rho}$ is irreducible. □

In the above, $(\chi|\chi)$ and $(\tilde{\chi}|\tilde{\chi})$ are inner products but over different groups. That is, $(\chi|\chi)$ has a sum over all elements in $G$ whereas $(\tilde{\chi}|\tilde{\chi})$ has a sum over all elements in $G/N$. Perhaps writing $(\chi|\chi)_G$ and $(\tilde{\chi}|\tilde{\chi})_{G/N}$ to serve as a reminder of this fact might prevent some future confusion. Let us rephrase the previous result in another way.

**Proposition 16.12** *If $\chi$ is a lift (or inflation) to $G$ of an irreducible character $\tilde{\chi}$, then $\chi$ is an irreducible character if and only if $\tilde{\chi}$ is an irreducible character.*

***Proof*** Above, we showed $(\chi|\chi)_G = (\tilde{\chi}|\tilde{\chi})_{G/N}$. They are either both equal to 1 and hence are irreducible characters, or not. □

## 16.14 Characters of Common Representations

This section collects theorems of characters of common representations and introduces a few new theorems.

**Proposition 16.13** *Let $G$ be a group. Let $\rho^{(1)} : G \to GL(V_1)$ and $\rho^{(2)} : G \to GL(V_2)$ be linear representations of $G$. Let $\chi^{(1)}$ and $\chi^{(2)}$ be their respective characters.*

*i) Let $\chi^{(\oplus)}$ be the character of $\rho^{(1)} \oplus \rho^{(2)}$. Then $\chi^{(\oplus)}(g) = \chi^{(1)}(g) + \chi^{(2)}(g)$ for any $g \in G$.*
*ii) Let $\chi^{(\otimes)}$ be the character of $\rho^{(1)} \otimes \rho^{(2)}$. Then $\chi^{(\otimes)}(g) = \chi^{(1)}(g)\chi^{(2)}(g)$ for any $g \in G$.*[2]

***Proof*** i) Choose a basis of $V_1 \oplus V_2$ so that

$$\rho_g^{(1)} \oplus \rho_g^{(2)} = \begin{array}{ccc} V_1 & V_2 & \\ \rho_g^{(1)} & \mathbf{0} & V_1 \\ \mathbf{0} & \rho_g^{(2)} & V_2 \end{array} \tag{16.82}$$

Clearly, $\mathrm{Tr}(\rho_g^{(1)} \oplus \rho_g^{(2)}) = \mathrm{Tr}(\rho_g^{(1)}) + \mathrm{Tr}(\rho_g^{(2)})$.

ii) This was proved at the end of Section 16.8. We copy the final lines of the proof here:

$$\begin{aligned} \mathrm{Tr}(\rho_g^{(1)} \otimes \rho_g^{(2)}) &= \sum_{k=1}^{m}\sum_{l=1}^{n} \left((\rho_g^{(1)} \otimes \rho_g^{(2)})\right)_{kl,kl} \\ &= \sum_{k=1}^{m}\sum_{l=1}^{n} \left(\rho_g^{(1)}\right)_{kk} \left(\rho_g^{(2)}\right)_{ll} \\ &= \mathrm{Tr}(\rho_g^{(1)})\,\mathrm{Tr}(\rho_g^{(2)}). \end{aligned} \tag{16.83}$$

**Proposition 16.14** *Let $G_1$ and $G_2$ be groups. Let $\rho^{(1)} : G_1 \to GL(V_1)$ and $\rho^{(2)} : G_2 \to GL(V_2)$ be linear representations of $G_1$ and $G_2$, respectively. Let $\chi^{(1)}$*

[2] Some books write $\chi^{(\otimes)} = \chi^{(1)}\chi^{(2)}$, where it is understood that this does not mean function composition of $\chi^{(1)}$ and $\chi^{(2)}$ but instead their products after evaluating them for a given $g \in G$. That is, $\chi^{(\otimes)} = \chi^{(1)}\chi^{(2)}$ means $\chi^{(\otimes)}(g) = \chi^{(1)}(g)\chi^{(2)}(g)$ for any $g \in G$.

*and $\chi^{(2)}$ be their respective characters. Let $\chi^{(\times)}$ be the character of $\rho^{(1)} \times \rho^{(2)} : G_1 \times G_2 \longrightarrow GL(V_1 \times V_2)$. Then $\chi^{(\times)}((g_1, g_2)) = \chi^{(1)}(g_1)\chi^{(2)}(g_2)$ for any $(g_1, g_2) \in G_1 \times G_2$.*[3]

***Proof*** The derivation/proof is similar to that of direct products and is omitted. □

**Proposition 16.15** *Use notation as in Proposition 16.14. If $\rho^{(1)}$ and $\rho^{(2)}$ are irreducible representations, then $\rho^{(1)} \times \rho^{(2)}$ is an irreducible representation on $G_1 \times G_2$.*

***Proof*** If $\rho^{(1)}$ and $\rho^{(2)}$ are irreducible, then

$$\frac{1}{|G_1|} \sum_{g_1} |\chi^{(1)}(g_1)|^2 = 1, \tag{16.84}$$

$$\frac{1}{|G_2|} \sum_{g_2} |\chi^{(2)}(g_2)|^2 = 1. \tag{16.85}$$

by Theorem 16.11. Therefore,

$$\frac{1}{|G_1|} \sum_{g_1} |\chi^{(1)}(g_1)|^2 \frac{1}{|G_2|} \sum_{g_2} |\chi^{(2)}(g_2)|^2 = 1, \tag{16.86}$$

$$\Rightarrow \frac{1}{|G_1| \cdot |G_2|} \sum_{g_1, g_2} |\chi^{(\times)}((g_1, g_2))|^2 = 1. \tag{16.87}$$

By Theorem 16.11, $\rho^{(1)} \times \rho^{(2)}$ is irreducible. □

**Proposition 16.16** *Let $G$ be a group. Let $\rho : G \longrightarrow GL(V)$ be linear representations of $G$. Let $\chi$ its character. Consider the $\rho \otimes \rho$ representation on $V \otimes V$. Recall that $V \otimes V = Sym^{(2)}(V) \oplus Alt^{(2)}(V)$. Recall that $\rho \otimes \rho$ restricted to $Sym^{(2)}(V)$ and $Alt^{(2)}(V)$ is $G$-stable.*

*i) Let $\chi^{(2)}_{Sym}$ be the character of $\rho \otimes \rho$ restricted to $Sym^{(2)}(V)$. Then*

$$\chi^{(2)}_{Sym}(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$$

*for any $g \in G$.*

*ii) Let $\chi^{(2)}_{Alt}$ be the character of $\rho \otimes \rho$ restricted to $Alt^{(2)}(V)$. Then*

$$\chi^{(2)}_{Alt}(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

*for any $g \in G$.*

[3] Some books write $\chi^{(\times)} = \chi^{(1)}\chi^{(2)}$, where it is understood that this does not mean function composition of $\chi^{(1)}$ and $\chi^{(2)}$ but instead their products after evaluating them for a given $(g_1, g_2) \in G_1 \times G_2$. That is, $\chi^{(\times)} = \chi^{(1)}\chi^{(2)}$ means $\chi^{(\times)}((g_1, g_2)) = \chi^{(1)}(g_1)\chi^{(2)}(g_2)$ for any $(g_1, g_2) \in G_1 \times G_2$.

*iii)* $\chi^{(2)}_{Sym}(g) + \chi^{(2)}_{Alt}(g) = \chi(g)^2$ *for any* $g \in G$.

***Proof*** Fix $g \in G$. WLOG, suppose that $\rho_g$ is unitary. Choose an eigenbasis so that $\rho_g$ is diagonal. Then $\rho_g \mathbf{e}_i = \lambda_i \mathbf{e}_i$ where $\lambda_i \in \mathbb{C}$. Therefore, $\chi(g) = \mathrm{Tr}(\rho_g) = \sum_i \lambda_i$ while $\chi(g^2) = \mathrm{Tr}(\rho_{g^2}) = \mathrm{Tr}(\rho_g \rho_g) = \sum_i \lambda_i^2$.

i) Recall that a basis for $\mathrm{Sym}^{(2)}(V)$ is $\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i$ with $i \leq j$. These are also an eigenbasis for $\mathrm{Sym}^{(2)}(V)$ with eigenvalues $\lambda_i \lambda_j$ since

$$(\rho_g \otimes \rho_g)(\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i) = \lambda_i \lambda_j (\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i). \tag{16.88}$$

The trace is the sum of the eigenvalues. Therefore,

$$\begin{aligned} \chi^{(2)}_{\mathrm{Sym}}(g) &= \sum_{i \leq j} \lambda_i \lambda_j = \sum_i \lambda_i^2 + \sum_{i<j} \lambda_i \lambda_j \\ &= \sum_i \lambda_i^2 + \frac{1}{2} \sum_{i \neq j} \lambda_i \lambda_j = \sum_i \lambda_i^2 + \frac{1}{2}((\sum_i \lambda_i)^2 - \sum_i \lambda_i^2) \\ &= \frac{1}{2}(\sum_i \lambda_i)^2 + \frac{1}{2} \sum_i \lambda_i^2 \\ &= \frac{1}{2}\chi(g)^2 + \frac{1}{2}\chi(g^2). \end{aligned} \tag{16.89}$$

ii) Recall that a basis for $\mathrm{Alt}^{(2)}(V)$ is $\mathbf{e}_i \otimes \mathbf{e}_j - \mathbf{e}_j \otimes \mathbf{e}_i$ with $i < j$. These are also an eigenbasis for $\mathrm{Alt}^{(2)}(V)$ with eigenvalues $\lambda_i \lambda_j$ since

$$(\rho_g \otimes \rho_g)(\mathbf{e}_i \otimes \mathbf{e}_j - \mathbf{e}_j \otimes \mathbf{e}_i) = \lambda_i \lambda_j (\mathbf{e}_i \otimes \mathbf{e}_j - \mathbf{e}_j \otimes \mathbf{e}_i). \tag{16.90}$$

The trace is the sum of the eigenvalues. Therefore,

$$\begin{aligned} \chi^{(2)}_{\mathrm{Alt}}(g) &= \sum_{i<j} \lambda_i \lambda_j = \frac{1}{2} \sum_{i \neq j} \lambda_i \lambda_j = \frac{1}{2}(\sum_i \lambda_i)^2 - \frac{1}{2} \sum_i \lambda_i^2 \\ &= \frac{1}{2}\chi(g)^2 - \frac{1}{2}\chi(g^2). \end{aligned} \tag{16.91}$$

iii) This follows from the previous two parts.

$$\begin{aligned} \chi^{(2)}_{\mathrm{Sym}}(g) + \chi^{(2)}_{\mathrm{Alt}}(g) &= \frac{1}{2}\chi(g)^2 + \frac{1}{2}\chi(g^2) + \frac{1}{2}\chi(g)^2 - \frac{1}{2}\chi(g^2) \\ &= \chi(g)^2. \end{aligned} \tag{16.92}$$

This makes sense since $\mathrm{Sym}^{(2)}(V) \oplus \mathrm{Alt}^{(2)}(V) = V \otimes V$. □

## 16.15 Number of Inequivalent Irreducible Representations of Finite Groups

Recall that a class function is a function $f : G \to \mathbb{C}$ such that $f(g) = f(hgh^{-1})$ for any $g, h \in G$.

**Definition 16.28** Let $C(G)$ be the set of all class functions on $G$. That is,

$$C(G) = \{f : G \to \mathbb{C} \mid f(g) = f(hgh^{-1}), \forall g, h \in G\}. \tag{16.93}$$

Theorem 16.9 shows that the characters of irreducible representations of a finite group $G$ form an orthonormal set of functions in $C(G)$. Actually, they are not just orthonormal in $C(G)$, but they also span $C(G)$. That is, any class function on $G$ can be written as a linear combination of the irreducible characters of $G$. Let us work to prove these claims.

**Theorem 16.14** *Let $G$ be a finite group and let $\rho : G \to GL(V)$ be a representation of $G$. Let $f$ be a class function on $G$. Construct a linear map $R_f : V \to V$ defined by*

$$R_f = \frac{1}{|G|} \sum_{g \in G} f(g)\rho_g. \tag{16.94}$$

*Let $n = \dim V$ and let $\chi$ be the character of $\rho$. If $\rho : G \to GL(V)$ is an irreducible representation, then $R_f$ is proportional to the identity map. In particular,*

$$R_f = \frac{1}{n}(f|\overline{\chi})I_{n\times n}. \tag{16.95}$$

***Proof*** Consider $\rho_h^{-1} R_f \rho_h$ for any $h \in G$. Then

$$\begin{aligned} \rho_h^{-1} R_f \rho_h &= \frac{1}{|G|} \sum_{g \in G} f(g)\rho_h^{-1}\rho_g\rho_h \\ &= \frac{1}{|G|} \sum_{g \in G} f(g)\rho_{h^{-1}gh} \\ &= \frac{1}{|G|} \sum_{g \in G} f(hgh^{-1})\rho_{h^{-1}gh} \\ &= R_f, \end{aligned} \tag{16.96}$$

where third equality holds because $f$ is a class function. Therefore, $R_f \rho_h = \rho_h R_f$ for any $h \in G$. By Schur's lemma (see Lemma 16.1), $R_f = \lambda I_{n\times n}$ for some constant $\lambda \in \mathbb{C}$. Taking the trace of both sides, we see that $\mathrm{Tr}(R_f) = n\lambda$. But

$$\mathrm{Tr}(R_f) = \frac{1}{|G|} \sum_{g \in G} f(g)\,\mathrm{Tr}(\rho_g) = \frac{1}{|G|} \sum_{g \in G} f(g)\chi(g) = (f|\overline{\chi}). \tag{16.97}$$

Therefore, $\lambda = \frac{1}{n}\operatorname{Tr}(R_f) = \frac{1}{n}(f|\overline{\chi})$ so $R_f = \frac{1}{n}(f|\overline{\chi})I_{n\times n}$. □

With this, we have enough information to prove that the irreducible characters of a finite group $G$ form an orthonormal basis of $C(G)$.

**Theorem 16.15** *Let $N_{irr}$ be the number of inequivalent irreducible representations of a finite group $G$. Let $\rho^{(1)} : G \to GL(V^{(1)}), \cdots, \rho^{(N_{irr})} : G \to GL(V^{(N_{irr})})$ be the irreducible representations of $G$. Let $\chi^{(1)}, \cdots, \chi^{(N_{irr})}$ be the characters of those irreducible representations. Then $\chi^{(1)}, \cdots, \chi^{(N_{irr})}$ form an orthonormal basis of $C(G)$.*

***Proof*** Theorem 16.9 shows that the characters of irreducible representations of a finite group $G$ forms an orthonormal set of functions in $C(G)$. We must show that any class function can be written as a linear combination of the irreducible characters. Suppose otherwise. Suppose there exists a function $f \in C(G)$ which has no components of the irreducible characters. That is, suppose $(f|\overline{\chi}^{(i)}) = 0$ for $i = 1, \cdots, N_{irr}$. Construct the functions $R_f^{(i)} = \frac{1}{|G|}\sum_{g\in G} f(g)\rho_g^{(i)}$ for $i = 1, \cdots, N_{irr}$. Applying this to all the irreducible representations, we conclude that $R_f^{(i)} = 0$ for all irreducible representations $i = 1, \cdots, N_{irr}$. Any other (finite-dimensional) representation is isomorphic to a direct sum of irreducible representations (see Theorem 16.4). Therefore, $R_f = 0$ for any (finite-dimensional) representation used to construct $R_f$. Consider the regular representation $\rho^{(reg)} : G \to GL(V^{(reg)})$ and construct $R_f^{(reg)} = \frac{1}{|G|}\sum_{g\in G} f(g)\rho_g^{(reg)}$. Then

$$0 = R_f^{(reg)}\mathbf{e}_e = \frac{1}{|G|}\sum_{g\in G} f(g)\rho_g^{(reg)}\mathbf{e}_e = \frac{1}{|G|}\sum_{g\in G} f(g)\mathbf{e}_g. \tag{16.98}$$

By construction in the regular representation, $\{\mathbf{e}_g \mid g \in G\}$ is a basis of $V^{(reg)}$. Therefore, $f(g) = 0$ for all $g \in G$. Thus, any function in $C(G)$ can be written as a linear combination of irreducible characters. □

**Theorem 16.16** *The number of conjugacy classes of a finite group $G$ is equal to the number of inequivalent irreducible representations of $G$.*

***Proof*** Let $[g_1], \cdots, [g_k]$ be the distinct conjugacy classes of $G$. Any function in $C(G)$ is determined by its value of these $k$ conjugacy classes. That is, $k$ numbers completely determine any conjuacy class function. The dimension of $C(G)$ is therefore $k$. However, Theorem 16.15 says that the dimension of $C(G)$ is $N_{irr}$, the number of inequivalent irreducible representations of $G$. Therefore, $k = N_{irr}$. The number of conjugacy classes of $G$ is equal to the number of inequivalent irreducible representations of $G$. □

As a mnemonic, the above theorem can be thought of as: "character tables are square." It is square in the sense that the number columns listing the conjugacy classes is equal to the number of rows listing the irreducible characters. Of course, one may also add a row at the very top for the sizes of the conjugacy classes and a column or two in other conventions, but the mnemonic is helpful for getting the gist of the above theorem.

**Theorem 16.17** *Let $G$ be a finite group. Let $|[s]|$ be the number of elements in the conjugacy class $[s]$. Then*

*i)* $\sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(s) = |G|/|[s]|$.
*ii) If $t \in G$ is not conjugate to $s$, then*

$$\sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(t) = 0. \tag{16.99}$$

***Proof*** Let $\Pi_s$ be a conjugacy class function that is equal to 1 on the conjugacy class $[s]$ and 0 otherwise. Since it is a class function, we can, according to Theorem 16.15, write it as

$$\Pi_s = \sum_{i=1}^{N_{irr}} \lambda_i \chi^{(i)} \tag{16.100}$$

for some $\lambda_i$. In fact, $\lambda_i = (\Pi_s|\chi^{(i)}) = \frac{|[s]|}{|G|}\overline{\chi^{(i)}(s)}$ (why?). Then for any $t \in G$, we find

$$\Pi_s(t) = \frac{|[s]|}{|G|} \sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(t). \tag{16.101}$$

By considering the case where $t$ belongs to $[s]$ or not, the previous equation proves both claims:

- If $t$ is conjugate to $s$, then $\Pi_s(t) = 1$ so

$$\begin{aligned} 1 &= \frac{|[s]|}{|G|} \sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(t), \\ \Rightarrow \frac{|G|}{|[s]|} &= \sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(t). \end{aligned} \tag{16.102}$$

- If $t$ is not conjugate to $s$, then $\Pi_s(t) = 0$ so

$$\begin{aligned} 0 &= \frac{|[s]|}{|G|} \sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(t), \\ \Rightarrow 0 &= \sum_{i=1}^{N_{irr}} \overline{\chi^{(i)}(s)}\chi^{(i)}(t). \end{aligned} \tag{16.103}$$

## 16.16 Irreducible Representations of Abelian Groups

**Theorem 16.18** *Let $G$ be a finite or infinite abelian group. Let $\rho : G \longrightarrow GL(V)$ be a representation. Let* $\dim V$ *be finite. If $\rho$ is an irreducible representation then* $\dim V = 1$.

***Proof*** This is Problem 16.21. You are asked to prove this using Schur's lemma. □

We can prove a stronger statement if the group $G$ is finite.

**Theorem 16.19** *A finite group $G$ is abelian if and only if all the irreducible representations of $G$ have degree 1.*

***Proof*** Let $N_{conj}$ be the number of conjugacy classes of $G$. Let $n_1, \cdots, n_{N_{conj}}$ be the degrees of the irreducible representations of $G$. Note that $n_1, \cdots, n_{N_{conj}}$ are positive integers. In abelian groups, every element is in its own conjugacy class. Therefore, $N_{conj} = |G|$ for finite abelian groups. We know that $|G| = n_1^2 + \cdots + n_{N_{conj}}^2$ (see Corollary 16.6). This is possible if and only if $n_i = 1$ for $i = 1, \cdots, N_{conj}$. □

The above theorem required $G$ to be a finite group. See Problem 16.21 for another proof that any irreducible representation of an abelian group has degree 1, but where $G$ doesn't have to be a finite group ($\dim V$ is still assumed to be finite, though).

**Theorem 16.20** *Let $G$ be a finite group. Let $A$ be an abelian subgroup of $G$. Each irreducible representation of $G$ has degree at most* $[G : A] = |G|/|A|$.

***Proof*** Let $\rho : G \longrightarrow GL(V)$ be an irreducible representation of $G$. Let $\theta : A \longrightarrow GL(V)$ be the restriction of $\rho$ to the subgroup $A$. Then clearly $\theta$ is a representation of $A$. Let $W \subseteq V$ be an irreducible subrepresentation of $V$ (see Definition 16.13 if a reminder is necessary). By Theorem 16.19, $\dim W = 1$. Let us define a subspace of $V$ as follows:

$$V' = \bigcup_{g \in G} \rho_g W. \tag{16.104}$$

$V'$ is clearly $G$-stable. Since $\rho$ is an irreducible representation, it must be that $V' = V$. This fact lets us put a bound on the dimension of $V$. Since $\dim W = 1$, it is also true that $\dim \rho_g W = 1$ for any $g \in W$. It would be incorrect to say that, therefore, $\dim V = |\bigcup_{g \in G} \rho_g W| = |G|$. For example, the vector subspace $\rho_g W$ could be the same for some $g \in G$. In fact, $\rho_g W$ depends only on the left coset of $A$ in $G$. Let $g = ra$, where $r \in G$ and $a \in A$. Then $\rho_g W = \rho_{ra} W = \rho_r \rho_a W = \rho_r W$, where the last equality is because $W$ is $A$-stable since it is a subrepresentation of $V$ for the representation $\theta : A \longrightarrow GL(V)$. Let $k = [G : A]$. Pick coset representatives $r_1, \cdots, r_k$ for the left cosets of $A$ in $G$. That is,

$$r_1 A, \cdots, r_k A \tag{16.105}$$

are the $k$ (distinct) left cosets of $A$ that form a partition of the group $G$. Then

$$V = \bigcup_{g \in G} \rho_g W = \bigcup_{j=1}^{k} \rho_{r_j} W. \tag{16.106}$$

It would be incorrect to say that, therefore, $\dim V = k = [G : A]$. For example, for some representations it might be that $\rho_e = I$ and $\rho_{r_i} = I$ for some coset representative $r_i$. In such a case, $\rho_e W = \rho_{r_i} W$. The best case scenario is that $\rho_{r_i} W \neq \rho_{r_j} W$ for $i \neq j$, but this is not guaranteed. Therefore, the best we can say from this work is that $\dim V \leq k = [G : A] = |G|/|A|$. □

*Example 16.14* Let $G = D_n$ for $n \geq 3$. Let $A = \langle r \rangle$. Then $A$ is an abelian subgroup of $D_n$ with $[D_n : \langle r \rangle] = 2$. By the previous theorem, all the irreducible representations of $D_n$ are at most degree 2. Since $D_n$ is not an abelian group, this means that $D_n$ has at least one irreducible representation of degree 2 (if it didn't, it would be an abelian group according to Theorem 16.19).

*Example 16.15* Let $G = Q_8$. Let $A = \langle -1 \rangle$. Then $A$ is an abelian subgroup of $Q_8$ with $[Q_8 : \langle -1 \rangle] = 4$. By the previous theorem, all the irreducible representations of $Q_8$ are at most degree 4. Since $Q_8$ is not an abelian group, this means that $Q_8$ has at least one irreducible representation of degree 2, 3, or 4 (if it didn't, it would be an abelian group according to Theorem 16.19).

## Further Reading

1. Serre, Jean-Pierre (1977) Linear Representations of Finite Groups.
2. Steinberg, Benjamin (2012) Representation Theory of Finite Groups: An Introductory Approach (Universitext).
3. Zee, Anthony (2016) Group Theory in a Nutshell for Physicists.

## Problems

**16.1** Let $G$ be a finite group and $f$ a function on the elements of $G$. Prove that

$$\sum_{g \in G} f(g) = \sum_{g \in G} f(g^{-1}) = \sum_{g \in G} f(gh) = \sum_{g \in G} f(hg) = \sum_{g \in G} f(hgh^{-1})$$

for any $h \in G$. This is sometimes called a rearrangement lemma.

**16.2** Let $\rho : G \longrightarrow GL(V)$ be a representation with degree $n < \infty$. For simplicity, consider $\rho_g$ as an $n \times n$ matrix for each $g \in G$. Show that $\tilde{\rho} \equiv (\rho_{g^{-1}})^T$ is also a representation, where the superscript $T$ denotes the transpose of the matrix.

**16.3** Let $\rho : G \longrightarrow GL_n(\mathbb{C})$ be a representation.

a) Show that setting $\psi_g = \overline{\rho_g}$ provides a representation $\rho : G \longrightarrow GL_n(\mathbb{C})$. It is called the conjugate representation. Give an example showing that $\psi$ and $\rho$ do not have to be equivalent.

b) Let $\phi : G \longrightarrow \mathbb{C}^{\times}$ be a degree-1 representation of $G$. Define a map $\rho^{\phi} : G \longrightarrow GL_n(\mathbb{C})$ by $\rho^{\phi}_g = \phi_g \rho_g$. Show that $\rho^{\phi}$ is a representation. Give an example showing that $\rho$ and $\rho^{\phi}$ do not have to be equivalent.

**16.4** Let $G$ be a finite group. Let $\rho : G \longrightarrow GL(V)$ be a representation. Let $\chi$ be the character of $G$. How many copies of the trivial representation does $\rho$ contain?

**16.5** Let $G$ be a finite group and let $\chi$ be the character of any nontrivial irreducible representation of $G$. Show that $\sum_{g \in G} \chi(g) = 0$.

**16.6** Show that $f : G \longrightarrow \mathbb{C}$ is a class function (that is, $f(g) = f(hgh^{-1})$ for any $g, h \in G$) if and only if $f(gh) = f(hg)$ for any $g, h \in G$.

**16.7** Let $G$ be a finite group and let $\chi$ be a character of a finite degree representation of $G$ such that $\chi(g) = 0$ for $g \neq e$. Show that $\chi$ is an integer multiple of the character $\chi^{reg}$ of the regular representation of $G$. That is, show that $\chi(g) = \lambda \cdot \chi^{reg}(g)$ for any $g \in G$ where $\lambda \in \mathbb{Z}$ (actually, $\lambda \in \mathbb{N}$).

**16.8** Let $G$ be a finite group.

a) Let $s \in G$. Show that $\chi(s) \in \mathbb{R}$ (that is, $\chi(s) = \overline{\chi(s)}$) for any irreducible character $\chi$ if and only if $s$ is conjugate to $s^{-1}$. (Hint: The following is incorrect (why? Hint: What if $\chi$ is the trivial character?): "If $\chi(s) = \chi(s^{-1})$ then, since characters are class functions, $s$ and $s^{-1}$ are conjugate.")

b) Conclude that $\chi(s) = \overline{\chi(s)}$ for any character $\chi$ of $G$ (irreducible or not) if and only if $s$ is conjugate to $s^{-1}$.

Such characters are sometimes called real characters.

**16.9** Let a finite group $G$ act on itself by conjugation. Find the character of this permutation representation.

**16.10** Let $\rho : G \longrightarrow GL_3(\mathbb{C})$ be a representation of a finite group. Show that $\rho$ is irreducible if and only if there is no common eigenvector for the matrices $\rho_g$ with $g \in G$.

**16.11** a) Find four degree-1 representations of $D_4$. Make a $4 \times 8$ table with the eight $g \in D_4$ across the top and the values $\rho_g$ in the body. Please put $e$ on the left, and place group elements in the same conjugacy class next to each other. (Hint: What is the smallest $H \trianglelefteq D_4$ such that $D_4/H$ is abelian? You want the smallest $H \trianglelefteq D_4$ with $D_4/H$ abelian because then $D_4/H$ has the largest possible order.)

b) Let $\mathbb{R}^2$ have the standard basis $\{\mathbf{e}_1, \mathbf{e}_2\}$. As usual with $D_4$, let $r$ rotate the plane 90° counterclockwise, and let $s$ be the reflection that fixes $\mathbf{e}_1$ and sends $\mathbf{e}_2 \mapsto -\mathbf{e}_2$. This defines a degree-2 representation $\rho$ of the abstract group $D_4 = \langle r, s \rangle$. Write down the $2 \times 2$ matrices[4] $\rho_g$ for all $g \in D_4$.

[4] Our convention is to define representations over $\mathbb{C}$. The $2 \times 2$ matrices are in $GL_2(\mathbb{R})$, but we can simply regard them as elements of $GL_2(\mathbb{C})$. For this problem, $\mathbb{R}$ is used for easier visualization of what is happening, but really it should be $\mathbb{C}$.

c) Argue that the degree-2 representation in the previous part is irreducible. (Hint: What are the subspaces that are stable under $s$? Are all of those subspaces stable under $r$? This idea is similar to using Theorem 16.5.)

Remark: $D_4$ has five conjugacy classes and we have found five irreducible representations. Therefore, we have found all of the irreducible representations (see Theorem 16.15). Theorem 16.4 implies that *every* finite degree representation of $D_4$ over $\mathbb{C}$ decomposes as a direct sum of copies of the five representations in a) and b).

**16.12** a) Find four degree-1 representations of $Q_8$. Make a $4 \times 8$ table with the eight $g \in Q_8$ across the top and the values $\rho_g$ in the body. Please put $e$ on the left, and place group elements in the same conjugacy class next to each other. (Hint: What is the smallest $H \trianglelefteq Q_8$ such that $Q_8/H$ is abelian? You want the smallest $H \trianglelefteq Q_8$ with $Q_8/H$ abelian because then $Q_8/H$ has the largest possible order.)

b) Argue that Problem 9.7 can be used to construct a degree-2 representation of $Q_8$. Write down the 2-by-2 matrices $\rho(g)$ for all $g \in Q_8$.

c) Argue that the degree-2 representation in the previous part is irreducible. (Hint: What are the subspaces that are stable under $i$? Are all of those subspaces stable under $j$? This idea is similar to using Theorem 16.5.)

Remark: $Q_8$ has five conjugacy classes and we have found five irreducible representations. Therefore, we have found all of the irreducible representations (see Theorem 16.15). Theorem 16.4 implies that *every* finite degree representation of $Q_8$ over $\mathbb{C}$ decomposes as a direct sum of copies of the five representations in a) and b).

**16.13** Let $G$ act on a finite set $X$. Let $\rho$ be the permutation representation associated with this action on $X$. (See Definition 16.4)

a) Show that, for all $g \in G$, the trace of $\rho_g$ (that is, character of $g$) equals the number of elements of $X$ that are fixed by $g$.

b) Complete this sentence: the trace in part a) is equal to the number of orbits of $\langle g \rangle$'s action on $X$ that ______________.

c) As a special case, let $G$ act on itself by left multiplication, as in Cayley's Theorem. The associated $\rho$ is called the regular representation of $G$. Find $\mathrm{Tr}(\rho_g)$ for all $g \in G$. (See Definition 16.3)

**16.14** Let $G = \langle a, b \rangle$, where $a$ and $b$ are independent commuting elements of order 3 (so $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$). Let $\omega = e^{2\pi i/3}$. Make a table of all nine degree-1 representations of $G$. The table will have 9 rows and 9 columns, with the columns labeled $e, a, a^2, b, ab, a^2b, b^2, ab^2, a^2b^2$. (Hint: Each representation is the product of a representation of $\langle a \rangle$ and a representation on $\langle b \rangle$.)

**16.15** Let $G = \mathbb{Z}_8 \times \mathbb{Z}_5$. Show that there is a unique degree-1 representation $\rho : G \to \mathbb{C}^\times$ with $\rho_{(1\ 2)} = e^{2\pi i/40}$. Give an expression for $\rho_{(a\ b)}$ for all $0 \le a < 8$ and $0 \le b < 5$. (Hint: There are a few ways to do this. If you are out of ideas, see Example 6.3 but simplify the formula as much as you can (for example, two modulo operations that can be combined into one).)

**16.16** This problem looks at the invariant scalar product. We consider two inner products on $\mathbb{R}$. The first is the standard dot product (consider vectors as column matrices)

$$\mathbf{x}\cdot\mathbf{y} = \mathbf{x}^T \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{y} = x_1y_1 + x_2y_2,$$

and the second is

$$(\mathbf{v}, \mathbf{w}) = \mathbf{v}^T A\mathbf{w}$$

where $A$ is a symmetric positive-definite $2 \times 2$ matrix that we will define.

a) For $g \in GL_2(\mathbb{R})$, show that $(g\mathbf{v}, g\mathbf{w}) = \mathbf{v}^T g^T Ag\mathbf{w}$. State the analogue for $g\mathbf{x}\cdot g\mathbf{y}$. From now on, let $G = S_3$. Let $\rho : G \longrightarrow GL_3(\mathbb{R})$ be the permutation representation of $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. We have shown in Example 16.7 that $\mathbb{R}^3 \cong W \oplus W^\perp$ as an orthogonal direct sum under the standard dot product. $W$ is the line spanned by $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}_e$ and $W^\perp = \{(x, y, z) \mid x + y + z = 0\}$. We also wrote down a basis $\{\mathbf{f}_1, \mathbf{f}_2\}$ of $W^\perp$ and started to work out $\rho_g^{W^\perp}$ for $g \in S_3$ as $2 \times 2$ matrices with respect to this basis.

b) Compute

$$A = \frac{1}{|G|} \sum_{g\in G} (\rho_g^{W^\perp})^T \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\rho_g^{W^\perp}).$$

Then $(\mathbf{v}, \mathbf{w})$ is an invariant scalar product.

c) Define $||\mathbf{v}||_A = \sqrt{(\mathbf{v}, \mathbf{v})}$, the $A$-length of $\mathbf{v}$. We have seen that the three vectors $\begin{bmatrix} 1 \\ 0 \end{bmatrix}_f, \begin{bmatrix} 0 \\ 1 \end{bmatrix}_f, \begin{bmatrix} -1 \\ -1 \end{bmatrix}_f$ are permuted by this representation. Find their $A$-lengths and show they're all the same.

d) Define the $A$-angle $\theta_A$ by $(\mathbf{v}, \mathbf{w}) = ||\mathbf{v}||_A||\mathbf{w}||_A \cos\theta_A$. Show that the three vectors in c) are all 120° away from each other in $A$-angle.

e) Using the $\rho_g^{W^\perp}$ found in the previous parts, calculate the character of $\rho^{W^\perp}$, call it std for standard. Together with the trivial representation and the sign representation, conclude that the character table of $S_3$ is as shown in Table 16.2.

By the way, since $D_3 \cong S_3$ from this problem one can conclude that the character table for $D_3$ is as shown in Table 16.3.

**16.17** Let $F$ be a field. Endow the vector space $F^n$ with the standard basis $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$. Identify the linear maps $F^n \longrightarrow F^m$ with the $m \times n$ matrices acting on column vectors.

Table 16.2: Character table of $S_3$.

| size | 1 | 3 | 2 |
|---|---|---|---|
| class | $e$ | (••) | (• • •) |
| triv | 1 | 1 | 1 |
| sgn | 1 | −1 | 1 |
| std | 2 | 0 | −1 |

Table 16.3: Character table of $D_3$.

| size | 1 | 3 | 2 |
|---|---|---|---|
| class | $e$ | $s$ | $r$ |
| $\chi^{(1)}$ | 1 | 1 | 1 |
| $\chi^{(2)}$ | 1 | −1 | 1 |
| $\chi^{(3)}$ | 2 | 0 | −1 |

a) Show that the set of all linear maps $F^n \longrightarrow F^m$ is a vector space over $F$. It is denoted $\mathrm{Hom}(F^n, F^m)$. Show that the space has dimension $mn$.

Let $G = S_3$, $\rho$ the permutation representation, and $W, W^\perp$ as in Problem 16.16.

b) Consider the $G$-linear maps from $\rho$ to $\rho$, that is, the $\tau : F^3 \longrightarrow F^3$ such that $\tau \circ \rho_g = \rho_g \circ \tau$ for all $g \in G$. Show directly from the definition that these $\tau$ form a two-dimensional subspace of $\mathrm{Hom}(F^3, F^3)$.

c) Show that $W^\perp$ is irreducible. (Hint/Outline: Assume the contrary, that $W^\perp$ has a proper subspace $\{\mathbf{0}\} \subsetneq W_1 \subsetneq W^\perp$ which is stable under $\rho^{W^\perp}$. The matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

is $\rho^{W^\perp}$ for some (which?) $g$. This matrix limits you to only finitely many possibilities for $W_1$. If some of the other matrices don't stabilize those possibilities, you have a contradiction.)

d) Use the previous part and Schur's lemma to give a second proof that the dimension of the space of $G$-linear maps is two.

**16.18** We know $A_4$ is the group of rotations of the regular tetrahedron. Arguing in the style of Problem 16.17 part (c), show that this degree-3 representation is irreducible.

**16.19** Let $V = \mathbb{C}^3$ with basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. The tensor product $V \otimes V$ is a vector space with a basis of nine elements. List them in lexicographic order

$$\mathbf{e}_1 \otimes \mathbf{e}_1, \mathbf{e}_1 \otimes \mathbf{e}_2, \mathbf{e}_1 \otimes \mathbf{e}_3, \mathbf{e}_2 \otimes \mathbf{e}_1, \cdots .$$

a) List a basis of $\mathrm{Sym}^{(2)}(V)$.

b) List a basis of $\mathrm{Alt}^{(2)}(V)$.

Let $G = \langle a \rangle$ be cyclic of order 3. Let $\rho : G \longrightarrow GL(V)$ be the regular representation, where

$$\rho_a = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

For the following representations $\sigma$ of $G$, write the matrix $\sigma_a$ explicitly, using the appropriate bases.

c) $\sigma \equiv \rho \otimes \rho$
d) $\sigma \equiv$ the representation on $\mathrm{Sym}^{(2)}(V)$
e) $\sigma \equiv$ the representation on $\mathrm{Alt}^{(2)}(V)$

Note: Once we find $\sigma_a$, we know $\sigma_g$ for any $g \in G = \langle a \rangle$ since $G$ is cyclic. But $\sigma_e$ is the identity matrix always and since $|G| = 3$ this really only helps with one other element: $a^2$. We have $\sigma_{a^2} = (\sigma_a)^2$.

**16.20** Let $G$ be a finite group. Let $\phi$ and $\psi$ be characters of $G$. Show that $\phi\psi$ is a character of $G$ as well, where $(\phi\psi)(g) \equiv \phi(g)\psi(g)$ for all $g \in G$.

**16.21** Let $G$ be a finite or infinite abelian group. Let $\rho : G \to GL(V)$ be a representation. Let $\dim V$ be finite. Show, using Schur's lemma, that if $\rho$ is an irreducible representation then $\dim V = 1$.

**16.22** Let $G$ be a finite group. Recall that $Z(G)$, the center of $G$, is

$$Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}.$$

a) Let $\chi$ be the character of any irreducible representation $\rho$ of $G$, where $\rho$ has degree $d$. Let $z \in Z(G)$. Use Schur's lemma to prove that $|\chi(z)| = d$.
b) Let $\rho : G \to GL(V)$ be a faithful (that is, injective) representation with character $\chi$. Let $z \in G$ and suppose $|\chi(z)| = d$ for every character $\chi$ of a faithful irreducible representation of degree $d$. Show that $z \in Z(G)$.
c) Prove that $d^2 \leq |G|/|Z(G)|$. (Hint: Let $\chi$ be an irreducible character and use $(\chi|\chi) = 1$ along with the first part of the problem.)
d) Let $\rho : G \to GL(V)$ be a faithful (that is, injective) representation. Show that $Z(G)$ must be a cyclic subgroup of $G$.

**16.23** Table 16.4 shows the character table of $S_5$, with parts left out.
In the top row, cycle shapes like (••) specify the conjugacy classes. Two letters $P, Q$ label conjugacy classes and their sizes $a, b$ are missing.
Let sgn be the sign representation. Let $\rho$ be the permutation representation on the five coordinates of $\mathbb{C}^5$. Define std, the standard representation, to be the one where $\rho = \text{triv} \oplus \text{std}$. Either $V$ is std and $W$ is sgn $\otimes$ std, or vice-versa.
By a theorem about $S_n$ (which we didn't prove), all the entries in the body of the table are in $\mathbb{Z}$.
Find $P, Q, V, W, a, b, c, d, e, f, g$.

**16.24** Let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ be the group of quaternions. Recall that $i^2 = j^2 = k^2 = ijk = -1$.

a) Find the conjugacy classes of $Q_8$.

Table 16.4: Character table of $S_5$, with parts left out.

| size | 1 | 10 | $a$ | $b$ | 20 | 24 | 30 |
|---|---|---|---|---|---|---|---|
| class | () | (••) | $P$ | $Q$ | (• • •)(••) | (• • • • •) | (• • ••) |
| triv | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| sgn | 1 | −1 | $c$ | $d$ | −1 | 1 | −1 |
| $V$ | 4 | 2 | 0 | 1 | −1 | −1 | 0 |
| $W$ | 4 | −2 | 0 | 1 | 1 | −1 | 0 |
|  | 5 | 1 | $e$ | $f$ | 1 | 0 | −1 |
|  | 5 | −1 | $e$ | $f$ | −1 | 0 | 1 |
|  | $g$ | 0 | −2 | 0 | 0 | 1 | 0 |

b) Show that $N = \{1, -1\}$ is a normal subgroup of $Q_8$.
c) What group is $Q_8/N$ isomorphic to? Why?
d) Use the previous part to obtain $|Q_8/N|$ degree-1 representations of $Q_8$. (Hint: See Corollary 16.3.)
e) Argue that Problem 9.7 can be used to construct a degree-2 representation of $Q_8$. Write down the 2-by-2 matrices $\rho(g)$ for all $g \in Q_8$.
f) Argue that the degree-2 representation in the previous part is irreducible. (Hint: What are the subspaces that are stable under $i$? Are all of those subspaces stable under $j$? This idea is similar to using Theorem 16.5.)
g) Construct the character table of $Q_8$.

**16.25** Let $\rho : G \to GL(V)$ be a linear representation with character $\chi$ and $\dim V$ finite. Let $V'$ be the dual of $V$ (that is, the space of linear forms on $V$). For $\mathbf{v} \in V$ and $\mathbf{v}' \in V'$ let $\langle \mathbf{v}', \mathbf{v} \rangle$ denote the value of the linear form $\mathbf{v}'$ at $\mathbf{v}$.

a) Show that there exists a unique linear representation $\rho' : G \to GL(V')$ such that

$$\langle \rho'_g \mathbf{v}', \rho_g \mathbf{v} \rangle = \langle \mathbf{v}', \mathbf{v} \rangle$$

for $\forall g \in G, \forall \mathbf{v} \in V, \forall \mathbf{v}' \in V'$. This is known as the contragredient or dual representation of $\rho$.
b) What is the character $\chi'$ of the contragredient (or dual) representation of $\rho$ in terms of the character $\chi$?

**16.26** Table 16.5 shows the character table of $S_4$. This problem will walk you through the derivation of this character table.

a) Prove that the "class" row includes all the conjugacy classes of $S_4$. (See Theorem 9.1 for a reminder of the conjugacy classes of $S_n$.)
b) Prove that the "size" row should indeed be $[1, 6, 3, 8, 6]$. (This is given in Table 9.1, but make sure you understand each of these steps so that you understand the derivation of the character table of $S_4$ fully.)
c) $S_4/V \cong S_3$, where $V$ is the Klein 4-group generated by, say, $(1\ 2)(3\ 4)$. The character table of $S_3$ was found in Problem 16.16. Those representations pull

Table 16.5: Character table of $S_4$.

| size | 1 | 6 | 3 | 8 | 6 |
|---|---|---|---|---|---|
| class | $e$ | (••) | (••)(••) | (• • •) | (• • ••) |
| triv | 1 | 1 | 1 | 1 | 1 |
| sgn | 1 | −1 | 1 | 1 | −1 |
| $\theta$ | 2 | 0 | 2 | −1 | 0 |
| $\psi$ | 3 | 1 | −1 | 0 | −1 |
| $\epsilon\psi$ | 3 | −1 | −1 | 0 | 1 |

back under the quotient map $S_4 \longrightarrow S_4/V$ to give representations of $S_4$. Show that they give the top three rows of the character table of $S_5$.

d) $S_4$ is the group of rotations of the octahedron. This is a degree-3 representation $\rho$ of $S_4$. Every nontrivial element is a rotation around some axis through some angle $2\pi/k$ for some $k \in \mathbb{Z}^+$. What is the trace of such a rotation? For finding the trace, why does it not matter what the axis is? Apply this to each conjugacy class, and show that the character of $\rho$ is the one the table calls $\epsilon\psi$. The representation is irreducible because no line or plane is preserved by all of the rotations. As a second proof that $\rho$ is irreducible, show that $(\epsilon\psi|\epsilon\psi) = 1$.

e) We now construct $\psi$. Let $W$ be a vector space with basis $\{\mathbf{e}_1, \cdots, \mathbf{e}_4\}$. Give $W$ the permutation representation where $S_4$ permutes the $\mathbf{e}_i$. Find the character of $W$. The line $W_1$ spanned by $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4$ is stable and is the trivial representation. The orthocomplement $W_1^\perp$ is the standard representation. Show that (character of $W$) minus (trivial character) equals $\psi$. Show that $(\psi|\psi) = 1$, which proves that $W_1^\perp$ is irreducible.

f) Describe the degree-3 representation whose character is $\psi$. Formally, it is sgn $\otimes$ (representation in part $d$), but what is it geometrically?

**16.27** Let's work out the character table of $A_5$.

a) List the conjugacy classes of $A_5$.

b) Start the character table with the trivial representation.

c) $A_5$ is the rotation group of the icosahedron. Work out the character $\phi$ of this degree-3 representation in the manner of the second part of Problem 16.26.

d) In $A_5$, conjugation by an odd permutation gives an automorphism of $A_5$ that is not an inner automorphism (we call it an outer automorphism). Compose the representation in the previous part with such an outer automorphism to get a different degree-3 representation $\phi'$. Verify that $(\phi'|\phi') = 1$ and $(\phi|\phi') = 0$.

e) Consider the permutation representation on a basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{e}_5\}$. Split off the trivial line through $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_5$ to obtain a degree-4 standard representation with character $\psi$. Verify that $(\psi|\psi) = 1$.

f) You now have four rows of a five-row table. Before finding the fifth row, how does Corollary 16.6 tell you what the degree of the fifth row must be?

g) Find the fifth row.

**16.28** At the end of Problem 16.27, you found a character of $A_5$ without knowing what the representation was. Show that the representation is obtained by removing the trivial representation from the permutation representation of $A_5$ on the set of its six subgroups of order five.

**16.29** Let $\rho : G \longrightarrow GL(V)$ be a representation with character $\chi$. Proposition 16.13 shows that $V \otimes V$ has character $\chi^2$. That is, the character $\chi^{(\otimes)}$ of $V \otimes V$ is $\chi^{(\otimes)}(g) = \chi(g)\chi(g)$ for every $g \in G$. Similarly, the $k$-th tensor power $V^{\otimes k} = V \otimes \cdots \otimes V$ with $k$ copies of $V$ has character $\chi^k$. (To be clear, $\chi^k$ means $(\chi^k)(g) = (\chi(g))^k$ for any $g \in G$.)

a) Let $G = A_4$ and let $\rho : G \longrightarrow GL(V)$ be the irreducible degree-3 representation of $A_4$. By adding up rows of the character table, show that $V^{\otimes 2}$ is a direct sum of one copy of each of the degree-1 representations, plus two copies of $V$.
b) With $\rho$ as in the previous part, give a general formula for $V^{\otimes k}$ as a direct sum of (how many?) copies of the four irreducibles.

Note: A plethysm is when we build a new representation from old ones by an algebraic construction, then identify the irreducible constituents in the new one. The special case of $V \otimes W$ is called the Clebsch-Gordan problem.

**16.30** Let $\rho : S_3 \longrightarrow GL(V)$ be the standard representation, with basis $\{\mathbf{e}_1, \mathbf{e}_2\}$ so that

$$\rho_{(1\ 2\ 3)} = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \rho_{(1\ 2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let $W = V \otimes V$, with basis $\{\mathbf{e}_i \otimes \mathbf{e}_j | 1 \le i, j \le 2\}$ in lexicographic order.

a) Use characters to show that

$$W \cong W_1 \oplus W_2 \oplus W_3,$$

one copy of each of the trivial, sign, and standard representations of $S_3$.
b) Write down the 4 × 4 matrices $(\rho \otimes \rho)_g$ for all $g \in S_3$.

**16.31** Let $X$ be a finite set on which a finite group $G$ acts on; call the action $\phi : G \longrightarrow S_X$. Let $\chi_\phi$ be the character of the permutation representation $\rho^{(\phi)}$ associated with the action $\phi$.

a) Recall that $\mathrm{Orb}(x) = \{\phi_g(x) | g \in G\}$ is called the orbit of $x \in X$. Let $N_{orb}$ be the number of distinct orbits. Show that $N_{orb}$ is equal to the number of times that $\rho^{(\phi)}$ contains the trivial representation. Conclude that $(\chi_\phi|\chi_{triv}) = N_{orb}$. In particular, if the action is transitive (that is, $N_{orb} = 1$. See Definition 11.4), $\rho^{(\phi)}$ can be decomposed into triv $\oplus\ \theta$ where $\theta$ does not contain the trivial representation. Letting $\chi_\theta$ be the character of $\theta$, then we have $\chi_\phi = \chi_{triv} + \chi_\theta$ and $(\chi_\theta|\chi_{triv}) = 0$.
b) Let $G$ act on the product $X \times X$ by the action $\psi : G \longrightarrow S_{X\times X}$ defined by $\psi = \phi \times \phi$. That is, $\psi_g((x, y)) = (\phi_g(x), \phi_g(y))$ for any $g \in G$. Show that the

character of the corresponding permutation representation $\rho^{(\psi)}$ associated with the action $\psi$ is equal to $\chi_\phi^2$. That is, $\chi_\psi(g) = \chi_\phi(g)^2$ for any $g \in G$.

c) Suppose that the action $\phi$ is transitive on $X$ and that $X$ has at least two elements. We say that $\phi$ is doubly transitive if $\phi$ is not only transitive but also for all $x, y, x', y' \in X$ with $x \neq y$ and $x' \neq y'$ there exists $s \in G$ such that $x' = \phi_s(x)$ and $y' = \phi_s(y)$. Prove the equivalence of the following properties:

   i) The action $\phi$ is doubly transitive.
   ii) The action $\psi$ on $X \times X$ has two orbits: the diagonal and its complement.
   iii) $(\chi_\psi|\chi_{triv}) = (\chi_\phi^2|\chi_{triv}) = 2$.
   iv) The representation $\theta$ in part a) is irreducible. (Hint: Showing that

$$(\chi_\theta^2|\chi_{triv}) = (\chi_\theta|\chi_\theta)$$

   might be useful.)

**16.32** Let $G$ be a finite group, and let $\hat{G}$ be the set of degree-one representations of $G$ over $\mathbb{C}$.

a) If $\chi_1, \chi_2$ belong to $\hat{G}$, show that the same is true of their product $\chi_1\chi_2$. (By $\chi_1\chi_2$, we mean that $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$ for $g \in G$.) Show that this makes $\hat{G}$ an abelian group. The group $\hat{G}$ is called the dual of the group $G$.
b) Show that $|\hat{G}| = |G|$.
c) For $x \in G$ show that the mapping $\hat{G} \to \mathbb{C}$ defined by $\chi \mapsto \chi(x)$ is a degree-1 representation of $\hat{G}$. Therefore, it is an element of the dual $\hat{\hat{G}}$ of $\hat{G}$ (the double dual of $G$). Show that the map $G \to \hat{\hat{G}}$ thus obtained is an injective homomorphism. Conclude (by comparing the orders of the two groups) that it is surjective as well and, hence, an isomorphism $G \cong \hat{\hat{G}}$.

**16.33** Let $\rho : G \to GL(V)$ be a representation and let $N \trianglelefteq G$.

a) If $N \leq \ker\rho$, show that there is a unique representation $\tilde{\rho} : G/N \to GL(V)$ defined by $\tilde{\rho}(gN) = \rho(g)$ for all $g \in G$.
b) Show that $\tilde{\rho}$ is irreducible if and only if $\rho$ is irreducible.
c) (If you did Problem 16.11) Let $G = D_4$ and $N = \langle r \rangle$. Of the five representations in Problem 16.11, which satisfy $N \leq \ker\rho$? For those that do, write out what $\tilde{\rho}$ is.

# Chapter 17
# Induced Representations

**Abstract** This chapter covers induced representations.

## 17.1 Induced Representations

Let $G$ be a group and let $H$ be a subgroup of $G$. Let us consider $G/H$ with $[G : H] = k$. Pick coset representatives $r_1, \cdots, r_k$. That is,

$$r_1H, \cdots, r_kH \tag{17.1}$$

are the $k$ (distinct) cosets that form a partition of the group $G$. Let $\rho : G \longrightarrow GL(V)$ be a representation for $G$. If we restrict $\rho$ to $H$, denote this as $\rho^H$, then $\rho^H : H \longrightarrow GL(V)$ is a representation of $H$. Suppose that there is a vector subspace $W \subseteq V$ such that $W$ is $H$-stable. Recall that this means that $\rho_x W = W$ for any $x \in H$. What if $x \notin H$? Since $G/H$ is a partition of $G$, we know that any $x \in G$ can be written as $x = r_j h$ for some coset representative $r_j$ and some $h \in H$. We then get that

$$\rho_x W = \rho_{r_j h} W = \rho_{r_j} \rho_h W = \rho_{r_j} W, \tag{17.2}$$

where the last equality used the assumption that $W \subseteq V$ was $H$-stable. Therefore, $\rho_x W$ depends only on which coset of $H$ in $G$ the element $x$ belongs to. If we consider the sum of the vector subspaces

$$\rho_{r_1} W, \cdots, \rho_{r_k} W, \tag{17.3}$$

let us call the result $V'$, then we see that it is $G$-stable since $\rho_g$ for $g \in G$ sends each $\rho_{r_j} W$ to $\rho_g \rho_{r_j} W = \rho_{r_a} W$ where $r_a$ is the coset representative of the coset to which $gr_j$ belongs to. This gives a subrepresentation $\rho : G \longrightarrow GL(V')$. We say that the representation $\rho : G \longrightarrow GL(V)$ is induced by $\theta$ if this subrepresentation $V' = V$, with $V$ is not just equal to $V'$ but rather $V$ is a direct sum of the subspaces $\rho_{r_1} W, \cdots \rho_{r_k} W$.

**Definition 17.1** Let $\rho : G \to GL(V)$ be any representation. Let $H$ be a subgroup of $G$. By restriction, we have a representation $\rho^H : H \to GL(V)$. Suppose that there is a vector subspace $W \subseteq V$ which is $H$-stable. Let $\theta : H \to GL(W)$ be this representation. We say $\underline{\rho \text{ is induced from } \theta}$ if

$$V = \bigoplus_{j=1}^{k} \rho_{r_j} W.$$

We write $\rho = \operatorname{Ind}_H^G \theta$ or $V = \operatorname{Ind}_H^G W$ when $\rho$ is induced from $\theta$.

See Figure 17.1 for some visual intuition for what it means to be an induced representation.

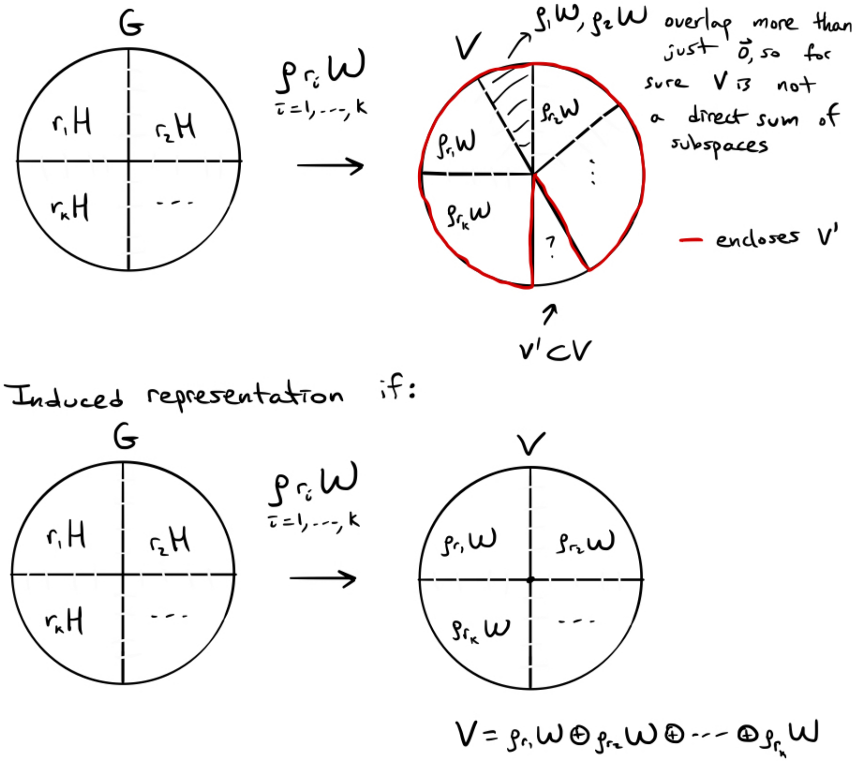


Fig. 17.1: Pictures to help visual what an induced representation means.

Perhaps some examples will make things more clear.

*Example 17.1* Let $G$ be a finite group. Let $\rho^{reg} : G \to GL(V)$ be the regular representation of $G$ (see Definition 16.3, if needed). Then the basis for $V$ is labeled by $\mathbf{e}_x$ for $\forall x \in G$ and $\rho_x^{reg}\mathbf{e}_y = \mathbf{e}_{xy}$ for all $x, y \in G$. Let $H$ be a subgroup of $G$. Let $W$ be the subspace spanned by $\mathbf{e}_x$ for $x \in H$. Then we have a representation $\theta : H \to GL(W)$, which is actually the regular representation of $H$. But $\rho^{reg}$ is induced by the representation $\theta$. Why? Suppose $[G : H] = k$ and $|H| = m$. Pick coset representatives $r_1, \cdots, r_k$ so that

$$r_1H, \cdots, r_kH \tag{17.4}$$

form a partition of $G$. Without loss of generality, suppose $r_1 = e$ so that $r_1H = eH$. A basis for $V$ in the regular representation is

$$\{\underbrace{\underbrace{\mathbf{e}_{r_1h_1}, \mathbf{e}_{r_1h_2}, \cdots, \mathbf{e}_{r_1h_m}}_{\text{spans } r_1H \text{ part of V}}, \underbrace{\mathbf{e}_{r_2h_1}, \mathbf{e}_{r_2h_2}, \cdots, \mathbf{e}_{r_2h_m}}_{\text{spans } r_2H \text{ part of V}}, \cdots, \underbrace{\mathbf{e}_{r_kh_1}, \mathbf{e}_{r_kh_2}, \cdots, \mathbf{e}_{r_kh_m}}_{\text{spans } r_kH \text{ part of V}}}_{\text{spans } G \text{ part (that is, all) of } V}\}. \tag{17.5}$$

In this notation, $W$ (the subspace that is $H$-stable) is the subspace spanned by

$$\{\mathbf{e}_{r_1h_1}, \mathbf{e}_{r_1h_2}, \cdots, \mathbf{e}_{r_1h_m}\} = \{\mathbf{e}_{h_1}, \mathbf{e}_{h_2}, \cdots, \mathbf{e}_{h_m}\}, \tag{17.6}$$

since, without loss of generality, we are choosing $r_1H = eH$ by choosing $r_1 = e$. What is $\rho_{r_2}^{reg}W$? Well, $\rho_{r_2}^{reg}W$ is the subspace of $V$ that is spanned by

$$\{\rho_{r_2}\mathbf{e}_{h_1}, \rho_{r_2}\mathbf{e}_{h_2}, \cdots, \rho_{r_2}\mathbf{e}_{h_m}\} = \{\mathbf{e}_{r_2h_1}, \mathbf{e}_{r_2h_2}, \cdots, \mathbf{e}_{r_2h_m}\}, \tag{17.7}$$

which we see is the subspace of $V$ that is spanned by the vectors corresponding to $r_2H$. Continuing the argument, we see that

$$V = \rho_{r_1}^{reg}W \oplus \rho_{r_2}^{reg}W \oplus \cdots \oplus \rho_{r_k}^{reg}W = \bigoplus_{j=1}^{k} \rho_{r_j}^{reg}W. \tag{17.8}$$

That is, $V = \mathrm{Ind}_H^G W$ (also written as $\rho^{reg} = \mathrm{Ind}_H^G \theta$). In words: the regular representation of $G$ is induced by the regular representation of a subgroup $H$ of $G$.

The previous example can be generalized a bit.

*Example 17.2* Let $G$ be a finite group and let $H$ be a subgroup of $G$. Let $[G : H] = k$. Pick coset representatives $r_1, \cdots, r_k$ so that

$$r_1H, \cdots, r_kH \tag{17.9}$$

form a partition of $G$. Without loss of generality, suppose $r_1 = e$ so that $r_1H = eH$. Define $V$ as the vector space spanned by the linearly independent vectors

$$\mathbf{e}_{r_1H}, \cdots, \mathbf{e}_{r_kH}. \tag{17.10}$$

That is, we associate a basis vector to each distinct left coset of $H$ in $G$. Let $\rho : G \to GL(V)$ to be the representation of $G$ defined by $\rho_g \mathbf{e}_{r_i H} = \mathbf{e}_{g r_i H}$. This is the permutation representation of $G$ associated with $G/H$ where the action is left translation of cosets (see Definition 16.4, if necessary) . Let $W$ be the subspace spanned by $\mathbf{e}_{r_1 H} = \mathbf{e}_{eH}$. Then $W = \mathbb{C}\mathbf{e}_{eH}$. $W$ is $H$-stable since $\rho_h \mathbf{e}_{eH} = \mathbf{e}_{hH} = \mathbf{e}_{eH}$ for any $h \in H$. Therefore, we have a representation $\theta : H \to GL(W)$. Notice that $\rho_{r_i} W$ is a vector space spanned by $\rho_{r_i}\mathbf{e}_{eH} = \mathbf{e}_{r_i H}$. It is then clear that

$$V = \rho_{r_1} W \oplus \rho_{r_2} W \oplus \cdots \oplus \rho_{r_k} W = \bigoplus_{j=1}^{k} \rho_{r_j} W. \tag{17.11}$$

That is, $V = \operatorname{Ind}_H^G W$ (also written as $\rho = \operatorname{Ind}_H^G \theta$).

Use notation as above. Given that $\rho$ and $\theta$ are related to one another, is there a formula relating the characters $\chi_\rho, \chi_\theta$ of $\rho, \theta$, respectively?

**Theorem 17.1** *If a representation $\rho$ is induced $\rho = \operatorname{Ind}_H^G \theta$ (or $V = \operatorname{Ind}_H^G W$), then*

$$\chi_\rho(u) = \sum_{\substack{r \in R \\ \text{such that} \\ r^{-1}ur \in H}} \chi_\theta(r^{-1}ur),$$

*where $R$ is a set of coset representatives of $G/H$.*

***Proof*** Suppose $[G : H] = k$ and let $R$ be a set of coset representatives $R = \{r_1, \cdots, r_k\}$. Choose an ordered basis for $V$ as follows: choose a basis of $\rho_{r_1} W$, then a basis of $\rho_{r_2} W$, etc... Fix $u \in G$. Let $r_j \in R$ be arbitrary. What does $\rho_u$ do to the subspace $\rho_{r_j} W$? That is, what is $\rho_u \rho_{r_j} W = \rho_{u r_j} W$? We know $u r_j$ belongs to some coset in $G/H$. Therefore, there exists $h_j \in H$ and $r_i \in R$ such that $u r_j = r_i h_j$. If $i \neq j$, then

$$r_i^{-1} u r_j = r_i^{-1} r_j h_j \neq e h_j. \tag{17.12}$$

In particular, $r_i = r_j$ if and only if $r_i^{-1} u r_j \in H$. There are two cases to consider.

i) If $i = j$, then $r_i^{-1} u r_j = r_j^{-1} u r_j \in H$ and

$$\rho_u \rho_{r_j} W = \rho_{u r_j} W = \rho_{r_i h_j} W = \rho_{r_i} \rho_{h_j} W = \rho_{r_i} W = \rho_{r_j} W, \tag{17.13}$$

where we have used the fact that $W$ is $H$-stable. Therefore, $\rho_u$ sends $\rho_{r_j} W$ to $\rho_{r_j} W$ and so is nonzero in the block corresponding to the subspace $\rho_{r_j} W$. This is along the diagonal so it contributes to $\operatorname{Tr}(\rho_u)$. More visually:

$$\rho_u = \begin{array}{cc} \cdots\ \rho_{r_j}W\ \cdots\cdots\cdots & \\ \begin{bmatrix} ? & \mathbf{0} & ? & ? & ? \\ ? & * & ? & ? & ? \\ ? & \mathbf{0} & ? & ? & ? \\ ? & \mathbf{0} & ? & ? & ? \\ ? & \mathbf{0} & ? & ? & ? \end{bmatrix} & \begin{array}{l} \vdots \\ \rho_{r_i}W = \rho_{r_j}W \\ \vdots \\ \vdots \\ \vdots \end{array} \end{array} \tag{17.14}$$

where $*$ denotes nonzero terms. Since that block is along the diagonal, it contributes to the trace.

ii) If $i \neq j$, then $r_i^{-1}ur_j \notin H$ and

$$\rho_u\rho_{r_j}W = \rho_{ur_j}W = \rho_{r_ih_j}W = \rho_{r_i}\rho_{h_j}W = \rho_{r_i}W \neq \rho_{r_j}W, \tag{17.15}$$

where we have used the fact that $W$ is $H$-stable. Therefore, $\rho_u$ sends $\rho_{r_j}W$ to $\rho_{r_i}W \neq \rho_{r_j}W$. This is off-diagonal and so contributes zero to $\mathrm{Tr}(\rho_u)$. More visually:

$$\rho_u = \begin{array}{cc} \cdots\ \rho_{r_j}W\ \cdots\ \rho_{r_i}W\ \cdots & \\ \begin{bmatrix} ? & \mathbf{0} & ? & ? & ? \\ ? & \mathbf{0} & ? & ? & ? \\ ? & \mathbf{0} & ? & ? & ? \\ ? & * & ? & ? & ? \\ ? & \mathbf{0} & ? & ? & ? \end{bmatrix} & \begin{array}{l} \vdots \\ \rho_{r_j}W \\ \vdots \\ \rho_{r_i}W \\ \vdots \end{array} \end{array} \tag{17.16}$$

where $*$ denotes nonzero terms. Since that block is off-diagonal, it contributes zero to the trace. □

Thus, we need to find the contribution to $\mathrm{Tr}(\rho_u)$ for $r_j \in R$ such that $r_j^{-1}ur_j \in H$. Let $\mathrm{Tr}(\rho_u)|_{\rho_{r_j}W}$ be a partial trace of $\rho_u$, where we only trace over the subspace corresponding to $\rho_{r_j}W$. That is, we restrict $\rho_u$ to the subspace $\rho_{r_j}W$ and take the trace of that part only. Thus,

$$\chi_\rho(u) = \sum_{\substack{j=1,\cdots,k \\ \text{such that} \\ r_j^{-1}ur_j \in H}} \mathrm{Tr}(\rho_u)|_{\rho_{r_j}W}\,. \tag{17.17}$$

However, if $i = j$, then

$$\rho_u\rho_{r_j} = \rho_{r_j}\rho_{r_j}^{-1}\rho_{ur_j} = \rho_{r_j}\rho_{r_j^{-1}ur_j}\,. \tag{17.18}$$

Let us restrict to $W$. Also, $r_j^{-1}ur_j \in H$ and, by definition of induced representation, $\rho_h$ restricted to $W$ is equal to $\theta_h$ for any $h \in H$. Therefore, $\rho_{r_j^{-1}ur_j} = \theta_{r_j^{-1}ur_j}$. Therefore,

$$\rho_u|_{\rho_{r_j}W}\rho_{r_j} = \rho_{r_j}\rho_{r_j}^{-1}\rho_{ur_j} = \rho_{r_j}\theta_{r_j^{-1}ur_j}. \tag{17.19}$$

Thus, we see that $\mathrm{Tr}(\rho_u)|_{\rho_{r_j}W} = \mathrm{Tr}(\theta(r_j^{-1}ur_j)) = \chi_\theta(r_j^{-1}ur_j)$ so that

$$\chi_\rho(u) = \sum_{\substack{j=1,\cdots,k\\ \text{such that}\\ r_j^{-1}ur_j\in H}} \chi_\theta(r_j^{-1}ur_j) = \sum_{\substack{r\in R\\ \text{such that}\\ r^{-1}ur\in H}} \chi_\theta(r^{-1}ur). \tag{17.20}$$

**Corollary 17.1** *If a representation $\rho$ is induced $\rho = \mathrm{Ind}_H^G\,\theta$ (or $V = \mathrm{Ind}_H^G\,W$), then*

$$\chi_\rho(u) = \frac{1}{|H|}\sum_{\substack{g\in G\\ \textit{such that}\\ g^{-1}ug\in H}} \chi_\theta(g^{-1}ug).$$

***Proof*** This follows because $G = r_1H \cup \cdots \cup r_kH$, the fact that each coset has the same cardinality (Corollary 7.3), and that characters are class functions (Theorem 16.2). Let $R$ be a set of coset representatives of $G/H$. Therefore,

$$\begin{aligned}
\sum_{\substack{g\in G\\ \text{such that}\\ g^{-1}ug\in H}} \chi_\theta(g^{-1}ug) &= \sum_{\substack{r\in R\\ \text{such that}\\ (rh)^{-1}u(rh)\in H}} \sum_{h\in H} \chi_\theta((rh)^{-1}u(rh)) \qquad (17.21)\\
&= \sum_{\substack{r\in R\\ \text{such that}\\ (rh)^{-1}u(rh)\in H}} \sum_{h\in H} \chi_\theta(h^{-1}r^{-1}urh)\\
&= \sum_{\substack{r\in R\\ \text{such that}\\ (rh)^{-1}u(rh)\in H}} \sum_{h\in H} \chi_\theta(r^{-1}ur)\\
&= \sum_{\substack{r\in R\\ \text{such that}\\ r^{-1}ur\in H}} \sum_{h\in H} \chi_\theta(r^{-1}ur)\\
&= \sum_{\substack{r\in R\\ \text{such that}\\ r^{-1}ur\in H}} |H|\chi_\theta(r^{-1}ur)
\end{aligned}$$

where for the fourth equality we used the fact that $r^{-1}ur \in H$ if and only if $h^{-1}r^{-1}urh = (rh)^{-1}u(rh) \in H$ since $H$ is a subgroup of $G$ and hence is closed under the binary operation (which we call multiplication, in multiplicative notation). Therefore,

$$\chi_\rho(u) = \sum_{\substack{r\in R\\ \text{such that}\\ r^{-1}ur\in H}} \chi_\theta(r^{-1}ur) = \frac{1}{|H|}\sum_{\substack{g\in G\\ \text{such that}\\ g^{-1}ug\in H}} \chi_\theta(g^{-1}ug), \tag{17.22}$$

as claimed. □

A good question to ask is the following: When is an induced representation irreducible? If $\chi_\theta$ is an irreducible character, this does not mean that $\chi_\rho$ is also an irreducible character. A standard thing to prove would be Mackey's irreducibility criterion, which gives conditions that are necessary and sufficient for an induced representation to be irreducible. We will not cover this here, as more machinery is needed to really do the derivation justice.

## 17.2 Motivation For Problem 17.2

Problem 17.2 is rather abstract. We add a section with an example to give intuition for what that problem is about. The notation below is in accordance with the notation set in Problem 17.2. Read this section when you are preparing to solve part d) of the problem.

Let $G = S_3$. Let $H = \langle(1\ 2\ 3)\rangle$. Let $W = \mathbb{C}$ and $\phi = e^{2\pi i/3}$. Then $\theta : (1\ 2\ 3) \mapsto \phi$ is a representation of $H$. Suppose $f(e) = a$. Then

$$f((1\ 2\ 3)e) = \theta_{(1\ 2\ 3)} f(e) = \phi a \tag{17.23}$$

$$f((1\ 2\ 3)^2 e) = \theta_{(1\ 2\ 3)^2} f(e) = (\theta_{(1\ 2\ 3)})^2 f(e) = \phi^2 a. \tag{17.24}$$

Suppose $f((1\ 2)) = b$. Then

$$f((1\ 3)) = f((1\ 2\ 3)(1\ 2)) = \theta_{(1\ 2\ 3)} f((1\ 2)) = \phi b \tag{17.25}$$

$$f((2\ 3)) = f((1\ 3\ 2)(1\ 2)) = \theta_{(1\ 3\ 2)} f((1\ 2)) = \phi^2 b. \tag{17.26}$$

A generic function $f$ therefore looks like

| $f(x)$ | $a$ | $\phi a$ | $\phi^2 a$ | $b$ | $\phi b$ | $\phi^2 b$ |
|---|---|---|---|---|---|---|
| $x$ | $e$ | $(1\ 2\ 3)$ | $(1\ 3\ 2)$ | $(1\ 2)$ | $(1\ 3)$ | $(2\ 3)$ |

Consider $w = a$.

| $f_a(x)$ | $a$ | $\phi a$ | $\phi^2 a$ | 0 | 0 | 0 |
|---|---|---|---|---|---|---|
| $x$ | $e$ | $(1\ 2\ 3)$ | $(1\ 3\ 2)$ | $(1\ 2)$ | $(1\ 3)$ | $(2\ 3)$ |

Next, let's work out $(\rho_{(1\ 2)} f_b)(u) = f_b(u(1\ 2))$. But $e(1\ 2) = (1\ 2)$, $(1\ 2\ 3)(1\ 2) = (1\ 3)$, $(1\ 3\ 2)(1\ 2) = (2\ 3)$, $(1\ 2)(1\ 2) = e$, $(1\ 3)(1\ 2) = (1\ 2\ 3)$, $(2\ 3)(1\ 2) = (1\ 3\ 2)$. This gives

| $(\rho_{(1\ 2)} f_b)(x)$ | 0 | 0 | 0 | $b$ | $\phi b$ | $\phi^2 b$ |
|---|---|---|---|---|---|---|
| $x$ | $e$ | $(1\ 2\ 3)$ | $(1\ 3\ 2)$ | $(1\ 2)$ | $(1\ 3)$ | $(2\ 3)$ |

We see that any "generic" $f$ in the problem can be written as $f = f_a + \rho_{(1\ 2)} f_b = \rho_e f_a + \rho_{(1\ 2)} f_b$. Therefore, $V = \mathrm{Ind}_H^G W$ (or $\rho = \mathrm{Ind}_H^G \theta$).

## Problems

**17.1** Show that each irreducible representation of $G$ is contained in a representation induced by an irreducible representation of $H$. Use the fact that an irreducible representation is contained in the regular representation at least once.

**17.2** Let $G$ be a group. Let $\theta : H \longrightarrow GL(W)$ be a linear representation of $H \leq G$. Let $V$ be the vector space of functions $f : G \longrightarrow W$ such that $f(tu) = \theta_t f(u)$ for $u \in G, t \in H$. That is,

$$V = \{f : G \longrightarrow W \mid f(tu) = \theta_t f(u) \text{ for } \forall u \in G, \forall t \in H\}.$$

Let $\rho$ be the representation of $G$ in $V$ defined by $(\rho_s f)(u) = f(us)$ for any $s, u \in G$. For $w \in W$ let $f_w \in V$ be defined by $f_w(t) = \theta_t w$ for $t \in H$ and $f_w(t) = 0$ for $t \notin H$.

a) Show that if $f^{(1)}, f^{(2)} \in V$ and $\alpha \in \mathbb{C}$, then $f^{(1)} + \alpha f^{(2)} \in V$.
b) Show that $\rho$ as defined above is indeed a representation. That is, show that $((\rho_s \rho_t) f)(u) = (\rho_{st} f)(u)$ for any $s, t, u \in G$ and $f \in V$.
c) Show that $w \mapsto f_w$ is an isomorphism (in the vector space sense, see the clarifying note after Definition 16.10) of $W$ onto the subspace $W_0$ of $V$ consisting of functions which vanish off $H$. That is,

$$W_0 = \{f : G \longrightarrow W \mid f(s) = 0 \text{ for } s \notin H\}.$$

d) Show that, if we identify $W$ and $W_0$ in this way, the representation $\rho : G \longrightarrow GL(V)$ is induced by the representation $\theta : H \longrightarrow GL(W)$.

**17.3** Let $G = A_4$ and let $H \trianglelefteq G$ be the Klein 4-group within $G$.

a) Write down the character table of $A_4$. Reconstruct it using methods from the previous chapter, if needed. Put the trivial character on top as usual. Put character(s) of degree greater than 1 below those of degree 1. Label the characters $\chi_0$, $\chi_1, \cdots$, from top to bottom. Let $\rho_0, \rho_1, \cdots$, be the corresponding irreducible representations.
b) To check the work in a), please do two computations: find the product $(\chi_i|\chi_i)$ of the bottom-most character, and the product of the bottom-most character with the second one from the bottom.
c) Write down the character table of $H$. Label its characters $\psi_0, \psi_1, \cdots$.
d) For each $\psi_i$, compute the character $\phi_i$ of the induced representation $\mathrm{Ind}_H^G \psi_i$. Decompose each $\phi_i$ as a sum of irreducibles for $A_4$. Which $\phi_i$ is irreducible? When are the $\phi_i'$s the same for different $\psi_i$?

**17.4** Let $\theta$ be a representation of $A_5$. Suppose its character has the values $u, \ldots, y$ as in Table 17.1.

Table 17.1: The character of $\theta$, a representation of $A_5$.

| $e$ | $(\bullet\bullet)(\bullet\bullet)$ | $(\bullet\bullet\bullet)$ | $(1\,2\,3\,4\,5)$ | $(1\,2\,3\,5\,4)$ |
|---|---|---|---|---|
| $u$ | $v$ | $w$ | $x$ | $y$ |

a) Find the character of $\mathrm{Ind}_{A_5}^{S_5}\,\theta$ in terms of $u, \ldots, y$. Write it out as a row of a table like the one in Table 17.2. The first two entries have been filled in for you.

Table 17.2: The character of $\mathrm{Ind}_{A_5}^{S_5}\,\theta$ in terms of $u, \ldots, y$.

| $e$ | $(\bullet\bullet)$ | $(\bullet\bullet)(\bullet\bullet)$ | $(\bullet\bullet\bullet)$ | $(\bullet\bullet\bullet\bullet)$ | $(\bullet\bullet\bullet\bullet\bullet)$ | $(\bullet\bullet)(\bullet\bullet\bullet)$ |
|---|---|---|---|---|---|---|
| $2u$ | 0 |  |  |  |  |  |

b) Let $\theta_{triv}$ be the trivial representation of $A_5$. Let $\rho_{triv}$ and $\rho_{sgn}$ be the trivial and sign representations of $S_5$, respectively. Show that

$$\mathrm{Ind}_{A_5}^{S_5}\,\theta_{triv} \cong \rho_{triv} \oplus \rho_{sgn}.$$

c) Generalizing the previous part, let $\theta$ be an irreducible representation of $A_5$ whose character satisfies the condition $x = y$. Show that $\mathrm{Ind}_{A_5}^{S_5}\,\theta$ is the direct sum of two different irreducible representations of $S_5$. If one of these is $\sigma$, show that the other is $\sigma \otimes$ (what?).

**17.5** Let $\rho : G \to GL(V)$ be a representation of a finite group $G$ on a finite-dimensional vector space $V$. Suppose there is an element $x \in G$ such that $\rho_x = -I$; that is, $\rho_x(\mathbf{v}) = -\mathbf{v}$ for any $\mathbf{v} \in V$.

a) Let $\rho' = \rho \otimes \rho$ be the representation on $\mathrm{Sym}^{(2)}(V)$ defined by $\rho$. Find $\rho'_x$, with proof.

b) With $x$ as above, show that no irreducible representation of $G$ occurs as a direct summand of both $V$ and $\mathrm{Sym}^{(2)}(V)$ (more precisely, as a summand of both $\rho$ and $\rho'$).

Note: If $G$ acts on a solid body by rotations and reflections, we say the body is *centrally symmetric* if $-I$ is part of the action. The tetrahedron is not centrally symmetric, but the other four Platonic solids are, as is the buckyball. Part b) is an example of a general effect in spectroscopy called the *exclusion rule*: For a molecule with a center of symmetry (sometimes called an inversion center), bonds that are active in the infrared will not be Raman-active and vice versa. That is, Raman shifts and infrared frequencies do not coincide.

**17.6** This problem is similar to Problem 16.24.
Let $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ be the group of quaternions. Recall that $i^2 = j^2 = k^2 = ijk = -1$.

a) Find the conjugacy classes of $G$.
b) Find the center $Z(G)$.
c) What group is $G/Z(G)$ isomorphic to? Why?
d) Use the previous part to obtain $|G/Z(G)|$ degree-1 representations of $Q_8$. (Hint: See Corollary 16.3.) Write down the first several rows of the character table of $G$. How many row(s) do you still need in order to complete the character table for $G$? (Leave room for that.)

- Recall that the quaternions are the divison ring

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

This is a 4-dimensional vector space over $\mathbb{R}$. The group $G$ acts on $\mathbb{H}$ by left translation. For instance, $i$ acts by

$$i \cdot (a + bi + cj + dk) = -b + ai - dj + ck.$$

This left translation action is a representation $\rho : G \longrightarrow GL_4(\mathbb{R})$.

e) Find the character $\chi$ of $\rho$.
f) Show that $\chi$ is orthogonal to all the characters in the table for $G$ so far. Find $(\chi|\chi)$. Is $\rho$ irreducible?
g) Let $\psi = \frac{1}{2}\chi$. Prove that this must be what completes the table for $G$. Put it into the character table.
h) Construct a representation $\rho : G \longrightarrow GL_2(\mathbb{C})$ whose character is $\psi$ as an induced representation $\sigma = \mathrm{Ind}_H^G \theta$ with $H = \langle i \rangle$ and $\theta =$ (what?). Find the $2\times2$ matrices $\sigma_i, \sigma_j, \sigma_k$.

# Chapter 18
# Pop Quiz on Part 2

**Abstract** In this chapter, we present a list of qualitative questions about the content of Part 2 in order to help readers test their understanding of (what we consider) the big, take-away ideas.

## 18.1 Important Questions on Part 2

- What is a linear representation of a group?
- What does it mean for two representations to be equivalent/isomorphic?
- What is an irreducible representation?
- What is a regular representation? Is it always irreducible?
- What is permutation representation? Is it always irreducible?
- Is there a relationship between regular representations and permutation representations in cases when $G$ is a finite group?
- Describe Weyl's unitary trick. (Why is it useful? Can you recall/sketch the main idea(s) of the proof?)
- Describe Schur's Lemma. (Can you recall/sketch the main idea(s) of the proof?)
- What is the character of a linear representation? What are some of the properties that characters have? (Can you recall/sketch the main idea(s) of the proof?)
- What is a character table?
- What sort of properties does the character table have (its rows? columns?). Can you describe how to derive/prove those properties?
- Describe a relationship between characters and linear representations.
- What is an induced representation?
- What is a useful formula for the character of an induced representation?

# Part III
# Applications

Part I and II covered the necessary definitions and theorems as preparation for the discussion of applications of group theoretic ideas in other fields.

# Chapter 19
# Noether's Theorem

**Abstract** In physics, conserved quantities can often be deduced by looking at the symmetries of the system. Noether's theorem suggests a systematic way for finding what the conserved quantity is in the case of a continuous symmetry.

## 19.1 Symmetries and Conservation Laws

In physics, one has the feeling that if a physical system has a symmetry then maybe there is some quantity which is somehow related to this symmetry. If there is indeed such a quantity, we would like to know how to find it, assuming we know what the symmetry is. Without a systematic method, finding the quantity can be similar to looking for a needle in a haystack.

In this part when we say symmetry we understand it to mean global symmetry. That is, it is a symmetry possessed by the entire system. One can also have local symmetry, and a slightly different discussion applies in that case.

## 19.2 Invariance and Conservation

Before proceeding, let's formalize some ideas. A quantity of a system is invariant if it takes the same value after a transformation has been applied to the system.

*Example 19.1* A translationally invariant system looks the same after a translation.

*Example 19.2* A rotationally invariant system looks the same after a rotation.

*Example 19.3* Electric charge is a Lorentz invariant because the value does not change when viewed from different inertial reference frames. (This is an experimental observation.)

On the other hand, a quantity is conserved if its value does not change as a function of time. In physics, the difference is that a quantity can be conserved *in a particular inertial reference frame* but not be invariant.

*Example 19.4* For those with a physics background, the 4-momentum $p^\mu = (E/c^2, \mathbf{p})$ is a conserved quantity. However, it is not Lorentz invariant. In fact, it is a Lorentz vector so in a different (call it primed) frame the quantity is $p'^\mu = L^\mu{}_\nu p^\nu$ when $L^\mu{}_\nu$ describes a Lorentz transformation.

## 19.3 The Euler-Lagrange equations

Consider the following combination of kinetic ($T$) and potential ($V$) energies:

$$L \equiv T - V. \tag{19.1}$$

This $L$ is called the Lagrangian. You are most likely used to seeing the combination $T + V$ in your introductory physics, which is the total energy. Consider a mass $m$ attached to a spring with spring constant $k$. We model this with $T = m\dot{x}^2/2$ and $V = kx^2/2$ so that

$$L = \frac{1}{2}m\dot{x}^2 - \frac{1}{2}kx^2. \tag{19.2}$$

Now consider the following equation:

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{x}}\right) = \frac{\partial L}{\partial x}. \tag{19.3}$$

This equation is called the Euler-Lagrange (E-L) equation. For now, don't worry where this combination comes from. For the mass on a spring, we have $\partial L/\partial \dot{x} = m\dot{x}$ and $\partial L \partial x = -kx$ so that Equation 19.3 gives

$$m\ddot{x} = -kx. \tag{19.4}$$

This equation is precisely what you would get if you applied Newton's equation $F = ma$ to the system. If there are more degrees of freedom, you apply the (E-L) equation to each additional variable.

Of course, this example is quite simple so this may appear to only be a happy little accident. Consider a slight generalization of our example, and suppose that instead of a spring we had an arbitrary potential $V(x)$. Then

$$L = \frac{1}{2}m\dot{x}^2 - V(x) \tag{19.5}$$

and the E-L equation gives

$$m\ddot{x} = -\frac{dV}{dx}. \tag{19.6}$$

However, the negative of the derivative of the potential energy gives the force acting on the object, so once again this gives $F = ma$. Generalizing to three spatial dimensions, we have $V(x, y, z)$ and

$$L = \frac{1}{2}m(\dot{x}^2 + \dot{y}^2 + \dot{z}^2) - V(x, y, z) \tag{19.7}$$

so the the E-L equations give

$$m\ddot{\mathbf{x}} = -\nabla V. \tag{19.8}$$

Once again, $-\nabla V = \mathbf{F}$ so this gives Newton's second law $\mathbf{F} = m\mathbf{a}$.

In a classical mechanics course, one would do many more examples and see that this is not an accident but another way to do classical mechanics that is equivalent to Newton's formulation. A benefit of this Lagrangian formulation of classical mechanics is that the involved quantities are scalars. $T$, the kinetic energy, is a scalar and is $V$, the potential energy. For more complicated systems, the Lagrangian formalism is a quite a bit easier as one does not need to worry about the vector nature of forces. This helps minimize errors due to signs. Once you get $T, V$ you plug them into the E-L equations and the equations will be the same as the more tedious Newton method.

## 19.4 The Principle of Stationary Action

Consider the following quantity:

$$S \equiv \int_{t_1}^{t_2} L(x, \dot{x}, t)dt. \tag{19.9}$$

This $S$ is called the action. In SI units, $S$ has units of (energy)×(time), which is the same units as angular momentum. $S$ depends on $L$, which depends on $x(t)$. Given any function $x(t)$, one can compute the relevant $L$ and, hence, the relevant $S$. Integrals such as $S$ are called functionals and $S$ is sometimes denoted $S[x(t)]$ to remind us of the fact that $S$ depends on $x(t)$. That is, $x(t)$ depends on one input $t$ whereas $S[x(t)]$ needs the entire function $x(t)$ in order to be calculated. If you want, you can think of $S$ as a function that depends on infinitely many values, which we label by $x(t)$. If you feel uneasy about infinites, imagine breaking up the time interval $[t_1, t_2]$ into pieces and then the integral can be approximated by a discrete sum.

Now suppose that $x(t)$ is fixed at the end points $x(t_1) = x_1$ and $x(t_2) = x_2$ but is otherwise arbitrary. What function $x(t)$ leads to a stationary value of $S$? A stationary value, like the calculus the reader is familiar with, is a minimum, maximum, or a saddle point.

**Theorem 19.1** *If the function $x_s(t)$ is fixed at the endpoints ($x_s(t_1) = x_1, x_s(t_2) = x_2$) and yields a stationary value of $S[x(t)]$ then it satisfies*

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{x}_s}\right) = \frac{\partial L}{\partial x_s}.$$

*Again, it is understood that we are considering the class of functions whose endpoints are fixed.*

***Proof*** If $S[x(t)]$ is stationary at $x_s(t)$ then this means that any other function close to $x_s(t)$ and satisfying the same conditions at the endpoints should have the same value as $S[x_s(t)]$, to first order in the deviation.

Suppose that $S[x(t)]$ is stationary at $x_s(t)$. Consider a function

$$x_s(t) \equiv x_s(t) + \epsilon\delta(t), \tag{19.10}$$

where $\delta(t)$ is some deviation from $x_s(t)$ that satisfies $\delta(t_1) = 0$ and $\delta(t_2) = 0$. Now, notice that

$$\begin{aligned}\frac{\partial}{\partial \epsilon}S[x(t)] &= \frac{\partial}{\partial \epsilon}\int_{t_1}^{t_2} L dt \\ &= \int_{t_1}^{t_2} \frac{\partial L}{\partial \epsilon} \\ &= \int_{t_1}^{t_2} \left(\frac{\partial L}{\partial x}\frac{\partial x}{\partial \epsilon} + \frac{\partial L}{\partial \dot{x}}\frac{\partial \dot{x}}{\partial \epsilon}\right) dt. \end{aligned} \tag{19.11}$$

We have that

$$\frac{\partial x}{\partial \epsilon} = \delta \tag{19.12}$$

$$\frac{\partial x}{\partial \epsilon} = \dot{\delta}, \tag{19.13}$$

so that

$$\frac{\partial}{\partial \epsilon}S[x(t)] = \int_{t_1}^{t_2} \left(\frac{\partial L}{\partial x}\delta + \frac{\partial L}{\partial \dot{x}}\dot{\delta}\right) dt. \tag{19.14}$$

Integrate that second-term by parts, to get

$$\frac{\partial}{\partial \epsilon}S[x(t)] = \int_{t_1}^{t_2} \delta \cdot \left(\frac{\partial L}{\partial x} - \frac{d}{dt}\frac{\partial L}{\partial \dot{x}}\right) dt + \frac{\partial L}{\partial \dot{x}}\dot{\delta}|_{t_1}^{t_2}. \tag{19.15}$$

Since $\delta(t_1) = \delta(t_2) = 0$, the boundary terms vanish and we find that

$$\frac{\partial}{\partial \epsilon}S[x(t)] = \int_{t_1}^{t_2} \delta \cdot \left(\frac{\partial L}{\partial x} - \frac{d}{dt}\frac{\partial L}{\partial \dot{x}}\right) dt. \tag{19.16}$$

By assumption, $S$ is stationary at $x_s(t)$ which means that $\partial S/\partial\epsilon = 0$ when evaluated at $\epsilon = 0$. Therefore,

$$0 = \int_{t_1}^{t_2} \delta\left(\frac{\partial L}{\partial x} - \frac{d}{dt}\frac{\partial L}{\partial \dot{x}}\right) dt \tag{19.17}$$

for any $\delta$ at $\epsilon = 0$. This means that

$$\frac{\partial L}{\partial x_s} - \frac{d}{dt}\frac{\partial L}{\partial \dot{x}_s} = 0. \tag{19.18}$$

□

We see that the Euler-Lagrange equation isn't unmotivated. It follows by looking for an $x(t)$ for which $S[x(t)]$ is stationary. Therefore, we can replace the $F = ma$ mantra familiar from high school physics with the following principle.

- **The principle of stationary action**: The path $x(t)$ of a particle observed in classical mechanics is the one that yields a stationary value of the action $S[x(t)]$.

This principle is sometimes called Hamilton's principle. It is equivalent to $\mathbf{F} = m\mathbf{a}$ since, by reading the proof of backwards, one can see that the Euler-Lagrange equations hold for $x(t)$ if and only the action $S$ is stationary for $x(t)$ and, as we have tried to motivate, the Euler-Lagrange equations are equivalent to $F = ma$. If there are more variables $x_1(t), \ldots, x_n(t)$ then the principle of stationary action is still applicable. The E-L equation could for each $x_i(t)$ and each such equation is equivalent to the corresponding component of $\mathbf{F} = m\mathbf{a}$ equation.

Of course, all this does is change the question of "Where does the Euler-Lagrange come from?" to "where does the principle of stationary action come from?" We leave such discussions to the physics textbooks.

By the way, we have been using Cartesian coordinates, but actually one can show that any change of basis from $\{x_i\}$ to $\{q_i\}$ still requires the E-L equations to be satisfied. That is, if

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{x}_i}\right) = \frac{\partial L}{\partial x_i} \tag{19.19}$$

for all $i$ then after a change of coordinates to

$$q_i = q_i(x_1, \ldots, x_n) \tag{19.20}$$

one still has

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}_i}\right) = \frac{\partial L}{\partial q_i} \tag{19.21}$$

for all $i$.

Therefore, if the E-L equations are valid in one coordinate system, then they are valid in all other coordinate systems. We have argued that they are valid in the

Cartesian coordinate systems for physical system. Thus, the E-L equations hold for any coordinate system used to describe the physics of some system.

## 19.5 Conservation Laws

### 19.5.1 Cyclic coordinates

Suppose we use the coordinate $\{q_i\}$ to describe our system. Suppose that the Lagrangian $L$ does not depend on $q_k$ for some $k$. Then

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}_k}\right) = \frac{\partial L}{\partial q_k} = 0 \tag{19.22}$$

$$\Rightarrow \frac{\partial L}{\partial \dot{q}_k} = C \tag{19.23}$$

for some $C$ that does not depend explicitly on $t$. We say that such a $q_k$ is a cyclic coordinate and that $\frac{\partial L}{\partial \dot{q}_k}$ is a conserved quantity. If the $\{q_i\}$ are the Cartesian coordinates, then $\partial L/\partial \dot{q}_k = m\dot{q}_k$ for all $k$ (assuming that the potential energy does not depend on velocity). Therefore, if $L$ does not explicitly depend on $q_k$ we see that $m\dot{q}_k$ is a conserved quantity. This is just the momentum in the $k^{th}$ direction, so we see that this is just a statement of conservation of momentum. For this reason, $\partial L/\partial \dot{q}_k$ is called the generalized momentum conjugate to the coordinate $q_k$.

*Example 19.5* **Linear momentum:** Suppose you are standing on a flat surface, which we consider to be the $x$-$y$ plane. Consider throwing a ball of mass $m$ into the air (the $z$ direction). Including 3 spatial degrees of freedom, the Lagrangian is

$$L = \frac{1}{2}m(\dot{x}^2 + \dot{y}^2 + \dot{z}^2) - mgz. \tag{19.24}$$

We see that $L$ does not depend on $x$ or $y$. Thus, we know that $\partial L/\partial \dot{x} = m\dot{x}$ and $\partial L/\partial \dot{y} = m\dot{y}$ are conserved quantities. In fact, these are just the $x$ and $y$ components of the momentum $\mathbf{p}$ of the ball. The Lagrangian doesn't depend on $x$ or $y$, so it shouldn't matter at one point in the plane one throws the ball upwards. All $x$ and $y$ points are "the same" and so the quantities that are important to the physics should also have this symmetry. We see that conservation of linear momentum along a particular Cartesian direction can be deduced from the translational invariance of the system along that direction.

*Example 19.6* **Angular momentum:** Consider a potential that only depends on the distance of the particle from the $z$ axis. The Cartesian coordinates would not be ideal in this case. Consider using cyclindrical coordinates $(\rho, \phi, z)$. In cylindrical coordinates, the Lagrangian is

$$L = \frac{1}{2}m(\dot{\rho}^2 + \rho^2\dot{\phi}^2 + \dot{z}^2) - V(\rho). \tag{19.25}$$

$L$ does not depend on $z$ or $\phi$. Therefore, $\partial L/\partial \dot{z} = m\dot{z}$ and $\partial L/\partial \dot{\phi} = m\rho^2\dot{\phi}$ are time-independent. The quantity $m\dot{z}$ is just the $z$ component of the linear momentum of the particle. What about $m\rho^2\dot{\phi}$. Note that $\rho\dot{\phi} = v_\phi$ is the instantaneous velocity of the particle in the $\mathbf{e}_\phi$ direction. Thus, we see that

$$\begin{aligned} \partial L/\partial \dot{\phi} &= m\rho^2\dot{\phi} \\ &= m\rho v_\phi \\ &= m(\mathbf{r} \times \mathbf{v})_\phi. \end{aligned} \tag{19.26}$$

We see that the second conserved quantity is the angular momentum of the particle around the $z$ axis. We see that conservation of angular momentum around the $z$ axis can be deduced from the rotational invariance of the system around the $z$ axis.

### 19.5.2 Time-invariance

In the previous discussion, we considered the coordinates $\{q_i\}$ as parametrized by $t$. We saw that is $L$ does not explicitly depend on $q_k$, then there is a conserved quantity. What if $L$ does not explicitly depend on $t$? Conservation of energy arises when the Lagrangian $L$ does not explicitly depend on $t$. This is slightly different from the previous discussion, since $t$ is not a coordinate that the stationary-action principle applies to. You can vary $\{q_i\}$ but it does not make sense to vary $t$, as $t$ is integrated over to get the action $S$. (As a side note, this is because we are discussing classical mechanics. Special relativity treats position and time equally, in that they get mixed up during a change of reference frame. Including Lorentz invariance in, for example, quantum field theories leads to a slightly different form of the conservation laws we have seen so far since $t$ is treated on equal footing as all the other spatial coordinates.) Therefore, the conservation of a quantity due to $dL/dt = 0$ must be proved differently than in the previous discussion. Consider the quantity

$$E = \left( \sum_{i=1}^{N} \frac{\partial L}{\partial \dot{q}_i} \dot{q}_i \right) - L. \tag{19.27}$$

It turns out that $E$ is usual the quantity that one considers as the energy. We will mention the motivation for introducing this $E$ later on, so accept for now that $E$ is an interesting and useful definition.

**Theorem 19.2** *If the Lagrangian has no explicit time dependence ($\partial L/\partial t = 0$) and the Euler-Lagrange equations are satisfied, then $E$ is conserved ($dE/dt = 0$).*

***Proof*** The proof is just an exercise in the chain rule. Start from the definition of $E$ and differentiate.

$$\begin{aligned}\frac{dE}{dt} &= \frac{d}{dt}\left(\sum_{i=1}^{N}\frac{\partial L}{\partial \dot{q}_i}\dot{q}_i\right) - \frac{dL}{dt} \\ &= \sum_{i=1}^{N}\left(\frac{\partial L}{\partial \dot{q}_i}\ddot{q}_i + \left(\frac{d}{dt}\frac{\partial L}{\partial \dot{q}_i}\right)\dot{q}_i\right) - \left(\sum_{i=1}^{N}\left(\frac{\partial L}{\partial q_i}\dot{q}_i + \frac{\partial L}{\partial \dot{q}_i}\ddot{q}_i\right) + \frac{\partial L}{\partial t}\right) \\ &= \sum_{i=1}^{N}\underbrace{\left[\left(\frac{d}{dt}\frac{\partial L}{\partial \dot{q}_i}\right) - \frac{\partial L}{\partial q_i}\right]}_{0}\dot{q}_i - \frac{\partial L}{\partial t} \\ &= -\frac{\partial L}{\partial t}.\end{aligned} \tag{19.28}$$

Thus, we see that if there is no explicit dependence of $L$ on $t$ (that is, $\partial L/\partial t = 0$), then $dE/dt = 0$. □

*Example 19.7* Suppose that the Lagrangian is

$$L = \frac{1}{2}m(\dot{x}^2 + \dot{y}^2 + \dot{z}^2) - V(x, y, z). \tag{19.29}$$

Then the definition of $E$ gives

$$E = \frac{1}{2}m(\dot{x}^2 + \dot{y}^2 + \dot{z}^2) + V(x, y, z), \tag{19.30}$$

which is indeed the total energy for a classical system.

It might seem like we did a whole lot of work for no reason, but actually the point is that this method proves conservation of energy in the Lagrangian formalism, without ever having to mention Newtonian methods.

In sum, we saw that

- translational invariance implied conservation of linear momentum.
- rotational invariance implied conservation of angular momentum.
- time translation invariance implied conservation of energy.

The quantity $E$ will be equal to the energy of the system if the entire system is represented by the Lagrangian. This means that the system must be a closed system, with no external forces acting on it. If the system is open, one can still use $E$ and it will be conserved if $\partial L/\partial t$ but it may not necessarily be the energy on the system that one thinks of in physics. For further discussions, I recommend reading Chapter 6 of David Morin's "Introduction to Classical Mechanics: With Problems and Solutions."

## 19.6 Noethers's Theorem

We have seen that conservation laws and symmetries seem related. A theorem by Noether provides a procedure for going from the action integrand (the Lagrangian) directly to the conserved quantity without having to consider equations of motions explicitly in intermediate steps. For concreteness, let's see the idea behind Noether's theorem in an example.

*Example 19.8* Let us illustrate the insight needed to prove Noether's theorem in the case of angular momentum, whose conservation follows, for example, from the rotational symmetry of a central force problem. The action for the central force problem (with motion restricted to a 2-D plane, for simplicity) is

$$S = \int_0^T \left(\frac{1}{2}m(\dot{r}^2 + r^2\dot{\phi}^2) - V(r)\right) dt. \tag{19.31}$$

We note that the action (and, also, the integrand) is left invariant under the variation

$$\phi(t) \to \phi(t) + \epsilon\alpha, \tag{19.32}$$

where $\epsilon\alpha$ is just some constant that we have chosen to write as $\epsilon\alpha$ with $\epsilon$ being a small, time-independent parameter. This invariance is the symmetry from which would we like to derive a conserved quantity. Note that so far, this is a mathematical identity. That is, no physics was needed to interpret any statements by, for example, requiring that the principle of stationary action be obeyed and, hence, that $r$ and $\phi$ obey the Euler-Lagrange equations.

Suppose now that $r$ and $\phi$ *do* obey the Euler-Lagrange equations. This means that $S$ is stationary for *any* infinitesimal variations in $r$ and $\phi$. In particular, $S$ must still be invariant under the specific variation

$$\phi(t) \to \phi(t) + \epsilon(t)\alpha \tag{19.33}$$

where now $\epsilon(t)$ is allowed to be time-dependent. The action still being stationary here is not just a mathematical identity, but follows from the fact that $r, \phi$ obey the equations of motion, which we interpret as having physical content. Proceeding,

$$\begin{aligned}\Delta S &= \int_0^T \left(\frac{m}{2}(\dot{r}^2 + r^2(\dot{\phi} + \dot{\epsilon}\alpha)^2) - V(r)\right) dt - \int_0^T \left(\frac{m}{2}(\dot{r}^2 + r^2\dot{\phi}^2) - V(r)\right) dt \\ &= \int_0^T \frac{m}{2}r^2(2\dot{\phi}^2\dot{\epsilon}\alpha + \dot{\epsilon}^2\alpha^2)dt.\end{aligned} \tag{19.34}$$

To linear order in the variation,

$$\delta S = \alpha \int_0^T (mr^2\dot{\phi})\dot{\epsilon}dt. \tag{19.35}$$

Notice that $\delta S$ depends on $\dot{\epsilon}$ and not just $\epsilon$. This makes sense since we saw that $\delta S = 0$ as a mathematical identity when $\epsilon$ is time-independent. Now, we want variations to $r(t)$ and $\phi(t)$ which are still fixed at the endpoints (recall that we considered the class of functions with fixed endpoints in the derivation of the Euler-Lagrange equations) so this requires $\epsilon(0) = \epsilon(T) = 0$. This allows an integration by parts to move the derivative off $\dot{\epsilon}$, at the introduction of a minus sign

$$\delta S = \alpha \int_0^T \left( \frac{d}{dt}(mr^2\dot{\phi}) \right) \epsilon(t) dt. \tag{19.36}$$

Here is the punch line. The fact that $r, \phi$ satisfies the equations of motions means that $\delta S = 0$ under any infinitesimal variations. Thus, given any infinitesimal variation $\epsilon(t)\alpha$ to $\phi(t)$, we must have $\delta S = 0$. This means that the coefficient of $\epsilon(t)$ in the above expression for $\delta S$ must be 0. That is,

$$0 = \frac{d}{dt}(mr^2\dot{\phi}), \tag{19.37}$$

which is a statement of the conservation of angular momentum. There is technically an $\alpha$, but we can divide it out to keep only the physical variables.

This suggests a general strategy.

i) Look for an invariance of the action $S$ under some symmetry transformation of the inputs to $S$ with a time-independent parameter. For such cases, the variation of the action is 0 as a mathematical identity, independent of whether the Euler-Lagrange equations are satisfied.
ii) Note that if the dynamical variables *do* satisfy the Euler-Lagrange equations then the action must be stationary for any infinitesimal variable of the dynamical variables, even if the time-independent parameter is changed to a time-dependent parameter.
iii) The resulting variation $\delta S$ of the action $S$ to linear order in the parameter will depend on the total time derivative of the parameter. In cannot depend on the parameter itself since, by construction/observation in the first part, $\delta S = 0$ as a mathematical identity when the parameter is time-independent.
iv) Integrate by parts to remove the time derivative from the time-dependent parameter and into whatever was its coefficient.
v) Since the parameter can be arbitrary and we must have $\delta S = 0$ due to the stationary of $S$ when the dynamical variables obey the Euler-Lagrange equations, the coefficient of the time-dependent variable will be a time derivative of some quantity. This time derivative must equal to 0. Thus, we have found a conserved quantity.

Actually, in many cases the Lagrangian itself posses the symmetry rather than only the action. This is a slightly strong statement since the Lagrangian can different by a total derivative after a transformation, but the integral of $dt$ of the total derivative can vanish so that the action is invariant while the Lagrangian changes by a total derivative. When the Lagrangian itself has a derivative, a version of Noether's theorem is straightforward to prove.

**Theorem 19.3** *Noether's theorem - If a Lagrangian has a continuous symmetry then, when the equations of motion as satisfied, there exists a conserved quantity whose conservation is related to the symmetry.*

***Proof*** In this case, continuous symmetry means that the change in the dynamical variables (the coordinates) can be continuously parameterized, where the parameter can be infinitesimally small. Suppose the Lagrangian is invariant, to first order in the small parameter $\epsilon$, under the change of coordinates

$$q_i \to q_i + \epsilon K_i(q), \tag{19.38}$$

where each $K_i(q)$ can depend on all the $q_i$, which we denote as $q$. The Lagrangian is invariant to first order in $\epsilon$, so

$$\begin{aligned} 0 &= \frac{dL}{d\epsilon} \\ &= \sum_i \left( \frac{\partial L}{\partial q_i} \frac{\partial q_i}{\partial \epsilon} + \frac{\partial L}{\partial \dot{q}_i} \frac{\partial \dot{q}_i}{\partial \epsilon} \right) \\ &= \sum_i \left( \frac{\partial L}{\partial q_i} K_i + \frac{\partial L}{\partial \dot{q}_i} \dot{K}_i \right). \end{aligned} \tag{19.39}$$

By assumption, the $q$ satisy the Euler-Lagrange equations so this is the same as

$$\begin{aligned} 0 &= \sum_i \left( \left( \frac{d}{dt} \frac{\partial L}{\partial \dot{q}_i} \right) K_i + \frac{\partial L}{\partial \dot{q}_i} \dot{K}_i \right) \\ &= \frac{d}{dt} \left( \sum_i \frac{\partial L}{\partial \dot{q}_i} K_i \right). \end{aligned} \tag{19.40}$$

Thus, $\sum_i \frac{\partial L}{\partial \dot{q}_i} K_i$ is a conserved quantity. □

In sum, we see that Noether's theorem formalizes the idea that

continuous symmetry ⇔ conserved quantity.

## Problems

**19.1** Consider a particle with electric charge $q$ with Lagrangian

$$L(\mathbf{x}, \dot{\mathbf{x}}) = \frac{1}{2} m \dot{\mathbf{x}}^2 - q\phi(\mathbf{x}) + q\dot{\mathbf{x}} \cdot \mathbf{A}(\mathbf{x}).$$

Here, $\phi(\mathbf{x})$ is the electrical potential and $\mathbf{A}(\mathbf{x})$ is the magnetic vector potential. Show that the Euler-Lagrange equations lead to

$$m\ddot{\mathbf{x}} = q(\mathbf{E} + \dot{\mathbf{x}} \times \mathbf{B}) \tag{19.41}$$

where

$$\mathbf{E} = -\nabla\phi - \frac{\partial \mathbf{A}}{\partial t}$$
$$\mathbf{B} = \nabla \times \mathbf{A}$$

are the electric and magnetic fields, respectively. Of course, Equation 19.41 is the equation of a charged particle in an electromagnetic field that one learns in a classical electrodynamics course.

# Chapter 20
# Coupled Oscillators

**Abstract** Group theory can provide insight into the structure of the spectrum of a physical system.

## 20.1 Two Coupled Oscillators - No Group Theory

Consider two identical blocks of mass $m$ coupled together by a spring with spring constant $k$. See Figure 20.1.

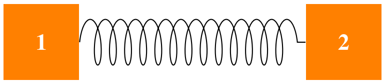


Fig. 20.1: Two blocks coupled by a spring obeying Hooke's law.

Suppose that the center of mass of the blocks is not moving. Let $x_1(t)$ and $x_2(t)$ be the deviation of the blocks *from their equilibrium positions* (in particular, not relative to the origin of a common coordinate system). The Lagrangian is

$$L = \frac{1}{2}m\dot{x}_1^2 + \frac{1}{2}m\dot{x}_2^2 - \frac{1}{2}k(x_1 - x_2)^2. \tag{20.1}$$

Then

$$\frac{\partial L}{\partial x_1} = -k(x_1 - x_2) \tag{20.2}$$

$$\frac{\partial L}{\partial x_2} = k(x_1 - x_2) \tag{20.3}$$

$$\frac{\partial L}{\partial \dot{x}_1} = m\dot{x}_1 \tag{20.4}$$

$$\frac{\partial L}{\partial \dot{x}_2} = m\dot{x}_2. \tag{20.5}$$

Apply the Euler-Lagrange equations to get

$$\frac{\partial L}{\partial x_1} - \frac{d}{dt}\left(\frac{\partial L}{\partial \dot{x}_1}\right) = 0 \Rightarrow -k(x_1 - x_2) = m\ddot{x}_1, \tag{20.6}$$

$$\frac{\partial L}{\partial x_2} - \frac{d}{dt}\left(\frac{\partial L}{\partial \dot{x}_2}\right) = 0 \Rightarrow k(x_1 - x_2) = m\ddot{x}_2. \tag{20.7}$$

Let us write this in matrix form.

$$m\frac{d^2}{dt^2}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} -k & k \\ k & -k \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{20.8}$$

$$m\frac{d^2}{dt^2}X = -KX, \tag{20.9}$$

where we have defined $X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ and $K = \begin{bmatrix} k & -k \\ -k & k \end{bmatrix}$. Let's look for solutions of the form

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} e^{-i\omega t} \tag{20.10}$$

$$X \equiv \tilde{X}e^{-i\omega t}. \tag{20.11}$$

Then the equations of motion become

$$-m\omega^2\begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} -k & k \\ k & -k \end{bmatrix}\begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} \tag{20.12}$$

$$\Rightarrow m\omega^2\tilde{X} = K\tilde{X}. \tag{20.13}$$

This is an eigenvalue problem. The eigenvalues of the matrix $K$ are found from

$$\det(\lambda I_{2\times 2} - K) = \det\begin{bmatrix} \lambda - k & k \\ k & -k \end{bmatrix} = 0 \tag{20.14}$$

$$(\lambda - k)^2 - k^2 = 0 \tag{20.15}$$

$$\lambda = k \pm k. \tag{20.16}$$

Thus, we see that $m\omega^2 = k \pm k$. That is, $\omega = 0$ and $\omega = \sqrt{\frac{2k}{m}}$ satisfy the eigenvalue equation. If $m\omega^2 = 0$, then

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} k & -k \\ -k & k \end{bmatrix} \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} \tag{20.17}$$

so that $\tilde{x}_1 = \tilde{x}_2$. If $m\omega^2 = 2k$, then

$$2k \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} k & -k \\ -k & k \end{bmatrix} \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} \tag{20.18}$$

so that $\tilde{x}_1 = -\tilde{x}_2$. Choose an orthonormal eigenbasis

$$\mathbf{f}_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{20.19}$$

$$\mathbf{f}_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}. \tag{20.20}$$

Then any solutions $x_1(t), x_2(t)$ can be written

$$\begin{aligned} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} &= A\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} e^{-i0t} + B\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} e^{-i\sqrt{\frac{2k}{m}}t} \\ &= A\mathbf{f}_1 + B\mathbf{f}_2 e^{-i\sqrt{\frac{2k}{m}}t} \end{aligned} \tag{20.21}$$

for some constants $A, B$.

- If $A \neq 0, B = 0$, then $x_1 = x_2$. This means that both blocks move the same distance and in the same direction from their equilibrium points. Of course, if this happens then the spring is not stretched at all from its equilibrium length. This corresponds to both blocks sliding at the same velocity, so that the spring is unstretched. In such cases, the blocks appear to not be moving in the center of mass frame. That is, they do not oscillate in the center of mass frame, so $\omega = 0$.
- If $A = 0, B \neq 0$ then $x_1 = -x_2$. This means that both blocks move the same distance from their equilibrium positions, but it opposite directions. In the center of mass frame, the blocks appear to move back and forth together but in opposite directions.

The point of Equation 20.21 is that the general motion of the two blocks is a linear combination of these two motions. The general motion can be thought of the center of mass moving uniformly across the surface where the blocks don't oscillate at all in the center of mass frame plus an oscillation of the two blocks in, as seen in the center of mass frame, opposite directions with some amplitude of oscillation $B$.

## 20.2 Two Coupled Oscillators - With Group Theory

Let us now consider the problem again, but let us use the fact the the problem has a symmetry. The system looks exactly the same after reflecting through the center of mass of the two blocks. You can think of this is a few ways. You can imagine swapping the blocks, or reflecting the system around the center of mass. See Figure 20.2.

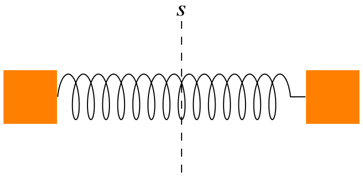


Fig. 20.2: Two equivalent blocks coupled by a spring obeying Hooke's law possess reflection symmetry around their center of mass.

The physics shouldn't change since, by assumption, the blocks are equivalent in the classical mechanics sense. That is, we are assuming they have the same size, shape, mass, etc. It should be clear that if they are swapped, then there should be no observable difference in the dynamics of the system. This symmetry group is $S_2 \cong \mathbb{Z}_2$. We already saw that the equations of motion can be written as

$$m\frac{d^2}{dt^2}X = -KX, \tag{20.22}$$

or, in the frequency domain, as

$$m\omega^2\tilde{X} = K\tilde{X}. \tag{20.23}$$

The $\tilde{X}$ vectors are eigenvectors of $K$, with eigenvalues $m\omega^2$. As soon as you see this eigenvalue problem, your first instinct is probably to compute the characteristic polynomial, find the eigenvalues, find the eigenvectors, etc just like we did above. It might seem like this is the only thing one can do, and that one needs to know what $K$ is for the system in order to do this procedure. However, even if we didn't know the full form of $K$, it turns out that we can still say some meaningful things about the solutions by using the known symmetries. Consider reflecting around the center of mass. Then it is clear that $x_1 \mapsto -x_2$ and $x_2 \mapsto x_1$. This corresponds to acting by

$$\rho_s = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \tag{20.24}$$

on the $\tilde{X}$ (and also the time-dependent $X$) column matrix. Again, the point is that the physics should be unchanged, meaning that $\rho_s\tilde{X}$ should obey the same equations required by physics:

$$m\omega^2\rho_s\tilde{X} = K\rho_s\tilde{X}. \tag{20.25}$$

However, we can also multiply $m\omega^2\tilde{X} = K\tilde{X}$ on the left by $\rho_s$ to find that

$$m\omega^2\rho_s\tilde{X} = \rho_s K\tilde{X} \tag{20.26}$$

$$m\omega^2\rho_s\tilde{X} = \rho_s K\rho_s^{-1}\rho_s\tilde{X}. \tag{20.27}$$

Since this holds for all $\tilde{X}$[1], we conclude that $\rho_s K\rho_s^{-1} = K$. Let us define

$$\rho_e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{20.28}$$

Then it is also true, trivially, that $\rho_e K\rho_e^{-1} = K$. However, note that $\{\rho_e, \rho_s\}$ form a degree-2 representation of $S_2 \cong \mathbb{Z}_2$. The symmetry group here is abelian. We know from previous chapters that this means that the representation $\rho$ must be reducible (see Theorem 16.19 or Theorem 16.18). That is, there exists an invertible matrix $\tau$ such that $\tau\rho_e\tau^{-1} \equiv \tilde{\rho}_e$ and $\tau\rho_s\tau^{-1} \equiv \tilde{\rho}_s$ break into smaller block-diagonal form. Since $\rho_e, \rho_s$ are 2-by-2, this means that $\tau\rho_2\tau^{-1}$ and $\tau\rho_s\tau^{-1}$ are diagonal. From, $\rho_g K\rho_g^{-1} = K$ for all $g \in G$, we conclude that $\tilde{\rho}_g\tau K\tau^{-1}\tilde{\rho}_g^{-1} = \tau K\tau^{-1}$. Since $\tilde{\rho}_g$ is in block-diagonal form, where the blocks are irreducible representations of $G$, Schur's lemma tells us that

$$\tau K\tau^{-1} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \tag{20.29}$$

for some $\lambda_1, \lambda_2$. It is clear that $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is an eigenvector of the right-hand side with eigenvalue $\lambda_1$ and that $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is an eigenvector of the right-hand side with eigenvalue $\lambda_2$. Therefore,

$$\tau K\tau^{-1}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \lambda_1\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad \tau K\tau^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \lambda_2\begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{20.30}$$

But this means that

$$K\tau^{-1}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \lambda_1\tau^{-1}\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad K\tau^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \lambda_2\tau^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{20.31}$$

That is, $\tau^{-1}\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\tau^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are eigenvectors of $K$, with eigenvectors $\lambda_1, \lambda_2$, respectively.

[1] In this simple physics model, $\tilde{X}$ is unconstrained. Of course, if $\tilde{X}$ gets too large then this harmonic oscillator model will break down and it won't be an accurate model in the real-world.

Without doing more work, this is all we can say. However, let's do a bit more work. First, let's find what $\tau$ is. Verify that

$$\tau = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{20.32}$$

satisfies

$$\tau \rho_e \tau^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{20.33}$$

$$\tau \rho_s \tau^{-1} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{20.34}$$

Therefore, this is a $\tau$ that Schur's lemma states exists. Then, by our discussion above, we know that

$$\tau^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{20.35}$$

is an eigenvector with eigenvalue $\lambda_1$ and

$$\tau^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{20.36}$$

is an eigenvector with eigenvalue $\lambda_2$. We see the normal modes that we found previously appearing.

What if we work a bit more? Suppose we knew that

$$K = \begin{bmatrix} k & -k \\ -k & k \end{bmatrix}. \tag{20.37}$$

Then we know that $\tau K \tau^{-1}$ is diagonal, and we can calculate to find

$$\begin{bmatrix} 0 & 0 \\ 0 & 2k \end{bmatrix}. \tag{20.38}$$

Thus, the eigenvalues of $K$ are $\lambda_1 = 0$ and $\lambda_2 = 2k$.

In the end, we have found the entire solution. This seems like a silly exercise. It certainly seems as if we have used a sledgehammer to crack a nut. Let's recap what we have seen, and see what depends on the specifics of the problem and what can be deduced using group theory alone.

- We have a physical system (in this case, involving a harmonic oscillator) which is governed by some equations of motion which can be cast into an eigenvalue problem $K\tilde{X} = \lambda\tilde{X}$.
- The physical system has some symmetries. Denote the symmetry group $G$. Let this symmetry group act on $\tilde{X}$, with matrices $\rho_g$. The statement that the system has a symmetry group $G$ is embodied in $\rho_g K \rho_g^{-1} = K$ for all $g \in G$.

- Since $\{\rho_g \mid g \in G\}$ is a representation of $G$, we can ask if it is reducible or irreducible. If it is irreducible, this means that there exists an invertible $\tau$ such that $\tau\rho_g\tau^{-1}$ is block-diagonal for all $g$, with the blocks being irreducible representations of $G$.
- From $\rho_g K\rho_g^{-1} = K$, we find $\tilde{\rho}_g\tau K\tau^{-1}\tilde{\rho}_g^{-1} = \tau K\tau^{-1}$, where $\tilde{\rho}_g = \tau\rho_g\tau^{-1}$ for all $g \in G$. Schur's lemma then requires that $\tau K\tau^{-1}$ be block-diagonal, and the blocks along the diagonal are proportional to the identity matrix within that subspace.
- We observe that $\tau^{-1}\mathbf{e}_i$ is an eigenvector of $K$ where eigenvalue is the constant multiplying the identity submatrix along the diagonal of $\tau K\tau^{-1}$ that we know exists due to Schur's lemma.
- In particular, we know that the number of eigenvalues of the $K$ that will have the same value is (at least) equal to the number of times an irrep appears in $\rho$ times the dimensional of that irrep.

Let us stop here. The last sentence is what we wish to focus on. In particular, no knowledge about the form of $K$ is needed to reach the last bullet point. Therefore, we see that group theory lets us predict some structure/pattern in the eigenvalues of $K$ independent of the actual details $K$. In physics terms, this means we can predict patterns in the eigenvalues (that it ultimately related to the dynamics of a system) are "independent of the microscopic details." Many physical systems can have different $K$ that describe their dynamics, but as long as they have the same symmetry group $G$ then we predict that the eigenvalues will have the same pattern, though the exact values of those eigenvalues will differ and depend on the exact form of $K$.

Before formalizing our observations even more, let's do another example that is a bit more complex to convince ourselves that what we are doing actually provides useful information.

## 20.3 Three Blocks and Springs

The previous example involved two blocks coupled by spring obeying Hooke's law. We restricted the motion along one dimension, and the symmetry there was reflection around the center of mass of the two equivalent blocks. This symmetry was isomorphic to $S_2$ (which is isomorphic to $\mathbb{Z}_2$). Suppose now that we have three identical (in the classical sense) blocks of mass $m$ that are coupled by three identical springs with spring constants $k$. See Figure 20.3.

The blocks are labeled 1, 2, and 3. We restrict the motion to a plane. Label the coordinates of blocks 1, 2, 3 *relative to their equilibrium positions* (in particular, not relative to the origin of a common coordinate system) as $(x_1, y_1)$, $(x_2, y_2)$, and $(x_3, y_3)$, respectively. The $x$ coordinates are horizontal deviations from the equilibrium positions, and the $y$ coordinates are vertical deviations from the equilibrium positions. Let $R(\phi)$ be rotation by angle $\phi$

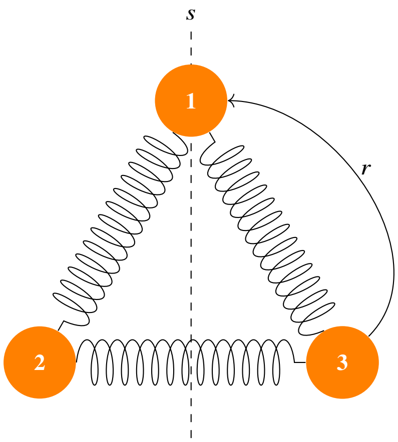


Fig. 20.3: A system of coupled cylindrical blocks, say, with reflection and rotation symmetries. The symmetry group is $D_3$ (which is isomorphic to $S_3$, which can be thought of as permuting the blocks 1, 2, 3 among themselves).

$$R(\phi) = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}. \tag{20.39}$$

The action of $r$ on the coordinates is described by

$$\rho_r \begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \\ x_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} R(120^\circ) \begin{bmatrix} x_3 \\ y_3 \end{bmatrix} \\ R(120^\circ) \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \\ R(120^\circ) \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \end{bmatrix} \tag{20.40}$$

so that

$$\rho_r = \begin{bmatrix} 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 \\ 0 & 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 & 0 \end{bmatrix}. \tag{20.41}$$

Also, we easily see that

$$\rho_s \begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \\ x_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} -x_1 \\ y_1 \\ -x_3 \\ y_3 \\ -x_2 \\ y_2 \end{bmatrix} \tag{20.42}$$

so that

$$\rho_s = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{20.43}$$

Of course, $\rho_e = I_{6\times 6}$. One could proceed similarly in this geometric fashion to find $\rho_g$ for all $g \in G$. However, given that the reader was very attentive in Parts I and II of the text, the reader knows that $D_3 = \langle r, s\rangle$ so any $g \in D_3$ can be written as $g = r^a s^b$ for some $a = 0, 1, 2, 3$ and $b = 0, 1$. Then, since $\rho$ is a homomorphism, the reader knows that

$$\rho_g = \rho_{r^a s^b} = (\rho_r)^a (\rho_s)^b. \tag{20.44}$$

Also, recall that the conjugacy classes of $D_3$ are

$$\{e\}, \{r, r^2\}, \{s, rs, r^2 s\}. \tag{20.45}$$

Thus, using only $\rho_e$, $\rho_r$, and $\rho_s$ one can compute the character $\chi$ of the representation $\rho$. From above, we see that $\mathrm{Tr}(\rho_e) = 6$, $\mathrm{Tr}(\rho_s) = 0$, and $\mathrm{Tr}(\rho_r) = 0$. See Table 20.1.

Table 20.1: Character of $\rho$, the degree-6 representation we just constructed.

| size | 1 | 3 | 2 |
|---|---|---|---|
| class | $e$ | $s$ | $r$ |
| $\chi$ | 6 | 0 | 0 |

$\chi$ is not irreducible. To prove this analytically, note that

$$\begin{aligned} (\chi|\chi) &= \frac{1}{6}(1\cdot 6\cdot 6 + 3\cdot 0\cdot 0 + 2\cdot 0\cdot 0) \\ &= 6 \\ &\neq 1 \end{aligned} \tag{20.46}$$

so, by Theorem 16.11, $\rho$ is reducible. Problem 16.16 works through the character table of $S_3 \cong D_3$. In case the reader hasn't derived the character for $S_3$ or $D_3$, we suggest working out that problem. In any case, Table 20.2 summarizes the information relevant to this discussion.

Table 20.2: Character table of $D_3$.

| size | 1 | 3 | 2 |
|---|---|---|---|
| class | $e$ | $s$ | $r$ |
| $\chi^{(1)}$ | 1 | 1 | 1 |
| $\chi^{(2)}$ | 1 | −1 | 1 |
| $\chi^{(3)}$ | 2 | 0 | −1 |
| $\chi$ | 6 | 0 | 0 |

Knowing that $\rho$ is reducible, let's calculate the following:

$$(\chi|\chi^{(1)}) = \frac{1}{6}(1\cdot 6\cdot 1 + 3\cdot 0\cdot 1 + 2\cdot 0\cdot 1) = 1 \tag{20.47}$$

$$(\chi|\chi^{(2)}) = \frac{1}{6}(1\cdot 6\cdot 1 + 3\cdot 0\cdot (-1) + 2\cdot 0\cdot 1) = 1 \tag{20.48}$$

$$(\chi|\chi^{(3)}) = \frac{1}{6}(1\cdot 6\cdot 2 + 3\cdot 0\cdot 0 + 2\cdot 0\cdot (-1)) = 2. \tag{20.49}$$

By Theorem 16.10, we conclude that

$$\rho = \rho^{(1)} \oplus \rho^{(2)} \oplus 2\rho^{(3)}. \tag{20.50}$$

That is, $\rho$ consists of two distinct degree-1 representations and two copies of a degree-2 representation. Since $\rho$ is reducible, we can find an invertible $\tau$ (a change of basis) such that

$$\tilde{\rho}_g \equiv \tau\rho_g\tau^{-1} = \begin{bmatrix} \rho_g^{(1)} & & & \\ & \rho_g^{(2)} & & \\ & & \rho_g^{(3)} & \\ & & & \rho_g^{(3)} \end{bmatrix} \tag{20.51}$$

for all $g \in G$. The blanks in the matrix are to be filled with zeros. As before, we can change bases so that the equation $\rho_g K \rho_g^{-1} = K$ (this embodies the fact that $G$ is a symmetry of the system) can be rewritten as $\tilde{\rho}_g \tau K \tau^{-1} \tilde{\rho}_g^{-1} = \tau K \tau^{-1}$ for all $g \in G$. Using Schur's lemma, we conclude that

$$\tau K \tau^{-1} = \begin{bmatrix} \lambda_1 I_{1\times 1} & & & \\ & \lambda_2 I_{1\times 1} & & \\ & & \lambda_3 I_{2\times 2} & \\ & & & \lambda_4 I_{2\times 2} \end{bmatrix}. \tag{20.52}$$

That is, we see that the eigenvalues of $K$ are, including multiplicities,

$$\lambda_1, \lambda_2, \lambda_3, \lambda_3, \lambda_4, \lambda_4. \tag{20.53}$$

with eigenvectors $\tau^{-1}\mathbf{e}_1, \tau^{-1}\mathbf{e}_2, \ldots, \tau^{-1}\mathbf{e}_6$. This is the power of group theory. Notice that we did not need the actual form of $K$ to conclude that the eigenvalues must have this structure/pattern. If one works out what $\tau$ is, then one would also know the normal modes of the system, even without knowing the exact form of $K$. The point is that the symmetry of the problem already tells us some information on the structure/pattern of the eigenvalues and eigenvectors of the problem. "All" $K$ does is control the particular values of the eigenvalues.

Remark: In the above example, group theory predicts 4 distinct eigenvalues, with multiplicities 1, 1, 2, 2. However, it may very well be that $\lambda_3 = \lambda_4$ and so there are only 3 distinct eigenvalues with multiplicities 1, 1, 4. *Symmetry considerations alone cannot predict when this happens.* The fact that, for example, $\lambda_3$ repeats at least twice is predicted by the symmetry considerations above. Therefore, even though $\lambda_3$ repeats we do not view this as a surprise or an accident. However, if some of the lambdas in blocks corresponding to different copies of irreducible representations after using Schur's lemma to simplify $\tau K \tau^{-1}$ happen to be equal, we say that there is an accidental degeneracy. To know when this happens, one needs to know more information than just the symmetry group $G$. For example, one needs to know the exact form of $K$ to see that the characteristic polynomial has more redundant roots for special values of parameters that appear in $K$ that one could not predict using only the symmetry group $G$.

## 20.4 Harmonic Systems of Masses and Springs

Let use generalize and formalize our findings. Consider a case of $N$ particles of equal mass that are coupled by ideal (that is, massless, to simplify the equations) springs in a $D$-dimensional space. Again, in classical physics this means $D$ spatial dimensions, and the time dimensional is considered the temporal dimension and is counted separately. Denote the deviation of the $a^{th}$ particle in the $i^{th}$ Cartesian coordinate direction*from it's equilibrium position* by $x_i^{(a)}$ (so, $i = 1, 2, \ldots, D$). Then the equations of motion look like

$$m \frac{d^2}{dt^2} x_i^{(a)} = -\sum_{b=1}^{N} \sum_{j=1}^{D} K_{i,a,j,b} x_j^{(b)}, \tag{20.54}$$

where $K_{i,a,j,b}$ is some expression involving the spring constants of the system. Collect the $x_i^{(a)}$ into a column vector $X$ of length $DN$

$$X = \begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_D^{(1)} \\ x_1^{(2)} \\ \vdots \\ x_D^{(2)} \\ \vdots \\ \vdots \\ x_D^{(N)} \end{bmatrix}. \tag{20.55}$$

Look for solutions of the form $X = \tilde{X}e^{-i\omega t}$, where $\tilde{X}$ has no time dependence. Then the equations of motion can be written as

$$m\omega^2\tilde{X} = K\tilde{X} \tag{20.56}$$

for some $DN$-by-$DN$ matrix $K$. Actually, the matrix $K$ will end up being symmetry due to Newton's third law. Without group theory, it appears that the only thing one can do is proceed with the eigenvalue problem $m\omega^2\tilde{X} = K\tilde{X}$.

### 20.4.1 Group Theory Gives Insight Into the Spectrum

In principle, it shouldn't be too difficult to construct the matrix $K$ if we know what the classical system is and what the spring constants involved are. However, let's ignore the exact form of $K$ except for the following fact: the system has some symmetries. Denote the symmetry group $G$. The group $G$ can act on the system, with the action on the coordinates $\tilde{X}$ being described by matrices $\rho_g$ for each $g \in G$. The physics should be invariant under this action. This fact ends up requiring that $\rho_g K \rho_g^{-1} = K$ for any $g \in G$. By construction, the matrices $\{\rho_g \mid g \in G\}$ form a representation of $G$. Once the representation $\rho$ is known, one can compute that character $\chi$ of $\rho$. If the symmetry group $G$ is known, one can construct it's character table. Let the irreducible representations be $\rho^{(1)}, \ldots, \rho^{(N_{irr})}$ with characters $\chi^{(i)}$ for $i = 1, \ldots, N_{irr}$. In general, $\rho$ will be a reducible representation. Therefore, there is an invertible $\tau$ such that

$$\tilde{\rho}_g \equiv \tau\rho_g\tau^{-1} \tag{20.57}$$

is block-diagonal, where the irreducible representations of $G$ appear along the diagonal. In particular, Theorem 16.10 we know that

$$\rho = m_1\rho^{(1)} \oplus \cdots \oplus m_{N_{irr}}\rho^{(N_{irr})} \tag{20.58}$$

where $m_i = (\chi|\chi^{(i)})$ in the number of times that the irrep $\rho^{(i)}$ appears in $\rho$. The condition that $\rho_g K \rho_g^{-1} = K$ for any $g \in G$ becomes $\tilde{\rho}_g \tau K \tau^{-1} \tilde{\rho}_g^{-1} = \tau K \tau^{-1}$. Denote the degree of the representation $\rho^{(i)}$ by $n_i$. By Schur's lemma, we conclude that

$$\tau K \tau^{-1} = \begin{bmatrix} \ddots & 0 & 0 & 0 & 0 \\ 0 & (\#) I_{n_r \times n_r} & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & (\#) I_{n_s \times n_s} & 0 \\ 0 & 0 & 0 & 0 & \ddots \end{bmatrix}. \tag{20.59}$$

The point is that this part follows solely from group theory considerations, and from this part we can conclude some properties of the spectrum. Namely, if $\rho^{(i)}$ appears in $\rho$ at least once, then we expect $n_i$ eigenvalues to be degenerate (the same). If $\rho^{(i)}$ appears multiple times, say $m_i$ times in $\rho$ then we expect $m_i$ sets of $n_i$ eigenvalues each where each set has degenerate eigenvalues. It could very well happen that some (or all) of these sets actually have the same eigenvalues, but group theory alone cannot predict this. In such cases, we say that we have accidental degeneracy. If you compute (either by hand, but realistically using numerical methods) the matrix $\tau$ then the eigenvectors of the system are $\tau^{-1}\mathbf{e}_k$ with eigenvalue the scalar in the $(k, k)$ entry of $\tau K \tau^{-1}$ where $k = 1, \ldots, DN$.

### 20.4.2 Just Think of It as a Harmonic Oscillator

As a closing comment, we address a concern that the reader might have. All of this work seems to work out nicely because the force is linear is the displace $X$, so we end up getting a eigenvalue problem for $X$. Isn't this too restrictive? Can't objects interaction with each other in ways involving ideal springs obeying Hooke's law? Yes, but actually many systems can, at low excitation energy, be thought of as interacting via springs. Consider an interaction potential $V_{int}(r)$ and assume that it only depends on the distance $r$ between two particles. Assuming that there exists a position, call it the equilibrium position, where there is no net force. Since $\mathbf{F} = -\nabla V$, this means that $\nabla V = 0$ at $r_{eq}$. In 1-D, this means $V'_{int}(r_{eq}) = 0$. For small deviations for $r$ from $r_{eq}$, we have find, using Taylor's theorem,

$$V_{int}(r_{eq} + r) = V_{int}(r_{eq}) + V'_{int}(r_{eq})r + \frac{1}{2} V''_{int}(r_{eq}) r^2 + \cdots . \tag{20.60}$$

For small deviations around the equilibrium point, we can keep only the second-order term and so

$$V_{int}(r) \approx V_{int}(r_{eq}) + \frac{1}{2} V''_{int}(r_{eq}) r^2. \tag{20.61}$$

The constant $V_{int}(r_{eq})$ can be dropped since constant shifts in the potential don't after the dynamics (which depends on $\mathbf{F} = -\nabla V_{int}$). Recall that the potential energy of an ideal spring that is stretched from its equilibrium position by $x$ stores energy $\frac{1}{2}kx^2$. Thus, we see that $V_{int}$ has a harmonic-spring-like interaction with $k = V''_{int}(r_{eq})$. Of course, if $V''(r_{eq}) = 0$ then this analogy breaks down, but this usually only happens for very special interactions. The point is that $N$ interacting particles can be thought of similarly. For small deviations of the $N$ particles from their equilibrium position, the linear terms sum to 0 and so, to lowest order, one has terms that look like harmonic-spring-like interactions.

### 20.4.3 Lennard-Jones

Let us consider molecular crystals composed on noble gas atoms. Omit solid helium, since the mass is small enough that quantum mechanical effects manifest and so classical mechanics reasoning doesn't work as well as it does for the heavier noble gases.[2] Noble gases has full valence shells, so the first instinct is to think of the atoms as just balls floating around and bouncing off of each other. However, they aren't completely free and they are able to interact with each other. This is because atoms aren't perfect point particles, so their charge isn't evenly concentrated at one point. Quantum mechanically, even if the expectation value of the charge density is 0, the expectation value of the variance of the charge density is not 0. This means that the electric field generated by a noble gas atom is on average 0, there are fluctuations. During these fluctuations, the electric field generated by one atom can jiggle the electrons in a neighboring atom, which will then also generated a nonzero electric field which will then result in an interaction with neighbors and so on. Thus, we expect some attraction mediated by the electromagnetic force between the noble gases and not just the gravitational attractive force. On the other hand, if the atoms get to close together than the cores of the atoms will start to get too close together. The core of an atom consists of protons (and neutrons), which will repel each other. We want to cook up a potential to capture this phenomenon.

To summarize, we want

- A potential that is attractive for far enough distances. Otherwise, the atoms would pass one another or bounce off one another and then fly off "to infinity" (away from one another).
- A potential that is repulsive for close enough distances, since we don't want all the atoms collapsing into a single spatial point.

[2] The wavelength associated to an object, called the de Broglie wavelength, is $\lambda = 2\pi\hbar/p$, where $p$ is the magnitude of the momentum. For low velocities where special relativity can be neglected, $p = mv$. Helium has the smallest mass of the noble gases, meaning it has the largest de Broglie wavelength at the same experimental conditions so quantum mechanical effects are observable more readily.

There are many ways to proceed. A common approach is to try to model this behavior using potentials in the form of power laws. Conventionally, the power is chosen to be 12 and the resulting potential has the form

$$V(r) = -\frac{A}{r^6} + \frac{B}{r^{12}}, \tag{20.62}$$

where $A$ and $B$ are some positive constants, determined for experimental data. Actually, it is common to write the potential in terms of dimensionless quantities

$$\frac{V(r)}{4\epsilon} = \left[\left(\frac{\sigma}{r}\right)^{12} - \left(\frac{\sigma}{r}\right)^{6}\right] \tag{20.63}$$

$$\sigma = (B/A)^{1/6} \tag{20.64}$$

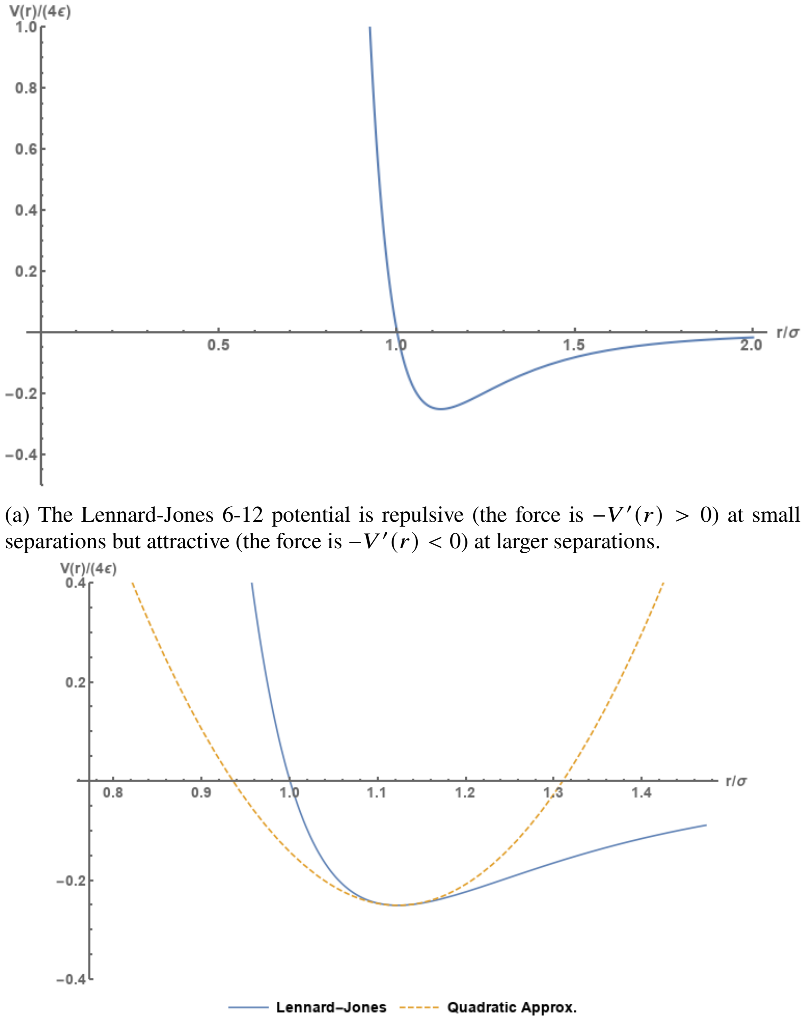
$$\epsilon = A^2/4B. \tag{20.65}$$

This is known as the Lennard-Jones 6-12 potential. See Figure 20.4. To emphasize again, this is just a convention. One could choose a different $V(r)$ with even more parameters to model the behavior. In any case, we see that if there are only two particles that interacting via a Lennard-Jones potential, that there is a separation $r_{eq}$ where the net force is zero ($-V'(r_{eq}) = 0$) and that small deviations around that point can be well approximated by a potential which is the Taylor series expansion of $V(r)$ to second order in the deviation. Thus, for small deviations from equilibrium the two particles appear to behave as if they were connected by an ideal spring with spring constant $V''(r_{eq})$.

## Problems

**20.1** Consider a system with eight blocks of mass $m$ coupled to each other by springs with spring constant $k$. Consider only nearest-neighbor coupled, as shown in Figure 20.5. In equilibrium, all the springs have the same length and there is no oscillation.

a) What is the symmetry $G$ of this dynamical system?
b) What are the conjugacy classes $G$?
c) How many degrees of freedom are there? (Hint: Don't use Cartesian coordinates.)
d) The group $G$ has some generator(s). Find $\rho_g$ when $g$ is equal to the generator(s) you listed.
e) What is the character table for $G$? Leave room for an extra row at the bottom of your character table for the next part.
f) Let $\chi$ be the character of $\rho$. Write it at the bottom of your character table.
g) What is $(\chi|\chi)$? Is $\rho$ irreducible?
h) Write $\rho$ as a direct sum of irreducible representations.



(a) The Lennard-Jones 6-12 potential is repulsive (the force is $-V'(r) > 0$) at small separations but attractive (the force is $-V'(r) < 0$) at larger separations.

(b) For small deviations about the minimum of $V(r)$, the quadratic approximation is good enough.

Fig. 20.4: The Lennard-Jones 6-12 potential is a common choice used to model the interaction between noble gases.

i) What does the previous part imply about the eigenfrequencies of this system? That is, what pattern/structure should one expect to see in the eigenfrequencies, assuming no accidental degeneracies?

j) Suppose one adds springs with spring constant $k_2$ that connects next-nearest-neighbors. What about the dynamics changes, and what conclusions still stay the same?

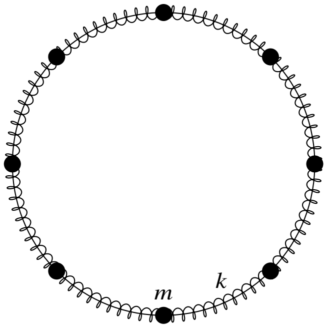


Fig. 20.5: Eight identical masses with mass $m$ are coupled by springs with spring constant $k$, as shown above.

# Chapter 21
# Quantum Mechanics and Group Theory

**Abstract** Group theory can provide insight into the structure of the spectrum of a physical system.

## 21.1 Quantum Mechanics and Superposition

Many of the techniques and conclusions from the previous chapter carry over to physical systems modeled using quantum mechanics (as opposed to classical/Newtonian physics as in the last chapter). In quantum mechanics, there is an operator known as the Hamiltonian of the system $\hat{H}$. The system is described by a wave function $\Psi(\mathbf{x}, t)$ which obeys Schrodinger's equation

$$i\hbar \frac{d}{dt}\Psi(\mathbf{x}, t) = \hat{H}\Psi(\mathbf{x}, t). \tag{21.1}$$

Here, $\hbar$ is Planck's constant. A common thing to do it write $\Psi(x, t) = \psi(\mathbf{x})e^{-iEt/\hbar}$. If $\hat{H}$ is independent of time, this is always possible since any complex number $c$ can always be written as $c = \tilde{c}e^{-iEt/\hbar}$ for an appropriate $\tilde{c}$. Then Schrodinger's time-dependent equation leads to the time-independent equation

$$\hat{H}\psi(\mathbf{x}) = E\psi(\mathbf{x}). \tag{21.2}$$

So far, $E$ is just a mathematical constant introduced when we factored $\Psi(\mathbf{x}, t)$ into a time-dependent and time-independent piece. Actually, $E$ will often end up being the energy of the system when the particle is in state $\psi(\mathbf{x})e^{-iEt/\hbar}$.

## 21.2 Degeneracy

One can solve $\hat{H}\psi = E\psi$ for the eigenvalues and eigenvectors $\{E_i, \psi_i\}$:

$$\hat{H}\psi_i = E_i\psi_i.$$

In general, we expect different eigenvectors $\psi_i, \psi_j$ $(i \neq j)$ to have different eigenvalues $E_i \neq E_j$. However, there could be a collection of $n$ eigenvectors, label then $\psi_a$ for $i = 1, 2, \ldots n$ such that they all have the same eigenvalue $E$:

$$\hat{H}\psi_a = E\psi_a \qquad \text{for } a = 1, 2, \cdots, n. \tag{21.3}$$

Assume that $d$ is finite. Then we say that the system has a $d$-fold degeneracy at the energy level $E$.

In the early days of quantum mechanics, scientists were measuring the emission spectrum and absorption spectra of different compounds. The existence of degeneracy was initially puzzling. In general, if have a matrix $H$ that you will diagonalize, you have no reason to expect that a number of eigenvalues will be the same. Of course, symmetry offers an explanation.

## 21.3 Degeneracy and Symmetries

The systems that one studies in physics often possess certain symmetries. This could be inversion, rotations, reflections, time-reversal symmetry, etc. Often, the symmetry can be represented by a unitary operator $\hat{U}$[1]. The symmetry is embodied in the equation

$$\hat{U}^\dagger\hat{H}\hat{U} = \hat{H}. \tag{21.4}$$

To see why, suppose that $\hat{O}$ is some observable operator. One cannot measure $\hat{O}$, but rather the expectation value $\langle\psi|\hat{O}|\psi\rangle$. Then $\hat{U}\psi$ should obey the same physics, and should be physical indistringuishable. This means that

$$\langle\psi|\hat{O}|\psi\rangle = (|\psi\rangle)^\dagger|\hat{O}|\psi\rangle \tag{21.5}$$

should equal

$$(\hat{U}|\psi\rangle)^\dagger|\hat{O}|\hat{U}\psi\rangle = \langle\psi|\hat{U}^\dagger\hat{O}\hat{U}|\psi\rangle. \tag{21.6}$$

That is,

$$\langle\psi|\hat{O}|\psi\rangle = \langle\psi|\hat{U}^\dagger\hat{O}\hat{U}|\psi\rangle. \tag{21.7}$$

Since this should hold for any $\psi$, this implies $\hat{O} = \hat{U}^\dagger\hat{O}\hat{U}$. When the observable operator is the Hamiltonian, this implies $\hat{H} = \hat{U}^\dagger\hat{H}\hat{U}$. Since $\hat{U}$ is unitary, $\hat{U}^\dagger = \hat{U}^{-1}$, so this is the same as $\hat{U}\hat{H} = \hat{H}\hat{U}$. Let $\psi_a$ be an eigenvector of $\hat{H}$ with eigenvalue $E$. Then

[1] A notable exception is time-reversal symmetry, which is represented by an anti-unitary operator.

$$\hat{H}\psi_a = E\psi_a \tag{21.8}$$

$$\hat{U}\hat{H}\psi_a = E\hat{U}\psi_a. \tag{21.9}$$

Therefore, unless we have reason to believe that $\hat{U}\psi_a = \psi_a$, then $\hat{U}\psi_a$ is a wave function distinct from $\psi_a$ that is also an eigenfunction of $\hat{H}$ with eigenvalue $E$. This means that $\hat{U}\psi_a$ is a linear combination of the $\psi_b$ for $b = 1, 2, \ldots n$:

$$\hat{U}\psi_a = \sum_{b=1}^{n} (D(U))_{ab}\psi_b. \tag{21.10}$$

This suggests that we can expect degeneracies in the spectrum. Suppose that $\hat{V}$ is another symmetry of the system. You can verify that $(\hat{V}\hat{U})\hat{H} = \hat{H}(\hat{V}\hat{U})$ as well. Let $G$ be the symmetry group of the system. Thinking of the operators as matrices, we can collect the matrices and relabel them by $\rho_g$. Then the symmetry of the system is embodied in

$$\rho_g H = H\rho_g \tag{21.11}$$

for all $g \in G$. In general, $\rho$ will be reducible. Let $\tau$ be the matrix such that

$$\tilde{\rho}_g \equiv \tau\rho_g\tau^{-1} \tag{21.12}$$

is is block-diagonal form for all $g \in G$. Then $\rho_g H \rho_g^{-1} = H$ can be written as

$$\tilde{\rho}_g(\tau H\tau^{-1})\tilde{\rho}_g^{-1} = \tau H\tau^{-1}. \tag{21.13}$$

In particular, Theorem 16.10 we know that

$$\rho = m_1\rho^{(1)} \oplus \cdots \oplus m_{N_{irr}}\rho^{(N_{irr})} \tag{21.14}$$

where $m_i = (\chi|\chi^{(i)})$ is the number of times that the irrep $\rho^{(i)}$ appears in $\rho$. Denote the degree of the representation $\rho^{(i)}$ by $n_i$. By Schur's lemma, this means that

$$\tau H\tau^{-1} = \begin{bmatrix} \ddots & 0 & 0 & 0 & 0 \\ 0 & (\#)I_{n_r\times n_r} & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & (\#)I_{n_s\times n_s} & 0 \\ 0 & 0 & 0 & 0 & \ddots \end{bmatrix}. \tag{21.15}$$

The point is that this part follows solely from group theory considerations, and from this part we can conclude some properties of the spectrum. Namely, if $\rho^{(i)}$ appears in $\rho$ at least once, then we expect $n_i$ eigenvalues to be degenerate (the same). If $\rho^{(i)}$ appears multiple times, say $m_i$ times in $\rho$ then we expect $m_i$ sets of $n_i$ eigenvalues each where each set has degenerate eigenvalues. It could very well happen that some (or all) of these sets actually have the same eigenvalues, but group theory alone cannot predict this. In such cases, we say that we have accidental degeneracy.

### 21.3.1 Symmetries and Degeneracies - A Relationship

We see that if the system has a symmetry, we expect degeneracies in the spectrum where the degeneracies are equal to the dimension of the irreducible representations of $G$, the symmetry group of the system. Conversely, this means that if we have a physical system and we observe a pattern in the spectrum, then we could try to work backwards to predict what the symmetry group is. Of course, this isn't an invertible process since character tables aren't distinct for distinct (that is, non-isomorphic) groups. For example, $Q_8$ and $D_4$ have the same character tables even though they are not isomorphic. However, by experimentally measuring the spectrum we can rule out certain symmetries. Suppose $G'$ is a group that predict some energy level $E^\star$ should have degeneracy $d^\star$.[2] From the experimental data, we see no such degeneracies so we conclude that $G'$ cannot be a symmetry of the system. We can proceed this way and narrow down the list of possible suspects. After the list is shortened, one could then try to find a method to further narrow down the list by seeing what properties of the system should experimentally differ between the different symmetries.

[2] Rather, at least $d^\star$ since accidental degeneracies may occur.

# Index