

Willoughby Seago

Theoretical Physics

# Symmetries of Quantum Mechanics

COURSE NOTES

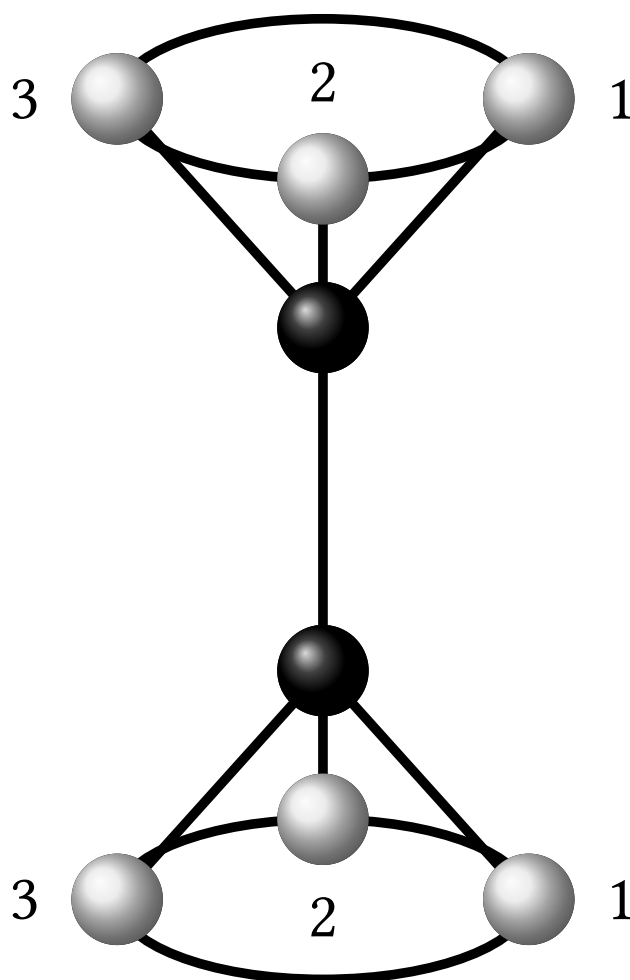
# Symmetries of Quantum Mechanics

Willoughby Seago

## Abstract

These are my notes from the course symmetries of quantum mechanics. I took this course as a part of the theoretical physics degree at the University of Edinburgh.

These notes were last updated at 20:06 on January 31, 2022. For notes on other topics see <https://github.com/WilloughbySeago/Uni-Notes>.



---

# Chapters

---

	Page
<b>Chapters</b>	<b>ii</b>
<b>Contents</b>	<b>iii</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Morphisms and Cosets</b>	<b>13</b>
<b>3 Group Action</b>	<b>20</b>
<b>4 Normal Subgroups</b>	<b>26</b>
<b>5 Products of Groups</b>	<b>33</b>
<b>6 Permutation Groups</b>	<b>38</b>
<b>Appendices</b>	<b>42</b>
<b>A Mathematical Preliminaries</b>	<b>43</b>
<b>B Groups</b>	<b>55</b>
<b>Index</b>	<b>61</b>

---

# Contents

---

	Page
<b>Chapters</b>	<b>ii</b>
<b>Contents</b>	<b>iii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Binary Operations . . . . .	1
1.1.1 Associativity . . . . .	1
1.1.2 Identity . . . . .	3
1.1.3 Inverse . . . . .	4
1.2 Groups . . . . .	4
1.2.1 Examples of Groups . . . . .	5
1.2.2 Basic Definitions . . . . .	6
1.2.3 Cayley Tables . . . . .	9
<b>2 Morphisms and Cosets</b>	<b>13</b>
2.1 Morphisms . . . . .	13
2.2 Group Presentations . . . . .	17
2.3 Cosets . . . . .	18
<b>3 Group Action</b>	<b>20</b>
3.1 Group Action . . . . .	20
3.2 Orbits and Stabilisers . . . . .	22
<b>4 Normal Subgroups</b>	<b>26</b>
4.1 Normal Subgroups . . . . .	26
4.2 Coset Groups . . . . .	28
<b>5 Products of Groups</b>	<b>33</b>
5.1 Direct Products . . . . .	33
5.2 Semidirect Product . . . . .	34
<b>6 Permutation Groups</b>	<b>38</b>
6.1 Symmetric Group . . . . .	38
<b>Appendices</b>	<b>42</b>

<b>A</b>	<b>Mathematical Preliminaries</b>	<b>43</b>
A.1	Basic Mathematics . . . . .	43
A.1.1	Notation . . . . .	43
A.1.2	Definitions . . . . .	44
A.2	Linear Algebra . . . . .	47
A.2.1	Vectors . . . . .	47
A.2.2	Matrices . . . . .	51
A.2.3	Combining Vector Spaces . . . . .	53
<b>B</b>	<b>Groups</b>	<b>55</b>
B.1	Finite Groups . . . . .	55
B.1.1	Other Finite Groups . . . . .	56
B.2	Discrete Groups . . . . .	57
B.3	Continuous Groups . . . . .	57
B.3.1	Scalars . . . . .	57
B.3.2	Matrices . . . . .	58
	<b>Index</b>	<b>61</b>

# One

## Introduction

### 1.1 Binary Operations

**Definition 1.1.1 — Binary Operation** A **binary operation** on a set  $X$  is a map,  $f: X \times X \rightarrow X$ .

**R** We say that  $X$  is **closed** under the binary operation since combining two elements of  $X$  gives another element of  $X$ .

**Notation 1.1.2** Binary operations are usually written with infix notation, for example, the binary operation  $\cdot: X \times X \rightarrow X$  maps  $(x, x') \mapsto x \cdot x'$  whereas for a normal function, say,  $f: X \times X \rightarrow X$ , we usually use prefix notation:  $(x, x') \mapsto f(x, x')$ .

The other common notation when there is only one (obvious) choice of binary operation is juxtaposing the two elements, for example  $(x, x') \mapsto xx'$ . This is exactly what we do with multiplication most of the time rather than writing  $x \cdot x$ , or  $x \times x$ . We will use this notation most of the time, particularly when the binary operation is denoted  $\cdot$ , and we will not comment on it further.

The notion of a binary operation is very general. We typically restrict ourselves to various classes of binary operations which are easier to work with due to possessing various properties.

#### 1.1.1 Associativity

**Definition 1.1.3 — Associativity** We say that the binary operation  $\cdot: X \times X \rightarrow X$  is **associative** if

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z. \quad (1.1.4)$$

From this it follows that an associative binary operation and any number of elements in a product the answer will be the same no matter how we write the brackets and so we usually don't write any brackets at all. For example, with four elements two possible ways to write the product of four elements are

$$(x_1 x_2)(x_3 x_4) = x_1(x_2(x_3 x_4)) = x_1 x_2 x_3 x_4. \quad (1.1.5)$$

Writing  $x_3x_4 = x$  it follows that  $(x_1x_2)(x_3x_4) = (x_1x_2)x = x_1(x_2x) = x_1(x_2(x_3x_4))$  where the second equality is where we apply the associativity axiom.

■ **Example 1.1.6 — Function Composition** Denote by  $\text{Hom}(A, B)$  the set of functions from  $A$  to  $B$ . We define **function composition** to be the binary operation  $\circ: \text{Hom}(B, C) \times \text{Hom}(A, B) \rightarrow \text{Hom}(A, C)$  for sets  $A$ ,  $B$ , and  $C$ , such that for  $f \in \text{Hom}(B, C)$  and  $g \in \text{Hom}(A, B)$  we have

$$(f \circ g)(a) = f(g(a)) \quad (1.1.7)$$

for all  $a \in A$ . An alternative way of saying this is that the following diagram commutes, meaning that the result is independent of the path taken:

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ & \searrow f \circ g & \downarrow f \\ & & C \end{array} \quad (1.1.8)$$

Function composition is associative. That is if  $f \in \text{Hom}(A, B)$ ,  $g \in \text{Hom}(B, C)$ , and  $h \in \text{Hom}(C, D)$  then

$$(f \circ (g \circ h))(d) = f((g \circ h)(d)) = f(g(h(d))) = (f \circ g)(h(d)) = ((f \circ g) \circ h)(d),$$

or in other words

$$f \circ (g \circ h) = (f \circ g) \circ h \quad (1.1.9)$$

and so  $\circ$  is associative.

The commutative diagram expressing this fact is

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\ & \searrow g \circ f & & \searrow h \circ g & & \searrow h \circ g \circ f & \\ & & & & & & \end{array} \quad (1.1.10)$$

One important corollary is that matrix multiplication is just composition of linear maps and so matrix multiplication is associative.

Many of the binary operations that we are familiar with are associative, such as addition, and multiplication, but not all, for example, subtraction isn't associative, consider  $5 - (2 - 3) = 6$  and  $(5 - 2) - 3 = 0$ .

■ **Example 1.1.11 — Nonassociativity** An example of a binary operation that *isn't* associative is the vector cross product,  $\times: \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$  (note that the first  $\times$  is the cross product of vectors and the second one is the Cartesian product of sets). This can be shown by an example. Take  $\mathbf{a} = (1, 1, 0)^\top$ ,

$\mathbf{b} = (0, 1, 0)^\top$ , and  $\mathbf{c} = (0, 0, 1)^\top$ . Then

$$\mathbf{a} \times \mathbf{b} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \implies (\mathbf{a} \times \mathbf{b}) \times \mathbf{c} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \quad (1.1.12)$$

whereas

$$\mathbf{b} \times \mathbf{c} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \implies \mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \quad (1.1.13)$$

### 1.1.2 Identity

**Definition 1.1.14 — Identity** Given a set,  $X$ , and a binary operation on  $X$ ,  $\cdot : X \times X \rightarrow X$ , we say that  $e \in X$  is the **identity** if

$$x \cdot e = e \cdot x = x \quad (1.1.15)$$

for all  $x \in X$ .

**Notation 1.1.16 — Identities** There are many notations for identities since it is an idea that emerged in many different areas before being unified by group theory and other algebraic concepts. The notation we will choose typically depends on both what the elements of  $X$  are and the nature of  $\cdot$ . For example,

- if the elements of  $X$  are matrices then the identity may be denoted  $I$ , or  $\mathbb{1}$ ,
- if the elements of  $X$  are functions then the identity may be denoted  $\text{id}$ , or  $\iota$ ,
- if  $\cdot$  can be thought of as multiplication then the identity is often denoted  $1$ , and
- if  $\cdot$  can be thought of as addition (in which case we are more likely to denote the operation  $+$ ) then the identity is often denoted  $0$ .

#### ■ Example 1.1.17 — Identities

- The identity for multiplication in  $\mathbb{R}$  is  $1$ .
- The identity for addition in  $\mathbb{Q}$  is  $0$ .
- The identity for matrix multiplication is  $I$ , which has  $\delta_{ij}$  as elements.
- The identity function is  $\text{id}_X : X \times X \rightarrow X$  defined by  $\text{id}_X(x) = x$  for all  $x \in X$ .

Not all binary operations have an identity, for example, there is no identity for the cross product. It is also important that the identity must be an element of  $X$ . For



${}^1\mathbb{Z}_{>0} := \{1, \dots\} = \mathbb{N} \setminus \{0\}$

example if we set  $X = \mathbb{Z}_{>0}$ <sup>1</sup> and take our operation to be addition then there is no identity since  $0 \notin \mathbb{Z}_{>0}$ .

### 1.1.3 Inverse

**Definition 1.1.18 — Inverse** Given a set,  $X$ , and a binary operation on  $X$ ,  $\cdot: X \times X \rightarrow X$ , such that  $e \in X$  acts as an identity element then we say that  $x \in X$  has an **inverse** in  $X$  if there exists some  $x^{-1} \in X$  such that

$$x \cdot x^{-1} = x^{-1} \cdot x = e. \quad (1.1.19)$$

**Notation 1.1.20 — Inverses** If we think of the binary operation,  $\cdot$ , as multiplicative then we write the inverse of  $x$  as  $x^{-1}$ , taking inspiration from division being the inverse of multiplication.

If we think of the binary operation,  $+$ , as additive then we write the inverse of  $x$  as  $-x$ , and we write  $y - x$  as shorthand for  $y + (-x)$ , taking inspiration from subtraction being the inverse of multiplication.

${}^2\mathbb{N} := \{0, 1, \dots\} = \mathbb{Z}_{>0} \cup \{0\}$ .

As with the identity it is important that the inverse is an element of  $X$ . For example, taking  $X = \mathbb{N}$ <sup>2</sup> and our operation to be addition we have an identity,  $0 \in \mathbb{N}$ , but no inverses (apart from 0, which is its own inverse), since, for example,  $-3$  is the inverse of 3, but  $-3 \notin \mathbb{N}$ .

## 1.2 Groups

**Definition 1.2.1 — Group** Formally a **group** is an ordered pair,  $(G, \cdot)$ , where  $G$  is a set and  $\cdot$  is a binary operation on  $G$  satisfying the following **group axioms**:

1. **Associativity**: For all  $g_1, g_2, g_3 \in G$

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3. \quad (1.2.2)$$

2. **Identity**: There exists some  $e \in G$  such that  $e \cdot g = g \cdot e = g$ .

3. **Inverse**: For all  $g \in G$  there exists some  $g^{-1}$  such that

$$g \cdot g^{-1} = g^{-1} \cdot g = e \quad (1.2.3)$$

where  $e$  is the identity of the group.



In practice we don't really think of groups as an ordered pair,  $(G, \cdot)$ , but as a set and an operation on the set and rather than saying "the group  $(G, \cdot)$ " most of the time we will say "the group  $G$  under  $\cdot$ ", or simply "the group  $G$ " when it is clear what the group operation.

Some sources include a fourth axiom:

4. **Closure**: The product of two elements of a group is another element of the group.

This is implicit however in the definition of a binary operation as a function  $X \times X \rightarrow X$  and so we leave it out. It will be important to consider when we think about subgroups by restricting the binary operation to a subset.

**Notation 1.2.4 — Multiple Groups** Say  $G$  and  $H$  are two groups of interest. Then we will use  $G$  and  $H$  as subscripts to differentiate between the two groups. For example the product of two elements in  $G$  may be written as  $g \cdot_G g'$ , as opposed to  $g \cdot_H g'$ , which is the product of  $H$  applied to elements of  $G$ , as we may sometimes have reason to do if, say,  $H \subseteq G$ . The identity in  $H$  may be denoted  $e_H$ , and so  $e_H \cdot_H h = h$ , but we may not have  $h \cdot_G e_H = h$ , since a different operation means we can have a different identity.

**Lemma 1.2.5** The identity of a group is unique.

*Proof.* Suppose that  $G$  is a group and  $e, e' \in G$  both act as identities. That is  $e'g = ge = g$  for all  $g \in G$ . Then  $e = e'e = e'$  where the first equality holds by the identity property of  $e'$  and the second by the identity property of  $e$ . This means  $e = e'$  and so the identity is unique.  $\square$

**Lemma 1.2.6** The inverse of a group element is unique.

*Proof.* Suppose that  $G$  is a group and  $g \in G$  is such that  $h, h' \in G$  act as inverses to  $G$ . That is  $hg = gh' = e$  where  $e \in G$  is the identity of  $G$ . Right multiplying  $hg = gh' = e$  by  $h'$  we have  $hgh' = gh'h'$ . Using the inverse property of  $h'$  on both sides we have  $he = eh'$  which implies  $h = h'$  and so the inverse is unique.  $\square$

**Lemma 1.2.7** Let  $G$  be a group and  $g, h \in G$ . Then  $(gh)^{-1} = h^{-1}g^{-1}$ .

*Proof.* The defining property of the inverse is that  $gg^{-1} = e$  so we simply need to show that  $(gh)(h^{-1}g^{-1}) = e$  and we can then identify that  $h^{-1}g^{-1} = (gh)^{-1}$ . Using associativity we can rewrite the brackets in the expression however we like and so we have  $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$ .  $\square$

**Lemma 1.2.8** Let  $G$  be a group, and  $g \in G$ . Then  $(g^{-1})^{-1} = g$ .

*Proof.* If  $(g^{-1})^{-1} = g$  then we expect that  $(g^{-1})^{-1}g^{-1} = e$ . We can identify that  $(g^{-1})^{-1}g^{-1} = (gg^{-1})^{-1}$  using [Lemma 1.2.7](#). We then have  $(g^{-1})^{-1}g^{-1} = (gg^{-1})^{-1} = e^{-1} = e$ , since  $ee = e$ , so clearly  $e^{-1} = e$ .  $\square$

### 1.2.1 Examples of Groups

■ **Example 1.2.9 — Additive Groups**  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  all form groups under addition. In particular the identity is 0, and the inverse of  $x$  is  $-x$ .

These same sets don't form groups under multiplication. The identity of multiplication is 1, and there is no number which acts as an inverse for multiplication by

zero, that is there are no solutions to  $0x = 1$  in  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , or  $\mathbb{C}$ . Noticing that zero causes issues with division it's sensible to consider these sets with zero removed. Denote by  $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$  the set of integers with zero removed. This is not a group since, for example, the multiplicative inverse of 2 is  $1/2$ , and  $1/2 \notin \mathbb{Z}^*$ .

■ **Example 1.2.10 — Multiplicative Groups**  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$ , and  $\mathbb{C}^*$  all form a group under multiplication, where we use the notation  $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ ,  $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ , and  $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ . The identity is 1 and the inverse of  $x$  is  $1/x$ .

**Definition 1.2.11 — Permutation** Formally a **permutation** on  $n$  objects is a bijection

$$\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}. \quad (1.2.12)$$

This idea can be extended to any set of size  $n$ , not just  $\{1, \dots, n\}$ . Informally we can think of a permutation as a way of ordering the  $n$  objects such that the  $m$ th object is in position  $\sigma(m)$ .

■ **Example 1.2.13 — Permutation Group** The **permutation group**,  $S_n$ , defined as the set of all permutations on  $n$  objects, is a group under function composition. What this means is that if we permute the objects then permute them again we will have a permutation of the objects (closure), we can always leave the objects in the order they are (identity), and we can always undo a permutation (inverse).

■ **Example 1.2.14 — Cyclic Group** Take some  $n \in \mathbb{Z}_{>0}$ . We define  $\mathbb{Z}_n := \{e^{2i\pi m/n} \mid m = 0, \dots, n-1\}$ . This is a group under multiplication, called the **cyclic group** of order  $n$ . Instead define  $\mathbb{Z}_n := \{0, \dots, n-1\}$ . This is a group under addition modulo  $n$ . This is actually the same group as the previous definition of  $\mathbb{Z}_n$  (they are isomorphic, a term defined later in [Definition 2.1.1](#)).

■ **Example 1.2.15 — Rotation Group** Define  $O(3) := \{O \in M_3(\mathbb{R}) \mid O^T O = 1\}$ . This is a group under matrix multiplication. The identity is the identity matrix and the inverse is the normal matrix inverse, which is guaranteed to exist since for  $O \in O(3)$  we have  $\det O = \pm 1 \neq 0$ . This is called the **rotation group**.



Strictly this is the fundamental representation of  $O(3)$ .

## 1.2.2 Basic Definitions

**Definition 1.2.16 — Group Size** Given some group  $G$  we classify it as **finite**, **discrete**, or **continuous**, depending on whether  $G$  has a finite number of elements, the same number of elements as  $\mathbb{Z}$ , or more elements than  $\mathbb{Z}$ .

Recall that two sets have the same cardinality if there is a bijection between them. For example,  $\mathbb{Z}$ ,  $\mathbb{Z}_{>0}$ ,  $\mathbb{N}$ , and  $\mathbb{Q}$  all have the same cardinality. A set is larger than a second set if there is an injective function from the first set to the second, but not vice versa. For example, there are more real numbers than integers.

■ **Example 1.2.17** Of the groups mentioned so far  $S_n$ , and  $\mathbb{Z}_n$  are finite.  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{Z}^*$ , and  $\mathbb{Q}^*$  are discrete.  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{R}^*$ ,  $\mathbb{C}^*$ , and  $O(3)$  are continuous.

**Definition 1.2.18 — Order** The **order** of a finite group,  $G$ , is the number of elements in  $G$ , denoted  $|G|$ .

Given some group,  $G$ , the **order** of  $g \in G$  is the smallest  $n \in \mathbb{Z}_{>0}$  such that  $g^n = e$ , where  $e$  is the group identity and  $g^n$  has the expected meaning of the product of  $g$  with itself  $n$  times.

Note that the order of the identity is always 1.

■ **Example 1.2.19 — Order** The order of  $S_n$  is  $|S_n| = n!$ . The order of  $\mathbb{Z}_n$  is  $|\mathbb{Z}_n| = n$ .

The order of  $e^{2i\pi/3} = e^{2i\pi/3} \in \mathbb{Z}_9$  is 3 since  $(e^{2i\pi/3})^1 = e^{2i\pi/3}$ ,  $(e^{2i\pi/3})^2 = e^{4i\pi/3}$ , and  $(e^{2i\pi/3})^3 = e^{6i\pi/3} = e^{2i\pi} = 1$ , which is the identity of  $\mathbb{Z}_n$ .

**Definition 1.2.20 — Abelian** A group,  $G$ , is **Abelian** if all of its elements commute. That is  $gg' = g'g$  for all  $g \in G$ . If this is not the case we say that  $G$  is non-Abelian.

■ **Example 1.2.21 — Abelian** Of the groups mentioned so far  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$ ,  $\mathbb{C}^*$ , and  $\mathbb{Z}^*$  are Abelian.  $S_n$  and  $O(3)$  are non-Abelian.

**Definition 1.2.22 — Subgroup** Let  $G$  be a group. We say that  $H$  is a **subgroup** of  $G$ , denoted  $H \subseteq G$ , if

- $H$  is a subset of  $G$ , and
- $H$  is a group under the group operation of  $G$  restricted to elements of  $H$ .

A subgroup is said to be a **proper subgroup** if the subgroup is not equal to the full group, or the **trivial group**,  $\{e\}$ .

■ **Example 1.2.23 — Subgroup**  $\mathbb{Z}_3$  is a subgroup of  $\mathbb{Z}_9$  since both are groups and  $\mathbb{Z}_3 = \{1, e^{2i\pi/3}, e^{4i\pi/3}\} \subset \mathbb{Z}_9$ .

**Definition 1.2.24 — Conjugate** Given a group,  $G$ , we say that  $g_1, g_2 \in G$  are **conjugate** if there exists  $g \in G$  such that  $g_1 = gg_2g^{-1}$ .

**Lemma 1.2.25** Let  $G$  be a group. Then the relation  $\sim$  defined by  $g \sim h$  if  $g$  and  $h$  are conjugate in  $G$  is an equivalence relation.

*Proof.* Let  $a \in G$ . Then  $a = eae^{-1}$  where  $e$  is the identity of  $G$ . This shows that  $a \sim a$  and so  $\sim$  is reflexive.

Let  $a, b \in G$  be such that  $a \sim b$ . Then  $a = bgb^{-1}$  for some  $g \in G$ . Right multiplying by  $g$  and left multiplying by  $g^{-1}$  this becomes  $g^{-1}ag = g^{-1}gbg^{-1}g = b$ . Noticing that  $g^{-1} = g' \in G$  and  $g = g'^{-1}$  this becomes  $b = g'ag'^{-1}$  which shows that  $b \sim a$  and so  $\sim$  is symmetric.

Let  $a, b, c \in G$  be such that  $a \sim b$  and  $b \sim c$ . Then there exists  $g, g' \in G$  such that  $a = bgb^{-1}$  and  $b = g'cg'^{-1}$ . Inserting the second equation into the first we see that  $a = gg'cg'^{-1}g^{-1}$ . Now we write  $g'' = gg' \in G$  and notice from [Lemma 1.2.7](#) that  $g'^{-1}g^{-1} = (gg')^{-1} = g''^{-1}$  we can write  $a = g''cg''^{-1}$  and so  $a \sim c$ , meaning that  $\sim$  is transitive. Hence  $\sim$  is an equivalence relation.  $\square$

**Definition 1.2.26 — Generators** Given a set  $\{g_i\} \subseteq G$  we say that  $\{g_i\}$  **generate**  $G$  if all elements of  $G$  can be written as a product of  $g_i$ . We call  $g_i$  **generators**.

The **rank** of a group is the size of the smallest set of generators.

If the rank of a group is 1 then there is one generator,  $g$ , and all elements are of the form  $g^n$ . We call such a group **cyclic**.

**Definition 1.2.27 — Centre** The **centre** of the group  $G$  is the set

$$Z(G) := \{z \in G \mid gz = zg \text{ for all } g \in G\}. \quad (1.2.28)$$

That is the centre is the set of all elements that commute with all other elements.

**R** Notice that the identity is always in the centre.

**R** The  $Z$  comes from the German *Zentrum* for centre.

**Lemma 1.2.29** Given a group  $G$  the centre,  $Z(G)$ , is a subgroup of  $G$ .

*Proof.* Clearly  $e \in Z(G)$  since  $eg = ge$  for all  $g \in G$ . Let  $z, z' \in Z(G)$ , then  $zz' \in Z(G)$  since

$$(zz')g = z(z'g) = z(gz') = (zg)z' = (gz)z' = g(zz') \quad (1.2.30)$$

for all  $g \in G$ . Finally let  $z \in Z(G)$ , then  $z^{-1} \in Z(G)$  since if  $gz = zg$  for all  $g \in G$  then left and right multiplying by  $z^{-1}$  we get  $z^{-1}gz z^{-1} = z^{-1}g = z^{-1}zg z^{-1} = gz^{-1}$ , and so  $z^{-1} \in Z(G)$ . We have shown that  $Z(G)$  is a group and by construction it is a subset of  $G$  so  $Z(G)$  is a subgroup of  $G$ .  $\square$

■ **Example 1.2.31 — Centre** If  $G$  is Abelian then  $Z(G) = G$ . The centre of  $S_3$  is the trivial group. The centre of  $O(3)$  is  $Z(O(3)) = \{1, -1\}$ .

**Theorem 1.2.32 — Subgroup Criteria.** Let  $G$  be a group and let  $H$  be a nonempty subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if  $g_1g_2^{-1} \in H$  for all  $g_1, g_2 \in H$ .

*Proof.* Suppose  $H$  is a subgroup of  $G$  and  $g_1, g_2 \in H$ . The group axioms require that  $g_2^{-1} \in H$ . In order for  $H$  to be closed we must have  $g_1g_2^{-1} \in H$ . Hence if  $H$  is a subgroup of  $G$  then  $g_1g_2^{-1} \in H$  for all  $g_1, g_2 \in H$ .

Now suppose that  $g_1g_2^{-1} \in H$  for all  $g_1, g_2 \in H$ . Take some  $g \in H$  and the condition gives  $gg^{-1} = e \in H$ , so the identity is in  $H$ . Using this we have  $eg^{-1} = g^{-1} \in H$ , so all elements of  $H$  have inverses in  $H$ . Take some  $g_1, g_2 \in H$ . We now know that  $g_2^{-1} \in H$  and so using [Lemma 1.2.8](#) we get  $g_1(g_2^{-1})^{-1} = g_1g_2 \in H$ , thus  $H$  is closed under the operation. Hence  $H$  is a group, and by definition it is a subset of  $G$  so  $H$  is a subgroup of  $G$ .  $\square$

### 1.2.3 Cayley Tables

**Definition 1.2.33 — Cayley Table** Given a finite group,  $G$ , we can list all possible products of pairs of group elements in a table, called a **Cayley table**, or **multiplication table**. This is done by listing the elements along the edge in some chosen order, usually starting with the identity, and taking the value in the  $i$ th row and  $j$ th column as the product of the  $i$ th and  $j$ th element of the group in the chosen order. That is

$$\begin{array}{c|cccc}
 G & e & a & b & c & \cdots \\
 \hline
 e & e & a & b & c & \cdots \\
 a & a & a^2 & ab & ac & \cdots \\
 b & b & ba & b^2 & bc & \cdots \\
 c & c & ca & cb & c^2 & \cdots \\
 \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
 \end{array} \tag{1.2.34}$$

The Cayley table for  $\mathbb{Z}_2$  is

$$\begin{array}{c|cc}
 \mathbb{Z}_2 & 1 & -1 \\
 \hline
 1 & 1 & -1 \\
 -1 & -1 & 1
 \end{array} \tag{1.2.35}$$

The Cayley table for  $\mathbb{Z}_3$  is

$$\begin{array}{c|ccc}
 \mathbb{Z}_3 & 1 & e^{2i\pi/3} & e^{2i\pi 2/3} \\
 \hline
 1 & 1 & e^{2i\pi/3} & e^{2i\pi 2/3} \\
 e^{2i\pi/3} & e^{2i\pi/3} & e^{2i\pi 2/3} & 1 \\
 e^{2i\pi 2/3} & e^{2i\pi 2/3} & 1 & e^{2i\pi/3}
 \end{array} \tag{1.2.36}$$

This isn't that easy to read. There is a perhaps simpler way to think of  $\mathbb{Z}_n$ , as the set  $\{0, \dots, n-1\}$ , with addition modulo  $n$  as an operation. Using this we get the Cayley table

$$\begin{array}{c|ccc} \mathbb{Z}_3 & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array} \quad (1.2.37)$$

Notice that the structure of these two tables is the same if we make the identification  $1 \leftrightarrow 0$ ,  $e^{2i\pi/3} \leftrightarrow 2$ , and  $e^{2i\pi 2/3} \leftrightarrow 2$ . This is made clearer by colouring the entries in to the tables matching the colours based on this correspondence:

$$\begin{array}{c|ccc} \mathbb{Z}_3 & 1 & e^{2i\pi/3} & e^{2i\pi 2/3} \\ \hline 1 & 1 & e^{2i\pi/3} & e^{2i\pi 2/3} \\ e^{2i\pi/3} & e^{2i\pi/3} & e^{2i\pi 2/3} & 1 \\ e^{2i\pi 2/3} & e^{2i\pi 2/3} & 1 & e^{2i\pi/3} \end{array} \quad \begin{array}{c|ccc} \mathbb{Z}_3 & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array} \quad (1.2.38)$$

We will see in a bit that what we really are saying here is that the multiplicative group  $\{1, e^{2i\pi/3}, e^{2i\pi 2/3}\}$  and the group  $\{0, 1, 2\}$  under addition modulo 3 are isomorphic, and so have the same structure and all of their group theoretical properties are the same. For this reason we often simply think of them as being the same and just consider a single group  $\mathbb{Z}_3$  using whichever of these groups is most useful at the moment.

We can make a similar identification between the group generated by multiplication of  $e^{2i\pi/n}$  and the group of  $\{0, \dots, n-1\}$  under addition modulo  $n$ , both of which can be thought of as  $\mathbb{Z}_n$  by identifying  $1 \leftrightarrow 0$  and  $e^{2i\pi m/n} \leftrightarrow m$ . For example we can think, of  $\mathbb{Z}_2$  as addition modulo 2 on  $\{0, 1\}$ .

**Notation 1.2.39 — Cycle Notation** A *k-cycle* is a way of writing a permutation down. For  $a_i \in \{0, 1, \dots, n\}$  we write  $(a_1, a_2, \dots, a_m)$  to denote the permutation in  $S_n$  that sends  $a_1$  to  $a_2$ ,  $a_2$  to  $a_3$ , and so on, sending  $a_{m-1}$  to  $a_m$ , and finally  $a_m$  to  $a_1$ . Using this notation the identity permutation is denoted  $()$ .

For example, consider the 2-cycle  $(1, 2)$  acting on the objects  $(a, b, c)$ . This sends 1, which here is the first object,  $a$ , to 2, which here is the second object  $b$ , and sends the second object to the first object. We can write this as

$$(1, 2)(a, b, c) = (b, a, c). \quad (1.2.40)$$

Applying this 2-cycle a second time we get

$$(1, 2)^2(a, b, c) = (1, 2)(1, 2)(a, b, c) = (1, 2)(b, a, c) = (a, b, c) \quad (1.2.41)$$

and so we see that  $(1, 2)^2 = ()$ .

Now consider the 3-cycle  $(1, 2, 3)$  acting on  $(a, b, c)$ . We see that

$$(1, 2, 3)(a, b, c) = (c, a, b), \quad (1.2.42)$$

$$(1, 2, 3)^2 = (1, 2, 3)(c, a, b) = (b, c, a), \quad (1.2.43)$$

$$(1, 2, 3)^3 = (1, 2, 3)(b, c, a) = (a, b, c), \quad (1.2.44)$$

so  $(1, 2, 3)^3 = ()$ .

Carrying on like this we can build up the Cayley table for  $S_3$ , notice that all 2-cycles are self-inverses (i.e. they are order 2, so square to give the identity):

$S_3$	$()$	$(1, 2)$	$(2, 3)$	$(1, 3)$	$(1, 2, 3)$	$(3, 2, 1)$
$()$	$()$	$(1, 2)$	$(2, 3)$	$(1, 3)$	$(1, 2, 3)$	$(3, 2, 1)$
$(1, 2)$	$(1, 2)$	$()$	$(1, 2, 3)$	$(3, 2, 1)$	$(2, 3)$	$(1, 3)$
$(2, 3)$	$(1, 3)$	$(3, 2, 1)$	$()$	$(1, 2, 3)$	$(1, 3)$	$(1, 2)$
$(1, 3)$	$(2, 3)$	$(1, 2, 3)$	$(3, 2, 1)$	$()$	$(1, 2)$	$(2, 3)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3)$	$(1, 2)$	$(2, 3)$	$(3, 2, 1)$	$()$
$(3, 2, 1)$	$(3, 2, 1)$	$(2, 3)$	$(1, 3)$	$(1, 2)$	$()$	$(1, 2, 3)$

(1.2.45)

Cayley tables can be a useful way to visualise group operations for small groups. For example, we can see that  $S_3$  has as a subgroup  $\{(), (1, 2)\}$ , which is the upper left hand corner of the table, and that this is equivalent to  $\mathbb{Z}_2$  after making the correspondence  $1 \leftrightarrow ()$  and  $-1 \leftrightarrow (1, 2)$ , again this can be seen more easily by colouring in the relevant entries:

		$S_3$	$()$	$(1, 2)$	$(2, 3)$	$\dots$
$\mathbb{Z}_2$	$1$	$-1$	$()$	$(1, 2)$	$(2, 3)$	$\dots$
	$1$	$-1$	$(1, 2)$	$(1, 2)$	$()$	$(1, 2, 3)$
	$-1$	$-1$	$(2, 3)$	$(1, 3)$	$(3, 2, 1)$	$()$
			$\vdots$	$\vdots$	$\vdots$	$\ddots$

(1.2.46)

**Theorem 1.2.47 — Rearrangement Theorem.** The rows and columns of a multiplication table are permutations of the group. That is they contain each element of the group exactly once.

*Proof.* Suppose that there is a row of the Cayley table for  $G$  such that  $g \in G$  appears more than once, say this is the row associated with  $g' \in G$ . That means that there exist two elements  $g_1, g_2 \in G$  such that  $g'g_1 = g'g_2 = g$ . Applying the left inverse to  $g'$  we get  $g_1 = g_2$ , and so  $g$  cannot appear more than once.

Since all columns of the table must be filled and there are  $|G|$  columns and  $|G|$  elements in order to have no repeats each element must appear once.  $\square$

Identifying the permutations giving the rows with the element of the group that is associated with that row we get the next theorem. The statement of the theorem is in terms of isomorphisms which we will define shortly but for now think of “is isomorphic to” as meaning “is equivalent to in the sense of the Cayley tables above having the same structure after renaming elements”. Skip the proof until we’ve covered isomorphisms and then come back and look at it.

**Theorem 1.2.48 — Cayley’s Theorem.** Any finite group is isomorphic to a subgroup of the symmetric group.

*Proof.* Let  $G$  be a finite group and let  $S_{|G|}$  be the permutation group of order  $|G|$ . Then for each  $g \in G$  we can define  $\sigma_g: G \rightarrow G$  to be  $\sigma_g(g') = gg'$ . This



function is invertible since  $\sigma_{g^{-1}}$  is its inverse, as can be seen by considering  $\sigma_{g^{-1}}(\sigma_g(g')) = \sigma_{g^{-1}}(gg') = g^{-1}gg' = g'$ . This means that  $\sigma_g$  is bijective and hence is a permutation on the set  $G$ .

Now define  $\varphi: G \rightarrow S_{|G|}$  by  $\varphi(g) = \sigma_g$ . Then  $\varphi$  is a homomorphism since

$$\begin{aligned} (\varphi(gg'))(g'') &= \sigma_{gg'}(g'') = gg'g'' = \sigma_g(g'g'') \\ &= \sigma_g(\sigma_{g'}(g'')) = (\sigma_g \circ \sigma_{g'})(g'') = (\varphi(g)\varphi(g'))(g''). \end{aligned} \quad (1.2.49)$$

Now suppose  $\varphi(g) = \varphi(g')$ , then  $\sigma_g = \sigma_{g'}$ , meaning  $gg'' = g'g''$  for all  $g'' \in G$ , which means that  $g = g'$  since we can apply  $g''^{-1}$  to the right of this equation. This shows that  $\varphi$  is injective.

The function  $\tilde{\varphi}: G \rightarrow \text{Im}(\varphi)$  given by  $\tilde{\varphi}(g) = \varphi(g)$  is a surjective. It remains only to show that  $\text{Im } \varphi$  is a subgroup of  $S_{|G|}$ . This will be proven in [Lemma 2.1.21](#) and so we have proven the theorem.  $\square$

Cayley's theorem is similar in nature to the Whitney embedding theorem which states that any manifold can be embedded into Euclidean space,  $\mathbb{R}^n$ , for suitable  $n$ . We just swap "manifold" with "group", "embedding" with "isomorphism", and "Euclidean space,  $\mathbb{R}^n$ " with "a subgroup of the permutation group,  $S_n$ ".

# Two

## Morphisms and Cosets

### 2.1 Morphisms

**Definition 2.1.1 — Morphism** A **homomorphism** between groups  $G$  and  $H$  is a map  $\varphi: G \rightarrow H$  which preserves the group product. That is for all  $g, g' \in G$  we have

$$\varphi(gg') = \varphi(g)\varphi(g'). \quad (2.1.2)$$

**R** The product  $gg'$  on the left is the group product of  $G$  whereas the product  $\varphi(g)\varphi(g')$  on the right is the group product of  $H$ . We can emphasise this by writing  $\varphi(g \cdot_G g') = \varphi(g) \cdot_H \varphi(g')$ .

A **isomorphism** between groups  $G$  and  $H$  is a bijective homomorphism. If there exists an isomorphism between  $G$  and  $H$  then we say that  $G$  and  $H$  are **isomorphic** and denote this  $G \cong H$ .

An isomorphism preserves all group structure. That means we can think of isomorphic groups as being the same group, just with the labels of the elements and the group operation renamed. We've already seen one example of this,  $\{\pm 1, \pm i\}$  with the group operation of multiplication is isomorphic to, and hence considered the same as,  $\{0, 1, 2, 3\}$  with the group operation of addition modulo 4.

In group theory we are almost always only interested in properties holding “up to isomorphism”. For example, we may say “there is one group up to isomorphism with some property”, by which we actually mean that all groups with this property are isomorphic. Often the “up to isomorphism” is left implicit and we just say “there is one group with some property”.

Homomorphism comes from ὁμός (*homos*) meaning same, and μορφή (*morphe*) meaning shape or form. Isomorphism comes from ἴσος (*isos*) meaning equivalent or equal, and μορφή (*morphe*) meaning shape or form.

Note that the relation  $\cong$  on the set of all groups defined by  $G \cong H$  if  $G$  and  $H$  are isomorphic is an equivalence relation (see [Example A.1.25](#)). This is what justifies us saying that two isomorphic groups are the same. Isomorphism is exactly what we mean when we say two groups are equivalent, rather than the stricter meaning of being exactly equal.

■ **Example 2.1.3 — Trivial Examples** Consider the trivial group,  $\{e\}$ , consisting of a single element, which must act as an identity. Then  $\varphi: G \rightarrow \{e\}$  for some group  $G$ , defined by  $\varphi(g) = e$  for all  $g \in G$  is a homomorphism since  $\varphi(gg') = e = ee = \varphi(g)\varphi(g')$ . This is not an isomorphism unless  $G = \{e\}$ . Similarly there exists a homomorphism between any two groups,  $G$  and  $H$ , by sending all elements of  $G$  to the identity of  $H$ . All groups are isomorphic to themselves since the identity function,  $\text{id}_G: G \rightarrow G$ , defined by  $\text{id}_G(g) = g$  for all  $g \in G$  is an isomorphism since  $\text{id}_G(gg') = gg' = \text{id}_G(g)\text{id}_G(g')$  and  $\text{id}_G$  is a self inverse, so bijective.

■ **Example 2.1.4 — Groups of Order 2 and 3**  $\mathbb{Z}_2$  and  $S_2$  are isomorphic. First notice that there are two permutations on 2 objects, we either leave them as is,  $()$ , or swap them,  $(1, 2)$ . Then  $() \mapsto 1$  and  $(1, 2) \mapsto -1$  is an isomorphism. To see this note that  $(1, 2)(1, 2) = ()$ , that is swapping and swapping back has no net effect, and so

$$\varphi(1 \cdot 1) = \varphi(1) = () = ()() = \varphi(1)\varphi(1), \quad (2.1.5)$$

$$\varphi((-1) \cdot (-1)) = \varphi(1) = () = (1, 2)(1, 2) = \varphi(-1)\varphi(-1), \quad (2.1.6)$$

$$\varphi(1 \cdot (-1)) = \varphi(-1) = (1, 2) = ()(1, 2) = \varphi(1)\varphi(-1). \quad (2.1.7)$$

The final  $\varphi((-1) \cdot 1)$  case is covered by the  $\varphi(1 \cdot (-1))$  case since both groups are Abelian.

In fact all groups of order two are isomorphic to  $\mathbb{Z}_2$  under the isomorphism of sending the identity to 1 and the non-identity to the  $-1$ . Similarly all groups of order three are isomorphic to  $\mathbb{Z}_3$ .

■ **Example 2.1.8 — Discrete Isomorphisms** The group  $\mathbb{Z}$  under addition is isomorphic to the group  $2\mathbb{Z}$  under addition. Here  $n\mathbb{Z}$  is understood to be the set of integer multiples of  $n$ , so  $2\mathbb{Z}$  is the set of even integers. One isomorphism,  $\varphi: \mathbb{Z} \rightarrow 2\mathbb{Z}$ , is the obvious choice of  $\varphi(n) = 2n$ . First we check that this is a homomorphism, given some  $m, n \in \mathbb{Z}$  we have

$$\varphi(n + m) = 2(n + m) = 2n + 2m = \varphi(n) + \varphi(m), \quad (2.1.9)$$

so this is indeed a homomorphism.

Next we check that this is injective. Suppose  $\varphi(n) = \varphi(m)$  for two elements  $n, m \in \mathbb{Z}$ . Then  $2n = 2m$ , which readily implies  $n = m$ , and so  $\varphi$  is injective. Finally we check that this is surjective. Consider some  $n \in 2\mathbb{Z}$ , since this is even<sup>a</sup>  $2|n$  and so  $n/2$  is an integer. It follows that for each  $n \in 2\mathbb{Z}$  we have  $n/2 \in \mathbb{Z}$  as the element such that  $\varphi(n/2) = n$ , and so  $\varphi$  is surjective.

Note that we could also have identified that  $\varphi^{-1}(n) = n/2$  is the inverse of  $\varphi$ . Either way  $\varphi$  is a bijective homomorphism and hence an isomorphism.

<sup>a</sup>Recall that  $m|n$  means  $m$  divides  $n$ , meaning that  $n$  is an integer multiple of  $m$  and  $n/m$  is an integer.

■ **Example 2.1.10 — Continuous Isomorphisms** The groups  $(\mathbb{R}, +)$  and  $(\mathbb{R}_{>0}, \cdot)$  of positive real numbers under multiplication are isomorphic. One isomorphism between these is  $x \mapsto e^x$ , which is a homomorphism since

$$e^{x+y} = e^x e^y \quad (2.1.11)$$

for all  $x, y \in \mathbb{R}$  and is bijective since  $x \mapsto \ln x$  is the inverse.

■ **Example 2.1.12 — Complex Numbers as Matrices** The multiplicative group of complex numbers is isomorphic to the subset of  $2 \times 2$  real matrices

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}. \quad (2.1.13)$$

An isomorphism between these two groups is given by

$$\varphi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \quad (2.1.14)$$

We first check that this is a homomorphism:

$$\varphi((a+bi)(c+di)) = \varphi((ac-bd) + (ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \quad (2.1.15)$$

and

$$\varphi(a+bi)\varphi(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & bd+ac \end{pmatrix} \quad (2.1.16)$$

So this is indeed a homomorphism.

We can see that this is bijective by noticing that the inverse is simply

$$\varphi^{-1} \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi. \quad (2.1.17)$$

What we have done here is find a two-dimensional real representation of  $\mathbb{C}^*$ . Notice that if we restrict ourselves to complex numbers with unit modulus then we can write  $a = \cos \vartheta$  and  $b = \sin \vartheta$  which allows us to make an identification between complex numbers of unit modulus and two-dimensional rotations. Denoting the multiplicative group of complex numbers with unit modulus by  $\mathbb{T}$ , the group of  $1 \times 1$  unitary matrices by  $U(1)$  and the group of two-dimensional rotations by  $SO(2)$  what we see here is that  $U(1) \cong \mathbb{T} \cong SO(2)$ , where the isomorphism between  $\mathbb{T}$  and  $U(1)$  is the obvious one mapping  $z \in \mathbb{T}$  to  $(z) \in U(1)$  and the isomorphism between  $\mathbb{T}$  and  $SO(2)$  is the restriction of  $\varphi$  to  $\mathbb{T}$ .

It isn't until we get to groups of order 4 that we get two groups which *aren't* isomorphic. The two groups of order 4 are  $\mathbb{Z}_2$  and the **Klein Vierergruppe**,  $\mathbb{Z}_2 \times \mathbb{Z}_2$ <sup>1</sup>, which has the unique property for a group of this order that all non-trivial (i.e. not

<sup>1</sup>this notation will make sense when we talk about direct products of groups in [Definition 5.1.1](#)

the identity) elements are of order 2. These two groups have the Cayley tables

$$\begin{array}{c|cccc} \mathbb{Z}_4 & 1 & -1 & i & -i \\ \hline 1 & 1 & -1 & i & -i \\ -1 & -1 & 1 & -i & i \\ i & i & -i & -1 & 1 \\ -i & -i & i & 1 & -1 \end{array} \quad \begin{array}{c|cccc} \mathbb{Z}_2 \times \mathbb{Z}_2 & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} \quad (2.1.18)$$

It is possible to fill the second one of these in by starting with the first row and column, which are simple taking  $e$  as the identity, and the leading diagonal, which must be  $e$  in every row since we have declared all nontrivial elements to be of order 2. This leaves the last two slots on the  $a$  line open, since each element must appear exactly once in each row and column these slots must be  $c$  and  $b$ . Continuing on we can fill out the rest of the table. Notice that we don't need to ever discuss what the elements  $e$ ,  $a$ ,  $b$ , and  $c$  are. It is enough to know that they form a group with this property of squaring to the identity. We will see later one possible set of elements that naturally form a group of this structure in .

There are some immediate consequences of these definitions that are worth considering.

**Lemma 2.1.19 — Homomorphisms Map Identities to Identities** Let  $G$  and  $H$  be groups. Then if  $\varphi: G \rightarrow H$  is a homomorphism  $\varphi(e_G) = e_H$  where  $e_G$  and  $e_H$  are the identities of  $G$  and  $H$  respectively.

*Proof.* By definition  $\varphi(gg') = \varphi(g)\varphi(g')$  for all  $g, g' \in G$ . In particular we have  $\varphi(e_G g) = \varphi(e_G)\varphi(g)$ , and  $\varphi(e_G g) = \varphi(g) = e_H \varphi(g)$ . Right multiplying these two results by  $\varphi(g)^{-1}$  we have  $\varphi(e_G) = e_H$ .  $\square$

**Lemma 2.1.20 — Homomorphisms Map Inverses to Inverses** Let  $G$  and  $H$  be groups and  $\varphi: G \rightarrow H$  a homomorphism. Then  $\varphi(g^{-1}) = \varphi(g)^{-1}$ .

*Proof.* By definition  $\varphi(gg') = \varphi(g)\varphi(g')$  for all  $g, g' \in G$ . By [Lemma 2.1.19](#) we have  $\varphi(e_G) = e_H$  where  $e_G$  and  $e_H$  are the identities of  $G$  and  $H$ . We then have  $\varphi(gg^{-1}) = \varphi(e_G) = e_H$ , and also  $\varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ . From this we see that  $e_H = \varphi(g)\varphi(g^{-1})$ , which is to say that  $\varphi(g^{-1}) = \varphi(g)^{-1}$  since  $\varphi(g)\varphi(g^{-1})$  gives the identity, which defines the inverse.  $\square$

**Lemma 2.1.21 — The Image of a Homomorphism is a Subgroup** Let  $G$  and  $H$  be groups and  $\varphi: G \rightarrow H$  a homomorphism. Then  $\text{Im } \varphi = \varphi(G)$  is a subgroup of  $H$ .

*Proof.* Consider  $h, h' \in \text{Im } \varphi$ . Then there exists  $g, g' \in G$  such that  $h = \varphi(g)$  and  $h' = \varphi(g')$ . Since  $G$  is a group  $gg'^{-1} \in G$ . We then have  $\varphi(gg'^{-1}) = \varphi(g)\varphi(g'^{-1}) = \varphi(g)\varphi(g')^{-1} = hh'^{-1}$  by [Lemma 2.1.20](#) and the defining property of a homomorphism. This means that  $hh'^{-1} \in \text{Im } \varphi$  and hence  $\text{Im } \varphi$  is a subgroup of  $H$  by the subgroup criterion of [Theorem 1.2.32](#).  $\square$

**Lemma 2.1.22** Every group of rank 1 is isomorphic to some cyclic group.

*Proof.* First suppose that  $G$  is a finite group of order  $n$ . Then elements of  $G$  are of the form  $g^i$  for some  $i = 0, \dots, n-1$ . In particular  $g^0 = e$ . Notice that  $f^i = g^j$  if  $i \equiv j \pmod n$ .

The map  $\varphi: G \rightarrow \mathbb{Z}_n$  defined by  $\varphi(g^i) = i$  is then an isomorphism, using  $\mathbb{Z}_n$  as the group of integers under addition modulo  $n$ . Clearly  $\varphi(g^i g^j) = \varphi(g^{i+j}) = i + j = \varphi(g^i) + \varphi(g^j)$  where addition outside of the argument of  $\varphi$  occurs modulo  $n$ .

The inverse of this map is simply  $\varphi^{-1}(i) = g^i$  and so this is a bijection. Meaning that  $\varphi$  is an isomorphism.  $\square$

## 2.2 Group Presentations

**Definition 2.2.1 — Group Presentations** A **group presentation** is a way of defining a specific group. A generic group presentation is of the form

$$G = \langle S \mid C \rangle \quad (2.2.2)$$

which we read as “ $G$  is the group generated by the elements of  $S$  subject to the constraints  $C$ ”.

■ **Example 2.2.3 — Cyclic Groups** The cyclic group,  $\mathbb{Z}_n$ , has the group presentation

$$\mathbb{Z}_n = \langle a \mid a^n = e \rangle. \quad (2.2.4)$$

We can identify  $a = e^{2i\pi/n}$  as one possible generator with the group operation of multiplication but it need not be the only one. For example if  $n = 3$  then  $a = e^{2i\pi 2/3}$  also works.

If instead we take the group operation to be addition modulo  $n$  then  $a = 1$  is a generator. For the  $n = 3$  case we can also choose  $a = 2$  as a generator.

■ **Example 2.2.5 — Permutation Group** The following is group presentations of  $S_3$ :

$$S_3 = \langle a, b, c \mid a^2 = b^2 = c^3 = abc = e \rangle. \quad (2.2.6)$$

We have a fair amount of choice here about exactly which elements  $a$ ,  $b$ , and  $c$  are, clearly  $e = ()$  is the identity. We can then choose  $a$  and  $b$  to be any of the 2-cycles,  $(1, 2)$ ,  $(1, 3)$ , and  $(2, 3)$ , and  $c$  as one of the 3-cycles,  $(1, 2, 3)$  or  $(3, 2, 1)$ .

Group presentations aren’t unique. For example, the following is another valid presentation of  $S_3$ :

$$S_3 = \langle A, B \mid A^2 = B^2 = (AB)^3 = e \rangle. \quad (2.2.7)$$

We can see from this that  $A$  and  $B$  must be 2-cycles and  $AB$  is a three cycle.

■ **Example 2.2.8 — Quaternion Group** The **quaternion group** is the group with the presentation

$$Q := \langle -e, i, j, k \mid (-e)^2 = e, i^2 = j^2 = k^2 = ijk = -e \rangle. \quad (2.2.9)$$

This group is of order  $|Q| = 8$ , with  $Q = \{\pm e, \pm i, \pm j, \pm k\}$ , where by  $-i$  we mean  $(-e)i$ .

Making the identification of  $e = 1$  and taking  $i, j$ , and  $k$ , as the quaternions  $i, j$ , and  $k$  respectively it is clear that this is a subset of the quaternions,  $\mathbb{H}$ .

We can think  $Q$  being to  $\mathbb{H}$  as  $\mathbb{Z}_4 = \{\pm 1, \pm i\}$  is to  $\mathbb{C}$ , or  $\mathbb{Z}_2 = \{\pm 1\}$  is to  $\mathbb{R}$ .

Another identification we can make is  $-e = -1$ ,  $i = \sigma_1$ ,  $j = \sigma_2$ , and  $k = \sigma_3$ , where  $\sigma_i$  are the Pauli matrices. In fact the Pauli matrices are a representation of the quaternion group.

## 2.3 Cosets

**Definition 2.3.1 — Coset** Given some group  $G$  and subgroup  $H$  we define for each  $g \in G$  the left (right) **coset** to be the set

$$gH := \{gh \mid h \in H\} \quad (2.3.2)$$

$$(Hg := \{hg \mid h \in H\}). \quad (2.3.3)$$

Typically we will state and prove things for left cosets and then the equivalent statement about right cosets will hold and be proven in exactly the same way. We will often refer simply to cosets when we mean left cosets.

**Definition 2.3.4 — Partition** Given a nonempty set,  $X$ , we say that the collection of sets  $\{P_i \subseteq X\}$  is a **partition** or **decomposition** of  $X$  if

- $\bigcup_i P_i = X$ , and
- $P_i \cap P_j = \emptyset$  if  $i \neq j$ .

That is every element of  $X$  is in exactly one of  $P_i$ . We can assume that  $P_i$  are non-empty.

**Lemma 2.3.5** Let  $G$  be a group with subgroup  $H$ . Then the set of all cosets,  $gH$ , partitions  $G$ . Further, all cosets are of the same size, meaning  $|gH| = |H|$  for all  $g \in G$ .

*Proof.* In order for the cosets to be a partition we must show that two cosets are either equal or disjoint. Consider some element  $g_1 \in G$  which is not in some coset  $g_2H$ . Clearly this means that the two cosets  $g_1H$  and  $g_2H$  are equal since  $e \in H$  so  $g_1e = g_1$  is in  $g_1H$ . Suppose then that  $g_1H \cap g_2H \neq \emptyset$ . Then it follows that there exist some  $h_1, h_2 \in H$  such that  $g_1h_1 = g_2h_2$ . This then means that  $g_1 = g_2h_2h_1^{-1}$ , however, since  $H$  is a group  $h_2h_1^{-1} \in H$ , and so  $g_1 = g_2h$  for some  $h = h_2h_1^{-1} \in H$  meaning that  $g_1 \in g_2H$ , which contradicts

our earlier assumption. Hence  $g_1H \cap g_2H = \emptyset$ . Combining this with noticing that for  $g \in G$  we have  $g \in gH$  since  $e \in H$  and so  $g = ge$  means that  $g \in gH$  proves the first part of the statement, that  $gH$  partition  $G$ . Consider the map  $g_1H \rightarrow g_2H$  defined by  $g_1h \mapsto g_2h$  for  $h \in H$ . This is invertible since inverses are unique and hence  $|g_1H| = |g_2H|$ . In particular taking  $g_1 = g$  and  $g_2 = e$  we have  $|gH| = |H|$ .  $\square$

The fact that  $gH$  partition  $G$  into sets of equal size allows us to prove the next famous theorem. But first, a definition.

**Definition 2.3.6 — Index** Given a finite group  $G$  with subgroup  $H$  we define the **index** of  $H$  in  $G$  to be

$$[G : H] := \frac{|G|}{|H|}. \quad (2.3.7)$$

**Theorem 2.3.8 — Lagrange's Theorem.** Given a finite group  $G$  with subgroup  $H$  the index  $[G : H]$  is an integer.

*Proof.* The cosets partition  $G$  into sets of size  $|H|$ . Suppose that there are  $n$  distinct cosets. Then  $|G| = n|H|$ , meaning that  $|G|/|H| = n$ .  $\square$

Lagrange's theorem says that a subset can be a subgroup only if the cardinality of the subset divides the order of the group. Notice that just because this holds does not mean that the subset is a subgroup. There is also no requirement that just because a number divides the order of the group that there is a subgroup of that order. Lagrange's theorem is much better for ruling out possible subgroups than it is for actually finding them.

■ **Application 2.3.9** In particle physics and statistical mechanics if a continuous global symmetry given by the group  $G$  is broken to some subgroup  $H$  then it is possible to formulate an effective field theory in terms of cosets. For example in the theory of strong interactions, quantum chromodynamics (QCD), the breaking of left-right symmetry, known as chiral symmetry, gives rise to the effective theory of pions, known as chiral perturbation theory.



# Three

## Group Action

### 3.1 Group Action

**Definition 3.1.1** Let  $G$  be a group and  $X$  a set. A **group action** is a map,  $\varphi: G \times X \rightarrow X$ , where we use the notation  $\varphi(g, x) = g \cdot x$ . This map must be compatible with the group structure, by which we mean

- $e \cdot x = x$  ( $\varphi(e, x) = x$ ) for all  $x \in X$ , and
- $(gg') \cdot x = g \cdot (g' \cdot x)$  ( $\varphi(gg', x) = \varphi(g, \varphi(g', x))$ ) for all  $g, g' \in G$  and  $x \in X$ .



Be careful to distinguish “ $\cdot$ ” used to the group action and “ $\cdot$ ” used to denote a group product, in general  $g \cdot g' \neq g \cdot g'$ . This is another good reason *not* to use a dot to denote the group product.



Technically what we have defined here is a *left* group action. We can also define a right group action in a similar way. Let  $G$  be a group and  $X$  a set. The right group action is a map,  $\varphi: X \times G \rightarrow X$ , where we use the notation  $\varphi(x, g) = x \cdot g$ . This map must be compatible with the group structure, by which we mean

- $x \cdot e = x$  ( $\varphi(x, e) = x$ ) for all  $x \in X$ , and
- $x \cdot (gg') = (x \cdot g) \cdot g'$  ( $\varphi(x, gg') = \varphi(\varphi(x, g), g')$ ) for all  $g, g' \in G$  and  $x \in X$ .

The difference between left and right group actions is subtle. For a left group action if we act on  $x$  with the product  $gg'$  then  $g'$  acts first, for a right group action  $g$  acts first.

An alternative definition for finite groups is that a group action is a group homomorphism from  $G$  into  $S_{|X|}$ . That is we can think of the action as taking an element of  $G$  and then determining how to reorder the elements of  $X$  based on this choice.

Identifying  $S_{|X|}$  with bijections from  $X$  to  $X$  we can further define a group action to be a homomorphism  $\varphi: G \rightarrow \text{Aut}(X)$ , where  $\text{Aut}(X)$  is the group of automorphisms on  $X$ , which is to say exactly the set of bijections  $X \rightarrow X$ , with the group product being function composition.

■ **Example 3.1.2 — General Examples** For any group  $G$  and set  $X$  the trivial

group action is

$$g \cdot x = x \quad (3.1.3)$$

for all  $x \in X$ .

For the special case of  $X = G$  we have a variety of choices for the group action of a group on itself:

- Left multiplication:  $g \cdot x = gx$  for all  $g, x \in G$ ,
- Right multiplication:  $g \cdot x = xg$  for all  $g, x \in G$  (strictly this is a *right* group action), and
- Conjugation:  $g \cdot x = gxg^{-1}$ .

■ **Example 3.1.4 — Specific Examples** Let  $S_n$  be the permutation group on  $n$  objects and  $X$  the set of all tuples  $(x_1, \dots, x_n)$  such that  $x_i$  are unique. Then  $S_n$  acts on  $x = (1, \dots, n) \in X$  by permuting the elements. Notice that by acting on  $x$  with  $S_n$  we can get any element of  $X$  and that  $|X| = n!$ . The group  $(\mathbb{Z}, +)$  acts on the set  $\mathbb{R}$  as  $m \cdot r = (-1)^m r$  for  $m \in \mathbb{Z}$  and  $r \in \mathbb{R}$ .

■ **Example 3.1.5 — Representation** The group action of a group on a linear space is called a representation and will be the subject of study of much of the rest of this course. The group action of a group on a nonlinear space is called a nonlinear representation, and is beyond the scope of this course.

■ **Application 3.1.6** Hilbert spaces describing wave functions are linear spaces. Particles correspond to representations of the Lorentz group,  $O(1, 3)$ , which is the set of all Lorentz transformations with matrix multiplication as a group action, as well as various internal symmetry groups. That is group actions of the Lorentz group, on the Hilbert space of wave functions gives particles.

■ **Application 3.1.7 — Gauge Theory** In a gauge theory the gauge group acts on the gauge potential.

One family of groups that appears in this context are the **unitary groups**

$$U(n) := \{U \in \mathcal{M}_n(\mathbb{C}) \mid U^\dagger U = UU^\dagger = \mathbf{1}\}. \quad (3.1.8)$$

In particular we often deal with

$$U(1) = \{z \in \mathbb{C} \mid z^* z = z z^* = |z|^2 = 1\} = \{e^{i\varphi} \mid \varphi \in \mathbb{R}\} \quad (3.1.9)$$

which is the group of complex numbers with unit modulus<sup>a</sup>. This particular group is the gauge group of (quantum) electrodynamics and its action on the gauge potential is

$$e^{i\varphi(x)} \cdot A_\mu = A_\mu + \partial_\mu \varphi(x). \quad (3.1.10)$$

Recall that adding the derivative of a function to the electromagnetic potential doesn't change the electric or magnetic fields,  $-\nabla A^0$  and  $\nabla \times \mathbf{A}$ .



See the notes for quantum theory for more discussion of gauge invariance, and the notes from the particle physics part of relativity, nuclear, and particle physics for a discussion of QED.

<sup>a</sup>Strictly the group of complex numbers with unit modulus is the circle group,  $\mathbb{T}$ , and  $U(1)$  is the group of  $1 \times 1$  unitary matrices over the complex numbers, however, under the obvious correspondence that  $(z) \in U(1)$  should correspond to  $z \in \mathbb{T}$  these two groups are isomorphic and therefore we don't distinguish between them.

## 3.2 Orbits and Stabilisers

**Definition 3.2.1 — Orbit** Given a group  $G$  which acts on the set  $X$  for each  $x \in X$  we define the **orbit** of  $x$  to be the set,  $g(x)$ , containing all elements of  $X$  which are reached by acting on  $x$  with an element of  $G$ . That is

$$g(x) := \{g \cdot x \mid g \in G\} \subseteq X. \quad (3.2.2)$$

**Notation 3.2.3** Sometimes the orbit is denoted  $G(x)$  or using a notation similar to cosets  $G \cdot x$ .

■ **Example 3.2.4** Consider the group of rotations in the plane about some point  $\mathbf{a}$ . The orbit of some other point  $\mathbf{b}$  is the circle of radius  $|\mathbf{a} - \mathbf{b}|$  around the point  $\mathbf{a}$ .

Consider the group of integers,  $\mathbb{Z}$ , acting on  $\mathbb{R}$  by  $n \cdot r = r + n$  for  $n \in \mathbb{Z}$  and  $r \in \mathbb{R}$ . The orbit of  $1 \in \mathbb{R}$  is the set  $\mathbb{Z} \subset \mathbb{R}$ .

Consider the group  $\mathbb{R}^*$  acting on some vector space,  $V$ , by  $r \cdot \mathbf{v} = r\mathbf{v}$  for  $r \in \mathbb{R}$  and  $\mathbf{v} \in V$ . Then the orbit of  $\mathbf{v}$  is all vectors parallel to  $\mathbf{v}$ .

**Definition 3.2.5 — Stabiliser** Given a group  $G$  which acts on the set  $X$  for each  $x \in X$  we define the **stabiliser** of  $x$  to be the subset,  $G_x$ , of  $G$  which leaves  $x$  invariant under the group action. That is

$$G_x := \{g \in G \mid g \cdot x = x\}. \quad (3.2.6)$$

■ **Example 3.2.7** Consider the group  $S_4$ , which acts on the set of strings  $(a, b, c, d)$  by permutation. The stabiliser of  $a$  is  $(S_4)_a = \{(), (3, 4)\}$ .

Consider the group  $GL(2, \mathbb{R})$  acting on  $\mathbb{R}^2$  by matrix multiplication. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \quad (3.2.8)$$

the stabiliser of  $(1, 0)^\top$  is

$$\mathrm{GL}(2, \mathbb{R})_{(1,0)^\top} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \middle| b, d \in \mathbb{R} \text{ and } d \neq 0 \right\}. \quad (3.2.9)$$

Note that we require  $d \neq 0$  so that  $\det A = d \neq 0$  for  $A \in \mathrm{GL}(2, \mathbb{R})_{(1,0)^\top}$ .

Let  $G$  be a group which acts on itself by conjugation. Then the stabiliser of  $a \in G$  is

$$G_a = \{g \in G \mid gag^{-1} = a\}, \quad (3.2.10)$$

which we can think of as the set of all elements,  $g$ , which commute with  $a$ , which follows by right multiplying the condition by  $g$  to get  $gag^{-1}g = ga = ag$ . This is sometimes called the **centraliser** of  $a$ , denoted  $C_G(a)$ . Compare this to the centre of  $G$ ,  $Z(G)$ , which is the set of all commuting elements in  $G$ .

**Lemma 3.2.11** If  $G$  is a group and acts on the set  $X$  then the stabiliser is a subgroup of  $G$  for any element of  $X$ .

*Proof.* Let  $x \in X$ . Suppose that  $g, h \in G_x$ , that is  $g \cdot x = h \cdot x = x$ . Then  $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x)$ . Since  $h^{-1}h = e$  we have that  $(h^{-1}h) \cdot x = e \cdot x = x$ , we also have that  $(h^{-1}h) \cdot x = h^{-1} \cdot (h \cdot x) = h^{-1} \cdot x$ . Hence  $h^{-1} \cdot x = x$ . Using this we have  $(gh^{-1}) \cdot x = g \cdot x = x$ , and so  $gh^{-1} \in G_x$ . Thus by the subgroup criterion ([Theorem 1.2.32](#))  $G_x$  is a subgroup of  $G$ .  $\square$

**Theorem 3.2.12 — Orbit-Stabiliser Theorem.** Let  $G$  be a group and  $g \in G$ . Define an action of  $G$  on some set  $X$  with  $x \in X$ . The map  $\varphi_g(x) \rightarrow G/G_x$ , where  $G/G_x$  is the set of all cosets of  $G_x$ , defined by  $g \cdot x \mapsto gG_x$  defines a bijection.

*Proof.* Since  $G_x$  is a subgroup of  $G$  by [Lemma 3.2.11](#) we can define cosets,  $gG_x$ , which partition  $G$  by [Lemma 2.3.5](#). Hence the map is surjective. To demonstrate that this map is injective we need to prove that if  $g_1G_x = g_2G_x$  then  $g_1 \cdot x = g_2 \cdot x$ . Notice that if  $g_1G_x = g_2G_x$  then there exists some  $g \in G_x$  such that  $g_1 = g_2g$  by the definition of a coset. We therefore have

$$g_1 \cdot x = (g_2g) \cdot x = g_2 \cdot g \cdot x = g_2 \cdot x \quad (3.2.13)$$

where in the last step we have used  $g \in G_x$  and so by definition  $g \cdot x = x$ . We have therefore demonstrated that this map is injective. Hence the map is a bijection.  $\square$

**Corollary 3.2.14** Given a finite group,  $G$ , which acts on a set  $X$  for all  $x \in X$  we have

$$|G| = |G_x| |g(x)|. \quad (3.2.15)$$

*Proof.* By Lagrange's theorem (Theorem 2.3.8)  $|G|/|G_x|$  is an integer. Further we can identify this as the number of sets in the partition of  $G$  by  $G_x$ , which has size  $|G/G_x|$ , which is exactly  $|g(x)|$ , since by the orbit-stabiliser theorem (Theorem 3.2.12) the set of sets partitioning  $G$  by  $G_x$ ,  $G/G_x$  is in bijection with the set of orbits,  $g(x)$ .  $\square$

Consider the limiting cases of this theorem. If  $G_x = G$  then  $|g(x)| = 1$ , since all elements of  $G$  leave  $x$  fixed. Clearly  $|G| = |G_x|$ , and so  $|G| = |G_x||g(x)|$  in accordance with the theorem.

If  $G_x = \{e\}$  then  $|g(x)| = |G|$ , since all elements of  $G \setminus \{e\}$  must change  $x$ . Then  $|G| = |G_x||g(x)|$  in accordance with the theorem.

**Theorem 3.2.16 — Cauchy's Theorem.** Let  $G$  be a group and let  $p$  be prime. If  $|G|/p$  is an integer then there exists an element of order  $p$  in  $G$ . That is there exists  $g \in G$  with  $g \neq e$  such that  $g^p = e$  where  $e$  is the identity of  $G$ .

*Proof.* Let  $G$  be a group with  $|G|/p$  an integer for some prime  $p$ . Define  $G^p$  to be the set of  $p$ -length strings of elements of  $G$ . That is  $x \in G^p$  is of the form  $(x_1, \dots, x_p)$  for  $x_i \in G$ . Define  $X \subset G^p$  to be the set of elements  $(x_1, \dots, x_p)$  such that  $x_1 \cdots x_p = e$ .

The size of  $X$  is  $|X| = |G|^{p-1}$ . This follows since for  $x_1$  we can pick any element of  $G$ . For  $x_2$  we can pick any element of  $G$ . So on until  $x_{p-1}$  for which we can pick any element of  $G$ . We then have to choose  $x_p$  such that  $x_p = (x_1 \cdots x_{p-1})^{-1}$ . We then have

$$x_1 \cdots x_p = (x_1 \cdots x_{p-1})x_p = (x_1 \cdots x_{p-1})(x_1 \cdots x_{p-1})^{-1} = e. \quad (3.2.17)$$

Hence we make a choice from a set of size  $|G|^{p-1}$  and so we have  $|G|^{p-1}$  possible elements in  $X$ .

Since  $|X|$  is a multiple of  $|G|$  and  $|G|$  is divisible by  $p$   $|X|$  is also divisible by  $p$ .

Define the group action of  $\overline{G} = \mathbb{Z}_p$  on  $X$  by cyclic permutation. That is given  $m \in \mathbb{Z}_p$  and  $x = (x_1, \dots, x_p) \in X$  define

$$m \cdot x = (x_{1+m}, \dots, x_{p+m}) = (x_{m+1}, \dots, x_p, x_1, \dots, x_m) \quad (3.2.18)$$

where addition in the indices is done modulo  $m$  to so the indices remain in  $\{1, \dots, m\}$ .

Clearly  $|\overline{G}| = |\mathbb{Z}_p| = p$ . Then by Corollary 3.2.14 it follows that  $p = |\overline{G}| = |\overline{G}_x||\overline{g}(x)|$ . Since  $p$  is prime either  $|\overline{G}_x| = p$  and  $|\overline{g}(x)| = 1$  or  $|\overline{G}_x| = 1$  and  $|\overline{g}(x)| = p$ .

If  $|\overline{g}(x)| = 1$  then  $x \in X$  must be of the form  $(g, \dots, g)$  for some  $g \in G$  since if this wasn't the case then a cyclic permutation would not leave  $x$  invariant. An example of this case is  $x = (e, \dots, e)$ . This cannot be the only example since then  $|X|$  is not divisible by  $p$ , since we can write  $|X|$  as  $|X| = np + m1$ , where  $n$  is the number of orbits of length  $p$  and  $m$  is the number of orbits of length 1. Clearly in order for  $|X|$  to be divisible by  $p$  we need  $m$  to be divisible by  $p$ . Therefore there must be some  $g \in G$  such that  $g \neq e$  but  $(g, \dots, g) \in X$ .

By the definition of  $X$  this means that  $g \cdots g = g^p = e$ , and so  $g$  is some element of order  $p$ .  $\square$

■ **Example 3.2.19**  $S_3$  is order 6 and hence has elements of order 2 and 3, for example  $(1, 2)$  is of order 2 and  $(1, 2, 3)$  is of order 3.  
 $\mathbb{Z}_6$  is of order 6 and hence has elements of order 2 and 3. Using addition modulo 6 as the group operation 3 is of order 2 and 2 is of order 3 in this group.

**Corollary 3.2.20** If  $G$  is a group and  $|G| = p$  for prime  $p$  then  $G$  is isomorphic to  $\mathbb{Z}_p$ .

*Proof.* By Cauchy's theorem ([Theorem 3.2.16](#))  $G$  has an element of order  $p$ . That is there exists  $g \in G$  such that  $g^p = e$ , further  $g^m \neq e$  for  $m < p$  since  $m$  doesn't divide  $p$ . Since there are  $p$  elements of  $G$  and each  $g^m$  must be distinct for  $m < p$  it follows that all elements of  $G$  are of the form  $g^m$  for some  $m \in [0, p) \cap \mathbb{Z}$ . Therefore  $G$  is cyclic and of order  $p$  and therefore  $G$  is isomorphic to  $\mathbb{Z}_p$ .  $\square$

# Four

## Normal Subgroups

### 4.1 Normal Subgroups

**Definition 4.1.1 — Normal Subgroup** Let  $G$  be a group and  $N$  be a subgroup of  $G$ . Then we say that  $N$  is a **normal subgroup** of  $G$  if  $N$  is invariant under the group action,  $N \times G \rightarrow N$ , of conjugation. That is for all  $n \in N$  and all  $g \in G$  we have that  $gng^{-1} \in N$ . A normal subgroup is also referred to as an **invariant subgroup**.

**Notation 4.1.2** If  $N$  is a normal subgroup of  $G$  we denote this  $N \trianglelefteq G$ . If  $N$  is a proper normal subgroup of  $G$ , that is  $N \neq \{e\}, G$ , then we denote this  $N \triangleleft G$ .

We can think of normal subgroups as groups which are invariant under relabelling of the elements, this relabelling is done by conjugation. Compare this to matrix transformation. Suppose that  $M$  is a matrix in some basis,  $\{e_i\}$ , and that  $\{e'_i\}$  is some other basis related to the first by  $e'_i = T_{ij}e_j$ . Then in this new basis  $M$  becomes  $TMT^{-1}$ .  $M$  describes the same transform in both bases but with different components.

■ **Example 4.1.3** For any group,  $G$ , both  $G$  and the trivial group,  $\{e\}$ , are normal subgroups.  
If  $G$  is an Abelian group and  $H$  is a subgroup of  $G$  then  $H$  is a normal subgroup since  $ghg^{-1} = gg^{-1}h = h \in H$  for all  $g \in G$  and  $h \in H$ .

■ **Example 4.1.4** Recall that the quaternion group has the presentation

$$Q = \langle -e, i, j, k \mid (-e)^2 = e, i^2 = j^2 = k^2 = ijk = -e \rangle. \quad (4.1.5)$$

We can define  $\mathbb{Z}_2$  to have the presentation  $\mathbb{Z}_2 = \langle -e \mid (-e)^2 = e \rangle$ , which has elements  $\{e, -e\}$ . This is a normal subgroup of  $Q$ . To see this note that

$i^{-1} = -i$ ,  $j^{-1} = -j$ ,  $k^{-1} = -k$ , and  $-e^{-1} = -e$  so

$$eee^{-1} = ee(-e) = -e^3 = -e, \quad (4.1.6)$$

$$(-e)e(-e)^{-1} = (-e)ee = -e^3 = -e, \quad (4.1.7)$$

$$e(-e)e^{-1} = e(-e)(-e) = e^3 = e, \quad (4.1.8)$$

$$(-e)(-e)(-e)^{-1} = (-e)(-e)e = e^3 = e, \quad (4.1.9)$$

$$iei^{-1} = ie(-i) = -i^2 = e, \quad (4.1.10)$$

$$i(-e)i^{-1} = i(-e)(-i) = i^2 = -e, \quad (4.1.11)$$

$$(-i)e(-i)^{-1} = (-i)ei = -i^2 = e, \quad (4.1.12)$$

$$(-i)(-e)(-i)^{-1} = (-i)(-e)i = i^2 = -e. \quad (4.1.13)$$

$$(4.1.14)$$

We also get the same results if we replace all  $i$ s with  $j$  or  $k$  and so  $\mathbb{Z}_2$  is invariant under conjugation and hence a normal subgroup of  $Q$ ,  $\mathbb{Z}_2 \triangleleft Q$ .

In the previous example all elements of  $\mathbb{Z}_2$  map to themselves under conjugation by elements of  $Q$  not in  $\mathbb{Z}_2$ . However, this need not be the case for a normal subgroup, as the next example shall show.

■ **Example 4.1.15** The permutations  $A_3 = \{(), (1, 2, 3), (3, 2, 1)\}$  form a normal subgroup of  $S_3$ , this subgroup is called the alternating group and we will study it more in the future.

First we have to show that  $A_3$  is a subgroup, which we can do via the subgroup criterion by considering  $(1, 2, 3)(3, 2, 1)^{-1} = (1, 2, 3)(1, 2, 3) = (3, 2, 1) \in A_3$  and  $(3, 2, 1)(1, 2, 3)^{-1} = (3, 2, 1)(3, 2, 1) = () \in A_3$ , and clearly if we have  $eg^{-1}$  or  $ge^{-1}$  with  $e = ()$  and  $g = (1, 2, 3)$  or  $g = (3, 2, 1)$  we will simply get  $g$  or  $g^{-1}$ , both of which are in  $A_3$  since  $(1, 2, 3)^{-1} = (3, 2, 1)$ .

■ **Example 4.1.16** Invertible transformations of some vector space form a group, since the composition of two transformations is again a transformation, by definition for an *invertible* transformation the inverse exists, and the identity transformation is in this set. Given a basis for this vector space we can write these transformations as matrices with nonzero determinants, and in doing so define the **general linear group**:

$$\text{GL}(n, \mathbb{F}) := \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det A \neq 0\}. \quad (4.1.17)$$

Here  $\mathbb{F}$  is a field,  $n$  is the dimension of the vector space, and  $\mathcal{M}_n(\mathbb{F})$  are all square  $n \times n$  matrices with entries from  $\mathbb{F}$ . Recall that  $A \in \mathcal{M}_n(\mathbb{F})$  is invertible if and only if  $\det A \neq 0$ .

Another group we can define is the **special linear group**:

$$\text{SL}(n, \mathbb{F}) := \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det A = 1\} \subseteq \text{GL}(n, \mathbb{F}). \quad (4.1.18)$$

$\text{SL}(n, \mathbb{F})$  is a subgroup of  $\text{GL}(n, \mathbb{F})$  since if  $A, B \in \text{SL}(n, \mathbb{F})$  then  $\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)/\det(B) = 1/1 = 1$ , so  $AB^{-1} \in \text{SL}(n, \mathbb{F})$ .



Further,  $SL(n, \mathbb{F})$  is a normal subgroup of  $GL(n, \mathbb{F})$  since if  $A \in SL(n, \mathbb{F})$  and  $B \in GL(n, \mathbb{F})$  we have

$$\det(BAB^{-1}) = \det(B) \det(A) \det(B^{-1}) = \det(B) \det(A) \frac{1}{\det(B)} = \det(A) = 1$$

so  $BAB^{-1}$  is again in  $SL(n, \mathbb{F})$ .

There is an easier way to test if a subgroup is normal, and it is to consider the cosets.

**Theorem 4.1.19.** Let  $H$  be a subgroup of some group,  $G$ . Then  $H$  is a normal subgroup of  $G$  if and only if the left and right cosets are equal. That is  $gH = Hg$  for all  $g \in G$ .

*Proof.* First, suppose that  $H$  is a normal subgroup. Consider some  $g \in G$  and  $h \in H$ . Then  $ghg^{-1} \in H$ , call  $h' = ghg^{-1}$ . Similarly since  $g^{-1} \in G$  we have  $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$ , call  $h'' = g^{-1}hg$ . Then  $gh = ghg^{-1}g = h'g \in Hg$  and  $hg = gg^{-1}hg = gh'' \in gH$ . Since  $gh \in Hg$  for all  $h \in H$  it follows that  $gH \subseteq Hg$ . Since  $hg \in gH$  for all  $h \in H$  it follows that  $Hg \subseteq gH$ . Hence  $gH = Hg$ .

Now, suppose that  $gH = Hg$  for all  $g \in G$ . Then for some  $g \in G$  and  $h \in H$  we have  $gh \in gH = Hg$ , which means there exists some  $h' \in H$  such that  $gh = h'g$ . Left multiplying by  $g^{-1}$  we have  $ghg^{-1} = h' \in H$ , and so  $H$  is invariant under conjugation and hence normal in  $G$ .  $\square$

## 4.2 Coset Groups

**Definition 4.2.1 — Coset Product** Let  $G$  be a group and  $N$  be a normal subgroup of  $G$ . Then we can define  $G/N$  to be the set of cosets of  $N$ , that is

$$G/N := \{gN \mid g \in G\} = \{Ng \mid g \in G\}. \quad (4.2.2)$$

We can define a binary operation on  $G/N$  according to

$$(gN)(g'N) := (gg')N. \quad (4.2.3)$$

With this operation  $G/N$  forms a group which we call the **quotient group** or **factor group**.

**Theorem 4.2.4.** If  $G$  is a group and  $N$  is a normal subgroup of  $G$  then  $G/N$  with the operation defined above is a group.

*Proof.* We must first show that the operation is well defined. That is that no matter which element of  $gN$  we choose to represent  $gN$  we get the same

result. Suppose  $gN = g'N$  and  $\tilde{g}N = \tilde{g}'N$ , the operation is well defined only if  $(g\tilde{g})N = (g'\tilde{g}')N$ . For this to be the case it is sufficient that  $g'\tilde{g}' \in (g\tilde{g})N$ . Since  $g'N = gN$  we know that  $g' = gn$  for some  $n \in N$  and since  $\tilde{g}'N = \tilde{g}N$  we know that  $\tilde{g}' = \tilde{g}\tilde{n}$  for some  $\tilde{n} \in N$ . We then have  $g'\tilde{g}' = gn\tilde{g}\tilde{n}$ . We need to show that this is of the form  $g\tilde{g}n''$  for some  $n'' \in N$ . Now, by definition since  $N$  is normal we have  $\tilde{g}n'\tilde{g}^{-1} = n$  for some  $n' \in N$ . From this it follows that  $\tilde{g}n' = n\tilde{g}$ . We then have

$$g'\tilde{g}' = (gn)(\tilde{g}\tilde{n}) \quad (4.2.5)$$

$$= g(n\tilde{g})\tilde{n} \quad (4.2.6)$$

$$= g(\tilde{g}n')\tilde{n} \quad (4.2.7)$$

$$= (g\tilde{g})(n'\tilde{n}) \quad (4.2.8)$$

$$= (g\tilde{g})n'' \quad (4.2.9)$$

where  $n'' = n'\tilde{n} \in N$ . hence this operation is well defined.

It remains to show that  $G/N$  is a group. To do so notice that  $eN = N$  acts as an identity:  $(eN)(gN) = (eg)N = gN$  for all  $g \in G$ , and that  $g^{-1}N$  is the inverse of  $gN$ , since  $(gN)(g^{-1}N) = (gg^{-1})N = eN = N$ . Associativity follows from associativity of the group product, that is if  $g_1, g_2, g_3 \in G$  then

$$[(g_1N)(g_2N)](g_3N) = [(g_1g_2)N](g_3N) \quad (4.2.10)$$

$$= ((g_1g_2)g_3)N \quad (4.2.11)$$

$$= (g_1(g_2g_3))N \quad (4.2.12)$$

$$= (g_1N)[(g_2g_3)N] \quad (4.2.13)$$

$$= (g_1N)[(g_2N)(g_3N)]. \quad (4.2.14)$$

Hence  $G/N$  is a group.  $\square$

■ **Example 4.2.15** Recall from [Example 4.1.4](#) that the quaternion group,  $Q$ , has as a normal subgroup  $\mathbb{Z}_2$ .

The quotient group in this case is  $Q/\mathbb{Z}_2$ . To see this we first write out all cosets:

$$\mathbb{Z}_2 = \{e, -e\}, \quad i\mathbb{Z}_2 = \{i, -i\}, \quad j\mathbb{Z}_2 = \{j, -j\}, \quad \text{and} \quad k\mathbb{Z}_2 = \{k, -k\}.$$

We can then construct the group table:

$Q/\mathbb{Z}_2$	$\mathbb{Z}_2$	$i\mathbb{Z}_2$	$j\mathbb{Z}_2$	$k\mathbb{Z}_2$
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$i\mathbb{Z}_2$	$j\mathbb{Z}_2$	$k\mathbb{Z}_2$
$i\mathbb{Z}_2$	$i\mathbb{Z}_2$	$\mathbb{Z}_2$	$k\mathbb{Z}_2$	$j\mathbb{Z}_2$
$j\mathbb{Z}_2$	$j\mathbb{Z}_2$	$k\mathbb{Z}_2$	$\mathbb{Z}_2$	$i\mathbb{Z}_2$
$k\mathbb{Z}_2$	$k\mathbb{Z}_2$	$j\mathbb{Z}_2$	$i\mathbb{Z}_2$	$\mathbb{Z}_2$

(4.2.16)

Here we have used  $ij = k$ ,  $jk = i$ , and  $ki = j$ ,  $i^2 = j^2 = k^2 = -e$ , and that permuting any two of  $i$ ,  $j$ , and  $k$  adds a negative sign.

Comparing this Cayley table with those in [Equation \(2.1.18\)](#) we see that  $Q/\mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . In particular we have the correspondence  $\mathbb{Z}_2 \leftrightarrow e$ ,  $i\mathbb{Z}_2 \leftrightarrow a$ ,  $j\mathbb{Z}_2 \leftrightarrow b$ , and  $k\mathbb{Z}_2 \leftrightarrow c$ .

■ **Example 4.2.17** Let  $n\mathbb{Z}$  denote the integer multiples of  $n$ , viewed as a subgroup of  $\mathbb{Z}$ . Then  $n\mathbb{Z}$  is a normal subgroup of  $\mathbb{Z}$ , since  $\mathbb{Z}$  is Abelian and so left and right cosets are equal. The cosets are of the form  $m + n\mathbb{Z} = \{m + nk \mid k \in \mathbb{Z}\}$ . There is then a natural isomorphism  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$ , namely  $m + n\mathbb{Z} \mapsto e^{2i\pi m/n}$ . For this reason a lot of people denote the group we have been calling  $\mathbb{Z}_n$  by  $\mathbb{Z}/n\mathbb{Z}$ .

**Definition 4.2.18 — Simple Group** If a group has no proper normal subgroups then we say that it is a **simple group**.

Thinking of the quotient groups,  $G/N$ , as division of groups, as the notation suggests, it makes sense to view simple groups as the “primes” of groups, in that they can’t be further divided.

Finite simple groups are classified up to automorphism. That is given any finite simple group it will be isomorphic to a group from a known set of groups. This classification of finite simple groups is not simple. The proof consists of tens of thousands of pages across several hundred journal articles written by approximately 100 authors over a period of more than 50 years, finally being completed in 2008.

**Theorem 4.2.19.** If  $G$  is a group and  $H$  is a subgroup of  $G$  and  $[G : H] = 2$  then  $H$  is a normal subgroup of  $G$ .

*Proof.* Since  $[G : H] = |G|/|H| = 2$  there are two cosets, namely  $H$  and  $gH$  for  $g \in G \setminus H$ . Considering right cosets instead we have  $H$  and  $Hg$ , again for  $g \in G \setminus H$ . By [Lemma 2.3.5](#) we also know that the cosets partition  $G$ , so that  $G = H \cup gH = H \cup Hg$ . Since  $H$  is the same in both of these and cosets are disjoint we must have that  $gH = Hg$  and so  $H$  is a normal subgroup of  $G$  by [Theorem 4.1.19](#).  $\square$

Note that in this case  $|G/H| = |G|/|H| = [G : H] = 2$  and so  $G/H \cong \mathbb{Z}_2$ .

As the name of the next theorem suggests there are multiple “isomorphism theorems” but we will discuss only on the first.

**Theorem 4.2.20 — First Isomorphism Theorem.** Let  $G$  and  $H$  be groups and  $\varphi : G \rightarrow H$  a homomorphism. Then

1. The image of  $\varphi$ ,  $\text{Im } \varphi$ , is a subgroup of  $H$ .
2. The kernel of  $\varphi$ ,  $\ker \varphi$ , is a normal subgroup of  $G$ .
3.  $G/\ker \varphi \cong \text{Im } \varphi$ .

*Proof.* The first statement is simply [Lemma 2.1.21](#).

Recall that  $\ker \varphi = \{k \in G \mid \varphi(k) = e\}$  where  $e$  is the identity of  $H$ . For the proof of the second statement consider  $k_1, k_2 \in \ker \varphi$ . Then

$$\varphi(k_1 k_2^{-1}) = \varphi(k_1) \varphi(k_2^{-1}) = \varphi(k_1) \varphi(k_2)^{-1} = ee = e \quad (4.2.21)$$

so  $k_1 k_2^{-1} \in \ker \varphi$  and so by the subgroup criterion ([Theorem 1.2.32](#))  $\ker \varphi$  is a

subgroup of  $G$ . Here we used [Lemma 2.1.20](#) to allow us to identify  $\varphi(k_2^{-1}) = \varphi(k_2)^{-1}$ .

It remains to show that  $\ker \varphi$  is a *normal* subgroup of  $G$ . Take  $k \in \ker \varphi$  and  $g \in G$ . Then

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e \quad (4.2.22)$$

where we have used [Lemma 2.1.19](#) to identify  $\varphi(e) = e$ . This shows that  $gkg^{-1} \in \ker \varphi$  and so  $\ker \varphi$  is a normal subgroup of  $G$ . This proves the second point.

For the third point we need to show that there is an isomorphism  $\psi: G/\ker \varphi \rightarrow \text{Im } \varphi$ . To do so we consider the obvious choice that  $\psi(gK) = \varphi(g)$ , where  $K = \ker \varphi$ . Since  $\psi$  is defined on representatives of the cosets we need to show that it is well defined. Let  $g_1, g_2 \in G$  be in the same coset, that is  $g_1K = g_2K$ . It follows that  $(g_1^{-1}K)(g_2K) = (g_1g_2)K$  but also  $(g_1^{-1}K)(g_2K) = (g_1^{-1}K)(g_1K) = (g_1^{-1}g_1)K = K$  and so  $g_1^{-1}g_2 \in K$ . Thus,  $\varphi(g_1^{-1}g_2) = e$ , since  $K = \ker \varphi$ . We then have  $\varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2)$  having used the definition of the homomorphism and [Lemma 2.1.20](#). We then have  $\varphi(g_1)^{-1}\varphi(g_2) = e$ , and so  $\varphi(g_1) = \varphi(g_2)$ . This shows that  $\psi$  is well defined.

Next, we verify that  $\psi$  is a homomorphism. To do so let  $g_1, g_2 \in G$  and so  $g_1K, g_2K \in G/K$ . We then have

$$\psi((g_1K)(g_2K)) = \psi((g_1g_2)K) \quad (4.2.23)$$

$$= \varphi(g_1g_2) \quad (4.2.24)$$

$$= \varphi(g_1)\varphi(g_2) \quad (4.2.25)$$

$$= \psi(g_1K)\psi(g_2K), \quad (4.2.26)$$

so  $\psi$  is a homomorphism.

Finally we show that  $\psi$  is an isomorphism, that is that it is bijective. The kernel of  $\psi$  consists of all cosets  $gK \in G/K$  such that  $\varphi(g) = e$ , but these are exactly the elements  $g \in G$  such that  $g \in K = \ker \varphi$ . Hence the kernel of  $\psi$  is the trivial group  $\{K\} \subset G/K$ . This proves that  $\psi$  is injective by . Finally let  $h \in \text{Im } \varphi$ . Then there exists  $g \in G$  such that  $\varphi(g) = h$ . We then have  $\psi(gK) = \varphi(g) = h$ , and so  $\psi$  is surjective.

So  $\psi$  is a bijective homomorphism and hence an isomorphism.  $\square$

An alternative statement of the first isomorphism theorem is that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & \text{Im } \varphi \subseteq H \\ \downarrow \pi & \searrow \psi & \\ G/\ker \varphi & & \end{array} \quad (4.2.27)$$

Here  $\pi: G \rightarrow G/\ker \varphi$  is the **natural projection** defined by  $\pi(g) = g \ker \varphi$ . We use the notation  $X \xrightarrow{\sim} Y$  to denote an isomorphism from  $X$  to  $Y$ .

One of the main uses of the first isomorphism theorem is to quickly check if a subgroup is normal. This works since if  $H$  is a subgroup of some group  $G$  and there exists some homomorphism  $\varphi: G \rightarrow \tilde{G}$  for some group  $\tilde{G}$  such that  $H = \ker \varphi$  then by the first isomorphism theorem  $\ker \varphi$ , and hence  $H$ , is normal in  $G$ .

# Five

## Products of Groups

### 5.1 Direct Products

**Definition 5.1.1 — Direct Product** Let  $H$  and  $J$  be groups. Then we define a new group,  $H \times J$ , called the **direct product** of  $H$  and  $J$  such that

$$H \times J := \{(h, j) \mid h \in H \text{ and } j \in J\}. \quad (5.1.2)$$

We extend the products of the two groups to define a product

$$(h, j)(h', j') = (hh', jj') \quad (5.1.3)$$

for  $h, h' \in H$  and  $j, j' \in J$ .

We can think of the direct product as extending the Cartesian product to groups. Notice that for finite groups  $|H \times J| = |H||J|$ .

**Theorem 5.1.4.** The direct product of two groups is a group.

*Proof.* Let  $H$  and  $J$  be groups. Consider  $h_1, h_2, h_3 \in H$  and  $j_1, j_2, j_3 \in J$ . Then

$$(h_1, j_1)[(h_2, j_2)(h_3, j_3)] = (h_1, j_1)(h_2h_3, j_2j_3) \quad (5.1.5)$$

$$= (h_1(h_2h_3), j_1(j_2j_3)) \quad (5.1.6)$$

$$= ((h_1h_2)h_3, (j_1j_2)j_3) \quad (5.1.7)$$

$$= (h_1h_2, j_1j_2)(h_3, j_3) \quad (5.1.8)$$

$$= [(h_1, j_1)(h_2, j_2)](h_3, j_3) \quad (5.1.9)$$

so associativity in  $H \times J$  follows from associativity in  $H$  and  $J$ .

let  $e_H$  be the identity of  $H$  and  $e_J$  the identity of  $J$ . Then

$$(h, j)(e_H, e_J) = (he_H, je_J) = (h, j) \quad (5.1.10)$$

for all  $h \in H$  and  $j \in J$  and so  $e_{H \times J} = (e_H, e_J)$  is the identity of  $H \times J$ .

Finally notice that for all  $h \in H$  and  $j \in J$  we have

$$(h, j)(h^{-1}, j^{-1}) = (hh^{-1}, jj^{-1}) = (e_H, e_J) = e_{H \times J} \quad (5.1.11)$$

and since  $h^{-1} \in H$  and  $j^{-1} \in J$  we have that  $(h^{-1}, j^{-1}) \in H \times J$  acts as the inverse for  $(h, j) \in H \times J$ .  
Hence  $H \times J$  is a group.  $\square$

■ **Example 5.1.12 — Klein Vierergruppe** The **Klein Vierergruppe** is most simply defined as the direct product group  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Note that

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\} \quad (5.1.13)$$

and all elements square to  $(1, 1)$ , which is the identity, for example,  $(-1, 1)^2 = ((-1)^2, 1^2) = (1, 1)$ . Hence  $\mathbb{Z}_2 \times \mathbb{Z}_2$  matches our earlier definition of the **Klein Vierergruppe**, namely the unique group of order 4 such that all elements square to the identity.

■ **Example 5.1.14** Let  $\mathbb{R}$  be the group of real numbers under addition. Then  $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$  is the group of two-component vectors,  $(x, y)$ , with addition defined by

$$(x, y) + (x', y') = (x + x', y + y'). \quad (5.1.15)$$

The direct product is both commutative and associative up to isomorphism. That is  $G \times H \cong H \times G$  and  $G \times (H \times J) \cong (G \times H) \times J$ , with the obvious isomorphisms  $(g, h) \mapsto (h, g)$  and  $(g, (h, j)) \mapsto ((g, h), j)$ , respectively. The latter means that we can define the direct product of multiple groups in a sensible way and so we typically write  $G \times H \times J$  and  $(g, h, j)$  and so on.

The order of  $(h, j) \in H \times J$  is the lowest common multiple of the orders of  $h$  and  $j$ . In particular if the orders of  $h$  and  $j$  are relatively prime then the order of  $(h, j)$  is the product of the orders of  $h$  and  $j$ . This means that if  $H$  and  $J$  are cyclic groups of relatively prime orders  $m$  and  $n$  their direct product is again cyclic:

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}. \quad (5.1.16)$$

Given two groups,  $G$  and  $H$ , it is common to view  $G$  and  $H$  as subgroups of  $G \times H$ , which can be done since we can identify  $G \cong \{e\} \times H$  and  $H \cong G \times \{e\}$  under the obvious isomorphisms  $g \mapsto (g, e)$  and  $h \mapsto (e, h)$ , respectively. Making this identification both  $G$  and  $H$  are normal subgroups of  $G \times H$ . We can show this easily for  $G$  and it can be shown similarly for  $H$ :

$$(g, h)(g', e)(g, h)^{-1} = (g, h)(g', e)(g^{-1}, h^{-1}) = (gg'g^{-1}, heh^{-1}) = (gg'g^{-1}, e) \in G \times \{e\} \quad (5.1.17)$$

since  $gg'g^{-1} \in G$  as  $G$  is a group.

## 5.2 Semidirect Product

**Definition 5.2.1 — Semidirect Product** Let  $H$  and  $J$  be groups and  $\varphi: H \times J \rightarrow J$  a group action of  $H$  on  $J$ . Then we can define a new group,  $H \ltimes J$ , as the set

$$\{(h, j) \mid h \in H \text{ and } j \in J\} \quad (5.2.2)$$

and the group product

$$(h, j)(h', j') = (hh', j\varphi(h, j')) = (hh', j(h \cdot j')) \quad (5.2.3)$$

for  $h, h' \in H$  and  $j, j' \in J$ .



The vertical line in the symbol  $\ltimes$  goes with the group which acts on the other group.

For each group action we technically have two semidirect product groups,  $H \ltimes J$  and  $J \rtimes H$ , but these differ only in the order of elements,  $(h, j)$  vs.  $(j, h)$ , and are isomorphic. The order of  $H \ltimes J$  is  $|H \ltimes J| = |H||J|$ .

■ **Example 5.2.4 — Isometries of Euclidean Space** The **isometries of Euclidean space** is the group which preserves Euclidean distance. This group is typically denoted  $\text{ISO}(n)$  or  $\text{E}(n)$ , where  $n$  is the dimension of the space on which the group acts. This group consists of rotations, reflections and translations. Transformations in the first two categories, rotations and reflections, form  $\text{O}(n)$ , that is the group of transformations which preserve Euclidean distance and leave the origin invariant. Translations can be viewed as  $\mathbb{R}^n$ . A point in Euclidean space can be viewed as  $x \in \mathbb{R}^n$ , which is somewhat confusing since  $\mathbb{R}^n$  appears twice, as both the translations and the Euclidean space upon which they act.

We can write  $\text{ISO}(n)$  as a semidirect product,  $\text{ISO}(n) = \text{O}(n) \ltimes \mathbb{R}^n$ . We just need to work out the correct group action. First we need to state how  $\text{ISO}(n)$  acts on  $\mathbb{R}^n$  (as Euclidean space). This is simple, given a rotation and/or reflection  $R \in \text{O}(n)$  and translation  $a \in \mathbb{R}^n$  this acts on  $x \in \mathbb{R}^n$  as  $(R, a) \cdot x = Rx + a$ , that is we rotate  $x$  with  $R$  and then translate by  $a$ , notice that the order is important, which we will see means that  $\text{ISO}(n)$  is *not* a direct product of  $\text{O}(n)$  and  $\mathbb{R}^n$ .

Consider what happens when we act on some  $x \in \mathbb{R}^n$  (as a point in Euclidean space) by two isometries,  $(R, a)$  and  $(R', a')$ , where  $R, R' \in \text{O}(n)$  and  $a, a' \in \mathbb{R}^n$  (as the group of translations). We then have

$$(R', a')(R, a) \cdot x = (R', a') \cdot (R, a) \cdot x \quad (5.2.5)$$

$$= (R', a) \cdot (Rx + a) \quad (5.2.6)$$

$$= R'(Rx + a) + a' \quad (5.2.7)$$

$$= R'Rx + R'a + a' \quad (5.2.8)$$

$$= (R'R, R'a + a') \cdot x. \quad (5.2.9)$$

So we identify the group action associated with the semidirect product as

$$R' \cdot a = R'a, \quad \text{or} \quad \varphi(R', a) = Ra, \quad (5.2.10)$$



which is probably what most people would expect, the rotation (or reflection) acts by rotating (or reflecting).

We can further generalise the isometries of Euclidean space by dropping the requirement that lengths be preserved and allowing uniform scaling. In this case the group of symmetries is the affine group,  $\text{Aff}(V)$ , which is the semidirect product  $\text{GL}(V) \ltimes V$  where  $\text{GL}(V)$  acts on the vector space  $V$  with the expected action,  $M \cdot v = Mv$  for  $M \in \text{GL}(V)$  and  $v \in V$ . This contains  $\text{ISO}(V)$  as a subgroup.

■ **Example 5.2.11 — Dihedral Group** The **dihedral group** of order  $2n$  can be defined abstractly as

$$D_n := \langle r, s \mid r^n = s^2 = e, s^{-1}rs = r^{-1} \rangle. \quad (5.2.12)$$

This can be identified as the group of symmetries of the regular  $n$ -gon. Here  $r$  is identified as a rotation by  $2\pi/n$  and  $s$  as a mirror symmetry or inversion in a perpendicular bisector of one of the sides.



Some sources denote the dihedral group of order  $2n$  by  $D_{2n}$ , since it has  $2n$  elements, whereas we denote it  $D_n$ , as it is the group of symmetries of the regular  $n$ -gon.

We can identify a subgroup generated by  $s$  as  $\mathbb{Z}_2 = \{e, s\}$ . We can identify a subgroup generated by  $r$  as  $\mathbb{Z}_n = \{e, r, \dots, r^{n-1}\}$ . It turns out that  $D_n$  can then be written as the semidirect product  $D_n = \mathbb{Z}_2 \ltimes \mathbb{Z}_n$ .

To see this it is best to just consider a few examples. First we identify  $\mathbb{Z}_2 = \{\pm 1\}$ , and  $\mathbb{Z}_n = \{e^{2i\pi m/n}\}$ . A few examples of products in  $D_n$  are then

$$(+1, e^{2i\pi m/n})(+1, e^{2i\pi m'/n}) = (+1, e^{2i\pi(m+m')/n}), \quad (5.2.13)$$

$$(-1, e^{2i\pi m/n})(+1, e^{2i\pi m'/n}) = (-1, e^{2i\pi(m-m')/n}), \quad (5.2.14)$$

$$(+1, e^{2i\pi m/n})(+1, e^{2i\pi m'/n}) = (-1, e^{2i\pi(m+m')/n}). \quad (5.2.15)$$

That is the group action associated with the semidirect product is  $\pm 1 \cdot e^{2i\pi m/n} = e^{\pm 2i\pi m/n}$ . We can further identify this as  $1 \cdot z = z$  and  $-1 \cdot z = z^*$ .

It is worth examining the dihedral group more, particularly as it comes up in geometry and chemistry. Starting with geometry we claimed that  $D_3$  is the group of symmetries of an equilateral triangle. By this we mean that  $D_3$  acts on an equilateral triangle such that there is no noticeable change. However, in order to keep track of what is happening we label the corners of the triangle, but these labels have no meaning besides keeping track of how  $D_3$  is acting. Taking  $r$  to be a clockwise rotation by  $120^\circ$  and  $s$  to be a reflection in the vertical. Graphically the action of  $r$  and  $s$  on the triangle is

$$r \cdot \begin{array}{c} 2 \\ \triangle \\ 1 \quad 3 \end{array} = \begin{array}{c} 1 \\ \triangle \\ 3 \quad 2 \end{array}, \quad \text{and} \quad s \cdot \begin{array}{c} 2 \\ \triangle \\ 1 \quad 3 \end{array} = \begin{array}{c} 2 \\ \triangle \\ 3 \quad 1 \end{array} \quad (5.2.16)$$

We should check that these symmetries really correspond to  $D_3$  as defined by the presentation above. First, notice that three rotations correspond to a rotation by  $3 \cdot 120^\circ = 360^\circ$ , which is the same as no rotation at all. Second, notice that repeating

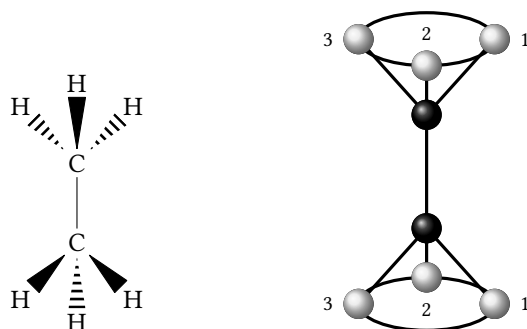


Figure 5.1: Ethane molecule.

a mirror symmetry undoes it so  $s^2 = e$ . Finally consider the action of  $srs^{-1}$  on the triangle, noticing that  $s^{-1} = s$ , we have

$$\begin{aligned}
 srs^{-1} \cdot \begin{array}{c} 2 \\ \triangle \\ 1 \quad 3 \end{array} &= sr \cdot \begin{array}{c} 2 \\ \triangle \\ 3 \quad 1 \end{array} \\
 &= s \cdot \begin{array}{c} 3 \\ \triangle \\ 1 \quad 2 \end{array} \\
 &= \begin{array}{c} 3 \\ \triangle \\ 2 \quad 1 \end{array} .
 \end{aligned} \tag{5.2.17}$$

Now compare this to the action of  $r^{-1}$ , which is an anticlockwise rotation by  $120^\circ$ :

$$r^{-1} \cdot \begin{array}{c} 2 \\ \triangle \\ 1 \quad 3 \end{array} = \begin{array}{c} 3 \\ \triangle \\ 2 \quad 1 \end{array} . \tag{5.2.18}$$

Noticing that these are the same we see that  $D_3$  does truly describe the symmetries of the equilateral triangle.

As well as the equilateral triangle  $D_3$  is also the symmetry group of an ideal  $C_2H_6$  molecule. This molecule is shown in [Figure 5.1](#). Here we identify  $r$  as a rotation around the carbon-carbon bond and  $s$  as a rotation by  $180^\circ$  about the perpendicular bisector to this bond in the page, such that the numbers on the upper and lower hydrogens match. Shown here is staggered ethane, which is such that viewed end on the hydrogens don't line up.  $D_3$  is also the symmetry group of eclipsed ethane, where viewed on the hydrogens line up, we just change  $s$  to be inversion about the centre of the carbon-carbon bond.

# Six

## Permutation Groups

### 6.1 Symmetric Group

**Definition 6.1.1 — Permutation** a permutation,  $\sigma$ , on  $n$  objects is a bijection  $\sigma: X \rightarrow X$  where  $|X| = n$ .

Typically we identify  $X$  as  $\{1, \dots, n\}$ .

**Definition 6.1.2 — Symmetric Permutation Group** The symmetric group on  $n$  objects is the set of all permutations on  $n$  objects with function composition as a group operation. This group is denoted  $S_n$ .

The order of  $S_n$  is  $n!$ , since we can choose to permute the first element to any of  $n$  possible options, the second to any of  $n-1$  options, and so on giving  $n(n-1) \cdots 1 = n!$  choices.

**Lemma 6.1.3** The symmetric group on  $n$  objects is a group.

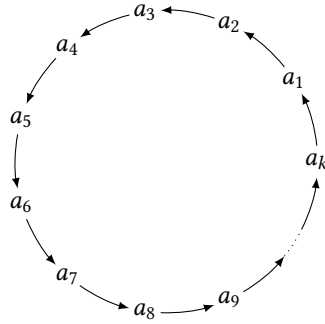
*Proof.* Let  $\sigma, \rho \in S_n$ . Then both of these are bijections on some set  $X$  with  $|X| = n$ . Their composition is defined by  $(\sigma \circ \rho)(x) = \sigma(\rho(x))$  for all  $x \in X$ . Straight away we see that this is indeed a permutation, since  $\sigma \circ \rho: X \rightarrow X$  and the inverse is  $\rho^{-1} \circ \sigma^{-1}$ , the existence of said inverses in  $S_n$  is guaranteed as  $\sigma \in S_n$  is a bijection and so its inverse exists and is also a bijection. This shows that  $S_n$  is closed.

The identity function,  $\text{id}_X: X \rightarrow X$  defined by  $\text{id}_X(x) = x$  for all  $x \in X$  is a permutation and  $\text{id}_X \circ \sigma = \sigma$  for all  $\sigma \in S_n$ . As previously discussed  $\sigma$  has the inverse  $\sigma^{-1}$ , which is such that  $\sigma \circ \sigma^{-1} = \text{id}_X$ . Hence  $S_n$  is a group.  $\square$

$S_n$  acts on the set of all tuples  $(x_1, \dots, x_n)$  where  $x_i \in X$  are distinct in the obvious way, namely by permuting the elements:

$$\sigma \cdot (x_1, \dots, x_n) = (\sigma(x_1), \dots, \sigma(x_n)). \quad (6.1.4)$$

**Definition 6.1.5 — Cycle** A  $k$ -cycle is a way of writing a certain permutation. Namely  $(a_1, \dots, a_k)$  with  $a_i \in X$  is the permutation that sends  $a_1$  to  $a_2$ ,  $a_2$  to  $a_3$ , and so on until  $a_{k-1}$  to  $a_k$  and  $a_k$  to  $a_1$ . All  $x \in X$  such that  $x \neq a_i$

Figure 6.1: The  $k$ -cycle  $(a_1, \dots, a_k)$ .

are left unchanged.

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

The identity is usually written as  $()$  when using cycle notation, although we could also write it as a 1-cycle,  $(a)$  for any  $a \in X$ .

Given a  $k$ -cycle  $(a_1, \dots, a_k)$  we can start on any element of this cycle, so this is equivalent to  $(a_m, \dots, a_k, a_1, \dots, a_{m-1})$ .

■ **Example 6.1.6** Consider  $S_4$ , this contains the 3-cycles  $(1, 4, 2)$  and  $(1, 2, 3)$ . We can work out their product by considering their action on some 4-tuple  $(a, b, c, d)$ :

$$(1, 4, 2)(1, 2, 3) \cdot (a, b, c, d) = (1, 4, 2) \cdot (c, a, b, d) \quad (6.1.7)$$

$$= (a, d, b, c) \quad (6.1.8)$$

$$= (2, 3, 4) \cdot (a, b, c, d), \quad (6.1.9)$$

hence, we have  $(1, 4, 2)(1, 2, 3) = (2, 3, 4)$ .

**Definition 6.1.10 — Disjoint Cycles** Two cycles are disjoint if no element of  $X$  appears in both cycles.

**Lemma 6.1.11** All permutations can be written as a product of disjoint cycles.

*Proof.* We proceed by induction on the size of  $n = |X|$ . Clearly if  $n = 1$  then the only permutation is the identity,  $()$ .

Let  $\sigma \in S_n$  and suppose that all cycles in  $S_{n-1}$  can be written as disjoint cycles. For simplicity we will take  $X = \{1, \dots, n\}$ . If  $\sigma(n) = n$  then we can consider  $\sigma$  as a permutation on  $\{1, \dots, n-1\}$  leaving  $n$  fixed and we are done since this can be written as a product of disjoint cycles. If  $\sigma(n) = k \neq n$  then consider the permutation  $\rho = (n, k)\sigma$ . We have that  $\rho(n) = (n, k)\sigma(n) = (n, k)k = n$ . So we can think of  $\rho$  as being a permutation on  $\{1, \dots, n-1\}$ , and hence can be written as a product of disjoint cycles,  $\rho = \tau_1 \cdots \tau_r$ . The cycles  $\tau_i$  only

contain the numbers  $1, \dots, n-1$ , and each appears in at most one of these cycles.

Clearly  $(n, k)(n, k) = ()$ , and so it follows that  $\sigma = (n, k)(n, k)\sigma = (n, k)\tau_1 \cdots \tau_r$ . If  $k$  doesn't appear in any of the cycles  $\tau_i$  then we are done as this is a product of disjoint cycles. Disjoint cycles commute, since by being disjoint they act on different elements of the tuple  $(x_1, \dots, x_n)$ , and so don't interact, meaning the order doesn't matter. Using this we are free to assume that the cycle in which  $k$  appears, if it appears, is  $\tau_1$ .

We are free to start on any element of the cycle so we write  $\tau_1 = (k, a_1, \dots, a_m)$ . We then have

$$(n, k)\tau_1 = (n, k)(k, a_1, \dots, a_m) = (n, k, a_1, \dots, a_m). \quad (6.1.12)$$

This follows by considering  $(n, k)\tau_1(k) = (n, k)a_1 = a_1$ ,  $(n, k)\tau_1(n) = (n, k)n = k$ ,  $(n, k)\tau_1(a_m) = (n, k)k = n$ , and  $(n, k)\tau_1(a_i) = (n, k)a_{i+1} = a_{i+1}$  for  $i \neq m$ . It follows then that we can write

$$\sigma = (n, k, a_1, \dots, a_m)\tau_2 \cdots \tau_r \quad (6.1.13)$$

which is a product of disjoint cycles.

Hence by induction we can write any permutation in  $S_n$  as a product of disjoint cycles for all  $n \in \mathbb{N}$ .  $\square$

One question that we may reasonably ask is how many  $m$ -cycles are there in  $S_n$  for some fixed  $m \in \{1, \dots, n\}$ . If the order of a cycle didn't matter then there would be  $\binom{n}{m}$   $m$ -cycles in  $S_n$ . However, the order does matter. Suppose we have chosen our  $m$  terms to appear in the cycle. We can start with any of them, reducing the number of choices that give distinct cycles by a factor of  $1/m$ . There are then  $(m-1)!$  choices for ordering the  $m-1$  elements remaining, giving the number of  $m$ -cycles to be

$$\binom{n}{m} \frac{1}{m} (m-1)! = \frac{n!}{(n-m)!m!} \frac{1}{m} (m-1)! = \frac{n!}{(n-m)!} \quad (6.1.14)$$

where we have used  $m(m-1)! = m!$ .

**Theorem 6.1.15.** The transpositions generate  $S_n$ . That is, all permutations can be written as a product of 2-cycles.

*Proof.* All elements of  $S_n$  are simply  $k$ -cycles for some  $k \in \{1, \dots, n\}$ . An arbitrary  $k$ -cycle can be written as

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2). \quad (6.1.16)$$

To see why this works we consider three cases. First, if this acts on some  $a_i$  with  $i \neq 1$ , on the left hand side we clearly see that  $a_i$  maps to  $a_{i+1}$ . On the right hand side  $a_i$  commutes with cycles until a cycle with  $a_i$  occurs, this cycle will be  $(a_1, a_i)$ , and so  $a_i$  will be sent to  $a_1$ . The next cycle is then  $(a_1, a_{i+1})$ , and hence  $a_1$  maps to  $a_{i+1}$  which then commutes with all of the remaining cycles. Hence  $a_i$  will map to  $a_{i+1}$ .

The second case is when this acts on  $a_1$ , in which case the first cycle sends

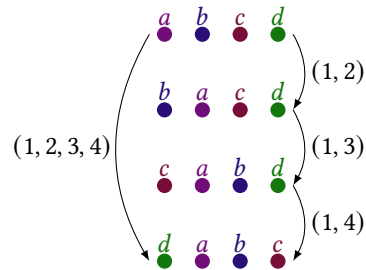


Figure 6.2: The permutation  $(1, 2, 3, 4)$  acts  $(a, b, c, d)$ , which can be done in steps where each step is a transposition.

$a_1$  to  $a_2$ , which then commutes with all remaining cycles and so  $a_1$  maps to  $a_2$ , which is what we want.

The final case is trivial, its where this acts on some  $a \neq a_i$  for any  $i$ , in which case on both the left and right this element is not changed and we are finished.

□

The above theorem is fairly obvious. It states that we can do any permutation just by swapping two items at a time. This is demonstrated in [Figure 6.2](#).

Notice that this theorem implies that the rank of  $S_n$  is at most  $\binom{n}{2}$ , although we will see it is less than this.

# Appendices

# A

## Mathematical Preliminaries

### A.1 Basic Mathematics

#### A.1.1 Notation

**Notation A.1.1 — Number Sets** The set of natural numbers is

$$\mathbb{N} := \{0, 1, 2, \dots\}. \quad (\text{A.1.2})$$

Note that the inclusion of zero in  $\mathbb{N}$  is subject to debate. The set of integers is denoted

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}. \quad (\text{A.1.3})$$

The set of positive integers is denoted

$$\mathbb{Z}_{>0} := \{1, 2, \dots\}. \quad (\text{A.1.4})$$

The set of rational numbers is denoted

$$\mathbb{Q} := \{p/q \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}. \quad (\text{A.1.5})$$

The set of real numbers is denoted  $\mathbb{R}$ , and the set of complex numbers  $\mathbb{C}$ . The set of *all* quaternions (as opposed to the quaternion group of order 8) is denoted  $\mathbb{H}$ .

**Notation A.1.6 — Sphere** The unit sphere in  $n + 1$  dimensions is

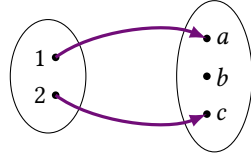
$$S^n := \{x \in \mathbb{R}^{n+1} \mid x_1^2 + \dots + x_{n+1}^2 = 1\}. \quad (\text{A.1.7})$$

Note that  $S^n$  is an  $n$ -dimensional manifold, which we view as embedded in  $(n + 1)$ -dimensional Euclidean space,  $\mathbb{R}^{n+1}$ .

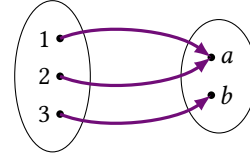
What we normally call the circle is  $S^1$  and what we normally call the sphere is  $S^2$ .

**Notation A.1.8 — Sets of Matrices** We denote the set of  $m \times n$  matrices with entries in  $\mathbb{F}$  (which is usually a field and usually  $\mathbb{R}$  or  $\mathbb{C}$ ) by  $\mathcal{M}_{m \times n}(\mathbb{F})$ . We denote the set of square  $n \times n$  matrices with entries in  $\mathbb{F}$  by  $\mathcal{M}_n(\mathbb{F})$ .

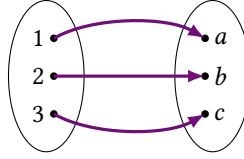




(a) An injective function,  $f: \{1, 2\} \rightarrow \{a, b, c\}$ . Note that  $f(x) \neq b$  for any  $x \in \{1, 2\}$  and so the function fails to be surjective.



(b) A surjective function,  $g: \{1, 2, 3\} \rightarrow \{a, b\}$ . Note that  $g(1) = g(2)$  but  $1 \neq 2$  and so the function fails to be injective.



(c) A bijective function,  $h: \{1, 2, 3\} \rightarrow \{a, b, c\}$ .

Figure A.1: Injective, surjective, and bijective functions.

We denote the set of invertible  $n \times n$  square matrices over  $\mathbb{F}$ , called the general linear group, by

$$\text{GL}(n, \mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det A \neq 0\}. \quad (\text{A.1.9})$$

If  $\mathbb{F}$  is evident from context we may simply write  $\text{GL}(n)$ . If  $V$  is an  $n$ -dimensional vector space over  $\mathbb{F}$  then we may also write this set as  $\text{GL}(V)$ .

**Notation A.1.10 — Einstein Summation Convention** When two identical indices appear in the same term then they are summed over, for example,

$$x_i y_i = \sum_i x_i y_i. \quad (\text{A.1.11})$$

## A.1.2 Definitions

**Definition A.1.12 — Function Types** Let  $\varphi: A \rightarrow B$ . Then  $\varphi$  is

- **injective** if for all  $a, a' \in A$   $\varphi(a) = \varphi(a')$  implies  $a = a'$ ,
- **surjective** if for all  $b \in B$  there exists  $a \in A$  such that  $\varphi(a) = b$ , and
- **bijective** if  $\varphi$  is both injective and surjective.

A function is invertible if and only if it is bijective.

**Definition A.1.13 — Kernel** Given a map  $\varphi: A \rightarrow B$  the **kernel** is defined as the set of elements of  $A$  which map to the trivial element of  $B$ , which is the

zero vector,  $\mathbf{0}$ , if  $B$  is a vector space, or the identity if  $B$  is a group:

$$\ker \varphi := \{a \in A \mid \varphi(a) \text{ is the trivial element of } B\} \subseteq A. \quad (\text{A.1.14})$$

**Definition A.1.15 — Image** Given a map  $\varphi: A \rightarrow B$  the **image** is set of  $b \in B$  for which there exists some  $a \in A$  such that  $\varphi(a) = b$ :

$$\text{Im } \varphi = \varphi(A) := \{b \in B \mid \exists a \in A \text{ such that } \varphi(a) = b\} \subseteq B. \quad (\text{A.1.16})$$

**Definition A.1.17 — Empty Set** The **empty set**,  $\emptyset$ , is the set containing no elements.

**Definition A.1.18 — Kronecker Delta** The **Kronecker delta**,  $\delta_{ij}$ , is defined as

$$\delta_{ij} := \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases} \quad (\text{A.1.19})$$

Note that  $\delta_{ij}$  are the elements of the identity matrix.

**Definition A.1.20 — Levi-Civita Symbol** The **Levi-Civita Symbol** in  $n$ -indices is the completely asymmetric (pseudo)tensor which is defined so that  $\varepsilon_{123\dots n} := 1$ . Antisymmetry then means that  $\varepsilon_{1\dots i\dots j\dots n} = -\varepsilon_{1\dots j\dots i\dots n}$ , for example  $\varepsilon_{213\dots n} = -1$ . Antisymmetry also means that Levi-Civita symbol vanishes if it has repeated indices. Most commonly  $n = 3$  and

$$\varepsilon_{ijk} := \begin{cases} 1, & \text{if } (i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2), \\ -1, & \text{if } (i, j, k) = (1, 3, 2), (2, 1, 3), (3, 2, 1), \\ 0, & \text{if any index is repeated.} \end{cases} \quad (\text{A.1.21})$$

**Definition A.1.22 — Equivalence Relations** Given two sets,  $A$  and  $B$ , a **relation**,  $R$ , is a subset of  $A \times B := \{(a, b) \mid a \in A \text{ and } b \in B\} \supseteq R$ . We say that  $a \in A$  is related to  $b \in B$ , which we denote with infix notation,  $a R b$ , if  $(a, b) \in R$ .

If  $A = B$  in the above definition then we call  $R$  a **binary relation** on  $A$ .

A relation,  $\sim$ , on a set  $A$  is a binary relation on  $A$  such that the following axioms hold for all  $a, b, c \in A$

- $\sim$  is **reflexive**, so  $a \sim a$ .
- $\sim$  is **symmetric**, so if  $a \sim b$  then  $b \sim a$ .
- $\sim$  is **transitive**, so if  $a \sim b$  and  $b \sim c$  then  $a \sim c$ .

A **equivalence class** of an element  $a \in A$  under some equivalence relation,  $\sim$ , is the set

$$[a] := \{x \mid a \sim x\}. \quad (\text{A.1.23})$$

We call elements of  $[a]$  representatives of the equivalence class. We denote the set of all equivalence classes by  $A/\sim$ .

■ **Example A.1.24 — Equivalence Relations**  $\sim$  is the prototypical equivalence relation.

Congruence modulo  $m \in \mathbb{Z}_{>0}$  is an equivalence relation on  $\mathbb{R}$ .

$\sim$  defined by  $z \sim w$  if  $|z| = |w|$  is an equivalence relation on  $\mathbb{C}$ .

$\sim$  defined by  $v \sim u$  if  $u$  and  $v$  are parallel is an equivalence relation on  $\mathbb{R}^n$ .

■ **Example A.1.25 — Isomorphism** Isomorphisms, as defined in the text, are equivalence relations:

- Let  $A$  be a group, then the identity function,  $\text{id}_A: A \rightarrow A$  defined by  $\text{id}_A(a) = a$  for all  $a \in A$  is an isomorphism since  $\text{id}_A(aa') = aa' = \text{id}_A(a)\text{id}_A(a')$  and clearly  $\text{id}_A$  is invertible, and is its own inverse.
- Let  $A$  and  $B$  be isomorphic groups. Then there exists some bijection  $\varphi: A \rightarrow B$  such that  $\varphi(aa') = \varphi(a)\varphi(a')$ . Since  $\varphi$  is a bijection  $\varphi^{-1}: B \rightarrow A$  exists and is also a bijection. Applying the inverse to both sides of the defining relation we have  $\varphi^{-1}(\varphi(aa')) = \varphi^{-1}(\varphi(a)\varphi(a'))$ . Since  $\varphi$  is surjective any element of  $B$  can be written in the form  $b = \varphi(a)$  for some  $a \in A$  and so it follows that  $\varphi^{-1}(\varphi(aa')) = \varphi^{-1}(b)\varphi^{-1}(\varphi(a'))$  where  $b, b' \in B$  are arbitrary and we choose  $a, a' \in A$  to be such that  $b = \varphi(a)$  and  $b' = \varphi(a')$ . From the defining relation for  $\varphi$  we know that  $\varphi(aa') = \varphi(a)\varphi(a') = bb'$ . It follows that  $\varphi^{-1}(\varphi(aa')) = \varphi^{-1}(bb') = \varphi^{-1}(b)\varphi^{-1}(b')$ , which means that  $B \cong A$ .
- Let  $A, B$ , and  $C$  be groups such that  $A \cong B$  and  $B \cong C$ . Then there exists isomorphisms  $\varphi: A \rightarrow B$  and  $\psi: B \rightarrow C$ . We claim that  $\psi \circ \varphi: A \rightarrow C$  is an isomorphism. Clearly  $\psi \circ \varphi$  is bijective, since  $\varphi^{-1} \circ \psi^{-1}$  is its inverse, as can be seen by considering  $(\varphi^{-1} \circ \psi^{-1})(\psi \circ \varphi)(a) = \varphi^{-1}(\psi^{-1}(\psi(\varphi(a)))) = \varphi^{-1}(\varphi(a)) = a$  for all  $a \in A$ .

It remains to show that  $\psi \circ \varphi$  is a homomorphism. To do so consider  $(\psi \circ \varphi)(aa') = \psi(\varphi(aa')) = \psi(\varphi(a)\varphi(a'))$ , which follows since  $\varphi$  is an isomorphism. Now write  $\varphi(a) = b$  and  $\varphi(a') = b'$ , where  $b, b' \in B$ . We then have  $(\psi \circ \varphi)(aa') = \psi(bb') = \psi(b)\psi(b')$ , which follows since  $\psi$  is an isomorphism. We then have  $(\psi \circ \varphi)(aa') = \psi(b)\psi(b') = \psi(\varphi(b))\psi(\varphi(b')) = (\psi \circ \varphi)(b)(\psi \circ \varphi)(b')$ , and so  $\psi \circ \varphi$  is a bijective homomorphism and hence an isomorphism, meaning  $A \cong C$ .

## A.2 Linear Algebra

### A.2.1 Vectors

**Definition A.2.1 — Vector Space** A vector space,  $V$ , over a field,  $\mathbb{F}$ , is a set of vectors,  $V$ , with two operations,  $\cdot: \mathbb{F} \times V \rightarrow V$ , known as scalar multiplication, and  $+: V \times V \rightarrow V$ , known as vector addition, which are defined such that the following hold for all  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$  and  $k, k' \in \mathbb{F}$ :

1. **Associativity:**  $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ ,
2. There exists a **zero vector**,  $\mathbf{0} \in V$ , such that  $\mathbf{u} + \mathbf{0} = \mathbf{u}$ .
3. There exists  $-\mathbf{u} \in V$  such that  $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$ . We write this as  $\mathbf{u} - \mathbf{u}$  for short.
4. **Commutativity:**  $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ .
5. Distributivity of scalar multiplication over vector addition  $k(\mathbf{u} + \mathbf{v}) = k\mathbf{u} + k\mathbf{v}$ .
6. Distributivity of scalar multiplication over field addition  $(k + k')\mathbf{u} = k\mathbf{u} + k'\mathbf{u}$ .
7. Compatibility of field and scalar multiplication  $(kk')\mathbf{u} = k(k'\mathbf{u})$ .
8.  $1\mathbf{u} = \mathbf{u}$  where 1 is the multiplicative identity of  $\mathbb{F}$ .

Note that the first three axioms make  $(V, +)$  a group and the fourth makes it Abelian.

**Definition A.2.2 — Hilbert Space** A **Hilbert space**,  $\mathcal{H}$ , is a vector space over either  $\mathbb{R}$  or  $\mathbb{C}$ , equipped with an inner product that induces a complete metric. We shall assume a complex Hilbert space, for a real Hilbert space simply ignore any complex conjugates and replace  $\mathbb{C}$  with  $\mathbb{R}$ .

An **inner product** is a function  $\langle -, - \rangle: \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$  such that for all  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{H}$  and  $k, k' \in \mathbb{C}$

1.  $\langle -, - \rangle$  is linear in its second argument, that is

$$\langle \mathbf{u}, k\mathbf{v} + k'\mathbf{w} \rangle = k\langle \mathbf{u}, \mathbf{v} \rangle + k'\langle \mathbf{u}, \mathbf{w} \rangle. \quad (\text{A.2.3})$$

2.  $\langle -, - \rangle$  is conjugate symmetric:

$$\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle^*. \quad (\text{A.2.4})$$

3.  $\langle -, - \rangle$  is positive definite, that is  $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$  with equality only if  $\mathbf{u} = \mathbf{0}$ .



Mathematicians often define an inner product to be linear in its first argument, so

$$\langle k\mathbf{u} + k'\mathbf{v}, \mathbf{w} \rangle = k\langle \mathbf{u}, \mathbf{w} \rangle + k'\langle \mathbf{v}, \mathbf{w} \rangle. \quad (\text{A.2.5})$$

The first two axioms are sometimes combined to give an extra axiom that  $\langle -, - \rangle$  is conjugate linear in its first argument (or second if we follow the other convention). That is

$$\langle ku + k'v, w \rangle = k^* \langle u, w \rangle + k'^* \langle v, w \rangle. \quad (\text{A.2.6})$$

We can then define a **norm** on  $\mathcal{H}$  by  $\|u\| := \sqrt{\langle u, u \rangle}$ .

The final condition for  $\mathcal{H}$  to be a Hilbert space is completeness. Namely that if the series  $\sum_{n=0}^{\infty} u_n$  converges absolutely, so that  $\sum_{n=0}^{\infty} \|u_n\|$  converges to a finite value then the original series,  $\sum_{n=0}^{\infty} u_n$ , converges to some vector in  $\mathcal{H}$ .

■ **Example A.2.7** The set of  $n$ -tuples of complex numbers,  $\mathbb{C}^n$ , is a Hilbert space over  $\mathbb{C}$  with the inner product

$$\langle u, v \rangle = \langle (u_1, \dots, u_n), (v_1, \dots, v_n) \rangle := \sum_{i=1}^n u_i^* v_i = u_i^* v_i \quad (\text{A.2.8})$$

where in the last term we use the Einstein summation convention.

■ **Example A.2.9 — Functions** The space of square integrable functions on  $X \subseteq \mathbb{R}^n$  forms a Hilbert space, denoted  $L^2(X)$ . A function,  $f: X \rightarrow \mathbb{C}$ , is square integrable if<sup>a</sup>

$$\int_X |f(x)|^2 dx \quad (\text{A.2.10})$$

exists and is finite. For example, the function defined by  $f(x) = e^{-x^2}$  is an element of  $L^2(\mathbb{R})$ .

Given  $f, g \in L^2(X)$  we define the inner product in this space to be

$$\langle f, g \rangle := \int_X f^*(x) g(x) dx. \quad (\text{A.2.11})$$

**R** Another subtlety that arises here is that we actually need to consider elements of  $L^2(X)$  to be equivalence classes of functions which are equal almost everywhere (meaning that the measure of the set of points where they are not equal is zero). Otherwise we may have some functions such that  $\langle f, g \rangle = 0$  but  $f \neq g$  since  $f$  and  $g$  disagree on some set of points with a vanishing measure. We say that we are considering the functions mod the equivalence relation of being equal almost everywhere.

This is an important example since we can often identify “square integrable functions” with “possible wave functions”, since square-integrability is a requirement for us to be able to normalise a wave function, which we do so by the procedure

$$\psi \rightarrow \frac{\psi}{\|\psi\|} = \frac{\psi}{\sqrt{\langle \psi, \psi \rangle}} = \left( \int |\psi(x)|^2 dx \right)^{-1/2} \psi. \quad (\text{A.2.12})$$

This only makes sense if  $\int |\psi(x)|^2 dx$  is finite (and nonzero).

<sup>a</sup>for this space to be complete (a requirement for Hilbert spaces) this must be a Lebesgue integral but in physics functions are usually nice enough that we can use the standard Riemann integral, which agrees with the Lebesgue integral when both exists.

**Notation A.2.13 — Bra-Ket Notation** In physics, particularly in quantum mechanics, we often use **bra-ket notation**, developed by Dirac. We identify vectors,  $\mathbf{u}$ , with **kets**,  $|u\rangle$ , and dual vectors,  $\mathbf{v}$ , with **bras**,  $\langle v|$ . The inner product  $\langle \mathbf{u}, \mathbf{v} \rangle$  is then written  $\langle v|u \rangle$ . This is the notation we will use for most of this course.

**Definition A.2.14 — Linear Operator** Given two vector spaces,  $V$  and  $W$ , over some field,  $\mathbb{F}$ , a function,  $f: V \rightarrow W$ , is said to be a linear operator if for  $\mathbf{u}, \mathbf{v} \in V$  and  $k \in \mathbb{F}$  we have

$$f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}), \quad \text{and} \quad f(k\mathbf{u}) = kf(\mathbf{u}). \quad (\text{A.2.15})$$

Instead of the function notation  $f(\mathbf{u})$  we typically use a multiplicative notation,  $A\mathbf{u}$ , which is due to the fact that if  $V$  is finite dimensional then we can choose a basis and represent a linear map by a matrix. Using bra-ket notation also we have

$$A(|u\rangle + |v\rangle) = A|u\rangle + A|v\rangle, \quad \text{and} \quad A(k|u\rangle) = kA|u\rangle. \quad (\text{A.2.16})$$

An operator is **antilinear** if

$$A(|u\rangle + |v\rangle) = A|u\rangle + A|v\rangle, \quad \text{and} \quad A(k|u\rangle) = k^*A|u\rangle. \quad (\text{A.2.17})$$

An example of such an operator is the time reversal operator,  $T$ , which takes  $t \rightarrow -t$ .

For simplicity from now on we will consider the complex vector space  $V = \mathbb{C}^N$ . This is  $N$ -dimensional ( $\dim V = N$ ), which we take to be finite, although many of these ideas work, possibly with slight modification, for infinite dimensional vector spaces. Most of the time we will also consider linear operators from  $V$  to  $V$ , since this is far more common in practice that linear operators from  $V$  to some different vector space,  $W$ .

**Definition A.2.18 — Basis** Given a vector space,  $V$ , we say that  $\{|e_i\rangle\}$  is a **linearly independent** set if the only solution to

$$\lambda_i |e_i\rangle = |0\rangle, \quad (\text{A.2.19})$$

where  $|0\rangle$  is the zero vector, is  $\lambda_i = 0$  for all  $i$ .

We say that  $\{|e_i\rangle\}$  is a **basis** for  $V$  if  $\{|e_i\rangle\}$  is a linearly independent set and spans  $V$ . That is given some  $|u\rangle \in V$  we can write

$$|u\rangle = u_i |e_i\rangle \quad (\text{A.2.20})$$

for some  $u_i \in \mathbb{C}$ .

The number of vectors in a basis is the **dimension** of the vector space, denoted  $\dim V$ .

We say that two vectors,  $|u\rangle, |v\rangle \in V$ , are **orthogonal** (with respect to some inner product) if  $\langle u|v\rangle = 0$ .

We say that a vector,  $|u\rangle \in V$ , is normalised if  $\|u\| = \sqrt{\langle u|u\rangle} = 1$ .

We say that  $\{|e_i\rangle\}$  is an orthonormal basis for  $V$  if it is a basis for  $V$ ,  $|e_i\rangle$  is normalised for all  $i$  and all of the basis vectors are mutually orthogonal. These last two conditions are summarised by requiring that

$$\langle e_i|e_j\rangle = \delta_{ij}. \quad (\text{A.2.21})$$

**Definition A.2.22 — Completeness Relation** Given a vector space,  $V$ , and an orthonormal basis,  $\{|e_i\rangle\}$ , we can write the identity operator,  $\mathbf{1}$ , as

$$\mathbf{1} = \sum_{i=1}^N |e_i\rangle\langle e_i|. \quad (\text{A.2.23})$$

Recall that the identity operator is defined such that

$$\mathbf{1}|u\rangle = |u\rangle \quad (\text{A.2.24})$$

for all  $|u\rangle \in V$ .

**Definition A.2.25 — Partition of the Identity** A **projection operator**,  $P_i$ , is an operator satisfying

$$P_i P_j = \delta_{ij} P_i, \quad \text{and} \quad P_i^\dagger = P_i. \quad (\text{A.2.26})$$

A **partition of the identity** is a collection of projection operators,  $\{P_j\}$ , such that

$$\mathbf{1} = \sum_{j=1}^{N_P} P_j \quad (\text{A.2.27})$$

where  $N_P = |\{P_j\}|$  is the number of projection operators in the partition. We can write each partition operator as

$$P_j = \sum_{i=1}^{N_j} |e_i\rangle\langle e_i| \quad (\text{A.2.28})$$

where  $N_j$  are such that

$$\dim V = N = \sum_{j=1}^{N_P} N_j. \quad (\text{A.2.29})$$

**Definition A.2.30 — Matrix Element** Given a linear operator,  $A: V \rightarrow V$ , and an orthonormal basis,  $\{|e_i\rangle\}$ , we define the **matrix elements** to be

$$A_{ij} := \langle e_i | A e_j \rangle = \langle e_i | A | e_j \rangle \quad (\text{A.2.31})$$

where  $A$  is understood to act on the right and  $|Ae_j\rangle := A|e_j\rangle$ .

If we know the matrix elements of  $A$  we can reconstruct  $A$  using

$$A = \sum_{i=1}^N \sum_{j=1}^N A_{ij} |e_i\rangle \langle e_j|. \quad (\text{A.2.32})$$

**Definition A.2.33 — Eigenvalues and Eigenvectors** Given a linear operator  $A$ , we call  $|v_i\rangle$  an **eigenvector** and  $\lambda_i \in \mathbb{C}$  an **eigenvalue** if

$$A|v_i\rangle = \lambda_i |v_i\rangle. \quad (\text{A.2.34})$$

There are  $N$  solutions to this, which follows from the **characteristic polynomial**,  $\det(A - \lambda \mathbf{1}) = 0$ , having  $N$  solutions, which in turn follows from the fundamental theorem of algebra.

## A.2.2 Matrices

**Definition A.2.35 — Transpose and Hermitian Conjugate** Given a matrix,  $A$ , with matrix elements  $A_{ij}$ , the **transpose** matrix,  $A^\top$ , has matrix elements  $A_{ij}^\top = A_{ji}$ .

A matrix is **symmetric** if  $A^\top = A$ , or **antisymmetric** if  $A^\top = -A$ .

Given a matrix,  $A$ , with matrix elements  $A_{ij}$ , the **Hermitian conjugate**,  $A^\dagger$ , has matrix elements  $A_{ij}^\dagger = A_{ji}^*$ . Here  $*$  denotes the **complex conjugate**, so  $(x + iy)^* = x - iy$  and  $(re^{i\vartheta})^* = re^{-i\vartheta}$  for  $x, y, r, \vartheta \in \mathbb{R}$ . That is the Hermitian conjugate is the complex conjugate of the transpose.

A matrix is **Hermitian** if  $A^\dagger = A$ , or **anti-Hermitian** if  $A^\dagger = -A$ .

**Lemma A.2.36** The eigenvalues of a Hermitian matrix are real.

*Proof.* Let  $A$  be a Hermitian matrix and  $\mathbf{v}$  an eigenvector with nonzero eigenvalue  $\lambda$ . Note that this means  $\mathbf{v}$  is nonzero. If 0 is an eigenvalue of  $A$  then this is real so we need not consider this case further. By definition  $A\mathbf{v} = \lambda\mathbf{v}$ . Taking the Hermitian conjugate of both sides we get  $\mathbf{v}^\dagger A^\dagger = \lambda^* \mathbf{v}^\dagger$ , where we have used  $(XY)^\dagger = Y^\dagger X^\dagger$ . Multiplying both sides on the right by  $\mathbf{v}$  we get  $\mathbf{v}^\dagger A\mathbf{v} = \lambda^* \mathbf{v}^\dagger \mathbf{v}$ . Identifying  $A\mathbf{v} = \lambda\mathbf{v}$  on the left hand side this becomes  $\mathbf{v}^\dagger \lambda\mathbf{v} = \lambda \mathbf{v}^\dagger \mathbf{v} = \lambda^* \mathbf{v}^\dagger \mathbf{v}$ . It follows that we must have  $\lambda = \lambda^*$ , which means we must have  $\lambda \in \mathbb{R}$ .  $\square$

We can choose the eigenvalues of a Hermitian matrix to be orthonormal, and hence they form a basis for the vector space. In this basis the matrix will be diagonal and the values on the diagonal are simply the eigenvalues.



Given a Hermitian matrix,  $A$ , with eigenvalues  $\lambda_i$  and corresponding eigenvectors  $|v_i\rangle$  we can write this matrix as

$$A = \sum_{i=1}^N \lambda_i |v_i\rangle\langle v_i|. \quad (\text{A.2.37})$$

This is diagonalised by the transformation  $V^\dagger AV$  where

$$V = \sum_{i=1}^N |v_i\rangle\langle e_i| \quad (\text{A.2.38})$$

where  $|e_i\rangle$  are the basis vectors in the original basis. It is easy to see that this transform gives the desired result:

$$V^\dagger AV = \underbrace{|e_i\rangle\langle v_i|}_{=V^\dagger} \underbrace{(\lambda_j |v_j\rangle\langle v_j|)}_{=A} \underbrace{|v_k\rangle\langle e_k|}_{=V} \quad (\text{A.2.39})$$

$$= \lambda_j |e_i\rangle\langle v_i|v_j\rangle\langle v_j|v_k\rangle\langle e_k| \quad (\text{A.2.40})$$

$$= \lambda_j \delta_{ij} \delta_{jk} |e_i\rangle\langle e_k| \quad (\text{A.2.41})$$

$$= \lambda_i |e_i\rangle\langle e_i| \quad (\text{A.2.42})$$

This last term is just a diagonal matrix with the eigenvalues,  $\lambda_i$ , as the diagonal elements, which is exactly what we wanted.

For non-Hermitian matrices it is possible that the eigenvalues aren't linearly independent. In this case the best we can do is Jordan normal form where the eigenvalues are on the diagonal and all other entries are either zero or one for elements in the subspace of degenerate eigenvalues.

**Definition A.2.43 — Inverse** The **inverse** of a matrix,  $A$ , is the matrix  $A^{-1}$  such that  $A^{-1}A = AA^{-1} = \mathbf{1}$ . Such a matrix exists only if the determinant is non-zero.

An equivalent requirement for  $A^{-1}$  to exist is for  $A$  to have no zero eigenvalues. For a Hermitian matrix the inverse in the eigenbasis is simply  $A^{-1} = \text{diag}(1/\lambda_1, \dots, 1/\lambda_N)$ .

**Definition A.2.44 — Orthogonal and Unitary** A matrix,  $O$ , is **orthogonal** if  $O^\top O = \mathbf{1}$ , that is  $O^\top = O^{-1}$ . A matrix,  $U$ , is **unitary** if  $U^\dagger U = \mathbf{1}$ , that is  $U^\dagger = U^{-1}$ .

The following holds:

$$\langle u|Av\rangle = \langle u|A|v\rangle = \langle A^\dagger u|v\rangle. \quad (\text{A.2.45})$$

For a unitary matrix,  $U$ , this implies

$$\langle Uu|Uv\rangle = \langle u|U^\dagger U|v\rangle = \langle u|\mathbf{1}|v\rangle = \langle u|v\rangle. \quad (\text{A.2.46})$$

We say that unitary transforms preserve the inner product, or that the inner product is invariant under unitary transforms.

**Definition A.2.47 — Trace** The **trace** of a matrix,  $A$  is

$$\text{tr } A := \sum_i \langle e_i | A | e_i \rangle = A_{ii} \quad (\text{A.2.48})$$

where in the last term we are using the Einstein summation convention to sum over  $i$ .

The trace of a matrix is simply the sum of its eigenvalues, this doesn't just hold for Hermitian matrices.

The trace is cyclic, meaning  $\text{tr}(AB) = \text{tr}(BA)$ ,  $\text{tr}(ABC) = \text{tr}(BCA) = \text{tr}(CAB)$ , etc.

The trace is linear, meaning  $\text{tr}(kA) = k \text{tr}(A)$  for scalar  $k$ .

$\langle A, B \rangle := \text{tr}(A^\dagger B)$  is an inner product on the vector space of matrices. This is called the **Gram-Schmidt inner product**.

**Definition A.2.49 — Determinant** The **determinant** of a matrix,  $A$ , is

$$\det A = |A| := \varepsilon_{i_1 \dots i_N} A_{1i_1} \cdots A_{Ni_N} \quad (\text{A.2.50})$$

with summation over indices implied.

The determinant of a matrix is the product of its eigenvalues.

The determinant of a product is the product of the determinants:

$$\det(AB) = \det(A) \det(B) = \det(B) \det(A) = \det(BA). \quad (\text{A.2.51})$$

**Definition A.2.52 — Diagonal** A matrix,  $A$ , is **diagonal** if  $A_{ij} = 0$  for  $i \neq j$ .

A matrix,  $A$ , is **block diagonal** if it can be written in the form

$$A = \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & A_n \end{pmatrix} \quad (\text{A.2.53})$$

where  $A_i$  are square matrices and the 0s represent matrices where all elements are zero.

### A.2.3 Combining Vector Spaces

**Definition A.2.54 — Direct Sum** Given vector spaces  $V$  and  $W$  we call  $V \oplus W$  the **direct sum**. It is defined by associating with each pair of vectors,  $|v_i\rangle \in V$  and  $|w_a\rangle \in W$ , a vector  $|v_i\rangle \oplus |w_a\rangle = |v_i \oplus w_a\rangle \in V \oplus W$  and extending the inner product to

$$\langle v_i \oplus w_a | v_j \oplus w_b \rangle_{V \oplus W} := \langle v_i | v_j \rangle_V + \langle w_a | w_b \rangle_W \quad (\text{A.2.55})$$

where the subscripts denote which vector space the inner product is in. Note that the notation  $|v \oplus w\rangle$  is non-standard.

The dimension of  $V \oplus W$  is

$$\dim(V \oplus W) = \dim V + \dim W. \quad (\text{A.2.56})$$

Given  $A \in \text{GL}(V)$  and  $B \in \text{GL}(W)$  the direct sum,  $A \oplus B$ , acts on  $|v\rangle \oplus |w\rangle \in V \oplus W$  as

$$(A \oplus B)(|v\rangle \oplus |w\rangle) := (A|v\rangle) \oplus (B|w\rangle). \quad (\text{A.2.57})$$

This shows we can think of  $V \oplus W$  as a  $(\dim V + \dim W)$ -dimensional vector space with operators represented by  $(v+w) \times (v+w)$  block diagonal matrices:

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}. \quad (\text{A.2.58})$$

We then think of  $|v\rangle \oplus |w\rangle \in V \oplus W$  as  $(v_1, \dots, v_{\dim V}, w_1, \dots, w_{\dim W})$ .

An important question is can a given vector space be written as a direct sum of vector spaces, this occurs when considering the irreducibility of representations.

**Definition A.2.59 — Direct Product** Given vector spaces  $V$  and  $W$  we call  $V \otimes W$  the **direct product**. It is defined by associating with each pair of vectors,  $|v_i\rangle \in V$  and  $|w_a\rangle \in W$ , a vector  $|v_i\rangle \otimes |w_a\rangle = |v_i w_a\rangle \in V \otimes W$  and extending the inner product to

$$\langle v_i \otimes w_a | v_j \otimes w_b \rangle_{V \otimes W} := \langle v_i | v_j \rangle_V \langle w_a | w_b \rangle \quad (\text{A.2.60})$$

where the subscripts denote which vector space the inner product is in. Note that the notation  $|v \otimes w\rangle$  is non-standard.

The dimension of  $V \otimes W$  is

$$\dim(V \otimes W) = \dim(V) \dim(W). \quad (\text{A.2.61})$$

Given  $A \in \text{GL}(V)$  and  $B \in \text{GL}(W)$  the direct product,  $A \otimes B$ , acts on  $|v\rangle \otimes |w\rangle \in V \otimes W$  as

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = (A|v\rangle) \otimes (B|w\rangle). \quad (\text{A.2.62})$$

■ **Application A.2.63** In quantum mechanics we can combine states from different Hilbert spaces representing different properties with direct products. For example, given an electron wave function with a spatial component and a spin component the direct product of these gives the state of the electron.

The direct product plays a role in representation theory in terms of what we will call Kronecker products. These can be used to obtain all representations from the fundamental representations.

# B

## Groups

### B.1 Finite Groups

**Definition B.1.1** The **trivial group** is the group containing only the identity,  $\{e\}$ . It is the only group of order 1.

- Order 1.
- Rank 1.
- Cyclic.
- Abelian.

The trivial group is isomorphic to  $\mathbb{Z}_1$ ,  $S_1$ , and  $\text{SO}(1)$ .

**Definition B.1.2**  $\mathbb{Z}_2$  is the cyclic group of order 2, see [Definition B.1.9](#). It is the only group of order 2.

- Order 2.
- Rank 1.
- Cyclic.
- Abelian.

$\mathbb{Z}_2$  is isomorphic to  $S_2$ .

**Definition B.1.3**  $\mathbb{Z}_3$  is the cyclic group of order 3, see [Definition B.1.9](#). It is the only group of order 3.

- Order 3.
- Rank 1.
- Cyclic.
- Abelian.

**Definition B.1.4**  $\mathbb{Z}_4$  is the cyclic group of order 4, see [Definition B.1.9](#). It is one of two groups of order 4.

- Order 4.
- Rank 1.
- Cyclic.
- Abelian.

**Definition B.1.5**  $\mathbb{Z}_2 \times \mathbb{Z}_2$  is the **Klein Vierergruppe**. It is one of two groups of order 4. It is a direct product of two copies of  $\mathbb{Z}_2$ .

- Order 4.
- Rank 2.
- Abelian.

**Definition B.1.6**  $S_3$  is the permutation group on 3 elements, see [Definition B.1.11](#).

- Order 6.
- Rank 2.
- Non-Abelian.

**Definition B.1.7** The **quaternion group**,  $Q$ , has the group presentation

$$Q = \langle -e, i, j, k \mid (-e)^2 = e, i^2 = j^2 = k^2 = ijk = e \rangle. \quad (\text{B.1.8})$$

- Order 8.
- Rank 2.
- Non-Abelian.

The Pauli matrices provide a two-dimensional complex representation by the correspondence  $(-e, i, j, k) \rightarrow (-1, \sigma_1, \sigma_2, \sigma_3)$ .

### B.1.1 Other Finite Groups

**Definition B.1.9** The **cyclic group** of order  $n$ , denoted  $\mathbb{Z}_n$ , is given by the presentation

$$\mathbb{Z}_n = \langle a \mid a^n = e \rangle. \quad (\text{B.1.10})$$

Identifying  $a = e^{2i\pi/n}$  and the operation as multiplication we get a group formed from the  $n$ th roots of unity. Identifying  $a = 1$  and the operation as addition modulo  $n$  we get a group formed from  $\{0, \dots, n-1\}$ .

- Order  $n$ .
- Rank 1.
- Cyclic.
- Abelian.

All finite cyclic groups are isomorphic to  $\mathbb{Z}_n$  for some  $n$ .

**Definition B.1.11** The **permutation group** on  $n$  objects is the group of all permutations (bijections) of  $\{1, \dots, n\}$ , with function composition as the group operation.

- Order  $n!$ .
- Rank 2.
- Non-Abelian ( $n > 2$ ).

$S_1$  and  $S_0$  are isomorphic to the trivial group.  
 $S_2$  is isomorphic to  $\mathbb{Z}_2$ .

## B.2 Discrete Groups

**Definition B.2.1** The integers,  $\mathbb{Z}$ , under addition.

- Rank 1.
- Abelian.
- Cyclic.

**Definition B.2.2** The rational numbers,  $\mathbb{Q}$ , under addition.

- Abelian.

**Definition B.2.3** The nonzero rational numbers,  $\mathbb{Q}^*$ , under multiplication.

- Abelian.

## B.3 Continuous Groups

### B.3.1 Scalars

**Definition B.3.1** The real numbers,  $\mathbb{R}$ , under addition.

- Abelian.

$(\mathbb{R}, +)$  is isomorphic to  $(\mathbb{R}_{>0}, \cdot)$ .

**Definition B.3.2** The nonzero real numbers,  $\mathbb{R}^*$ , under multiplication.

- Abelian.

**Definition B.3.3** The complex numbers,  $\mathbb{C}$ , under addition.

- Abelian.

**Definition B.3.4** The nonzero complex numbers,  $\mathbb{C}^*$ , under multiplication.

- Abelian.

### B.3.2 Matrices

**Definition B.3.5** The **general linear group**

$$\mathrm{GL}(n, \mathbb{F}) = \{M \in \mathcal{M}_n(\mathbb{F}) \mid \det M \neq 0\}. \quad (\text{B.3.6})$$

If  $V$  is a vector space of dimension  $n$  over  $\mathbb{F}$  then this group is also denoted  $\mathrm{GL}(V)$ . If  $\mathbb{F}$  is obvious from context then this group is denoted  $\mathrm{GL}(n)$ .

- Non-Abelian ( $n > 1$ ).

**Definition B.3.7** The **special linear group**

$$\mathrm{SL}(n, \mathbb{F}) = \{M \in \mathcal{M}_n(\mathbb{F}) \mid \det M = 1\}. \quad (\text{B.3.8})$$

If  $V$  is a vector space of dimension  $n$  over  $\mathbb{F}$  then this group is also denoted  $\mathrm{SL}(V)$ . If  $\mathbb{F}$  is obvious from context then this group is denoted  $\mathrm{SL}(n)$ .

- Non-Abelian ( $n > 1$ ).

$\mathrm{SL}(n, \mathbb{F})$  is a subgroup of  $\mathrm{GL}(n, \mathbb{F})$ .

**Definition B.3.9** The **orthogonal group**

$$\mathrm{O}(n) = \{O \in \mathcal{M}_n(\mathbb{R}) \mid O^\top O = OO^\top = \mathbf{1}\}. \quad (\text{B.3.10})$$

- Non-Abelian ( $n > 1$ ).

$\mathrm{O}(n)$  is a subgroup of  $\mathrm{GL}(n, \mathbb{R})$ .

$\mathrm{O}(n)$  is the group of distance preserving transformations of Euclidean space which leave the origin invariant.

$\mathrm{O}(n)$  is the group of rotations and inversions of  $\mathbb{R}^n$ .

**Definition B.3.11** The **special orthogonal group**

$$\mathrm{SO}(n) = \{O \in \mathcal{M}_n(\mathbb{R}) \mid O^\top O = OO^\top = \mathbf{1} \text{ and } \det O = 1\}. \quad (\text{B.3.12})$$

- Non-Abelian ( $n > 1$ ).

$\mathrm{SO}(n)$  is a subgroup of  $\mathrm{O}(n)$  and  $\mathrm{SL}(n, \mathbb{R})$ .

$\mathrm{SO}(n)$  is the group of rotations of  $\mathbb{R}^n$ .

$\mathrm{SO}(2)$  is isomorphic to  $\mathrm{U}(1)$  and the circle group,  $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$  under multiplication.

**Definition B.3.13** The **unitary group**

$$\mathrm{U}(n) = \{U \in \mathcal{M}_n(\mathbb{C}) \mid U^\dagger U = UU^\dagger = \mathbf{1}\}. \quad (\text{B.3.14})$$

- Non-Abelian ( $n > 1$ ).

$U(n)$  is a subgroup of  $GL(n, \mathbb{C})$ .

$U(n)$  is the group which preserves the standard inner product on  $\mathbb{C}^n$ .

$U(1)$  is isomorphic to  $SO(2)$  and the circle group,  $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$  under multiplication.

**Definition B.3.15** The **special unitary group**

$$SU(n) = \{U \in \mathcal{M}_n(\mathbb{C}) \mid U^\dagger U = UU^\dagger = \mathbf{1} \text{ and } \det U = 1\}. \quad (\text{B.3.16})$$

- Non-Abelian ( $n > 1$ ).

$SU(n)$  is a subgroup of  $U(n)$  and  $SL(n, \mathbb{C})$ .

**Definition B.3.17** The **isometries of Euclidean space**

$$ISO(n) = O(n) \ltimes \mathbb{R}^n \quad (\text{B.3.18})$$

where  $(R, \mathbf{a})(R', \mathbf{a}') := (RR', \mathbf{a} + R\mathbf{a}')$ .

- Non-Abelian

$ISO(n)$  is the group of distance preserving transformations of Euclidean space.

$ISO(n)$  is the group of rotations, reflections, and translations of  $\mathbb{R}^n$ .

$ISO(n)$  has both  $O$  and  $\mathbb{R}^n$  as normal subgroups.

**Definition B.3.19** The **Lorentz group**,  $O(1, 3)$ , is the group of all Lorentz transformations of Minkowski space.

- Non-Abelian.

$O(1, 3)$  is the group that preserves the quadratic form  $(t, x, y, z) \mapsto t^2 - x^2 - y^2 - z^2$ .

$SO^+(1, 3)$  is the subgroup of  $O(1, 3)$  which preserves the orientation of space (S for special, that is unit determinant) and direction of time (that's what the + represents).

**Definition B.3.20** The **Poincaré group** is the group of all isometries of Minkowski space, sometimes denoted  $ISO(1, 3)$ . That is it is the group of all Lorentz transformations and translations.

- Non-Abelian.

The Poincaré group can be identified as the semidirect product  $ISO(1, 3) =$



$\mathbb{R}^{1,3} \rtimes O(1, 3)$  where  $\mathbb{R}^{1,3}$  is the group of spacetime translations of Minkowski space and  $O(1, 3)$  is the Lorentz group.

---

# Index

---

## Symbols

$-^*$ , complex conjugate, 43  
 $-^*$ , nonzero elements, 6  
 $-\dagger$ , Hermitian conjugate, 43  
 $-\top$ , transpose, 43  
 $-^{-1}$ , inverse, 44  
 $|-|$ , determinant, 45  
 $\langle -|- \rangle$ , inner product, 41  
 $\langle -|$ , bra, 41  
 $\otimes$ , direct product, 46  
 $\oplus$ , direct sum, 45  
 $1$ , identity matrix, 42  
 $\langle -, - \rangle$ , inner product, 39  
 $| - \rangle$ , ket, 41  
 $\| - \|$ , norm, 40

## A

Abelian, 7  
accociative, 39  
anti-Hermitian, 43  
antilinear, 41  
antisymmetric, 43  
associative, 1

## B

basis, 41  
bijective, 36  
binary  
    operation, 1  
    relation, 37  
block diagonal, 45  
bra, 41  
bra-ket notation, 41

## C

Cayley table, 9  
Cayley's Theorem, 11  
centraliser, 23

centre, 8  
characteristic  
    polynomial, 43  
closed, 1  
commutative, 39  
complex conjugate, 43  
conjugate, 7  
continuous, 6  
coset, 18  
cycle, 10  
cyclic, 8  
cyclic group, 6, 48

## D

decomposition, *see* partition  
det, determinant, 45  
determinant, 45  
diagonal, 45  
dim, dimension, 42  
dimension, 42  
direct product, 32, 46  
direct sum, 45  
discrete, 6

## E

eigenvalue, 43  
eigenvector, 43  
empty set, 37  
equivalence class, 38

## F

factor group, *see* quotient group  
finite, 6  
first isomorphism theorem, 30  
function composition, 2

## G

general linear group, 27, 50

generate, 8  
 generators, 8  
 $GL(n, \mathbb{F})$ , general linear group, 50  
 Gram–Schmidt inner product, 45  
 group, 4  
 group action, 20  
 group axioms, 4  
 group presentation, 17

## H

$\mathbb{H}$ , quaternions, 18  
 Hermitian, 43  
 Hermitian conjugate, 43  
 Hilbert space, 39  
 homomorphism, 13

## I

identity, 3  
 image, 37  
 index, 19  
 injective, 36  
 inner product, 39  
 invariant subgroup, *see* normal subgroup  
 inverse, 4, 44  
 $ISO(1, 3)$ , Poincaré group, 51  
 isomorphic, 13  
 isomorphism, 13

## K

kernel, 36  
 ket, 41  
 Klein *Viergruppe*, 15, 33, 48  
 Kronecker delta, 37

## L

Levi-Civita Symbol, 37  
 linearly independent, 41  
 Lorentz group, 51

## M

matrix element, 43  
 multiplication table, *see* Cayley table

## N

natural projection, 31  
 norm, 40  
 normal subgroup, 26  
 $n\mathbb{Z}$ , integer multiples of  $n$ , 14

## O

$O(1, 3)$ , Lorentz group, 51  
 $O(3)$ , rotation group, 6  
 $O(n)$ , orthogonal group, 50  
 orbit, 22  
 order  
   element, 7  
   group, 7  
 orthogonal  
   matrix, 44  
   vectors, 42  
 orthogonal group, 50

## P

partition, 18  
 partition of the identity, 42  
 permutation, 6  
 permutation group, 6, 48  
 Poincaré group, 51  
 projection operator, 42

## Q

$Q$ , quaternion group, 48  
 quaternion group, 18, 48  
 quotient group, 28

## R

rank, 8  
 reflexive, 37  
 relation, 37  
 rotation group, 6

## S

simple group, 30  
 $SL(n, \mathbb{F})$ , special linear group, 50  
 $S_n$ , permutation group, 6  
 $SO(n)$ , special orthogonal group, 50  
 special linear group, 27, 50  
 special orthogonal group, 50  
 special unitary group, 51  
 stabiliser, 22  
 $SU(n)$ , special unitary group, 51  
 subgroup, 7  
   proper, 7  
 surjective, 36  
 symmetric, 43  
   relation, 37

## T

tr, trace, 45  
 trace, 45  
 transitive, 37

transpose, [43](#)

trivial group, [7](#), [47](#)

## U

$U(n)$ , unitary group, [21](#), [50](#)

unitary, [44](#)

unitary group, [21](#), [50](#)

## Z

$Z(G)$ , centre, [8](#)

$\mathbb{Z}_2 \times \mathbb{Z}_2$ , Klein *Vierergruppe*, [15](#)

$\mathbb{Z}_n$ , cyclic group, [6](#)