Intro to Groups

Simi Hellsten

November 7, 2020

Introduction

Groups are, in a sense, the cornerstone of higher algebra. They're not the simplest of structures, nor the most intuitive, but I feel strike the best balance between simplicity and utility. They are also generally introduced first in maths courses, and as such lots of other structures, such as vector spaces and rings, are defined in terms of groups.
This approach is inspired by both the first part of the Prelims course at Oxford called "Groups and Group Actions" taught by the wonderful Vicky Neale, and Napkin by Evan Chen, a comprehensive overview of much of higher mathematics whose intuitive approach I greatly enjoyed. However, I hope to have struck a balance between the rigour and detail of the former with the breadth of the latter.

§0.1 Pre-requisites

I will also assume knowledge of the following notation.

(i) A **map** is just another name for a function: it is a way of taking points in a domain to points somewhere else.

(ii) A **subset** of a set exactly what you think. For example $\{1,3\}$, $\{1\}$ and $\{1,2,3\}$ are subsets of $\{1,2,3\}$. A **proper subset** is a subset that is not the original set. The first two were proper subsets, the third was not. We therefore write $\{1,3\} \subsetneq \{1,2,3\}$ and $\{1,2,3\} \subseteq \{1,2,3\}$, similar to $<$ and $\leq$.

(iii) $\mathbb{Z}$ for integers, $\mathbb{N}$ for strictly positive integers, $\mathbb{Q}$ for the rational numbers, or fractions, $\mathbb{R}$ for the real numbers, $\mathbb{C}$ for the complex numbers, and the 'in' symbol $\in$ to represent set membership. $n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$ is the set of multiples of n. Thus, $1.5 \in \mathbb{R}$, and $1.5 \in \mathbb{Q}$, but $1.5 \notin \mathbb{Z}$. $3 \in \mathbb{Z}$ but $3 \notin 2\mathbb{Z}$. The **Cartesian product** of two sets is much less scary than it sounds: it's a just the set of pairs. For example, $\mathbb{Z} \times \mathbb{C}$ is just the set $\{(z,c) \,|\, z \in \mathbb{Z}, c \in \mathbb{C}\}$. Think of this most naturally as $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the xy-plane. We could say that $\left(\theta, e^{i\theta}\right) \in (\mathbb{R}, \mathbb{C})$.

(iv) Towards the end, I will write sums in the following form:

$$\sum_{n \in S} f(n),$$

for example. This means "sum over all n in the set S". So

$$\sum_{n=1}^{4} f(n) = \sum_{n \in \{1,2,3,4\}} f(n)$$

and

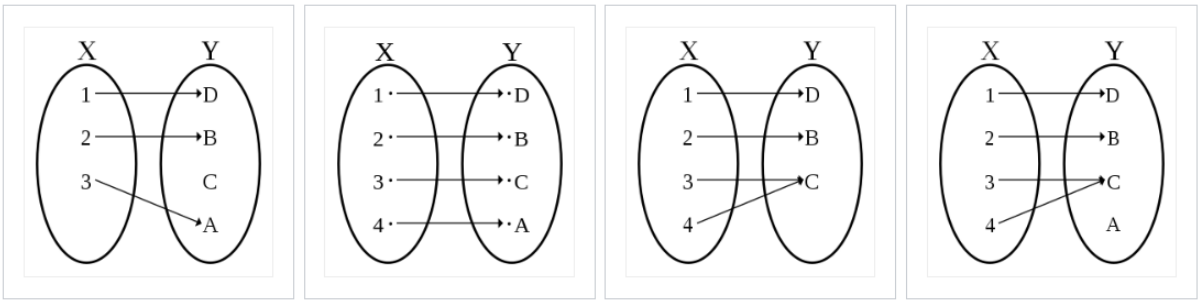
$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n=-\infty}^{\infty} f(n).$$

§0.1.i A pre-note on functions

This is a quick note on the notation and vocabulary I will use for functions. It's not immediately relevant, but I want to leave it here so it doesn't break up later chapters.
I will use the notation $f : X \to Y$ to represent functions. Here, f takes values in X, its **domain**, and $f(x) \in Y$, which we call the **codomain**. This is slightly different to the concept of a range you learn in school. For example, we can say that $f : \mathbb{R} \to \mathbb{R}$ by $x \mapsto x^2$, even though the range of f is not $\mathbb{R}$, it's $\mathbb{R}^{\geq 0} = \{x \in \mathbb{R} \,|\, x \geq 0\}$. However, it is not right to say that $\sqrt{-} : \mathbb{R} \to \mathbb{R}$, as $\sqrt{x}$ is not defined for negative x, so the domain is wrong. If a function takes two inputs, say from sets A and B, we write $f : A \times B \to Y$; that is, we think of the input being a pair, rather than two distinct inputs.

Definition 0.1.1. We call a function **surjective** if every element in the codomain gets mapped to: that is, the range is equal to the codomain. More formally, $f : X \to Y$ is surjective if, for every $y \in Y$, there is an $x \in X$ such that $f(x) = y$. This is sometimes called being **'onto'**.
We call a function **injective** if $f(a) = f(b)$ implies that $a = b$. This is sometimes called being **'1-to-1'**.
A function $f : X \to Y$ is **bijective** if it is both injective and surjective. That is, every element in Y gets mapped to by exactly one element in X. This is then the necessary condition for a function to have an inverse function.
Clearly, and very importantly, if there is a bijection between two finite sets, they have the same number of elements.

For example, $\tan : \mathbb{R} \to \mathbb{R}$ is surjective, but not injective, while $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ is bijective. $(-)^2 : \mathbb{N} \to \mathbb{N}$ is injective, but not surjective. However, $(-)^2 : \mathbb{Z} \to \mathbb{Z}$ is neither injective nor surjective. $(-)^3 : \mathbb{R} \to \mathbb{R}$ is bijective. $\mathbb{Z} \to \mathbb{Z}$ by $x \mapsto x + 1$ is bijective.



An injective non-surjective function (injection, not a **bijection**) | An injective surjective function (**bijection**) | A non-injective surjective function (surjection, not a **bijection**) | A non-injective non-surjective function (also not a **bijection**)

Remark 0.1.2 (Application) — Injectivity and surjectivity aren't only useful for pure maths, but also important in physics. Consider a function $f : S \to S$, where S is the set of possible states of some system, showing how a system changes from one state to another. If f is injective, so $f(a) = f(b) \Rightarrow a = b$, then given any final state, we can determine the previous one. This obviously allows us to go back arbitrarily far through time. Suppose S is *not* surjective. Then there are certain states that the system can never reach after it's initial condition.

§0.2 An overview

In replacement for a content page, I will offer the following chapter summaries. Chapter 1 will, after defining a group begin with a very long discussion of examples, and will prove some very basic propositions. There will then be a discussion of Cayley tables as a way to visualise groups, see which groups are 'the same', and find all of the small groups.
Chapter 2 will formalise this notion of 'the same', with a deeper exploration into symmetric groups, the first groups that were truly studied.
Chapter 3 will discuss subgroups and cyclic groups, showing how 'cyclic with extra conditions' describes almost all groups.
Chapter 4 will introduce the strange concept of a coset, before proving Lagrange's theorem, the most famous result in group theory. From there, I will prove many corollaries, including famous theorems like Fermat's little theorem. This is the end of the 'true' introduction, and if you wish to stop here you can. The two remaining chapters will be more technical.
Nevertheless, I highly recommend reading Chapter 5, which introduces homomorphisms as a special type of function, before defining quotient groups. I believe that this chapter captures the essence of group theory the best.
Chapter 6 will be the final chapter, discussing applications of group theory to other problems via group actions. In particular, we will prove the lemma that is not Burnside's, and perhaps find another proof for Fermat's little.
There will be various questions (easier) and exercises (harder) scattered throughout each chapter. These should help with understanding, so please do attempt them, especially if there is a proof that

I have left as an exercise. There may be sketches of solutions given. There will also be a block of exercises at the end of each chapter. These vary more in difficulty, but all (apart from maybe the last per chapter) should be doable.

1 Groups: The Basics

Finally, we may begin our discussion of groups.

§1.1 Intuitions and definitions

Here are three examples of groups that you (hopefully) feel relatively familiar with. First though, a group consists of a set and a **binary operation**: an operation like $+$ or $\times$ that takes two elements of the same set and returns only one, again from that set. For example, $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, or $\div : \mathbb{R}^\times \times \mathbb{R}^\times \to \mathbb{R}^\times$, where $\mathbb{R}^\times$ are the non-zero reals. However, the 3D vector dot product is not a binary operation, as $\cdot : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$, so the domains and codomain are different.

Example 1.1.1 (Some well-known examples)

(a) The integers $\mathbb{Z}$ form an infinite group under addition, but not under multiplication. Note that every number n corresponds to a negative $-n$.

(b) The non-zero rational numbers $\mathbb{Q}^\times$ and the non-zero reals $\mathbb{R}^\times$ form a group under multiplication (with q corresponding to q^{-1}), while $\mathbb{Q}$ and $\mathbb{R}$ form groups under addition.

(c) The 52! ways to shuffle a deck of cards form a group, under composition: that is, shuffling again.

Remembering these examples basically tells you what a group is already, but let's cover the official definition.

Definition 1.1.2. A **group** is a pair $G = (G, \star)$, consisting of a set G and a binary operation $\star$ on G such that:

(i) G has an **identity** element, usually denoted one of e or 1_G, but sometimes one of 0_G, 0 or 1, with the property that
$$1_G \star g = g \star 1_G = g.$$

(ii) The operation is **associative**, that is
$$a \star (b \star c) = (a \star b) \star c,$$
for any $a, b, c \in G$. Thus, we don't ever have to write parentheses.

(iii) Each element $g \in G$ has an **inverse** $h \in G$, which is an element such that
$$g \star h = h \star g = 1_G.$$
Note that g can be equal to h, or can not be. Notation for the inverse varies, but it's usually g^{-1}, or sometimes $-g$.

Conditions (i)-(iii) are called the group axioms.

Abuse of Notation 1.1.3. We use G to represent both the group and the set because there's no real room for confusion. If there are any operations happening, we mean the group; if we're talking just about elements, then there's no difference between the elements of the set and the group. As such, I will often just abbreviate $(G, \star)$ as G when there is no likelihood of confusion. Also, when there is only one operation, so it is unambiguous, I will use associativity to abbreviate $(a \star b) \star c = a \star (b \star c) = abc$.

Remark 1.1.4 (Unimportant pedantry) — Some people, such as Edexcel, include a fourth axiom: **closure**. That is, if $g, h \in G$, then $g \star h \in G$. However, defining $\star$ as a binary operation as we did guarantees this. Regardless, it should feel obvious that we wouldn't care about $\star$ if that wasn't the case.

Remark 1.1.5 (Much more important note) — Notice that we *do not* need $\star$ to be **commutative**; that is $g \star h = h \star g$. Many useful groups have this property, but most do not.

Definition 1.1.6. Let $G = (G, \star)$ be a group. If $\star$ commutes - that is, if $g \star h = h \star g$ for all $g, h \in G$ - we call G **abelian**, after Norwegian mathematician Niels Abel. If this is not the case, we call it **non-abelian**.

Example 1.1.7 (Non-examples)

Here are some non-examples of groups. You will probably see a theme here.

(a) $(\mathbb{Q}, \times)$ is not a group, as 0 does not have an inverse.

(b) $(\mathbb{Z}, \times)$ is not a group for the reason above, but even more so: only ± 1 does have an inverse. The inverse of 2 would be $\frac{1}{2}$, but that is not an integer.

(c) Let $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ be the set of 2×2 real-valued matrices. Then $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), \times)$ is also not a group, as singular matrices have no inverse.

Here then are some abelian groups.

Example 1.1.8 (Complex unit circle)

Let S^1 be the set of complex numbers with absolute value 1; that is

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Then $\left(S^1, \times\right)$ is an abelian group, because

- the number $1 \in S^1$ is the identity,
- we have $(z_1 z_2) z_3 = z_1 (z_2 z_3)$ and $z_1 z_2 = z_2 z_1$,
- every number z has an inverse z^{-1}, with $\left|z^{-1}\right| = |z|^{-1} = 1^{-1} = 1$, and
- we have closure, as $|z_1 z_2| = |z_1|\,|z_2| = 1$.

Example 1.1.9 (Addition modulo n)

Let $n > 1$ be an integer. We consider the residues (remainders) modulo n. For example, the residues modulo 6 are $\{0, 1, 2, 3, 4, 5\}$. These form a group under addition, with elements $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$. We call this the **cyclic group of order** n, and denote it $\mathbb{Z}/n\mathbb{Z}$ pronouced "Z mod n Z". Both the name and the notation will make more sense later. The identity is $\overline{0}$. We often write the operation as $+_n$ to be clear. For example, $\mathbb{Z}/4\mathbb{Z} = \left(\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}, +_4\right)$, with operations like $\overline{2} +_4 \overline{3} = \overline{1}$. However, if we know the context, we will usually just write $2 + 3 = 1$.

Question 1.1.10. Find the inverses for $\mathbb{Z}/6\mathbb{Z}$.

Example 1.1.11 (Multiplication modulo p)

Let p be a prime. Then we consider the non-zero residues, which we denote $(\mathbb{Z}/p\mathbb{Z})^\times$. For example, the non-zero residues of 5 are $\{1,2,3,4\}$. These form a group under multiplication. Note that p needs to be prime for this to work. We often write the operation as $\times_p$ to be clear, and put the little overline on the numbers, e.g. $\overline{2}$. Thus, again, $\overline{2} \times_5 \overline{3} = \overline{1}$.

Question 1.1.12. Show that $(\mathbb{Z}/7\mathbb{Z})^\times$ is a group under multiplication, by finding it's identity and inverses. Show that $(\mathbb{Z}/6\mathbb{Z})^\times$ is not.

Here are some non-abelian examples. Make sure that you convince yourself that all of these do satisfy our axioms.

Example 1.1.13 (Linear groups)

Let n be a positive integer. Then $\mathrm{GL}_n(\mathbb{R})$ is the set of $n \times n$ matrices with a non-zero determinant. It turns out that $(\mathrm{GL}_n(\mathbb{R}), \times)$ does form a group, called the **general linear group**. You should know that all the matrices have an inverse. It is also clearly closed by using the area interpretation of the determinant. Similarly, the **special linear group** $(\mathrm{SL}_n(\mathbb{R}), \times)$ of matrices with determinant 1 is also a group.

Question 1.1.14. Convince yourself that both groups really are closed.

These two are arguably two of the most important types of groups.

Example 1.1.15 (Symmetric groups)

Let S_n be the set of permutations of $\{1,\ldots,n\}$. By viewing these permutations as functions from $\{1,\ldots,n\}$ to itself, we can consider composition of permutations. For example, if σ takes $(1,2,3) \mapsto (2,1,3)$ by swapping the first two elements, and π takes $(1,2,3) \mapsto (1,3,2)$ by swapping the last two, then $\sigma \circ \pi$ takes $(1,2,3) \mapsto (1,3,2) \mapsto (3,1,2)$, remembering that we apply π first, as it is on the right. Then $S_n = (S_n, \circ)$ called the **symmetric group on n elements** is a group because

- there is an identity permutation which doesn't change the order, and
- every permutation has an inverse.

We will cover permutations in more detail next chapter.

We will go over two good ways to think about symmetric groups later, but here's a taste. If all of this is confusing, however, leave it until next chapter.

Question 1.1.16. Suppose $s \in S_5$ and s maps $1 \mapsto 3 \mapsto 4 \mapsto 1$, and $2 \mapsto 5 \mapsto 2$. Then we write, using **cycle notation**, that $s = (1\,3\,4)(2\,5)$. Write $\tau : (1,2,3,4,5) \mapsto (4,3,2,5,1)$ in this form, and find τ^{-1}.

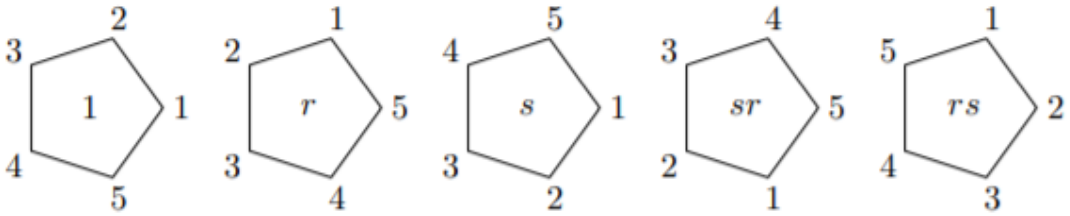
Example 1.1.17 (Dihedral group)

Again, let n be a positive integer, and consider a regular n-gon. The **dihedral group of order $2n$**, denoted D_{2n} is the group of symmetries, being reflections and rotations. We can write

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{-1}\},$$

where r is a rotation by $\frac{2\pi}{n}$, and s is a mirror reflection. So sr^2 means rotate twice, then reflect. Notice that $r^n = s^2 = 1$.

Here is a sample of D_{10}.



Question 1.1.18. Find all of the elements of D_6, and whata they represent on a triangle.

Example 1.1.19 (Product groups)
Let $(G, \star)$ and $(H, \circ)$ be any two groups. We can define a **product group** $(G \times H, \cdot)$ of G and H as follows. The elements of the group are the pairs $(g, h) \in G \times H$, and the operation is defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 \circ h_2).$$

All of the group properties follow from $(G, \star)$ and $(H, \circ)$.

Question 1.1.20. What are the identity and inverses of a product group?

This leads us on to the following example.

Example 1.1.21 (Klein 4-Group)
The Klein 4-Group, named after the German Felix Klein of bottle fame, is given by $K_4 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Although it is technically just pairs of numbers in $\mathbb{Z}/2\mathbb{Z}$ under addition, e.g. $(0, 1) +_2 (1, 1) = (1, 0)$, it is often thought of as simply 4 elements, all of which are **self-inverse**.

Question 1.1.22. Show that all elements of K_4 are self inverse.

Example 1.1.23 (Trivial group)
The **trivial group** is just the element 1. It does not matter what the operation is, as the only thing that can happen is $1 \star 1 = 1$. If you really want, you can think of this as $(\mathbb{Z}/2\mathbb{Z})^\times$.

Question 1.1.24. Show that this does satisfy all of the group axioms.

Exercise 1.1.25. Which of the following are groups?

(a) Rational numbers with odd denominators (in simplest form), where the operation is addition. (This includes integers, written as $n/1$, and $0 = 0/1$).

(b) The set of rational numbers with denominator at most 2, where the operation is addition.

(c) The set of rational numbers with denominator at most 2, where the operation is multiplication.

(d) The set of non-negative integers, where the operation is addition.

First, then, here are some basic propositions. I will include proofs, although I encourage you to try them yourself.

Proposition 1.1.26 (Group basics)
Let G be a group. Then the following propositions hold.

(i) The identity 1_G is unique.

(ii) The inverse of any element $g \in G$ is unique.

(iii) For any $g \in G$, $\left(g^{-1}\right)^{-1} = g$.

(iv) For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. Most are simply formal manipulations.

(i) Suppose that both 1_G and $1'_G$ were identities. Then $1_G = 1_G \star 1'_G = 1'_G$.

(ii) Suppose both h and h' were inverses. Then $h' = h' \star 1_G = h' \star (g \star h) = (h' \star g) \star h = 1_G \star h = h$.

(iii) From the definition of an inverse, $g^{-1} \star g = 1_G$ and $g \star g^{-1} = 1_G$.

(iv) $(gh)\left(h^{-1}g^{-1}\right) = g\left(hh^{-1}\right)g^{-1} = gg^{-1} = 1_G$ and $\left(h^{-1}g^{-1}\right)(gh) = h^{-1}\left(g^{-1}g\right)h = h^{-1}h = 1_G$.

□

§1.2 Cayley Tables

Abuse of Notation 1.2.1. We will write, for integer n,

$$g^n = \begin{cases} \underbrace{g \star g \star \cdots \star g}_{n \text{ times}} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ \underbrace{g^{-1} \star g^{-1} \star \cdots \star g^{-1}}_{-n \text{ times}} & \text{if } n < 0 \end{cases}.$$

Question 1.2.2. Show that $(g^n)^{-1} = g^{-n}$.

Now comes the first major result. This is fairly simple, but still incredibly powerful and somewhat surprising.

Lemma 1.2.3 (Left multiplication is a bijection)
Let G be a group, and pick any $g \in G$. Then $f : G \to G$ by $x \mapsto gx$ is a bijection. That is, there is one and only one way to get to any element in G by multiplying by g.

Proof. We check both injectivity and surjectivity. First, suppose $f(x) = f(y)$; that is $gx = gy$. Multiplying by g^{-1} on the left gets us $g^{-1}gx = g^{-1}gy \Rightarrow x = y$. Secondly, we can reach any $y \in G$, as $f(g^{-1}y) = g\left(g^{-1}y\right) = y$ for any y. □

Example 1.2.4 (Multiplication modulo 7)

Let $G = (\mathbb{Z}/7\mathbb{Z})^\times$, and pick $g = \overline{3}$. The lemma claims that $x \mapsto \overline{3}x$ is a bijection, and we can see that it is.

$$\begin{aligned}
\overline{1} &\mapsto \overline{3} \times \overline{1} = \overline{3} \pmod 7 \\
\overline{2} &\mapsto \overline{3} \times \overline{2} = \overline{6} \pmod 7 \\
\overline{3} &\mapsto \overline{3} \times \overline{3} = \overline{2} \pmod 7 \\
\overline{4} &\mapsto \overline{3} \times \overline{4} = \overline{5} \pmod 7 \\
\overline{5} &\mapsto \overline{3} \times \overline{5} = \overline{1} \pmod 7 \\
\overline{6} &\mapsto \overline{3} \times \overline{6} = \overline{4} \pmod 7.
\end{aligned}$$

Definition 1.2.5. The size of a group $|G|$ is called **order** of G, and is the number of elements in the set. If $|G|$ is finite, we say say that G is **finite**.

Example 1.2.6

(a) $|\mathbb{Z}/n\mathbb{Z}| = n$ for any n, while $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1$ for any p.

(b) $(\mathbb{Z}, +)$ is clearly not finite.

(c) $|D_{2n}|$ is $2n$, as the name suggests. Why?

(d) $|S_n| = n!$, the number of ways of permuting n objects.

(e) For any two groups G, H, we have $|G \times H| = |G|\,|H|$, as there $|G|$ choices for the first of the pair and $|H|$ for the second.

Cayley tables, named after English mathematician Arthur Cayley, are very helpful ways to visualise finite groups. For example, here are three Cayley tables, for $\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z})^\times$ and the Klein 4-group, K_4 (omitting overlines). These are read by looking picking a square, say the 3 in the second row of the first table. Look at the row header, 1, then the column header, 2. So $1 +_4 2 = 3$, which fits. In the third, we get $\mathrm{a} \star \mathrm{c} = \mathrm{b}$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

All three of these are groups with 4 elements. But what do you notice? Each row and each column contain each element in the group, as expected from Lemma 1.2.3 above. This why it is sometimes called the **latin square** property of groups. It is clear which element is the identity, as its row matches the header. Also, you can clearly find the inverses: if a square has the identity in, then the column and row headers are inverses.

Exercise 1.2.7. Draw the Cayley tables for:

(a) D_6 and S_3 - do you notice anything?

(b) D_8 and $\mathbb{Z}/8\mathbb{Z}$.

(c) The very small $\mathbb{Z}/2\mathbb{Z}$

(d) $(\mathbb{Z}/7\mathbb{Z})^\times$.

(e) Try to draw a Cayley table of $(\mathbb{Z}/6\mathbb{Z})^\times$ and show why it is not a group.

I'll give you D_6 and D_8 here, as there's something that I want to point out. Finding that $s \circ r = sr = r^{n-1}s$ geometrically, we get

$\circ$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

$\circ$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

I'll admit, they're a bit of a mess. But look what happens when we only look at rotations.

$\circ$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

$\circ$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

Looking at just the powers, we see that these are in essence the same as $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$. We will cover how exactly they are the same soon.

Let's try looking at the symmetries of a rectangle. Clearly, this will be similar to D_8, being the symmetries of a square, but different. Rotations by $\frac{\pi}{2}$ and $\frac{3\pi}{2}$ are not symmetries of a rectangle, so let us D_8 without r and r^3.

$\circ$	e	r^2	s	r^2s
e	e	r^2	s	r^2s
r^2	r^2	e	r^2s	s
s	s	r^2s	e	r^2
r^2s	r^2s	s	r^2	e

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

But notice: if we rename $r^2 = \mathrm{a}$, $s = \mathrm{b}$ and $r^2s = \mathrm{c}$, we get the Klein 4-group above. Thus, we can think of the Klein 4-group as either $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, the group of 4 self-inverse elements, or the symmetries of a rectangle! Remember, because we're only really interested in the structure of a group, it really doesn't matter what label we give the elements. This is similar to how it doesn't matter whether we call it $1 + \sqrt{3}i$ or $2e^{\frac{\pi}{3}i}$; the only thing that matters is how the number behaves.

§1.3 Groups of small order

How many ways are there to fill out a Cayley table for a group of order n, where $n \leq 4$?

For $n = 1$ it is easy: there is only one way. This gives us the trivial group. Thus the trivial group is (unsurprisingly) the only group of order 1.

For $n = 2$, the products e^2, ea and ae are clear, and the latin square property tells us that we need $a^2 = e$, else a has no inverse. Thus again, there is only one group of order 2, and it is $\mathbb{Z}/2\mathbb{Z}$ (where we have written $\overline{0}$ as e and $\overline{1}$ as a).

For $n = 3$, the products e^2, ea, eb, ae and be are clear. From the latin square property, we can see that ab and ba can be neither a nor b, so $ab = ba = e$. That lets us say that $a^2 = b$ and $b^2 = a$. This is then the same as $\mathbb{Z}/3\mathbb{Z}$, with $e = \overline{0}$, $a = \overline{1}$, and $b = \overline{2}$. Thus again, there is only one group of order 3.

$\star$	e
e	e

$\star$	e	a
e	e	a
a	a	e

$\star$	e	a	b
e	e	a	b
a	a	e	b
b	b	a	e

For $n = 4$, the situation gets more complicated, as ab can either be e or c without issue. If $ab = e$, then $ba = e$ as well as $b = a^{-1}$. Then, as there can only be one e per row and per column, $c^2 = e$.

Looking at the a-row, c can only go in $a^2 = c$. Similarly, we must have $b^2 = c$. Then $ac = b$, $bc = a$, $ca = b$ and $cb = a$.

$\star$	e	a	b	c
e	e	a	b	c
a	a		e	
b	b	e		
c	c			

$\star$	e	a	b	c
e	e	a	b	c
a	a	c	e	
b	b	e	c	
c	c			e

$\star$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

But if we then rename $e = \overline{0}$, $a = \overline{1}$, $b = \overline{3}$ and $c = \overline{2}$, this is the Cayley table for $\mathbb{Z}/4\mathbb{Z}$. Also, if we rename $e = \overline{1}$, $a = \overline{2}$, $b = \overline{3}$ and $c = \overline{4}$, we get the Cayley table for $(\mathbb{Z}/5\mathbb{Z})^\times$. Thus, in this way that we haven't pinned down yet, $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/5\mathbb{Z})^\times$ are somehow 'the same', even though we defined them very differently. All of their Cayley tables are stripes.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$\star$	e	a	c	b
e	e	a	c	b
a	a	c	b	e
c	c	b	e	a
b	b	e	a	c

We still have the second case. If $ab = c$, then look at a^2. It cannot be a or c, so it must be either b or e. If $a^2 = b$, then $ac = e$ by latin square, so $ca = e$ and $b^2 = e$. However, filling this in, we realise that we get the same Cayley table as above, just with b and c swapped. Thus again, we have found $\mathbb{Z}/4\mathbb{Z}$.

$\star$	e	a	b	c
e	e	a	b	c
a	a		c	
b	b			
c	c			

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c		
c	c	e		

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Thus, we can try $ab = c$, $a^2 = e$. By latin square, we can say $ac = b$, and $ba = c$ and $ca = b$. Then $c^2 = (ba)(ab) = ba^2b = b^2$. If $b^2 = c^2 = a$, we get the same group again. However, if $b^2 = c^2 = e$, we have a fundamentally different, group, as every element is self-inverse, and there are no generators. This you should recognise as the Klein 4-group. You can see that every element is self-inverse, as e always goes on the $\diagdown$ diagonal.

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	
b	b			
c	c			

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\star$	e	b	a	c
e	e	b	a	c
b	b	a	c	e
a	a	c	e	b
c	c	e	b	a

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

That's every way of filling out a Cayley table. Thus, there are only two groups of order 4.

Remark 1.3.1 — Here, the only two distinct ways of filling out a Cayley table both gave us a group. However, this is not necessarily the case. Try to construct a 5×5 latin square with elements e, a, b, c, d that is *not* a group, and justify why.

It turns out that there is only one group of each order 1, 2, 3, 5, and 7, all $\mathbb{Z}/n\mathbb{Z}$; two of order 4 ($\mathbb{Z}/4\mathbb{Z}$ and K_4), 6 ($\mathbb{Z}/6\mathbb{Z}$ and S_3, which is 'the same' as D_6), 9 ($\mathbb{Z}/9\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$) and 10 ($\mathbb{Z}/10\mathbb{Z}$ and D_{10}). However, there are 5 distinct groups of order 8.

§1.4 Exercises

Exercise 1.4.1. Some problems to have a go at.

(a) See if you can find all 5 groups of order 8. You already know $\mathbb{Z}/8\mathbb{Z}$ and D_8.

(b) A group is abelian if its Cayley table is symmetrical about the $\diagdown$ diagonal. Why?

(c) Show that $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ is 'the same' as $\mathbb{Z}/6\mathbb{Z}$, and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ is 'the same' as $\mathbb{Z}/10\mathbb{Z}$

(d) An **affine transformation** of $\mathbb{R}^2$ is one of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} + \boldsymbol{b},$$

where A is a 2×2 real matrix, and $\boldsymbol{b}$ is a 2×1 column vector. Show that the set of affine transformations of $\mathbb{R}^2$ forms a group under composition.

2 Isomorphisms and Permutations

In this chapter, I hope to establish what we meant last chapter by 'the same', and also explain the importance of symmetric groups through something called Cayley's theorem.

§2.1 Isomorphisms

Before, we said that two groups were the same if we could, in essence, relabel the elements of one to get the other. Let's think about this relabelling as a function, φ. For example, let's consider the symmetries of a rectangle, $\{e, r, s, rs\}$, where r is a rotation by π, and s a reflection, being the same as $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, as we know they are both the Klein 4-group. We want this renaming to unambiguous, and both groups need to have the same number of elements: that means our renaming function is bijective. We also want it to not matter whether we rename before or after we apply our operations. That is, if $\varphi(r) = (0,1)$, and $\varphi(s) = (1,0)$, we want

$$\varphi(r \cdot s) = (1,1) = (0,1) +_2 (1,0) = \varphi(r) +_2 \varphi(s).$$

Another example would be for $\mathbb{Z}$ being the same as $10\mathbb{Z} = \{\ldots, -20, -10, 0, 10, 20, \ldots\}$, with the renaming just being multiplication by 10. We obviously have

$$10(x + y) = 10(x) + 10(y).$$

This heuristic actually becomes our definition of an isomorphism.

Definition 2.1.1. Let $(G, \star)$ and $(H, \circ)$ be groups. A *bijection* $\varphi : G \to H$ is called an **isomorphism** if, for all $g_1, g_2 \in G$,

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

If there exists an isomorphism from G to H, then we say G and H are **isomorphic**, and write $G \cong H$.

Note that, in this definition, the left hand side of the equation $\varphi(g_1 \star g_2)$ uses the operation from G, while the right hand side $\varphi(g_1) \circ \varphi(g_2)$ uses the operation from H. We basically consider two groups to be the same if they are isomorphic.

Example 2.1.2 (Trivial examples)
Let G and H be groups.

(a) $\mathbb{Z} \cong n\mathbb{Z}$ by $x \mapsto nx$.

(b) $G \times H \cong H \times G$ by $(g, h) \mapsto (h, g)$.

(c) The identity map $g \mapsto g$ ensures that $G \cong G$.

(d) Also, $\mathbb{Z} \cong \mathbb{Z}$ by $x \mapsto -x$.

However, many isomorphisms are more complicated, like $\varphi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times$, as we showed before.

Example 2.1.3 (Primitive roots modulo 7)
We claim that $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$. The bijection is

$$\varphi(a \pmod 6) = 3^a \pmod 7.$$

We can check that this is a bijection:

$$(3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6) = (1, 3, 2, 6, 4, 5).$$

It also respects the group action, as

$$\varphi(a+b) = 3^{a+b} = 3^a 3^b.$$

Thus, this is a valid isomorphism.

Question 2.1.4. Show that $\mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^\times$ by finding an isomorphism.

This leads us to an interesting concept.We call $\mathbb{Z}/n\mathbb{Z}$ the cyclic group, because successive 'powers' (really multiples) of $\overline{1}$ cycle through all of the elements. That is, $\mathbb{Z}/4\mathbb{Z} = \{\overline{1}^0 = \overline{0},\ \overline{1},\ \overline{1}^2 = \overline{2},\ \overline{1}^3 = \overline{3}\}$. Thus, in some way $\overline{1}$ *generates* $\mathbb{Z}/n\mathbb{Z}$.

Thus, although cyclic groups appear in lots of different contexts (anything involving just rotation, for example), we can always just think about them in terms of our modular arithmetic.

Definition 2.1.5. A **cyclic group** is any group G with an element $g \in G$ such that $G = \{1_G, g, g^2, \ldots\}$. g is called the **generator** of G.

Example 2.1.6 (Cyclic groups)
Any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ by $g^i \mapsto \bar{i}$. Any infinite cyclic group is isomorphic to $\mathbb{Z}$ by $g^i \mapsto i$

§2.2 Permutations

With that out of the way, we can turn our attention to permutations, and why they're useful. I'm sure that you know what a permutation is, but here is the formalisation.

Definition 2.2.1. A **permutation** of a set X is a bijection $X \to X$. The set of all permutations is written $\mathrm{Sym}(X)$. If $X = \{1, \ldots, n\}$, we write $S_n = \mathrm{Sym}(X)$. The **composition** of two permutations, $\tau \circ \sigma$ is the permutation that arises by performing τ on the set X after having already been permuted by σ; that is, like $g \circ f$, perform σ first, then τ.

I will write $\sigma(x)$ for the position of $x \in X$ after the application of $\sigma \in \mathrm{Sym}(X)$, as this is the most common, but you may also find $x\sigma$ in places, such as the Oxford Maths Undergraduate course. Then, of course, $\tau \circ \sigma\,(x) = \tau\,(\sigma\,(x))$ is written $x\sigma\tau$.

Example 2.2.2
Suppose $X = \{a, b, c\}$. Then $\mathrm{Sym}(X)$ has the following 6 elements:

- Leaving everything as is: $(a, b, c) \mapsto (a, b, c)$
- Swapping two elements: $(a, b, c) \mapsto (b, a, c),\ (c, b, a),\ (a, c, b)$
- Cycling the elements: $(a, b, c) \mapsto (c, a, b),\ (b, c, a)$.

§2.2.i Notations

Suppose $\sigma \in S_5$, and it acts by

$$\sigma : (1,2,3,4,5) \mapsto (4,3,2,5,1).$$

I've already briefly introduced cycle notation, but I will do so fully again here. First, pick one element, traditionally 1. Find the 'chain' of where it maps. Here, $1 \mapsto 4 \mapsto 5 \mapsto 1$. This is now a 'cycle', as we have gotten back to 1. As it is of length 3, it is specifically a 3-cycle. We write this cycle $(1\,4\,5)$. Clearly, this is equivalent to $(4\,5\,1)$ and $(5\,1\,4)$. Then, pick another element, and find it's chain. Here $2 \mapsto 3 \mapsto 2$. That's all the elements, so we write $\sigma = (1\,4\,5)(2\,3)$. Similarly, if

$$\tau : (1,2,3,4,5) \mapsto (1,4,2,5,3),$$

then $\tau = (1)(2\,4\,5\,3)$. To find inverses, that is, the permutation that undoes this one, we simply reverse the order of the cycles, so $\sigma^{-1} = (5\,4\,1)(3\,2) = (1\,5\,4)(2\,3)$ and $\tau^{-1} = (1)(\,3\,5\,4\,2) = (1)(2\,3\,5\,4)$. Note that we usually don't write 1-cycles, so $\tau = (2\,4\,5\,3)$ would also be correct.

Question 2.2.3. Write $\sigma : (1,2,3,4,5) \mapsto (3,2,5,1,4)$ and $\tau : (1,2,3,4,5) \mapsto (4,3,2,1,5)$ and their inverses in cycle notation.

This is, in some ways, the most elegant way to write permutations, by a slightly more immediately obvious way is to write the σ and τ above as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}.$$

This is called two-line notation. Hopefully, this should be more easily understandable: the element in the top row maps to the element in the bottom row. The order of the columns then doesn't matter. Equally, finding inverses is fairly simple; just swap the top and bottom rows.

$$\sigma^{-1} = \begin{pmatrix} 4 & 3 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}.$$

However, the real advantage of this method is that it makes composition very easy. Using just cycle notation, it can take a while to work out what $\tau \circ \sigma$ should be, but with two-line notation it's very easy:

$$\begin{aligned} \tau \circ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 4 & 3 & 2 & 5 & 1 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}. \end{aligned}$$

Take for example 3. $\sigma(3) = 2$, and $\tau(2) = 4$, so $\tau\sigma(3) = 4$. Two-line notation allows for easy reordering, so this becomes much easier.

Question 2.2.4. If $\sigma : (1,2,3,4,5) \mapsto (3,2,5,1,4)$ and $\tau : (1,2,3,4,5) \mapsto (4,3,2,1,5)$ then find $\tau \circ \sigma$ and $\sigma \circ \tau$.

§2.3 Symmetry Groups

Here are some basic propositions.

Proposition 2.3.1 (Basics of symmetry groups)
Let X be a set of size n. Then the following are true.

(i) $\mathrm{Sym}(X)$ is a group under composition, called the **symmetry group of X**.

(ii) If $n \geq 3$, then $\mathrm{Sym}(X)$ is non-abelian.

(iii) $|\mathrm{Sym}(X)| = n!$.

(iv) $\mathrm{Sym}(X) \cong S_n$.

Proof. (i) The identity map leaving everything unchanged is clearly the identity. Using the techniques above, we can find an inverse to any permutation. We know that function composition is associative, and we can check that with the method for two-line notation.

(ii) Let $x_1, x_2, x_3 \in X$. Then define $f, g \in \mathrm{Sym}(X)$ by $f = (x_1\, x_2)$ and $g = (x_2\, x_3)$ in cycle notation. That is, x_i and x_j swap for relevant i, j and everything else is unchanged. Then $f \circ g(x_1) = f(x_1) = x_2$, while $g \circ f(x_1) = g(x_2) = x_3$. Thus, $f \circ g \neq g \circ f$, so $\circ$ does not commute.

(iii) Let $\sigma \in \mathrm{Sym}(X)$, and name the elements of X as $x_1, \ldots, x_n$. The order doesn't matter. There are n choices for $\sigma(x_1)$. There are then $n-1$ choices for $\sigma(x_2)$, and so on, until there is only one choice for $\sigma(x_n)$. Thus, there are $n \times (n-1) \times \cdots \times 1 = n!$ possibilities for σ. As all possible permutations are in $\mathrm{Sym}(X)$, we get $|\mathrm{Sym}(X)| = n!$.

(iv) Again, label the elements of X as $x_1, \ldots, x_n$ in some order. Then $\varphi : X \to \{1, \ldots, n\}$ by $x_i \mapsto i$ is an isomorphism.

□

Exercise 2.3.2 (For the brave)**.** We glossed over several details above. Here, you can chose to make them rigorous. First, we call two cycles **disjoint** if they have no elements in common. First, prove that disjoint cycles commute. That is, if the permutations $\sigma, \tau \in S_n$ are both a single cycle, and no element is affected by both σ and τ, then $\sigma\tau = \tau\sigma$. Then prove that any element of S_n is a composition of disjoint cycles. If you want, you can prove that this is unique, up to reordering cycles and elements within the cycles.

I provide a sketch of a solution below.
Even if you did not attempt the question, we will now be assuming the following lemma:

Lemma 2.3.3 (Cycle notation)
Disjoint cycles commute, and any $\sigma \in S_n$ can be written uniquely as a composition of disjoint cycles.

Sketch of proof. As they affect different elements, commutivity of disjoint cycles should be obvious.
Existence. Take $a_1 \in \{1, \ldots, n\}$. Consider $a_1, \sigma(a_1), \sigma^2(a_2), \ldots$. This is an infinite sequence, but all elements are from the finite set $\{1, \ldots, n\}$, so some element must repeat. Let this be $\sigma^r(a_1) = \sigma^s(a_i)$, with $r < s$. Applying σ^{-r}, we get $a_i = \sigma^{s-r}(a_i)$, so a_i is the first element to be repeated. Then if $\{a_1, \ldots, \sigma^{s-r-1}(a_i)\} = \{1, \ldots, n\}$, then σ is just one cycle. If not, there is an element a_2 not of the form $\sigma^k(a_1)$, which we can apply the same process to. The cycles of a_1 and a_2 must be disjoint, as else $\sigma^m(a_1) = \sigma^n(a_2) \Rightarrow a_2 = \sigma^{m-n}(a_1)$, so a_2 is in the cycle of a_1.
Uniqueness. Suppose that $\sigma = \pi_1 \circ \cdots \circ \pi_r = \tau_1 \circ \cdots \circ \tau_s$, where all π_i are disjoint, and all τ_j are disjoint. Then 1 appears in exactly one π_i and one τ_j. By reordering the cycles, let this be π_1 and τ_1. Then $\pi_1 = \tau_1 = \big(1\, \sigma(1)\, \ldots\, \sigma^{k-1}(1)\big)$, where $\sigma^k(1) = 1$. By finding elements not in π_1 and repeating, we get that all $\pi_i = \tau_i$. □

Corollary 2.3.4 (Powers of disjoint cycles)
Let $\sigma = \pi_1\pi_2\cdots\pi_n$, where π_i are disjoint cycles. Then $\sigma^k = \pi_1^k\pi_2^k\cdots\pi_n^k$.

Proof. $\sigma^k = (\pi_1\pi_2\cdots\pi_n)\circ\cdots\circ(\pi_1\pi_2\cdots\pi_n) = \pi_1^k\pi_2^k\cdots\pi_n^k$ by commutivity. □

We will now define the order of an element. This is very distinct concept to the order of a group; I don't know why they have the same name.

Definition 2.3.5. Let G be a group, and $g \in G$. Suppose k is the smallest positive integer such that $g^k = 1_G$. Then we define the **order** of g to be $\operatorname{ord} g = k$. If no such k exists, we say that $\operatorname{ord} g$ is infinite.

Example 2.3.6
The order of -1 in $\mathbb{Q}^\times$ is 2, while in $\mathbb{Z}$ it has infinite order. In fact, every element other than 0 has infinite order in $\mathbb{Z}$.
In the other extreme, every element of K_4 has order 2.

This is particularly important in cyclic groups.

Example 2.3.7 (Cyclic groups)
Let g be the generator of a cyclic group. Then clearly, $\operatorname{ord} g = |G|$. It turns out that any group with an element of order $|G|$ is cyclic, although we will not prove that just yet. However, this is the basis of the proof that $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Every group $(\mathbb{Z}/p\mathbb{Z})^\times$ has an element of order $p-1$, called a primitive root. These are very important in number theory.

Question 2.3.8. Find the order of all of the elements in $\mathbb{Z}/6\mathbb{Z}$ and D_6.

Exercise 2.3.9. Let G be a finite group. Show that $\operatorname{ord} g$ is finite for any $g \in G$.

Now, finding the order of a permutation is actually very simple.

Theorem 2.3.10 (Permutation order)
Let $\sigma \in S_n$, and $\sigma = \pi_1\cdots\pi_n$, where π_i are disjoint cycles. Let $|\pi_i|$ be the length of the cycle π_i; that is, the number of elements it affects. Then

$$\operatorname{ord}\sigma = \operatorname{lcm}\left(|\pi_1|, \ldots, |\pi_n|\right),$$

where lcm is the lowest common multiple.

Sketch of proof. Let $\operatorname{ord} g = k$. Then by Corollary 2.3.4, we get

$$\sigma^k = \mathrm{id} = \pi_1^k\cdots\pi_n^k,$$

where id is the identity map. Thus, all of π_i^k are the identity, so k is a multiple of $|\pi_i|$ for all i. The smallest value of this, by definition, is the lowest common multiple. □

There is one final theorem that I believe is fundamental to group theory.

Theorem 2.3.11 (Cayley's theorem, 1854)
Let G be a finite group, with $|G| = n$. Then G is isomorphic so a subgroup of S_n.

Proof. Recall that left multiplication is a bijection. Thus, $G \to G$ by $g' \to gg'$ for some g is a permutation. Thus, consider $\varphi : G \to H$, where $H \leq \mathrm{Sym}(G)$ by

$$g \to \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}.$$

You can show that this is an isomorphism as

$$\varphi(gh) = \begin{pmatrix} g_1 & \cdots & g_n \\ ghg_1 & \cdots & ghg_n \end{pmatrix} = \begin{pmatrix} hg_1 & \cdots & hg_n \\ ghg_1 & \cdots & ghg_n \end{pmatrix} \circ \begin{pmatrix} g_1 & \cdots & g_n \\ hg_1 & \cdots & hg_n \end{pmatrix} = \varphi(g) \circ \varphi(h),$$

and we can define it to be a bijection by simply letting H be the set of such permutations. Then $G \cong H \leq \mathrm{Sym}(G) \cong S_n$, so G is isomorphic to some subgroup of S_n. □

Remark 2.3.12 — The proof of this result is overly technical. The overview is that we can think of each element of G as permuting the elements of G in a distinct way. Thus, lots of results which apply trivially to symmetry groups must also apply to all finite groups.

§2.4 Exercises

Exercise 2.4.1. Some problems to have a go at.

(a) (Representation theory). Let G be a finite group. Find an integer n such that G is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{R})$ (Example 1.1.13).

(b) Let $\tau \in S_n$ be given by

$$\tau : \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \end{pmatrix}.$$

Let $\sigma \in S_n$. Show that $\sigma \circ \tau \circ \sigma^{-1}$ is given by

$$\sigma \circ \tau \circ \sigma^{-1} : \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n) \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_{n-1}) & \sigma(a_n) \end{pmatrix}.$$

(c) Hence, let

$$\alpha = (1\,2\,3)(4\,5), \quad \beta = (1\,2\,3\,4), \quad \gamma = (2\,3).$$

Find $\left(\alpha\beta^5\gamma^3\alpha^2\gamma\beta^3\alpha^5\right)^3$.

(d) Show that $V_4 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is abelian, and isomorphic to K_4. How many isomorphisms are there from $V_4 \to K_4$?

(e) Find all $\sigma \in S_7$ such that $\sigma^3 = (1\,2\,3\,4)$.

3 Subgroups and Cyclic Groups

The definition of a subgroup is fairly simple.

Definition 3.0.1. Let $(G, \star)$ be a group. We say that $(H, \star)$ is a **subgroup** of G, written $H \leq G$, if H is a subset of G, written $H \subseteq G$, and is a group under the operation $\star$. That is, if

(i) $1_G \in H$

(ii) if $g_1, g_2 \in H$ then $g_1 \star g_2 \in H$

(iii) if $g \in H$ then $g^{-1} \in H$

with associativity following from G being a group.

Remark 3.0.2 (Subsets and subgroups) — It is important to distinguish between subsets and subgroups. Subsets are written $A \subseteq B$; for example, $\{\overline{1}, \overline{3}, \overline{4}\} \subseteq \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \mathbb{Z}/6\mathbb{Z}$. However, $\left(\{\overline{1}, \overline{3}, \overline{4}\}, +_6\right) \not\leq \mathbb{Z}/6\mathbb{Z}$, as it is not a group.

§3.1 Facts and examples

I showed you some examples earlier, like $\mathbb{Z}/4\mathbb{Z} \leq D_8$; here are some more.

Example 3.1.1 (Trivial examples)
Let G be any group.

(a) The trivial group $\{1_G\} \leq G$

(b) $G \leq G$, unhelpfully

(c) For any a, b we have $\mathbb{Z}/a\mathbb{Z}$ is isomorphic to a subgroup of $\mathbb{Z}/ab\mathbb{Z}$, by just looking at the multiples of b.

Some non-examples include

Example 3.1.2 (Non-examples)
Consider $\mathbb{Z} = (\mathbb{Z}, +)$.

(a) The set $\{0, 1, \ldots\}$ is not a subgroup as it does not have inverses

(b) The set $\{n^3 \mid n \in \mathbb{Z}\} = \{\ldots, -8, -1, 0, 1, 8, \ldots\}$ is not a subgroup, as the sum of two cubes is rarely a cube

(c) The empty set is never a subgroup, as it lacks an identity (although vacuously, every element does have an inverse, and any operation is associative).

Some more relevant examples include

Example 3.1.3 (Better subgroups)

(a) $\{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z} \leq \mathbb{Z}$, even though $2\mathbb{Z} \cong \mathbb{Z}$!

(b) Consider S_n, and let $T = \{\tau \in S_n \mid \tau(n) = n\}$. Then $T \leq S_n$, and $T \cong S_{n-1}$.

(c) Consider $G \times H$, and the set $G' = \{(g, 1_H) \mid g \in G\}$. Then $G' \leq G \times H$, with $G' \cong G$.

Question 3.1.4. Find a subgroup of D_{2n} isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

However, there is one particularly important subgroup.

Definition 3.1.5. Let x be an element of a group G. Then consider the set

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1_G, x, x^2, \dots\}.$$

This forms a subgroup of G known as the **subgroup generated by** x, or the **cyclic subgroup** of x.

Question 3.1.6. Show that this is in fact a subgroup.

Remark 3.1.7 (Note on orders) — Notice that if $\operatorname{ord} x$ is finite, then $\langle x \rangle \cong \mathbb{Z}/(\operatorname{ord} x)\,\mathbb{Z}$. If $\operatorname{ord} x = \infty$, then $\langle x \rangle \cong \mathbb{Z}$. In particular, for an integer n, $\langle n \rangle = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ is the set of multiples of n, or $n\mathbb{Z}$.

This gives us the following fact.

Corollary 3.1.8 (Cyclic groups)
A group G is cyclic precisely when there is an element $g \in G$ such that $\langle g \rangle = G$.

This shows us again that any cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. We can also generalise this to subgroups generated by sets. I like to think of this less algebraically but more like putting a set S in a box, shaking it around vigorously, and looking at all of the possible resulting clumps of terms.

Theorem 3.1.9 (Generated subgroups)
Let G be a group, and S be a subset of G ($S \subseteq G$). Then

$$\langle S \rangle = \{s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \mid s_i \in S,\ k_i \in \mathbb{Z}\}$$

is a subgroup $\langle S \rangle \leq G$ called the **subgroup generated by S**. Notice that the s_i need not be distinct: if $S = \{a, b\}$, then $a^2bab^3a^{-1} \in \langle S \rangle$.

Exercise 3.1.10. Prove that this is also a group.

An important fact about generated subgroups, which some people give as the definition.

Theorem 3.1.11 (Generated subgroups are the smallest subgroups)
Let G be a group, and $S \subseteq G$. Then $\langle S \rangle$ is the smallest subgroup of G which contains S.

Proof. Let $T \leq G$ be the smallest subgroup with $S \subseteq T$. By closure, it must contain any element of the form $s_1^{k_1} s_2^{k_2} \cdots$ for $s_i \in S$, $k_i \in \mathbb{Z}$. Thus, $\langle S \rangle \leq T$, as T contains all of the elements of $\langle S \rangle$. As $\langle S \rangle$ is a group, and smaller or equal to T, they must be equal, as T is the smallest. Thus, $\langle S \rangle$ is the smallest subgroup containing S. □

It turns out that there is a test for whether a subset forms a subgroup. It's not overly useful, but its quite nice to know. Again, we don't need to check for associativity, as it follows from the group operation of G.

Lemma 3.1.12 (Subgroup test)
Let G be a group. Then $H \subseteq G$ forms a subgroup $H \leq G$ if and only if H isn't empty and $h_1 h_2^{-1} \in H$ for every $h_1, h_2 \in H$.

Proof. ($\Rightarrow$) First, we assume that H is a subgroup. Then $1_G \in H$, so it is not empty. Also, $h_2^{-1} \in H$ by inverses. Then $h_1 h_2^{-1} \in H$ by closure.
($\Leftarrow$) Next, assume H is non-empty and $h_1 h_2^{-1} \in H$ for any $h_1, h_2 \in H$.

- $h_1 h_1^{-1} = 1_G \in H$, so we have an identity.
- $1_G h_1^{-1} = h_1^{-1} \in H$, so we have inverses.
- $h_1 \left(h_2^{-1}\right)^{-1} = h_1 h_2 \in H$, so we have closure.

□

Exercise 3.1.13. Show that, if $H_1, H_2 \leq (G, \star)$, then then $H_1 \cap H_2 = (H_1 \cap H_2, \star)$ is a subgroup of G.

Exercise 3.1.14. Let G be a cyclic group, and let $H \leq G$. Show that H is cyclic.

Remark 3.1.15 (Subgroups of $\mathbb{Z}$) — By Exercise 3.1.14, any subgroup of $\mathbb{Z}$ is cyclic, and it must be infinite, thus isomorphic to $\mathbb{Z}$ itself by 3.1.7.

§3.2 (Optional) More on generated subgroups

In fact, this last remark leads us to a set of very interesting deductions. For example, take $\langle 14, 21\rangle$. We can write out elements and realise that $\langle 14, 21\rangle = \langle 7\rangle = 7\mathbb{Z}$. Also, $\langle 14\rangle \cap \langle 21\rangle = \langle 42\rangle = 42\mathbb{Z}$. Notice: $7 = \gcd(14, 21)$ and $42 = \operatorname{lcm}(14, 21)$.
Recall that $a \mid b$ means a divides b.

Theorem 3.2.1 (gcd and lcm)
Let m, n be integers. Let g, l be integers such that $\langle m, n\rangle = \langle g\rangle$, and $\langle m\rangle \cap \langle n\rangle = \langle l\rangle$. Then the following are true:

(i) (Bézout's Lemma). There are $a, b \in \mathbb{Z}$ such that $g = am + bn$;

(ii) $g \mid m$ and $g \mid n$ (that is, g is a common factor of m and n);

(iii) If $d \mid m$ and $d \mid n$, then $d \mid g$ (that is, g is divisible by every common factor of m and n);

(iv) $m \mid l$ and $n \mid l$ (that is, l is a common multiple of m and n);

(v) If $m \mid c$ and $n \mid c$, then $l \mid c$ (that is, any common multiple of m and n is a multiple of l).

A lot of little theorems, but none are too tough to prove. In fact, most are one-liners. Recall Remark 3.1.7, which says that $\langle i\rangle$ is the group of multiples of i, so any element of $\langle i\rangle$ is a multiple of i.

Proof. (i) $g \in \langle g\rangle = \langle m, n\rangle$, so $g = am + bn$ for some a, b, by the definition of a generated subgroup. (Here we have used the fact that $\mathbb{Z}$ is abelian.)

(ii) We have $m \in \langle m, n\rangle = \langle g\rangle$, so m is a multiple of g, so $g \mid m$. By the same logic, $g \mid n$.

(iii) Suppose $d \mid m$ and $d \mid n$. Then $d \mid (rm + sn)$ for any r, s. Choosing $r, s = a, b$ from (ii), we get that $d \mid g$.

(iv) We have $l \in \langle l \rangle$, so $l \in \langle m \rangle$ and $l \in \langle n \rangle$, so $m \mid l$ and $n \mid l$.

(v) Suppose $m \mid c$ and $n \mid c$, so $c \in \langle m \rangle$ and $c \in \langle n \rangle$. Then $c \in \langle m \rangle \cap \langle n \rangle = \langle l \rangle$, so $l \mid c$.

□

Thus, we can define the two terms that you already know from school, but with respect to group theory.

Definition 3.2.2. Define g and l as in 3.2.1. Then we call g the **greatest common divisor** and l the **lowest common multiple**.

Remark 3.2.3 — I use the term greatest common divisor as it is the most commonly used in maths in general. However, division is not defined for the group of integers, so many people prefer the term highest common factor.

§3.3 Finale

For anyone who skipped the above section, I'll restate one important lemma.

Lemma 3.3.1 (Bezout's lemma)
Let m, n be integers, and g be an integer such that $\langle m, n \rangle = \langle g \rangle$. Then $g = \gcd(m, n)$, and there are $a, b \in \mathbb{Z}$ such that $g = am + bn$.

We can then round off this chapter with two very famous theorems. This first is a weaker version of a theorem we will prove in full later. The second is a very important theorem in Olympiad number theory.

Theorem 3.3.2 (Multiples of the order)
Let G be a group, with $g \in G$ such that $d = \operatorname{ord} g$ is finite. Then $g^k = 1_G$ if and only if $d \mid k$.

Proof. ($\Leftarrow$) Assume that $d \mid k$. Then let $k = ad$ for some a, so $g^k = g^{ad} = \left(g^d\right)^a = (1_G)^a = 1_G$.
($\Rightarrow$). Assume that $g^k = 1_G$. Let $k = qd + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < d$. Then

$$g^r = g^{k-qd} = g^k \left(g^d\right)^{-q} = 1_G.$$

Since $r < d$, but $d = \operatorname{ord} g$ is the smallest *positive* integer such that $g^n = 1_G$, we must have $r = 0$. Thus $k = qd$, so $d \mid k$. □

Remark 3.3.3 — I here used the fact that, for any two integers k, d we can write $k = qd + r$ for an integer q and integer $0 \leq r < d$. This is called the **division algorithm**: $k \div d$ is q rm r. You can prove that this always exists but it should be fairly obvious.

Theorem 3.3.4 (Chinese remainder theorem, 1247)
Let m, n be **coprime** integers; that is, $\gcd(m, n) = 1$. Then $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(mn)\mathbb{Z}$, so is cyclic.

This is by far the toughest proof so far. Don't be scared to go over it a few times, and do some working out to fill in details.

Proof. We will consider $\mathbb{Z}/m\mathbb{Z} \cong \langle g \rangle$ and $\mathbb{Z}/n\mathbb{Z} \cong \langle h \rangle$ for some g, h. For example, $g = \overline{1} \in \mathbb{Z}/m\mathbb{Z}$ and $h = \overline{1} \in \mathbb{Z}/n\mathbb{Z}$. Recall that this implies $\operatorname{ord} g = m$ and $\operatorname{ord} h = n$. I will let e_m and e_n be their respective identities. First, we claim that $(g, h) \in (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ has order mn.
$(g,h)^{mn} = ((g^m)^n, (h^n)^m) = (e_m, e_n)$, so $\operatorname{ord}(g,h)$ is at most mn. Also, for any positive integer k, if $(g,h)^k = (e_m, e_n)$, then $g^k = e_m$ and $h^k = e_n$. Thus, by Theorem 3.3.2, $m \mid k$ and $n \mid k$. But as m, n are coprime, this means $mn \mid k$, so $mn \mid \operatorname{ord} g$. Thus, $mn \leq \operatorname{ord}(g,h) \leq mn$, so $\operatorname{ord}(g,h) = mn$.
Now, $|(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})| = |\mathbb{Z}/m\mathbb{Z}| \times |\mathbb{Z}/n\mathbb{Z}| = mn$, so $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ is a group of order mn, with an element of order mn, so is cyclic, and $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(mn)\mathbb{Z}$. □

Remark 3.3.5 — Clearly, this form of the theorem is not used in Olympiads, nor is it the form proposed in 3rd century AD by Sun-tzu, or proved in 1247 by Qin Jiushao. However, an equivalent statement of the theorem is as follows: Suppose we have two coprime integers m, n and any two integers a, b. Then the simultaneous equivalences

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a unique solution for $0 \leq x < mn$. That is, any pair ($a \pmod m$, $b \pmod n$) corresponds to exactly one number $x \pmod{mn}$.

§3.4 Group representations

Generated subgroups are nice and all, but in practise, the generators typically satisfy certain properties. For example, $\mathbb{Z}/100\mathbb{Z} = \langle \overline{1} \rangle$, but only when we know that $\overline{1} \in \mathbb{Z}/100\mathbb{Z}$ in the first place. In particular, that means that $\overline{1}^{100} = \overline{0}$, the identity. But surely it would be nicer to just specify that $\mathbb{Z}/100\mathbb{Z} = \langle x \rangle$, where $x^{100} = \overline{0}$. This is exactly what group presentations do.

Definition 3.4.1. A **group presentation** is a way of specifying a group from a set of generators and relations on those generators. If a group is generated by a set S, with relations R, we write

$$G = \langle S \mid R \rangle .$$

Notice that if two groups have the same group presentation, they are isomorphic.

Example 3.4.2 (Cyclic groups, again)
Cyclic groups are the classic example. For any integer n, we get that

$$\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1_G \rangle .$$

Example 3.4.3 (Dihedral groups)
Dihedral groups are the other classic example.

$$D_{2n} = \langle s, r \mid r^n = s^2 = e,\ rs = sr^{-1} \rangle .$$

Thus each element can be written in the form r^a or sr^a, where $a = 0, \ldots, n-1$.

Question 3.4.4. Make sure that this makes sense.

Example 3.4.5 (Klein 4-group)
We can even write

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = K_4 = \langle a, b \,|\, a^2 = b^2 = e,\ ab = ba \rangle .$$

Our four elements are then e, a, b, ab.

Question 3.4.6. Draw a Cayley table to check that this is the Klein 4-group.

Example 3.4.7 (Free group)
The **free group on n elements**, written F_n, is the group with n generators and no relations:

$$F_n = \langle x_1, \ldots, x_n \rangle .$$

Abuse of Notation 3.4.8. Unfortunately the notation for "the subgroup generated by a and b" and the notation for F_2 are the same: $\langle a, b \rangle$. I'll try to always be clear which one I mean.

Question 3.4.9. What is F_1? Can you think of a possible use for F_{26}?

Group presentations are nice, because they let you express a group's properties very simply. However, they have one major shortcoming.

Example 3.4.10 (Presentations can look very different)
This is another example of a presentation for D_{2n}.

$$D_{2n} = \langle x, y \,|\, x^2 = y^2 = (xy)^n = 1 \rangle .$$

Question 3.4.11. Show that these generate the same group by letting $x = r$, $y = rs$.

In fact, group presentations are formally useless. Determining whether two general group presentations represent the same group is undecidable; it can't be done, even theoretically. We have to literally write out the Cayley table to be certain. We can't even always tell if a group is finite from it's presentation.

§3.5 Exercises

Exercise 3.5.1. Some problems to have a go at.

(a) Let $(g, h) \in G \times H$. Show that $\operatorname{ord}(g, h) = \operatorname{lcm}(\operatorname{ord} g, \operatorname{ord} h)$.

(b) Find, in D_8, $\langle rs \rangle$ and $\langle rs, s \rangle$.

(c) Suppose that G is a finite group with an element $g \in G$ such that $|G| = \operatorname{ord} g$. Show that G is cyclic.

(d) Prove whether the following groups are or are not cyclic.
- $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$
- $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$
- $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$
- $\langle (1\,2)(3\,4)(5\,6),\ (1\,4\,5)(2\,3\,6) \rangle \leq S_6$
- $\langle (1\,2\,3)(4\,5\,6) \rangle \leq S_6$

(e) Let G be a group with presentation given by

$$G = \langle a, b, c \,|\, ab = c^2a^4,\ bc = ca^6,\ ac = ca^8,\ c^{2018} = b^{2019} \rangle .$$

Determine the order of G. Hint: one approach uses induction.

(f) Let G be a finite group, and H, K subgroups. Let $HK = \{hk \mid h \in H, k \in K\}$. Define the function $\lambda : H \times K \to HK$ by $\lambda(h,k) = hk$. Define $\lambda^{\text{pre}}(g) = \{(h,k) \in H \times K \mid \lambda(h,k) = g\}$.

(i) Show that $|\lambda^{\text{pre}}(g)| = |H \cap K|$ for any $g \in HK$. Hence deduce that

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

(ii) Show that if G is abelian and $H \cap K = \{e\}$, then $HK \cong H \times K$.

4 Cosets and Lagrange

The aim of this chapter is really just to prove Lagrange's theorem. To do this, I will introduce a construct that may seem odd at first, but will be vital for next chapter. I will also prove a lot of smaller corollaries of Lagrange.

§4.1 Cosets

We will begin by defining a coset.

Definition 4.1.1. Let G be a group, and $H \leq G$ a subgroup. A **left coset** of H in G is a set

$$g \star H = gH = \{gh \mid h \in H\},$$

for any $g \in G$. The set of left cosets in G is denoted G/H, pronounced "G mod H". The size of this set is called the **index** of H in G, denoted $[G : H]$. Right cosets Hg are defined similarly.

Remark 4.1.2 (Abelian groups) — If G is abelian, then $gh = hg$, so $gH = Hg$ and left and right cosets are the same. If G is not abelian, they may be the same or they may be different.

Example 4.1.3 (Cosets of $\mathbb{Z}$)

Let $n\mathbb{Z}$ be a subgroup of $\mathbb{Z}$. Then the left coset of $r \in \mathbb{Z}$ is $r + n\mathbb{Z}$. Notice that we here do write the operation $+$ to avoid confusion. Notice also that $r + n\mathbb{Z} = (r + n) + n\mathbb{Z}$.

Question 4.1.4. Explain why this is. Thus explain why $[\mathbb{Z} : n\mathbb{Z}] = n$.

This finally explains why we have been writing $\mathbb{Z}/n\mathbb{Z}$ for the cyclic group of order n: it is the set of left cosets of $n\mathbb{Z}$, which just happen to form a group. For example, as

$$3 + 5\mathbb{Z} = 8 + 5\mathbb{Z} = 32423 + 5\mathbb{Z} = \{\ldots, -2, 3, 8, \ldots\},$$

we write

$$\overline{3} = \{\ldots, -2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 8 + 5\mathbb{Z}, \ldots\}.$$

We define $(r + 5\mathbb{Z}) +_5 (s + 5\mathbb{Z}) = (r + s) + 5\mathbb{Z}$. Then, if we want $\overline{2} +_5 +\overline{4}$, we pick some representative of each: say $7 + 5\mathbb{Z}$ and $14 + 5\mathbb{Z}$. Then we work out their sum, which is $21 + 5\mathbb{Z}$. But $21 + 5\mathbb{Z} \in \overline{1}$, so we get $\overline{2} +_5 \overline{4} = \overline{1}$. However, this technicality is far more than confusing that necessary.

Example 4.1.5 (Symmetric groups)

Let $G = S_3$, and $H = \langle (1\,2) \rangle = \{e, (1\,2)\}$. The left cosets are

$$\begin{aligned}
eH &= H \\
(1\,2)H &= \{(1\,2), e\} = H \\
(1\,3)H &= \{(1\,3), (1\,3\,2)\} \\
(2\,3)H &= \{(2\,3), (1\,2\,3)\} \\
(1\,2\,3)H &= \{(1\,2\,3), (1\,2\,3)(1\,2)\} = \{(2\,3), (1\,2\,3)\} \\
(1\,3\,2)H &= \{(1\,3\,2), (1\,3\,2)(1\,2)\} = \{(1\,3), (1\,3\,2)\}.
\end{aligned}$$

Thus $[G : H] = 3$.

Question 4.1.6. Show that if $h \in H$, $hH = H$.

§4.2 Lagrange's theorem

The two most important lemmas about cosets are probably as follows.

Lemma 4.2.1 (Cosets partition G)
Let G be a group and $H \leq G$ a subgroup. Then every $g \in G$ is in one and only one left coset in G/H.

Proof. Clearly, every $g \in G$ is in the left coset gH, as $1_G \in H$.

Exercise 4.2.2. Show that if $x \in g_1H$ and $x \in g_2H$, then $g_1H = g_2H$, even if $g_1 \neq g_2$.

Thus, if any element $x \in G$ is in two cosets, those cosets are the same. Thus, every element is in one and only one left coset. □

Lemma 4.2.3 (Coset bijections)
Given any group G with subgroup $H \leq G$, we have a bijection between gH and H for any $g \in G$. In particular then, all left cosets have the same size.

Question 4.2.4. I recommend trying this yourself.

Proof. Pick some $g \in G$, and define $f : H \to gH$ by $h \mapsto gh$. This is clearly injective: if $gh_1 = gh_2$, applying g^{-1} gets $h_1 = h_2$. It is also surjective: by definition, the elements of gH are all the elements of the form gh. Thus f is bijective. Also, as there is a bijection between gH and H, and $g'H$ and H, composing the two bijections gives us a bijection between gH and $g'H$, for any two g, g'.
As there is a bijection, $|H| = |gH| = |g'H|$. □

And just those two facts prove the most well-known, and most useful, theorem in elementary group theory. Despite the name, Joseph-Louis Lagrange did not actually prove the following theorem. He stated the special case where $G = S_n$ in 1771 without proof; Gauss proved the special case of $(\mathbb{Z}/p\mathbb{Z})^\times$ in 1801; Cauchy proved the case of S_n in 1844. Finally, Camille Jordan proved the general case. Despite of all of these famous names, with the foundation you have, it becomes very simple.

Theorem 4.2.5 (Lagrange's theorem, 1861)
Let G be a group, and $H \leq G$ be a subgroup. Then $|H|$ divides $|G|$.

Proof. By Lemma 4.2.1, we can place every element of G into exactly one left coset in G/H. By Lemma 4.2.3, these left cosets all have size $|H|$. Thus,

$$|G| = |G/H| \times |H|,$$

so $|H|$ divides $|G|$. In particular,

$$|G| \div |H| = |G/H| = [G : H].$$

□

Remark 4.2.6 (Left and right cosets) — All of these properties of left cosets also hold with right cosets. However, mathematicians have agreed that, for some reason, they prefer the left cosets to right cosets. Maybe writing Hg would risk mercury consumption...

§4.3 Some corollaries

We will now prove 5 results that follow immediately from this result, although the last two take a little more effort. I say we: I want you to try all of them before reading the proof.

Corollary 4.3.1 (Lagrange for orders of elements)
Let G be a finite group with $g \in G$. Then $\operatorname{ord} g$ divides $|G|$.

Question 4.3.2. Try to prove this yourself.

Sketch of proof. Note that $\langle g \rangle = \{1_G, g, \dots, g^{\operatorname{ord} g - 1}\} \leq G$. Then apply Lagrange. □

Corollary 4.3.3 (Groups of prime order)
Let G be a group of order p, where p is prime. Then G is cyclic.

Exercise 4.3.4. Prove this.

Sketch of proof. Take $g \in G$, $g \neq 1_G$. Use Corollary 4.3.1. □

Remark 4.3.5 (Isomorphisms of cyclic groups) — This not only shows that all groups of prime order are isomorphic, but also that any non-identity element generates it. Thus, when setting up an isomorphism $\varphi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times$, any of $\varphi(x) = 2^x$, 3^x, or 4^x is valid.

Corollary 4.3.6 (Power of the order)
Let G be a finite group. Then, for any $g \in G$, $g^{|G|} = 1_G$.

Question 4.3.7. Again.

Sketch of proof. Recall Theorem 3.3.2. Combine this with Corollary. 4.3.1. □

Remark 4.3.8 — This is easiest to remember with cyclic groups, but is a very powerful result in any context.

Corollary 4.3.9 (Groups of even order)
Let G be a group of even order. Then G has an element of order 2.

Exercise 4.3.10. This is a tough one; but give it a go. A hint: consider self-inverse elements.

Proof. Let G be a group. For each $g \in G$, we define $S_g = \{g, g^{-1}\}$.

Question 4.3.11. Show that: (a) if g is self-inverse, $S_g = \{g\}$; (b) if $h \in S_g$, then $S_h = S_g$. Thus every $g \in G$ is in exactly one set of the form S_x.

Thus, every set S_g has size either 1, if g is self-inverse, or 2 else. Let there be m sets of size 1 and n sets of size 2. Then $|G| = m + 2n$. As $|G|$ is even, m must be even. Also, 1_G is self-inverse, so $m \geq 1$. Thus, $m \geq 2$, so there is at least one non-identity element which is self-inverse, and thus of order 2. □

§4.3.i (Optional) Groups of order $2p$

This actually gives us a more interesting theorem. We can think of it as a one-up on Corollary 4.3.3.

Corollary 4.3.12 (Groups of order $2p$)
Let G be a group of order $2p$, where $p \geq 3$ is prime. Then either $G \cong \mathbb{Z}/2p\mathbb{Z}$ or $G \cong D_{2p}$.

Question 4.3.13. Easily the hardest so far. The way to about it is to see what happens if it isn't cyclic.

Proof. Assume that G is not cyclic, so there is no element of order $2p$. Then the possible orders of elements are 1 (the identity only), 2 or p. By Corollary 4.3.9, there is at least one element x of order 2. If all $g^2 = 1_G$, then

$$G = (\mathbb{Z}/2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2\mathbb{Z}),$$

which is not possible, as that gives $|G| = 2^n$, for some n.

Question 4.3.14. Verify the above.

Thus, there is at least one element $y \in G$ of order p. Then $\langle y \rangle = \{1_G, y, y^2, \ldots, y^{p-1}\}$ is a cyclic (sub)group of order p, so all $p-1$ elements y^n are order p; in particular, remembering the element x of order 2, $x \notin \langle y \rangle$, so $xy^i \notin \langle y \rangle$. By closure, we then get

$$G = \{1_G, y, \ldots, y^{p-1}, x, xy, \ldots, xy^{p-1}\},$$

as all of those elements are distinct and in G, and there are $2p$ of them.
Now, the product yx is somewhere in G.

Question 4.3.15. Show that $yx = y^i$ is a contradiction.

Thus, we have $yx = xy^j$ for some j. We can look at the order of yx. Looking at odd and even powers of yx, we get

$$(yx)^{2k} = \left[(yx)\left(xy^j\right)\right]^k = y^{k(j+1)}$$
$$(yx)^{2k+1} = \left(xy^j\right)\left(y^{k(j+1)}\right) = xy^{kj+k+j}.$$

Thus, yx must have even order, because xy^j is never the identity. In particular then, $\operatorname{ord} yx = 2$. Then $y^{k(j+1)} = 1_G$ for any k, so $j + 1 = p$. Thus, $yx = xy^{p-1}$. Finally, we are done:

$$G = \left\langle x, y \,|\, x^2 = y^p = 1,\ yx = xy^{p-1} \right\rangle = D_{2p}.$$

□

§4.4 Some more famous results

Theorem 4.4.1 (Fermat's little theorem, 1640)
Let p be a prime, and a an integer such that $\gcd(a, p) = 1$; we say a and p are **coprime**. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exercise 4.4.2. Not too hard. Think about which group will help you here.

Sketch of proof. $(Z/p\mathbb{Z})^\times$ is a group of order $p-1$. Apply Corollary 4.3.6. □

In fact, we can generalise Fermat's little theorem to cope with non-prime numbers.

Theorem 4.4.3 (Fermat-Euler theorem, 1736)
Let $n \geq 2$ be an integer. Let a be an integer such that $\gcd(a,n) = 1$ (a and n are coprime). Define the **Euler totient function** φ as

$$\varphi(n) = |\{k \in \mathbb{N} \,|\, 1 \leq k \leq n,\, \gcd(k,n) = 1\}|.$$

That is, $\varphi(n)$ is the number of numbers less than n which has no common factors.
Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Exercise 4.4.4. Definitely the hardest so far. Still, it's worth the effort.

Proof. Consider $\mathbb{Z}/n\mathbb{Z}$; the set of left cosets of $n\mathbb{Z}$, under addition. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the set of subsets of $\mathbb{Z}/n\mathbb{Z}$, where the representatives are coprime to n. For example, if $n = 6$, then $(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}$; if $n = 15$, then $(\mathbb{Z}/15\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$. By definition, $\left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \varphi(n)$. We claim that $(\mathbb{Z}/n\mathbb{Z})^\times$ forms a group under multiplication modulo n.

- 1 is coprime to any integer, so $\overline{1} \in (\mathbb{Z}/n\mathbb{Z})^\times$. We therefore have an identity.
- If a, b are coprime to n, then ab is coprime to n, so $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Recall that, e.g. $\overline{4} \times_{15} \overline{7} = \overline{28} = \overline{13}$. We therefore have closure.
- Suppose a is coprime to n, so $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. By Bezout's lemma, we have integers x, y such that $ax + ny = 1$. Looking modulo n, we get $ax \equiv 1 \pmod{n}$, so $\overline{a} \times_n \overline{x} = \overline{1}$, and $\overline{x} = \overline{a}^{-1}$. Notice that $ax + ny = 1$ implies that x is coprime to n; else the left hand side would be a multiple of n, while the right isn't. Thus $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Associativity follows from multiplication.

Thus, $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group of order $\varphi(n)$, with $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then 4.3.6 gives us our result. □

Remark 4.4.5 (Totient function) — The totient function φ was introduced by Euler in 1760. It has some very interesting properties:

- $\varphi(p) = p - 1$ if p is prime.
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.
- $\varphi(mn) = \varphi(m)\varphi(n)$.

All are worth proving in their own right.

§4.5 Exercises

You've (hopefully) done a lot of work this chapter; I'll save you from any exercises. But here is fun challenge problem: let p be a prime, and define F_n to be the Fibonacci numbers, with $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$, $n > 2$. Show that $F_{2p(p^2-1)}$ is divisible by p. As a hint, look at 2×2 matrices modulo p, with a particular restriction on the determinants.

5 Homomorphisms and Quotient Groups

This chapter has two main aims: firstly, to introduce the concept of a homomorphism, and why it is more useful than an isomorphism; and secondly, introduce quotient groups in, what I believe, is their most natural form.

§5.1 Homomorphisms

Recall our Definition 2.1.1 of an isomorphism, and how we described it as basically just renaming elements in a systematic way. This is very useful for say exactly how groups behave: if two groups are isomorphic, they behave exactly the same. However, sometimes it is more useful to know when two groups are *similar*, rather than exactly the same. This is what a homomorphism does.

Definition 5.1.1. Let $(G, \star)$ and $(H, \circ)$ be groups. A (group) **homomorphism** is a function $\varphi : G \to H$ such that, for any $g_1, g_2 \in G$,

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Remark 5.1.2 — Notice that this makes an isomorphism just a bijective homomorphism.

Example 5.1.3 (Simple examples)

(a) Any isomorphism $G \to H$ is a homomorphism. In particular, the identity map $G \to G$ is a homomorphism.

(b) The **trivial homomorphism** sends $g \mapsto 1_H$ for all g.

(c) There is a surjective homomorphishm $\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ by $n \mapsto \overline{n}$.

(d) There is an injective homomorphism $\mathbb{Z} \to \mathbb{Z}$ by $x \mapsto 10x$. This same map is an isomorphism, if the codomain is $10\mathbb{Z}$.

(e) There is an injective homomorphism $S_n \to S_{n+1}$ by thinking of any permutation on $\{1, \dots, n\}$ as a permutation on $\{1, \dots, n+1\}$ but leaving $n+1$ as a fixed point.

(f) For any subgroup $H \leq G$, **inclusion** is a homomorphism $H \to G$ by $h \mapsto h$.

(g) There are homomorphisms $\pi_1 : G \times H \to G$ by $\pi_1(g, h) = g$ and $\pi_2 : G \times H \to H$ by $\pi_2(g, h) = h$.

Exercise 5.1.4. Verify that all of the above are homomorphisms.

I recommend rereading the example groups at the start of Chapter 1, before doing these examples.

Example 5.1.5 (Some slightly harder homomorphisms)

(a) Recall $\mathrm{GL}_n(\mathbb{R})$ from Example 1.1.13. Then the determinant map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism, as $\det(AB) = \det(A)\det(B)$.

(b) The map $\mathbb{R} \to S^1$ by $x \mapsto e^{ix}$ is a surjective homomorphism.

(c) The map $\mathbb{C}^\times \to \mathbb{R}^\times$ by $z \mapsto |z|$ is a surjective homomorphism.

(d) Let G be a group, and $a \in G$. Then the map $G \to G$ by $g \mapsto aga^{-1}$ is an isomorphism called **conjugation**.

Exercise 5.1.6. Again, verify that all of these are homomorphisms.

Of course, there are some obvious properties of homomorphisms.

Proposition 5.1.7 (Homomorphism basics)
Let $\varphi : G \to H$ be a group homomorphism. Then $\varphi(1_G) = 1_H$, $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$ and in general $\varphi(g^n) = \varphi(g)^n$

Proof. Both boring and simple. □

Question 5.1.8. Show that $\operatorname{ord}\varphi(g)$ divides $\operatorname{ord} g$ for any homomorphism φ and for any g.

Exercise 5.1.9. Determine all groups G such that $\varphi : G \to G$ by $\varphi(g) = g^2$ is a homomorphism.

Consider these two final homomorphisms:

Example 5.1.10

(a) A homomorphism $D_{12} \to D_6$ is given by $s_{12} \mapsto s_6$ and $r_{12} \mapsto r_6$.

(b) Any homomorphism $\varphi : \mathbb{Z} \to G$, for any group G is fully defined by specifying $\varphi(1)$.

This tells us something interesting: given a group G whose presentation has generators $a_1, \ldots, a_n$, we can fully define any homomorphism $\varphi : G \to H$ by specifying $\varphi(a_i)$. This is very similar to how, in linear algebra, we can define any linear map (matrix) by just specifying where the basis vectors end up. However, we still need to make sure that the homomorphism definition is satisfied.

Question 5.1.11. Show that all homomorphisms $\mathbb{Z} \to \mathbb{Z}$ are given by $x \mapsto nx$ for some integer n.

§5.2 Kernels and images

You may already be familiar with the image of a function, but I doubt that you will be familiar with the kernel.

Definition 5.2.1. Let $\varphi : G \to H$ be a group homomorphism. Then we have the following definitions.

(i) the **image** of φ is the set $\operatorname{im}\varphi = \{\varphi(g) \mid g \in G\} \subseteq H$.

(ii) the **kernel** of φ is the set $\ker\varphi = \{g \in G \mid \varphi(g) = 1_H\} \subseteq G$.

Example 5.2.2 (Our earlier examples.)
Recall Example 5.1.3.

(a) In an isomorphism φ, $\ker\varphi = \{1_G\}$ and $\operatorname{im}\varphi = H$.

(b) The trivial homomorphism is defined so $\ker\varphi = G$.

(c) Left as an exercise.

(d) Left as an exercise.

(e) Embedding S_n in S_{n+1} has a kernel of just the identity.

(f) Inclusion has the kernel of just $\{1_G\}$ and an image of H.

(g) Left as an exercise.

Question 5.2.3. Find the kernels and images of $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $n \to \overline{n}$; of $\mathbb{Z} \to \mathbb{Z}$ by $x \to 10x$; and of π_1 and π_2 as defined in Example 5.1.3.

Exercise 5.2.4. Find the kernels and images of the homomorphisms in Example 5.1.5.

Now you may have noticed something: injective homomorphism seem to have $\ker\varphi = \{1_G\}$. This is in fact always true, as is the converse.

Lemma 5.2.5 (Injective kernels)
Let $\varphi : G \to H$ be a group homomorphism. Then $\ker\varphi = \{1_G\}$ if and only if φ is injective.

Proof. Suppose $\ker\varphi = \{1_G\}$. Then

$$\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1)\varphi(g_2)^{-1} = \varphi\left(g_1 g_2^{-1}\right) = 1_H \Rightarrow g_1 g_2^{-1} = 1_G \Rightarrow g_1 = g_2,$$

so φ is injective.
Recall that $\varphi(1_G) = 1_H$ always. Thus, if φ is injective, $\varphi(g) = 1_H \Rightarrow g = 1_G$, so $\ker\varphi = \{1_G\}$. □

We have one final theorem before we move on.

Theorem 5.2.6 (Kernels and images are groups)
Let $(G, \star)$ and $(H, \cdot)$ be groups, and $\varphi : G \to H$ be a homomorphism. Then $(\ker\varphi, \star)$ and $(\operatorname{im}\varphi, \cdot)$ are groups.

Exercise 5.2.7. I highly recommend trying these proofs yourself, they aren't too tricky.

Proof. First, let us consider $\ker\varphi$. Clearly $1_G \in \ker\varphi$, so we have an identity. Also, if $g \in \ker\varphi$, then

$$\varphi\left(g^{-1}\right) = 1_H \cdot \varphi\left(g^{-1}\right) = \varphi(g) \cdot \varphi\left(g^{-1}\right) = \varphi\left(g \star g^{-1}\right) = \varphi(1_G) = 1_H,$$

so $g^{-1} \in \ker\varphi$. Associativity of $\star$ follows from G. We also have closure, as given $g_1, g_2 \in \ker\varphi$, then

$$\varphi(g_1 \star g_2) = \varphi(g_1) \cdot \varphi(g_2) = 1_H,$$

so $g_1 g_2 \in \ker\varphi$.
Now let us consider the image $\operatorname{im}\varphi$. Again, $\varphi(1_G) = 1_H$, so we have an identity. Also,

$$\varphi(g)^{-1} = \varphi\left(g^{-1}\right) \in \operatorname{im}\varphi,$$

so we have inverses. Finally, we also have closure as

$$\varphi(g_1) \cdot \varphi(g_2) = \varphi(g_1 \star g_2) \in \operatorname{im} \varphi,$$

and associativity follows from H. □

These proofs are obviously shorter using the subgroup test in Lemma 3.1.12, but I feel that it is more enlightening showing that all of the requirements hold.
We actually have a special name for both of these groups. Images we will come to later, but the kernel groups will be very important in this chapter.

Definition 5.2.8. Let G be a group. We call a subgroup $N \leq G$ **normal** if there is some homomorphism $\varphi : G \to H$ for some group H, such that $N = \ker \varphi$. We write this $N \trianglelefteq G$.

Notice that what the homomorphism is, is irrelevant. So long as there is *some* homomorphism with N as the kernel, then N is normal

§5.3 Quotient groups

Recall in Chapter 4, when we said that $\mathbb{Z}/n\mathbb{Z}$ was actually the set of cosets of $n\mathbb{Z}$ in $\mathbb{Z}$, which just happened to form a group. The aim of this section is to show you when G/H does form a group, and hopefully why. It will also hopefully give you a feeling for what G/H represents as a group.
In truth, this is not the simplest way to introduce quotient groups; in fact, it is one I have only seen done by Chen in Napkin, although he references others. The approach found in most lecture courses for maths and physics undergraduates begins with the algebraic definition that we will end with, before almost working backwards. However, I feel that this gives you a better understanding of what is going on.
We will begin with a motivating observation.

Lemma 5.3.1 (Cosets of the kernel)
Let $\varphi : G \to H$ be a group homomorphism. Let $K = \ker \varphi$. If $\varphi(g_1) = \varphi(g_2)$, then g_1 and g_2 are in the same left coset of K. If $\varphi(g_1) \neq \varphi(g_2)$, then g_1 and g_2 are in different cosets.

Proof. This is actually very simple.

$$\varphi(g_1) = \varphi(g_2) \iff \varphi\left(g_2^{-1} g_1\right) = 1_H \iff g_2^{-1} g_1 \in K \iff g_1 \in g_2 K.$$

Also, $1_G \in K$, so $g_1 \in g_1 K$. Then, by Exercise 4.2.2, $g_1 K = g_2 K$, so they are in the same coset. Equally, going from right to left, we see that two elements in the same coset must map to the same output. □

Remark 5.3.2 — Notice that anything in the image of φ gets mapped to, so must be mapped to by a whole coset.

Remark 5.3.3 — This seems to give us a link between left cosets of the kernel and the image of a homomorphism. In fact, if the left cosets form a group, this should be isomorphic to the image.

In fact, it turns out that G/N for any normal subgroup (and thus G/K for any kernel) does form a group!

Theorem 5.3.4 (Quotient groups)

Let G be a group and $N \trianglelefteq G$. Let $N = \ker \varphi$, where $\varphi : G \to Q$ is a homomorphism. Then G/N forms a group under the operation $\cdot$ defined as follows.

- Let $A, B \in G/N$. Let $\varphi(a) = q_a$ for any $a \in A$, and $\varphi(b) = q_b$ for any $b \in B$, by Lemma 5.3.1.
- Let $C \in G/N$ be the coset such that, for any $c \in C$, $\varphi(c) = q_a q_b$.
- Then we define $A \cdot B = C$.

We call this group the **quotient group**.

Proof. We must first show that the operation $\cdot$ is well-defined; that is, for any choices of $A, B \in G/N$, there is a unique coset C satisfying $A \cdot B = C$.
First, $q_a, q_b \in \operatorname{im} \varphi$ which is a group, so by closure $q_a q_b \in \operatorname{im} \varphi$. Then Remark 5.3.2 guarantees that there is a coset C which maps to $q_a q_b$. Lemma 5.3.1 then guarantees that this coset is unique. Thus, our operation is well-defined, giving us closure.
We finish with the easier task of showing that this is a group.

(i) Consider the coset N, which maps to 1_Q. By our definition of $\cdot$, this is the identity of G/N.

(ii) Associativity follows from Q being a group. $A \cdot (B \cdot C)$ is the coset mapping to $q_a (q_b q_c) = (q_a q_b) q_c$, which is also mapped to by $(A \cdot B) \cdot C$. By Lemma 5.3.1, these must be the same coset.

(iii) Inverse follows from $\operatorname{im} \varphi$ being a group. A^{-1} is the coset mapping to q_a^{-1}, which must exist as $q_a^{-1} \in \operatorname{im} \varphi$ by $\operatorname{im} \varphi$ inverse on $\operatorname{im} \varphi$.

Therefore, G/N forms a group as described. □

Question 5.3.5. Go over this again. Make sure that you fully understand it.

Remark 5.3.6 — Notice that this definition only works if N is the kernel of a homomorphism. In particular, it relies heavily on Lemma 5.3.1, which only works for kernels. Cosets of any other subgroup have no such special relationship to any homomorphisms.

Now for the simpler consequence.

Theorem 5.3.7 (First isomorphism theorem)

Let $\varphi : G \to Q$ be a homomorphism, where $N = \ker \varphi$. Then $G/N \cong \operatorname{im} \varphi$.

Exercise 5.3.8. Fill out the details of the proof yourself, if you want.

Sketch of proof. Define $\psi : G/N \to \operatorname{im} \varphi$ by sending each coset to its output in Q. □

Question 5.3.9. Show that, in particular, if φ is surjective, then $G/N \cong Q$.

Remark 5.3.10 — This, I would argue is the "correct" way to think about quotient groups: they are the group representing the image of a homomorphism. Think about how this works with $\mathbb{Z}/4\mathbb{Z}$. The homomorphism is $\gamma : \mathbb{Z} \to \mathbb{Z}$ by $\gamma(n) = n \pmod 4$. This clearly has kernel $4\mathbb{Z}$. Then, $\overline{2} = \{\ldots, -6, -2, 2, 6, \ldots\}$ is the coset $2 + 4\mathbb{Z}$ that maps to 2.

We can actually give an algebraic definition of a normal subgroup too. This is often how they are defined, before showing that any such subgroup is the kernel of a homomorphism.

Proposition 5.3.11 (Normal subgroups)
Let G be a group, and $H \leq G$. Then the following to statements are equivalent.

(i) H is the kernel of a homomorphism.

(ii) For any $g \in G$, $h \in H$, we have $g^{-1}hg \in H$. That is, $gH = Hg$.

Proof. We will show both ways separately.

(i) ($\Rightarrow$) Suppose H is the kernel of a homomorphism $\varphi : G \to Q$. Then

$$\varphi\left(ghg^{-1}\right) = \varphi(g) \cdot \varphi(h) \cdot \varphi\left(g^{-1}\right) = \varphi(g) \cdot 1_Q \cdot \varphi(g)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} = 1_Q,$$

so $ghg^{-1} \in H$.

(ii) Suppose H is such that $ghg^{-1} \in H$. Then consider the left cosets G/H, and define $\cdot$ over G/H such that $A \cdot B = C$ if $ab \in C$ for any $a \in A$, $b \in B$. Then $(G/H, \cdot)$ forms a group.

- $H = 1_G H$ is the identity.
- $(gH)^{-1} = \left(g^{-1}\right) H$, so we have inverses
- Associativity follows from G.
- $\cdot$ is well-defined. Let $A = g_1 H$, and $B = g_2 H$. Let $a = g_1 h_1 \in g_1 H$ and $b = g_2 h_2 \in g_2 H$, for some h_1, h_2. Then $C = g_1 g_2 H$ as follows:

$$ab = g_1 h_1 g_2 h_2 = g_1 \left(g_2 g_2^{-1}\right) h_1 g_2 h_2 = g_1 g_2 \left(g_2^{-1} h_1 g_2\right) h_2 = g_1 g_2 \left(h_1'\right) h_2 \in g_1 g_2 H,$$

where $g_2^{-1} h_1 g_2 = h_1' \in H$ by our property.

Finally, the homomorphism $G \to G/H$ by $g \mapsto gH$ has kernel H, so H is the kernel of a homomorphism.

□

Remark 5.3.12 — Clearly, the group we defined in part (ii) was our quotient group G/H. In fact, it is probably easier to show that it is a group using this algebraic definition of a normal subgroup. However, I find it much less informative, as it gives no intuition about what G/H is.

If you recall the conjugation isomorphism from the start of the chapter, you can now see than an alternative definition of a normal subgroup is a subgroup $H \leq G$ which maps to itself under conjugation.
If you are still confused, don't be worried. Reread the entire chapter if you have to. If, however, you prefer the idea of normal subgroups being defined by $g^{-1}hg \in H$, or even if you just want to see why that can also be seen as a natural definition, I refer you to Tim Gowers' 2011 blog post entitled "Normal subgroups and quotient groups".

Exercise 5.3.13. Using part (ii) of the proof, or otherwise, show that for G/N to be a group, N must be normal.

Question 5.3.14. Understand how an injective homomorphism $G \to H$ 'embeds' a copy of G in H.

Exercise 5.3.15. Consider some $G \times H$, and define $G' = \{(g, 1_H)\, g \in G\} \cong G$. Show that $(G \times H)/G' \cong H$, as notation would suggest.

Remark 5.3.16 — Here's an idea, more than an exerise. Suppose G is a group that has a group presentation with n generators. Recall the free group on n elements $F_n = \langle x_1, \dots, x_n \rangle$. Is there a way to write $G = F_n/N$, for some subgroup $N \trianglelefteq F_n$?

§5.4 Exercises

Exercise 5.4.1. Some problems to have a go at.

(a) Suppose G is an abelian group. Show that any subgroup $N \leq G$ is normal.

(b) Are $\langle r \rangle$ and $\langle s \rangle$ normal subgroups of D_{10}? If so, compute $G/\langle r \rangle$ and $G/\langle s \rangle$ up to isomorphism.

(c) Does S_4 have a normal subgroup of order 3?

(d) Define $\varphi : D_8 \to \mathbb{Z}/4\mathbb{Z}$ by $r \to \overline{2}$ and $s \to \overline{2}$. Find $N = \ker \varphi$. Show that $\operatorname{im} \varphi \cong D_8/N \cong \mathbb{Z}/2\mathbb{Z}$.

(e) Let G, H be finite groups such that $|G| = 1000$ and $|H| = 999$. Show that any homomorphism $G \to H$ must be trivial.

(f) Let $\mathbb{C}^\times$ be the non-zero complex numbers under multiplication. Show that there are 5 homomorphisms $\mathbb{Z}/5\mathbb{Z} \to \mathbb{C}^\times$, but only two homomorphisms $D_{10} \to \mathbb{C}^\times$, even though $\mathbb{Z}/5\mathbb{Z}$ is a subgroup of D_{10}.

(g) Find a non-abelian group G such that every subgroup of G is normal.

6 Group Actions

Most first introductions to groups describe them as being all about 'symmetry', without really defining what this means. And in a sense, this is true: dihedral groups are about rotational and reflective symmetry; symmetric groups are about the symmetry of permutation; cyclic groups are about the symmetry of repetition (think tiling). However, this is all very abstract, and ignores the wide variety of more natural interpretations of groups, being any structure with a set and appropriate operation. However, this chapter will, through something called a group action, draw the attention of groups back to the symmetries they represent.

§6.1 A motivating example

Here is an old AIME (US exam, roughly equivalent to BMO1, but slightly easier) question, that will serve as our motivation for our definitions.

Example 6.1.1 (AIME 1996)
Two of the squares of a 7×7 checkerboard are painted yellow, and the rest are painted green. Two color schemes are equivalent if one can be obtained from the other by applying a rotation in the plane of the board. How many inequivalent color schemes are possible?

Of course, this is relatively easily solvable without any group theory, as I'm sure was the intended solution. But there is a more 'natural' group theoretic interpretation. Let X be the set of $\binom{49}{2}$ possible colours. What are these rotations? In some way, $\mathbb{Z}/4\mathbb{Z} = \langle r \, r^4 = e \rangle$ is somehow 'acting' on X by sending one colouring $x \in X$ to another $r \cdot x$ by a 90° rotation. We then consider two colour schemes x, y equivalent if there is some $n \in \mathbb{Z}/4\mathbb{Z}$ such that $y = n \cdot x$.
We will make all of these ideas rigorous using the language of group actions.

§6.2 Some definitions

Definition 6.2.1. Let X be a set and G a group. A **group action** is a binary function $\cdot : G \times X \to X$ which lets a $g \in G$ send an $x \in X$ to anothe $g \cdot x \in X$. It must satisfy the axioms

(i) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$, and

(ii) $1_G \cdot x = x$,

for any $g_1, g_2 \in G$ and $x \in X$.

Example 6.2.2 (Some group action examples)

(a) The group $\mathbb{Z}/4\mathbb{Z}$ can act on the ways to colour a 7×7 checkerboard yellow and green by rotation.

(b) In fact $\mathbb{Z}/4\mathbb{Z} = \langle r \mid r^4 = e \rangle$ can act on $\mathbb{R}^2$ by $r \cdot (x, y) = (y, -x)$; that is, a 90° rotation.

(c) The dihedral group D_{2n} acts on colourings of the verices of a regular n-gon, and K_4 acts on the colourings of the vertices of a rectangle.

(d) The group S_n acts on the set $X = \{1, \ldots, n\}$ by $\sigma \cdot x = \sigma(x)$.

(e) Any group $(G, \star)$ can act on itself (or rather, the set G), by $g \cdot g' = g \star g'$.

(f) The additive group of the real numbers $\mathbb{R}$ acts on the phase space of "well-behaved" systems in classical mechanics by time translation.

Question 6.2.3. Why do we only need to specify $r \cdot x$ when working with $G = \mathbb{Z}/4\mathbb{Z} = \langle r \,|\, r^4 = e \rangle$?

If you know about equivalence relations, think of orbits as equivalence classes. If not, then we have the following definition.

Definition 6.2.4. An **orbit** of an element $x \in X$ under $\cdot$ is the set

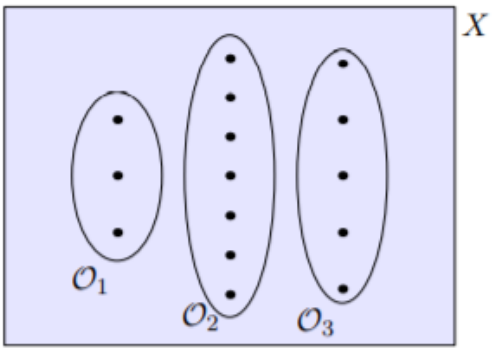
$$G \cdot x = \{g \cdot x \,|\, g \in G\} \subseteq X.$$

We typically denote orbits with the symbol $\mathcal{O}$; I will also use my own notation of $\mathcal{O}_x$ for $G \cdot x$, the orbit containing x.

This means that two elements $x, y \in X$ are in the same orbit if there is a $g \in G$ such that $y = g \cdot x$.

Question 6.2.5. Show that if $y \in G \cdot x$, then $x \in G \cdot y$. Thus, orbits partition X into distinct sets.

Here's a vaguely helpful diagram.



A highly related concept is that of a stabiliser.

Definition 6.2.6. The **stabiliser** of an element $x \in X$ is the set

$$\mathrm{Stab}_G(x) = \{g \in G \,|\, g \cdot x = x\} \subseteq G.$$

That is, $\mathrm{Stab}_G(x)$ is the set of elements in G which do not affect x.

Question 6.2.7. Show that $\mathrm{Stab}_G(x)$ is a subgroup of G for any x.

Remark 6.2.8 (Non-standard notation) — The typical notation is $G \cdot x$ for an orbit and G_x for a stabiliser. However, I find this unnecessarily confusing, so I tend to stick to $\mathcal{O}_x$ and $\mathrm{Stab}_G(x)$. Nevertheless, I do introduce $G \cdot x$ for an orbit, as that almost functions as a definition. You may also come across the notation $\mathrm{Orb}(x)$.

A very important thing to remember: for any orbit $\mathcal{O}$, $\mathcal{O} \subseteq X$, while any stabiliser $\mathrm{Stab}_G(x) \leq G$; they take elements from different sets.

Example 6.2.9 (AIME 1996)

We return to our AIME problem. We now see that the question is asking for the number of orbits under $\mathbb{Z}/4\mathbb{Z}$, as two elements in the same orbit can be mapped to each other by a rotation, so are equivalent.
Let x be the configuration where two opposite corners are coloured yellow. Clearly e fixes x, but so does a 180° rotation by r^2. Thus $\mathrm{Stab}_G(x) = \{e, r^2\} \cong \mathbb{Z}/2\mathbb{Z}$.

Now, we can prove the only important theorem in basic group actions. It was introduced to me as 'the theorem about how big an orbit is', and that is a fairly accurate description of its uses.

Theorem 6.2.10 (Orbit-stabiliser theorem)

Let $\mathcal{O}$ be an orbit, and pick any $x \in \mathcal{O}$. Let $S = \mathrm{Stab}_G(x)$ be a subset of G. Then there is a natural bijection between the elements of $\mathcal{O}$ and the left cosets of S. In particular,

$$|\mathcal{O}|\,|S| = |G|\,,$$

so every stabiliser $\mathrm{Stab}_G(o)$ has the same size, for $o \in \mathcal{O}$.

Proof. We define the mapping $\varphi : G/S \to \mathcal{O}$ by $gS \mapsto g \cdot x$. This is well-defined, as if $gS = hS$, then $h^{-1}gS = S$, so $h^{-1}g \in S$, and $h^{-1}g \cdot x = x \Rightarrow g \cdot x = h \cdot x$. Thus we can pick any representation of each coset.
We claim that this map is a bijection. First, it is an injection, as if $g \cdot x = h \cdot x$, then $h^{-1}g \in S$, so $gS = hS$. It is also a surjection by definition, as $\mathcal{O} = \{g \cdot x \mid g \in G\} = \operatorname{im}\varphi$. Thus, φ is a bijection. Therefore, $|\mathcal{O}| = |G/S| = |G| \div |S|$, and we have our result. □

§6.3 The lemma that is not Burnside's

Although Theorem 6.2.10 is the most important of the chapter, this is the crux.

Theorem 6.3.1 (Burnside's lemma, 1845)

Let G act on X. Then the number of orbits is given by

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}\,g|\,,$$

where $\mathrm{Fix}\,g = \{x \in X \mid g \cdot x = x\}$ is the elements $x \in X$ fixed under g.

Exercise 6.3.2. I highly recommend proving this yourself. It actually isn't too difficult, and is very neat. I will provide the proof, but later, as motivation for trying it yourself.

Remark 6.3.3 — As often happens in maths, Burnside's lemma was not proven by Burnside, hence its nickname 'the lemma that is not Burnside's'. Burnside attributed it to Frobenius (1887), but it appears in Cauchy's work in 1845

Example 6.3.4 (AIME 1996)

We may now finish our AIME question.
We know that $G = \mathbb{Z}/4\mathbb{Z}$ acts on our set X of $\binom{49}{2}$ possible colourings by rotation. We may now compute $\mathrm{Fix}(g)$ explicitly for our 4 elements.

- If $g = e$, we have that every colouring is fixed, so $\mathrm{Fix}(g) = \binom{49}{2} = 1176$.
- If $g = r^2$, there are exactly 24 fixed colourings, which occur when the two squares are a 180° rotation apart. This number can be found by picking any of the 48 non-centre squares, and rotating to find a valid colouring. However, each one has been counted twice, so there are 24 distinct colourings.
- If $g = r$ or $g = r^3$, there are no fixed colourings.

Thus, the number of unequivalent colours, which is the number of orbits, is given by $\frac{1176+24+0+0}{4} = 300$.

Exercise 6.3.5. (MathCounts Chapter Target Round). A circular spinner has seven sections of equal size, each of which is colored either red or blue. Two colorings are considered the same if one can be rotated to yield the other. In how many ways can the spinner be colored?
(Answer: 20)

I'll let you see the proof now.

A proof of Burnside's lemma. Consider the sum $\sum_{g\in G}|\operatorname{Fix} g|$. This is counting the number of pairs (g,x) where $g\cdot x = x$. However, we can equally find this sum by $\sum_{x\in X}|\operatorname{Stab}_G(x)|$. Thus, we get

$$\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix} g| = \frac{1}{|G|}\sum_{x\in X}|\operatorname{Stab}_G(x)| = \sum_{x\in X}\frac{|\operatorname{Stab}_G(x)|}{|G|} = \sum_{x\in X}\frac{1}{|\mathcal{O}_x|},$$

by the orbit-stabiliser theorem. But we clearly sum $\frac{1}{|\mathcal{O}|}$ once for each $y\in\mathcal{O}$, for a total $|\mathcal{O}|$ times, giving us a sum of 1 for each orbit. Thus, our sum gives us the total number of orbits. □

§6.4 Conjugation

Recall the isomorphism of conjugation from Example 5.1.5. This can equally be thought of as a group action.

Definition 6.4.1. We define the group action of **conjugation** by $:: G\times G\to G$ by $g : h\mapsto ghg^{-1}$. We call the orbits under conjugation **conjugacy classes**. We say that two elements are **conjugate** elements if they are in the same conjugacy class.

Question 6.4.2. Show that this satisfies our group action axioms.

Also, recall Exercise 2.4.1(b).

Exercise 6.4.3. Let $\tau\in S_n$ be given by

$$\tau : \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \end{pmatrix}.$$

Let $\sigma\in S_n$. Show that $\sigma\circ\tau\circ\sigma^{-1}$ is given by

$$\sigma\circ\tau\circ\sigma^{-1} : \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n) \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_{n-1}) & \sigma(a_n) \end{pmatrix}.$$

Thus, conjugation $\sigma:\tau$ doesn't really change the structure of τ, it just renames elements using σ. I won't go into it here, but remember Cayley's theorem: this isn't just symmetric groups acting nicely under conjugation, all groups do in some sense.

Example 6.4.4 (Orbits in S_n)

Intuitively, the discussion above says that two elements of S_n should be conjugate if they have the same "shape", regardless of what the elements are named. The right way to make the notion of "shape" rigorous is cycle notation. Consider the permutation $\sigma_1 \in S_5$ given by

$$\sigma_1 = (1\,3\,5)(2\,4).$$

It is conjugate to $\sigma_2 \in S_5$ given by

$$\sigma_2 = (1\,2\,4)(3\,5)$$

by renaming. In particular, if $\pi = (2\,3)(4\,5)$, then $\pi : \sigma_1 = \sigma_2$.
Thus, by renaming in the right way, we get that the orbit of σ_1 is the set of permutations of the form

$$(-\ -\ -)(-\ -).$$

More generally, you can show that two elements of a symmetric group are conjugate, and so in the same conjugacy class, if and only if they have the same "shape" in cycle notation.

A sometimes useful structure is the following.

Definition 6.4.5. Let G be a group. Then the **centre** of G, denote $Z(G)$, is the set of elements $x \in G$ such that $xg = gx$. More succinctly,

$$Z(G) = \{x \in G \mid gx = xg \text{ for all } g \in G\}.$$

Question 6.4.6. Check that this is a subgroup of G. Show that in fact, $Z(G) \trianglelefteq G$.

Question 6.4.7. What are the conjugacy classes of the elements in $Z(G)$?

This gives us a not-very-interesting corollary.

Corollary 6.4.8 (Conjugacy classes in abelian groups)

If G is abelian, then the conjugacy classes all have size one.

Question 6.4.9. Not that hard.

□

§6.5 Exercises

Exercise 6.5.1. Some problems to have a go at.

(a) WITHOUT USING GROUP ACTIONS, determine the number of rotational symmetries of a cube. Now translate your idea into the language of group actions.

(b) Find the number of different types of circular necklaces that could be made from three black and three white beads. Do not count as different a necklace N_2 that could be obtained by rotating or flipping over a necklace N_1.

(c) Taotao wants to buy a bracelet consisting of seven beads, each of which is orange, white or black. (The bracelet can be rotated and reflected in space.) Find the number of possible bracelets.

(d) Using the same idea as above, find an alternative proof of Fermat's little theorem. Hint: consider a bracelet of p beads of a colours.

(e) Find the number of different colourings of the faces of a regular tetrahedron with two white faces and two black faces. Do not count as different a tetrahedron T_2 that could be obtained by rotating a tetrahedron T_1.

(f) Find the number of ways of painting a cube using only 3 colours. Two colourings are considered the same if one can be rotated into another.

(g) How many different chemical compounds can be made by attaching H, CH_3, or OH radicals to the each of the carbon atoms in a hexagonal benzene ring? Do not count as different a compound C_2 that could be obtained by rotating or reflecting a compound C_1.

(h) Show that two elements in the same conjugacy class have the same order.

(i) Let G be a finite group. We define the **centraliser** $C_G(x) = \{g \in G \,|\, xg = gx\}$ for each $x \in G$. Show that

$$|G| = |Z(G)| + \sum_{s \in S} \frac{|G|}{|C_G(s)|},$$

where $S \subseteq G$ is defined as follows: for each conjugacy class $\mathcal{O} \subseteq G$ with $|\mathcal{O}| > 1$, we pick one representative element if $\mathcal{O}$ and add it to S.

(j) Assume G is a finite group and p is the smallest prime dividing its order. Let H be a subgroup of G with $|G| \div |H| = p$. Show that H is normal in G.

A hint for the final exercise: if you want to use orbit-stabiliser, let H act on G/H. Else, define a homomorphism from $G \to S_p$ with H as a kernel.