Clarkson Institute Summer School: Group theory

Notes by James Moore
Email: jmm232@cam.ac.uk

Chapter 1

Groups: definitions, examples, and isomorphism

Many objects in mathematics have similar properties under certain operations, despite seeming very different. For example, consider the set of complex numbers (excluding zero) under multiplication, and the set of n-dimensional real vectors under vector addition. These two sets and operations both satisfy very similar rules:

Complex numbers, excluding zero	**n-dimensional vectors**
If z, w are complex numbers, then their product is also a complex number: $z \cdot w$.	If $\mathbf{v}, \mathbf{w}$ are vectors, then their sum is also a vector: $\mathbf{v} + \mathbf{w}$.
Given three complex numbers z, w, u, it does not matter where we put the brackets in a product. We have: $$z \cdot (w \cdot u) = (z \cdot w) \cdot u.$$	Given three vectors $\mathbf{v}, \mathbf{w}, \mathbf{u}$, it does not matter where we put the brackets in a sum. We have: $$\mathbf{v} + (\mathbf{w} + \mathbf{u}) = (\mathbf{v} + \mathbf{w}) + \mathbf{u}.$$
There is a complex number, 1, satisfying: $$1 \cdot z = z = z \cdot 1$$ for all complex numbers z.	There is a vector, $\mathbf{0}$, satisfying: $$\mathbf{0} + \mathbf{v} = \mathbf{0} = \mathbf{v} + \mathbf{0}$$ for all vectors $\mathbf{v}$.
For every complex number $z \neq 0$, there is a complex number $1/z$ satisfying: $$z \cdot (1/z) = 1 = (1/z) \cdot 1.$$	For every vector $\mathbf{v}$, there is a vector $-\mathbf{v}$ satisfying: $$\mathbf{v} + (-\mathbf{v}) = \mathbf{0} = (-\mathbf{v}) + \mathbf{v}.$$

The modern mathematical subject of *abstract algebra* unifies seemingly distinct sets and operations such as these. It does so by studying the *algebraic rules* that structures have in common, rather than studying the structures individually. By studying the algebraic rules in their own right, we can deduce properties of many different structures in mathematics at the same time (e.g. properties applying to complex number multiplication, and also to vector addition).

The most basic example of a collection of algebraic rules are the four *group axioms*;[1] when we study the group axioms we are doing *group theory*, the subject of this course. The properties we compared above are the group axioms, which we shall formalise shortly.

Perhaps most surprisingly, the group axioms are satisfied by all sets of *symmetries* of objects. This means that people often refer to group theory as the 'study of symmetry', and this is a key idea which will emerge throughout the text.

[1] More advanced common examples include the axioms for rings, fields, vector spaces, and modules.

In this introductory chapter, we shall cover the following:

- First, we shall define a *group*, a set with an algebraic operation which satisfies the *group axioms*. We shall define the terms *order of a group* (referring to the group's size) and *Abelian groups* (which satisfy an additional, important axiom).
- In the main part of the chapter, we shall give many examples of groups, some familiar and some unfamiliar. The examples we shall cover are the following:
  - Groups of numbers: the integers, rationals, reals, and complex numbers under addition and multiplication; modular groups of integers under addition and multiplication; quaternions.
  - Groups of symmetries: the cyclic group of rotations; the dihedral group of rotations and reflections; the chiral and full tetrahedral groups.
  - Groups of matrices: $n \times n$ matrices under addition and matrix multiplication; some finite groups of matrices.
- Finally, we shall introduce the idea of two groups being the 'same' - *isomorphism*. This helps to motivate one of the central tasks for the first part of the course: classifying groups of small order up to isomorphism.

1.1 Definition of a group

Following on from the introductory motivation, we shall begin with the formal mathematical definition of a group.

Definition 1.1: A *group* is a set G together with a *binary operation* $*$ (a rule for combining two elements of G to produce something new) satisfying the following four properties, called the *group axioms*:

(G1) *Closure.* For all $x, y \in G$,[2] we have $x * y \in G$. That is, when we combine two elements x, y under the binary operation, then we stay in the original set.

(G2) *Associativity.* For all $x, y, z \in G$, we have:

$$(x * y) * z = x * (y * z).$$

That is, it does not matter where we place the brackets in the multiplication of three elements, so we can unambiguously write $x * y * z$.

(G3) *Identity.* There exists some special element, $e \in G$, such that for all other elements $x \in G$, we have:

$$e * x = x \qquad \text{and} \qquad x * e = x.$$

(G4) *Inverses.* For each element $x \in G$, there exists a special element $x^{-1} \in G$ such that:

$$x * x^{-1} = e \qquad \text{and} \qquad x^{-1} * x = e,$$

where e is the identity element from axiom (G3).

[2] The symbol $\in$ means 'is a member of the set'.

These four basic rules, whilst deceptively simple, contain lots of rich mathematics which we shall explore in subsequent chapters. We start here by focussing on examples though - this helps us understand the definition further, and also gives us lots of examples to play with when we study the general theory in later chapters.

We have now already seen two examples: the set of complex numbers excluding zero forms a group under multiplication, and the set of vectors forms a group under addition. We will see many more throughout this chapter.

Before diving in further, though, it is useful to make two further definitions about groups.

> **Definition 1.2:** The *order* of a group G is the number of elements in the group. If there are infinitely many elements, the group is said to have *infinite order*. The order is often written as $|G|$.

The two groups we have seen so far, the complex numbers excluding zero, and the set of vectors, are both *infinite order* groups. We will see lots of examples of both infinite order and finite order groups later in this chapter.

> **Definition 1.3:** An *Abelian group* is a group G satisfying the addition fifth axiom:
>
> (G5) *Commutativity.* For all $x, y \in G$, we have:
>
> $$x * y = y * x.$$
>
> That is, it does not matter the order in which we multiply elements in the group.

The two groups we have seen so far are also both Abelian groups. This is because for any two complex numbers z, w, we have $z \cdot w = w \cdot z$. For any two vectors $\mathbf{v}, \mathbf{w}$, we have $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$. Not all groups are Abelian though - we will see an example in the next section.

1.2 Examples of groups from arithmetic

Similar to our complex number example, many familiar examples of groups come from basic arithmetic:

- **The integers, rationals, reals, and complex numbers under addition.** The set of integers, written $\mathbb{Z}$, is a group under the operation of addition. Checking each of the axioms in turn, we have:

  (G1) *Closure.* Given two integers a, b, we have $a + b$ is an integer.

  (G2) *Associativity.* Given three integers a, b, c, we have $(a + b) + c = a + (b + c)$.

  (G3) *Identity.* The identity is 0, since for all integers a, we have $0 + a = a = a + 0$.

  (G4) *Inverses.* The inverse of the element a is $-a$, since $a + (-a) = 0 = (-a) + a$.

  Similarly, the set of rational numbers $\mathbb{Q}$ is a group under addition, the set of real numbers $\mathbb{R}$ is a group under addition, and the set of complex numbers $\mathbb{C}$ is a group under addition.

  All of these groups have infinite order. They are also Abelian groups, since $a + b = b + a$ in all of these sets.

- **The rationals, reals, and complex numbers under multiplication.** The set of rationals excluding zero, written $\mathbb{Q}^*$, is a group under multiplication. Checking each of the axioms in turn, we have:

  (G1) *Closure.* Given two rationals p, q, we have pq is a rational.

  (G2) *Associativity.* Given three rationals p, q, r, we have $(pq)r = p(qr)$.

  (G3) *Identity.* The identity is 1, which is a rational, since for all rationals p, we have $1 \cdot p = p = p \cdot 1$.

  (G4) *Inverses.* The inverse of the element p is $1/p$, which exists since p is not zero. This satisfies $(1/p) \cdot p = 1 = p \cdot (1/p)$.

  Similarly, the set of real numbers excluding zero $\mathbb{R}^*$ is a group under multiplication, and the set of complex numbers excluding zero $\mathbb{C}^*$ is a group under multiplication. Again, all of these groups have infinite order and are Abelian groups.

  Note that $\mathbb{Q}$, including zero, is *not* a group under multiplication because 0 has no inverse. Similarly, the integers excluding zero are not a group under multiplication, because - for example - 2 has no inverse.

- **The integers modulo n under modular addition.** A perhaps less familiar example of a group comes in the form of the integers modulo n, written $\mathbb{Z}_n$, under addition. The set $\mathbb{Z}_n$ is defined to be the set of all possible remainders when an integer is divided by n,

$$\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-2, n-1\}.$$

  Whenever we perform an arithmetic operation on the set $\mathbb{Z}_n$, we only keep the remainder after division by n.

  More concretely, we can consider the example of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. In this set, we have $2 + 2 = 4$, but we also have $2 + 3 = 0$, since $2 + 3$ has zero remainder when divided by 5. Similarly, we have $2 + 4 = 1$. A nice way of visualising this kind of arithmetic is to imagine that $\mathbb{Z}_5$ is represented as a clock face, as shown in Fig. 1. When we add 2 and 3, we are 'adding 3 hours to 2 o'clock' on the clock face, taking us back to 0, for example.

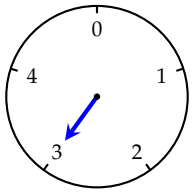

Figure 1: *A clock is a useful ways of visualising the set $\mathbb{Z}_n$; the clock face above shows the set $\mathbb{Z}_5$.*

  We can check that $\mathbb{Z}_n$ under addition is indeed a group by verifying the group axioms:

  (G1) *Closure.* If $a, b \in \mathbb{Z}_n$, then $a + b \in \mathbb{Z}_n$ by definition.

  (G2) *Associativity.* This is inherited from the associativity of addition in the full set of integers.

  (G3) *Identity.* The identity is 0, since $0 + a = a = a + 0$ for all $a \in \mathbb{Z}_n$.

  (G4) *Inverses.* The inverse of the element a is $n - a$ (for all $a = 1, ..., n-1$), since $a + (n - a) = 0 = (n - a) + a$ (and the inverse of 0 is just 0).

For finite groups like $\mathbb{Z}_n$, there is a useful visual aid to help us understand the effect of the group operation on the elements of the group.

> **Definition 1.4:** Let G be a finite group with operation $*$. The *group table* (or *Cayley table*) of the group G is defined to be a table with rows labelled by each of the group elements, and columns labelled by each of the group elements. In the (g, h)-entry of the table, we write the product $g * h$ of the group elements.

As an example, the group tables of $\mathbb{Z}_3$ and $\mathbb{Z}_4$ are shown in Fig. 2.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

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

Figure 2: *The group tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$ under addition.*

Some of the group axioms are naturally seen from a group table's structure: note that the closure of the operation is represented in the table by the entries all being drawn from the row and column labels, and the existence of an identity is represented by a row whose entries are identical to the column labels, and a column whose entries are identical to the row labels. For both of the above group tables, the symmetry of the table about the leading diagonal represents the fact that the group is Abelian.

- **The integers modulo n under modular multiplication.** Similarly, we can consider the set $\mathbb{Z}_n$ under multiplication of integers. However, here we must be more careful - usually, this set does *not* form a group!

  Let's begin by considering $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under multiplication. Constructing the candidate multiplication table, we have:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

  The table shows that if $\mathbb{Z}_4$ was a group, we would have that 1 was the identity. But then 0, for example would be non-invertible, because 1 does not appear in the 0 row or 0 column. Similarly, 2 would be non-invertible, because 1 does not appear in the 2 row or 2 column.

  To fix this problem, we introduce the set $\mathbb{Z}_n^*$, which is the set of all possible remainders when an integer is divided by n, which *also possess a multiplicative inverse*. For example, in the above we have $\mathbb{Z}_4^* = \{1, 3\}$.

  We claim that $\mathbb{Z}_n^*$ is indeed a group under multiplication; we can check the axioms as follows:

  (G1) *Closure.* Suppose that $a, b \in \mathbb{Z}_n^*$. Certainly we have $ab \in \mathbb{Z}_n$. Further, we claim that ab has a multiplicative inverse; this follows because a, b both have multiplicative inverses a^{-1}, b^{-1}. We can then construct $a^{-1}b^{-1}$ as the inverse of ab, since $(ab)(a^{-1}b^{-1}) = 1$.

  (G2) *Associativity.* This is inherited from associativity of multiplication in the full set of integers.

  (G3) *Identity.* We have that 1 is the identity, since $1 \cdot a = a = a \cdot 1$ for all $a \in \mathbb{Z}_n^*$.

(G4) *Inverses.* By definition of $\mathbb{Z}_n^*$, every element has an inverse. That is, for each $a \in \mathbb{Z}_n^*$, there exists some $a^{-1} \in \mathbb{Z}_n^*$ such that $a \cdot a^{-1} = 1 = a^{-1} \cdot 1$.

It can be shown generally that an element a of $\mathbb{Z}_n$ is in $\mathbb{Z}_n^*$ if and only if a and n are coprime (i.e. they possess no common factors, except one); this requires a bit of number theory, though, and takes us slightly off course![3] This fact tells us that the order of $\mathbb{Z}_n^*$ is the number of positive integers less than n which are coprime to n; this is the *Euler totient function* $\phi(n)$.

- **The quaternions.** To finish our survey of groups of numbers, we will give a completely unfamiliar example: the set of *quaternions*. Like the complex numbers, the quaternions extend the real numbers with some new symbols - but unlike the real numbers, the quaternions introduce *three* new formal square roots of negative one, written i, j, k, satisfying:

$$i^2 = j^2 = k^2 = -1.$$

The general form of a quaternion is $a + bi + cj + dk$ where a, b, c, d are real numbers. Now, note that unlike complex numbers, in order to work out the product of two quaternions, e.g. $(1+i)(2+j) = 2+2i+j+ij$, we need more than just i^2, j^2, k^2 to be known; we additionally need to know the products ij, ik, jk, etc.

The key relation is:[4]

$$ijk = -1. \qquad (\dagger)$$

Multiplying (†) on the right by k, we have $ijk^2 = -k$, which gives $ij = k$. Multiplying (†) on the left by ji, we have:

$$ji \cdot ijk = -ji \qquad \Rightarrow \qquad k = -ji.$$

So we see that $ij = k$, but $ji = -k$. Thus, *multiplication of quaternions is not commutative*. This should surprise you, since multiplication of complex numbers *is* commutative!

Repeatedly using the relation (†), we can similarly derive the following multiplication table for the basic quaternions i, j, k.

$\cdot$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

This allows us to compute arbitrary products of quaternions, for example the above product can be computed as $(1+i)(2+j) = 2+2i+j+k$.

It is true that the set of quaternions forms a group under addition, and the set of non-zero quaternions forms a group under multiplication, just like the complex numbers from earlier. The proof in the multiplicative case is quite long and tedious though, and involves a lot of nasty algebra - we therefore omit it from this text (you may like to attempt it as an exercise though).

[3] This can be established quickly using *Bézout's identity*, if you know it.

[4] A bit of history: the discovery of quaternions was first published in 1843 by William Rowan Hamilton (although Gauss wrote privately about them in 1819), in his quest to generalise the geometric properties of complex numbers (as scaled rotations of the plane) to three dimensions. He discovered that it was in fact impossible to introduce just two new complex units (i, j), but that three were required (i, j, k), obeying the fundamental relations given above. Three-dimensional rotations are therefore 'hidden' inside some four-dimensional space. Hamilton discovered this fact when he was walking with his wife along the Royal Canal in Dublin. He carved the relations given above with a pen-knife into a bridge on the way, which you can still see today!

More generally, Hamilton was an exceptionally interesting character, who contributed not only to the theory of quaternions, but also to fundamental physics - the *Hamiltonian* is an absolutely fundamental concept in both classical and quantum physics. He is also famous for his contribution to the variational principle governing optics. See https://www.youtube.com/watch?v=SZXHoWwBcDc&list=RDSZXHoWwBcDc&start_radio=1 for a fun summary!

However, it is quite easy to identify a small, interesting, finite subset of quaternions which form a group: the set of quaternions $\{1, -1, i, j, k, -i, -j, -k\}$ form a group under multiplication called Q_8. Its (rather lengthy) multiplication table is given below.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Figure 3: *The set of eight basic quaternions $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$ forms a group under multiplication, with the above group table. Note that it is non-Abelian, since e.g. $ij = k$ but $ji = -k$.*

1.3 Examples of groups from geometry

Next, we shall see groups arise in an area seemingly unrelated to algebra: sets of *symmetry transformations* of geometric objects. As alluded to in the introduction, the set of symmetry transformations of *any* geometric object forms a group, which is one of the reasons people often call group theory the 'study of symmetry'.[5]

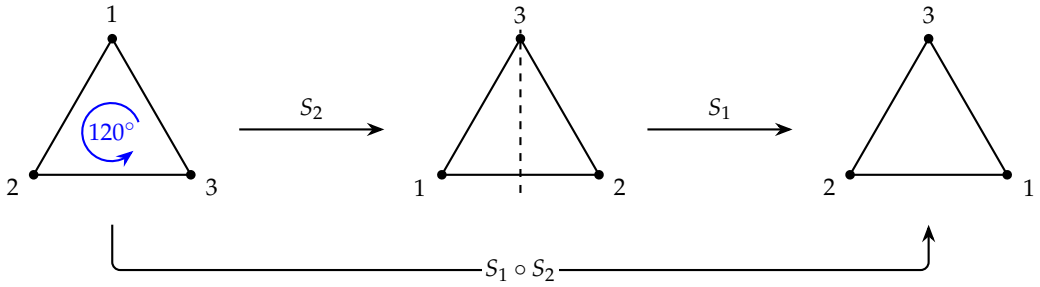

Figure 4: *An example of composition of two symmetry transformations. Here, S_2 is a rotation of an equilateral triangle by an angle 120° anticlockwise about the origin; the vertices are labelled to help track the transformation. The transformation S_1 is a reflection of the triangle in the vertical axis of symmetry. This is equivalent to some new symmetry transformation $S_1 \circ S_2$ (in this case, a reflection about the axis through the initial 2-vertex).*

In order to prove this rather remarkable fact, we must first decide on the operation which combines symmetry transformations. Whenever we deal with groups of symmetries, the operation is called *composition of symmetries*. Given one symmetry transformation, S_1, and another symmetry transformation, S_2, the *composition* $S_1 \circ S_2$ is the symmetry transformation that results from applying S_2 first, then S_1 (note the order carefully!). An example of this is given in Fig. 4.

[5] Perhaps even more surprisingly, the converse is also true: *any* group can be regarded as the set of symmetries of *some* object. This result is called *Cayley's theorem*, and we shall prove it later in the course. For example, the group $\mathbb{R}$ under addition is the set of all translational symmetries of a straight line - the real number $x \in \mathbb{R}$ tells you how much to translate by!

Now we have identified the group operation, we can prove that the set of symmetry transformations of any object form a group under composition of symmetries.

- *Closure.* If we perform a symmetry transformation S_2 followed by another symmetry transformation S_1, the resulting overall transformation $S_1 \circ S_2$ must also be a symmetry transformation (at all stages, the geometric object is left invariant). Hence the composition $S_1 \circ S_2$ is in the set, so the operation is closed.
- *Associativity.* Suppose we have three symmetry transformations S_1, S_2, S_3. Then the sequence of doing S_3 first, then S_2, then S_1 can be factored in two ways:

  $$S_1 \circ (S_2 \circ S_3) = (S_1 \circ S_2) \circ S_3.$$

  The first way regards S_2 and S_3 as a single combined transformation, while the second regards S_1 and S_2 as a single combined transformation. In either case, exactly the same three transformations are performed in exactly the same order, so the overall result is identical. Hence composition of symmetry transformations is associative.
- *Identity.* Doing nothing is a symmetry transformation - the identity, I.
- *Inverses.* A symmetry transformation is necessarily invertible; if a map S is a symmetry, it maps all points in an object to other points in the object. Each point has to be mapped to exactly once, otherwise two distinct points would occupy the same position after the transformation, or some point of the object would fail to be reached. Hence, symmetry transformations are *invertible maps*; indeed S^{-1} must exist. Moreover, S^{-1} is also a symmetry transformation, since it simply undoes the action of S, returning every point of the object to its original position. Thus every symmetry transformation has an inverse which is also a symmetry.

Now, we can give some examples:

- **Rotation groups.** The set of all rotational symmetries of a regular n-gon forms a group, called the *cyclic group of order n*, and written C_n. The elements of the group can be written as:

  $$C_n = \left\{ I, \quad R_{2\pi/n}, \quad R_{4\pi/n}, \quad R_{6\pi/n}, \quad ..., \quad R_{2(n-1)\pi/n} \right\},$$

  where I is the identity symmetry (i.e. doing nothing to the n-gon), and R_θ is an anticlockwise rotation of the n-gon about its centre by an angle θ (measured in radians).

  We know that this forms a group, because it is the set of all possible symmetries of a *directed* regular n-gon; see Fig 5. To see this, label the vertices 1 to n. A symmetry must map a vertex to a vertex, so vertex 1 has n choices as to where it can go. After this, the entire symmetry is determined, because the orientation of the n-gon must stay the same (as it has a direction).[6]

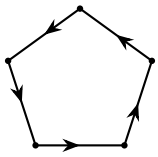

Figure 5: *A directed regular pentagon (i.e. a regular pentagon with arrows on each side); rotations are symmetry transformations, but reflections are not.*

[6]The eagle-eyed reader will have noticed that there is a bit of an issue with this argument. We could, for example, do a transformation that just scales one of the sides non-linearly - it stretches one part of the edge more than another. If we demand that distances between points are fixed by the transformation, i.e. it is an *isometry*, then the only possibilities become rotations and reflections as discussed in this chapter.

Alternatively, we can verify the group axioms directly. We notice that the composition of symmetries in this case can be expressed as the group law:

$$R_\theta R_\phi = R_{\theta+\phi},$$

where $I = R_0$, and we adjust the angle $\theta + \phi$ so that it is taken in the range $0 \leq < \theta + \phi < 2\pi$, if necessary.

Verifying the group axioms, we have:

(G1) The set is clearly closed under the operation.

(G2) Note that $(R_\theta R_\phi)R_\tau = R_{\theta+\phi}R_\tau = R_{(\theta+\phi)+\tau}$ and $R_\theta(R_\phi R_\tau) = R_\theta R_{\phi+\tau} = R_{\theta+(\phi+\tau)}$, so associativity follows from the associativity of real numbers.

(G3) The identity is $I = R_0$, since $R_\theta I = R_\theta = IR_\theta$.

(G4) The inverse of R_θ is $R_{2\pi-\theta}$, since $R_\theta R_{2\pi-\theta} = R_0 = I = R_0 = R_{2\pi-\theta}R_\theta$.

The group has finite order, n, and is Abelian.

As a more concrete example, the elements of the cyclic group C_4 are shown in Fig. 6. The group table is given in Fig. 7.

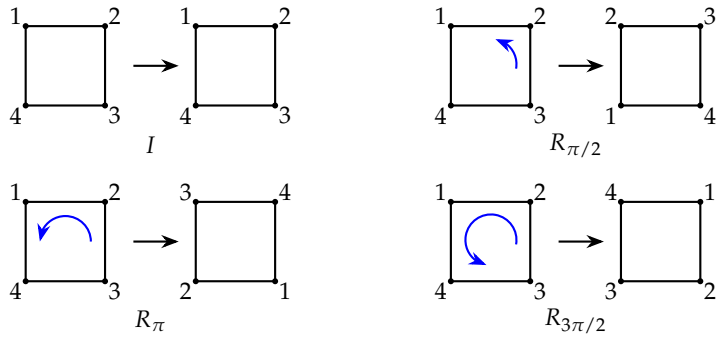

Figure 6: *The elements of the cyclic group C_4 are the rotational symmetries of a square. They consist of the identity I (doing nothing), an anticlockwise rotation $R_{\pi/2}$ by $\pi/2$, an anticlockwise rotation R_π by π, and an anticlockwise rotation $R_{3\pi/2}$ by $3\pi/2$. The transformations are shown in each of the four panels.*

$\circ$	I	$R_{\pi/2}$	R_π	$R_{3\pi/2}$
I	I	$R_{\pi/2}$	R_π	$R_{3\pi/2}$
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	I
R_π	R_π	$R_{3\pi/2}$	I	$R_{\pi/2}$
$R_{3\pi/2}$	$R_{3\pi/2}$	I	$R_{\pi/2}$	R_π

Figure 7: *The group table of the cyclic group of rotations C_4. Note that the reflectional symmetry about the leading diagonal indicates the fact that the group is Abelian.*

- **Dihedral groups.** The set of all rotational *and* reflectional symmetries of a regular n-gon form a group, called the *dihedral group of order* n, and written D_n.[7] The elements of the group can be written as:

$$D_n = \left\{ I, \quad R_{2\pi/n}, \quad R_{4\pi/n}, \quad R_{6\pi/n}, \quad ..., \quad R_{2(n-1)\pi/n}, \quad m_1, \quad m_2, \quad m_3, \quad m_4, \quad ..., \quad m_n \right\},$$

where the elements $I, R_{2\pi/n}, ..., R_{2(n-1)\pi/n}$ are the same rotations as those of the cyclic group, and the elements $m_1, ..., m_n$ are each of the reflectional symmetries.

Again, we know this is a group because it is the set of all possible symmetries of a regular n-gon (this time, without direction, as oppose to the cyclic group case). Indeed, if we label the vertices of an n-gon from 1 to n, and think about where the 1-vertex goes, we have n choices. After that, we know that the 2-vertex must be connected to the 1-vertex after the symmetry; however, there is no requirement that the original orientation is preserved, so there are two choices for where it can go. Once we have decided that, there is no more freedom; this gives the $2n$ symmetries above. Hence, the group has finite order, $2n$, as expected.

The group is also *non-Abelian* when $n > 2$. To see this, consider the effect of a rotation followed by a reflection, versus the same reflection followed by the same rotation. These give *different results in general*, as can be seen in Fig. 8. In order for agreement to be reached, if we rotate by an angle θ anticlockwise first, then reflect, this is equivalent to reflecting, then rotating by an angle θ *clockwise* instead, establishing the identity:

$$m_i R_\theta = R_{2\pi-\theta} m_i.$$

When $n = 2$, the only rotation available is R_π, and since $R_\pi = R_{2\pi-\pi}$, this problem does not occur - indeed, we shall shortly see that the group is in fact *Abelian* in this case.

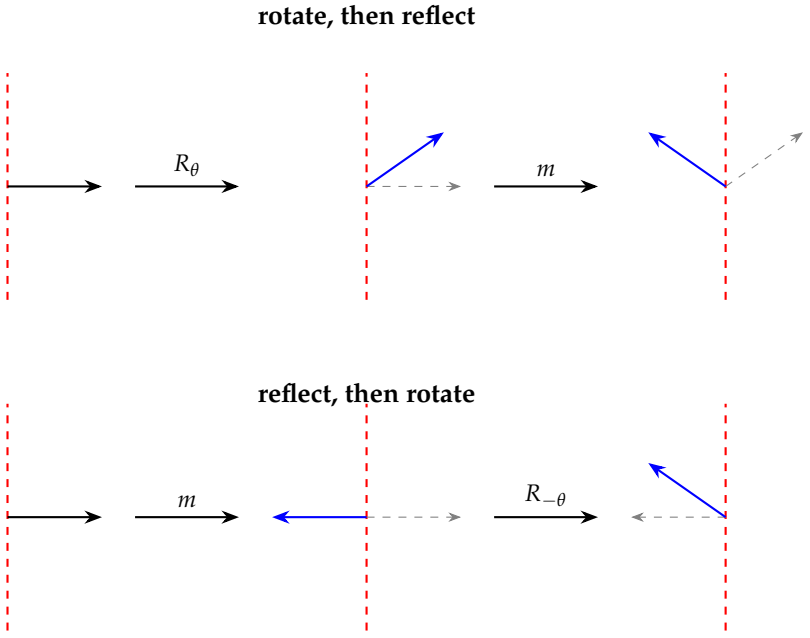

Figure 8: *A rotation by angle θ anticlockwise followed by a reflection is equivalent to first performing the reflection, but then rotating by the angle θ clockwise instead. Note that if we had used an anticlockwise rotation in the lower panel, we would have obtained inequivalent results. Hence the dihedral group is non-Abelian for* $n > 2$.

[7] Chemists use a slightly different notation; D_n is instead called C_{nv} (understood to be the group C_n together with reflections in vertical mirror planes, perpendicular to the plane of the polygon - which is the plane of a molecule in chemistry, usually).

Unhelpfully, some mathematicians also write this group as D_{2n}, rather than D_n, to emphasise the order of the group rather than the number of vertices of the n-gon. Make sure you understand which convention is being used!

A more concrete example can be constructed if we consider the case D_3, the set of reflectional and rotational symmetries of a triangle. The symmetries in D_3 are shown in Fig. 9, where the vertices of the triangle are labelled as $1, 2, 3$ to make clear the effect of the symmetry transformations in each case.

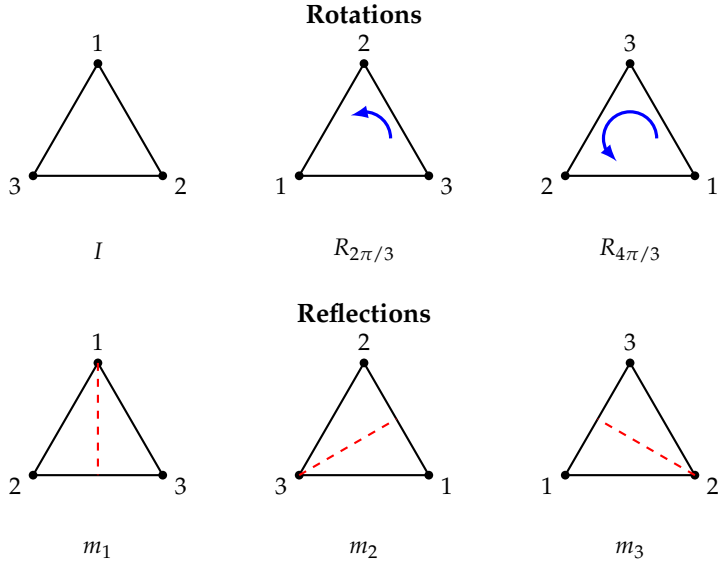

Figure 9: *The elements of the dihedral group D_3, the symmetry group of the equilateral triangle. The top row consists of the three rotations of the triangle, while the bottom row consists of the three reflections. The transformed vertex labels show the action of each symmetry. Rotations are indicated by blue arrows and reflections by dashed red axes.*

The combination of rotations follows the same rule as the cyclic group, namely $R_\theta R_\phi = R_{\theta+\phi}$, with all angles ψ restricted to lie in the range $0 \leq \psi < 2\pi$, and $R_0 \equiv I$. Meanwhile, the discussion above tells us that $R_\theta m_i = m_i R_{-\theta}$; that is, a reflection followed by a rotation is equivalent to the same rotation, but in the *opposite sense*, followed by the same reflection. Finally, we can observe that $m_i^2 = I$, since a rotation repeated twice is equivalent to doing nothing.

These facts leaves only $R_\theta m_1, R_\theta m_2, R_\theta m_3$ and $m_i m_j$ for $i \neq j$ to compute. For example, we can calculate:

$$R_{2\pi/3} m_1 = m_3$$

by considering the effect of the transformations on the triangle carefully. First, we perform the reflection m_1 which swaps the original $2, 3$ vertices. On that transformed triangle, we then rotate by an angle $2\pi/3$ anticlockwise to produce a configuration identical to that which would have been obtained by just m_3 alone. This composition is shown in Fig. 10 below.

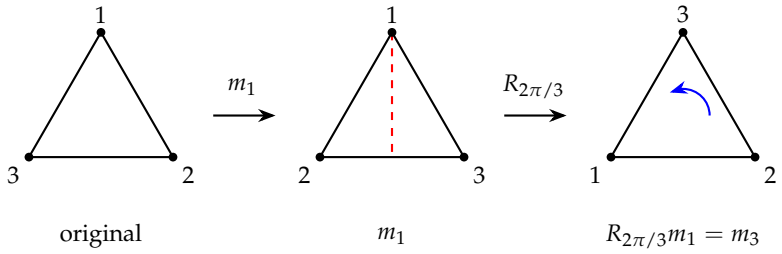

Figure 10: *The composition $R_{2\pi/3} m_1 = m_3$. First, the reflection m_1 swaps vertices 2 and 3. The resulting configuration is then rotated anticlockwise by $2\pi/3$, producing the same permutation of vertices as the reflection m_3.*

Calculating the remaining products then, we can produce the complete group table: FIX TABLE

$\circ$	I	$R_{2\pi/3}$	$R_{4\pi/3}$	m_1	m_2	m_3
I	I	$R_{2\pi/3}$	$R_{4\pi/3}$	m_1	m_2	m_3
$R_{2\pi/3}$	$R_{2\pi/3}$	$R_{4\pi/3}$	I	m_3	m_1	m_2
$R_{4\pi/3}$	$R_{4\pi/3}$	I	$R_{2\pi/3}$	m_2	m_3	m_1
m_1	m_1	m_3	m_2	I	$R_{4\pi/3}$	$R_{2\pi/3}$
m_2	m_2	m_1	m_3	$R_{2\pi/3}$	I	$R_{4\pi/3}$
m_3	m_3	m_2	m_1	$R_{4\pi/3}$	$R_{2\pi/3}$	I

Observe that constructing this table was an extremely tedious, laborious task, given we had to keep thinking about the geometry of the square. In Chapter 2 we will introduce the concept of *generators* and *relations* for groups, and hence derive a much more efficient way of calculating products of elements in dihedral groups. This is the way that we should normally construct these group tables.

- **The Klein four-group, D_2.** A particular special case of interest within the dihedral groups, that will occur repeatedly throughout the text, is the dihedral group D_2. This group is often called the *Klein four-group*, and written K_4, or the *Vierergruppe*, written V_4.

  Using our previous interpretation, this group consists of the symmetries of a 'regular 2-gon'. Evidently, this is a degenerate case - a 2-gon is a line segment. To keep things consistent with the other dihedral groups D_n though, we should think of it as two vertices $1, 2$ joined by *two* edges (mirroring the structure of the other polygons). The group then contains four symmetry transformations:

  $$D_2 = \{I, \quad R_\pi, \quad m_1, \quad m_2\}$$

  which are respectively doing nothing, a rotation by π, a reflection in the horizontal m_1, and a reflection in the vertical m_2. The transformations are shown in Fig. 11 below.

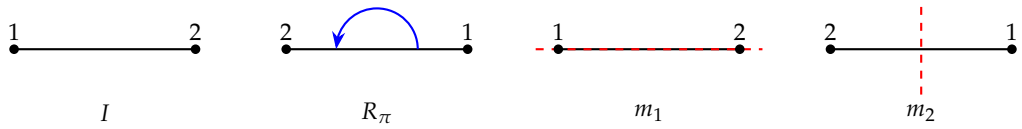

Figure 11: *The four symmetry transformations of the dihedral group D_2, also known as the Klein four-group. The object is a line segment with labelled endpoints, so that the effect of each transformation can be seen as a permutation of the labels.*

Superficially, the symmetries I and m_1 seem identical, for example - however, if we think of the vertices $1, 2$ as being connected by two edges, then I does nothing whilst m_1 swaps the edges. See Fig. 12 for a visual explanation.

Note that the viewpoint of having 'two edges' also ensures that our 'symmetry counting' arguments don't break down - here, the vertex 1 must be mapped to the vertex 1 or 2 by the transformation, so there are only two options. But, the 'two edges' can also be swapped, resulting in a total of four choices, and hence four symmetries overall.

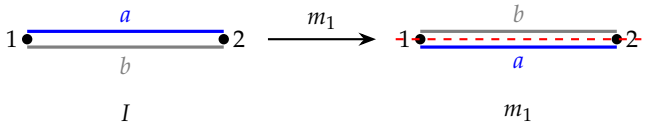

Figure 12: *Although the identity I and the horizontal reflection m_1 appear identical when the 2-gon is drawn as a line segment, they act differently on the two edges of the degenerate polygon. The reflection m_1 fixes the vertices but swaps the two edges.*

By keeping track of both the vertices, *and* the edges, the group table can be constructed as:

$\circ$	I	R_π	m_1	m_2
I	I	R_π	m_1	m_2
R_π	R_π	I	m_2	m_1
m_1	m_1	m_2	I	R_π
m_2	m_2	m_1	R_π	I

We note that D_2 is an *Abelian group*, since its group table is reflectionally symmetric about its leading diagonal. The group is of order four.

- **Chiral tetrahedral group.** The set of all rotational symmetries of a regular tetrahedron form a group, called the *chiral tetrahedral group*, written T. The set of all rotations and reflections forms a group because of the general symmetry argument we made at the start of this section. However, the set of all *rotations* can be identified as a group because they are the symmetries that *preserve the handedness of the tetrahedron*.

  By this, we mean that if we label the vertices of the tetrahedron 1 to 4, we have two options generally. One way of labelling is to choose a vertex to be the vertex 1, then put our right hand at vertex 1, point our index finger in the direction of vertex 2, our middle finger in the direction of vertex 3, and our thumb in the direction of vertex 4. Alternatively, we could do this with our left hand, putting our left hand at vertex 1, then point our *left* index finger in the direction of vertex 2, our middle finger in the direction of vertex 3, and our thumb in the direction of vertex 4. The two respective labellings are shown in Fig. 13 shown below.

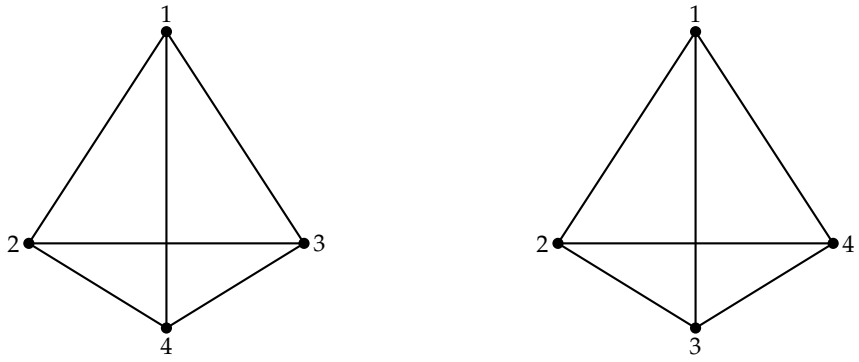

Figure 13: *The two possible handedness choices for a labelled tetrahedron. The right-handed and left-handed configurations cannot be transformed into one another by rotations alone; a reflection is required to reverse the handedness.*

If we are only allowed to perform rotations, then we *cannot* transform a left-handed tetrahedron into a right-handed tetrahedron, or vice-versa. If we could, we would suddenly have been able to transform our right-hand into our left-hand just via rotations, which is impossible! Therefore, the set of rotations alone forms a group, since it is the set of symmetries of a tetrahedron with a *fixed handedness* chosen.

To count the order of the group, we label the vertices 1 to 4. Vertices must be mapped to vertices, so the vertex 1 has four options as to where it can go. Then, vertex 2 has a choice of three options as to where it can go; after this, the handedness of the tetrahedron is fixed, as we are only allowed to use rotations, and hence the complete configuration is determined. Thus there are $4 \cdot 3 = 12$ total symmetries.

What do the elements actually look like? We can enumerate them as follows:

- There is of course the identity symmetry, I, doing nothing.
- For each vertices, we can perform either a $2\pi/3$ or $4\pi/2$ about the axis that passes through that vertex and the centre of the opposite face. This gives a total of eight symmetries. See Fig. 14 for a visualisation of the axis of rotation. There are three possible such rotations, given there are three pairs of opposite vertices.

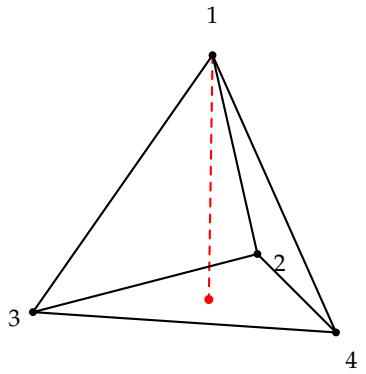

Figure 14: *An axis about which there is a three-fold rotational symmetry of the tetrahedron. Rotations by $2\pi/3$ or $4\pi/2$ around these axes give eight possible rotational symmetries of the tetrahedron, when we account for the four possible vertices through which such axes can pass.*

- The remaining symmetries are rotations by an angle π about axes which pass through the mid-points of opposite edges of the tetrahedron (these require a little bit more thinking about in your head as to why they work!). See Fig. 15 for a visualisation of the axis of rotation.

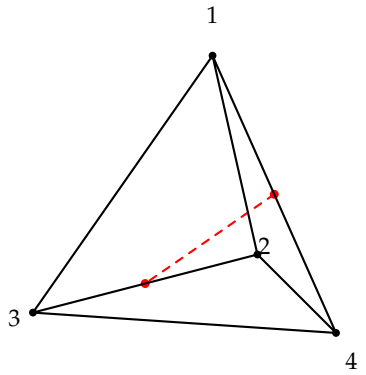

Figure 15: *An axis about which there is a two-fold rotational symmetry of the tetrahedron. A rotation by π about this axis gives one of three additional possible rotational symmetries of the tetrahedron, when we account for the three pairs of opposite vertices.*

Having identified all the symmetries, we could in principle construct the group table. This is rather tedious though, and we won't spend further time on this. Indeed, we shall actually see in Chapter 7 (when we study *permutation groups*) that there is an extremely efficient representation of the elements of this group that allow for fast calculations, bypassing the geometry altogether.[8]

[8] We shall see that the chiral tetrahedral group is in fact the same as (isomorphic to) the *alternating group* A_4, consisting of the even permutations of four symbols.

- **Full tetrahedral group.** The set of all rotational *and* reflectional symmetries of a regular tetrahedron form a group, called the *full tetrahedral group*, written T_h. This time, we don't worry about the handedness being preserved - thus, once we have mapped 1 to one of four vertices, then 2 to one of the three adjacent vertices, we have complete freedom to map 3 to either of the remaining two vertices (using a reflection to swap handedness if possible). This gives an order $4 \cdot 3 \cdot 2 = 24$ group.[9]

1.4 Examples of groups from matrix algebra

Matrix algebra also provides a plentiful sources of groups. We shall only see a couple of examples in this course; an advanced course in *Lie group theory* is the place to go for more information on matrix groups. With our quick review of matrix algebra complete, we can start to study groups of matrices.

- **Matrices under addition.** The set of all $n \times m$ (real or complex) matrices forms a group under matrix addition. Verifying each of the axioms in turn, we have:

  (G1) *Closure.* Let A, B be $n \times m$ matrices. Then $A + B$ is an $n \times m$ matrix, so the operation is closed.

  (G2) *Associativity.* Given three $n \times m$ matrices A, B, C, we have $A + (B + C) = (A + B) + C$.

  (G3) *Identity.* The identity is the $n \times m$ zero matrix 0, since we have $A + 0 = A = 0 + A$ for all $n \times m$ matrices A.

  (G4) *Inverses.* The inverse of the matrix A is the matrix $-A$, whose entries are the negatives of all the corresponding entries of the matrix A. This follows since $A + (-A) = 0 = (-A) + A$.

- **The general linear group.** The set of all invertible $n \times n$ real matrices forms a group under matrix multiplication, called the *real general linear group*, and written $GL(n, \mathbb{R})$. Verifying each of the axioms in turn, we have:

  (G1) *Closure.* The product of two invertible real $n \times n$ matrices A, B is necessarily a real $n \times n$ matrix AB. This matrix is invertible, with inverse $B^{-1}A^{-1}$ since $AB(B^{-1}A^{-1}) = I$, so the set is closed under the operation.

  (G2) *Associativity.* Matrix multiplication is associative; this can be verified directly in the case of 2×2 matrices, but can be proved generally using an argument with summation notation.

  (G3) *Identity.* The identity matrix I is clearly the identity of the operation, since $AI = A = IA$ for all matrices A.

  (G4) *Inverses.* By definition, every element of the set is invertible, with $AA^{-1} = I = A^{-1}A$.

  Similarly, the set of all invertible $n \times n$ complex matrices forms a group under matrix multiplication, called the *complex general linear group*, and written $GL(n, \mathbb{C})$. Both groups $GL(n, \mathbb{R}), GL(n, \mathbb{C})$ obviously have infinite order, but are non-Abelian.

- **Finite matrix groups.** It is also possible to have *finite* groups of matrices. Consider for example the set of matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

  Calculating all possible products of the matrices, we observe that

$$\begin{aligned} A^2 &= B, & A^3 &= C, & A^4 &= I, \\ B^2 &= I, & C^2 &= B, & C^3 &= A, \\ AB &= BA = C, & AC &= CA = I, & BC &= CB = A. \end{aligned}$$

[9] We shall see that this group is in fact the same as (isomorphic to) the *symmetric group* S_4, consisting of all possible permutations of four symbols.

Hence, the set is closed under matrix multiplication. Further, matrix multiplication is associative, the identity is included in the set, and clearly all the matrices are invertible from the above calculation. Hence this set forms a group under matrix multiplication. The group multiplication table is:

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

1.5 Isomorphic groups

Some of the groups we have seen in this chapter 'feel' inherently the same as one another. For example, consider the groups $\mathbb{Z}_4$, C_4, and the finite matrix group from the last section. They have the following group tables:

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

$\mathbb{Z}_4$

$\circ$	I	$R_{\pi/2}$	R_{π}	$R_{3\pi/2}$
I	I	$R_{\pi/2}$	R_{π}	$R_{3\pi/2}$
$R_{\pi/2}$	$R_{\pi/2}$	R_{π}	$R_{3\pi/2}$	I
R_{π}	R_{π}	$R_{3\pi/2}$	I	$R_{\pi/2}$
$R_{3\pi/2}$	$R_{3\pi/2}$	I	$R_{\pi/2}$	R_{π}

C_4

$\cdot$	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

Matrix group

The group tables are identical, except for the names of the elements; if we were to identify:

$$0 \leftrightarrow I \leftrightarrow I, \qquad 1 \leftrightarrow R_{\pi/2} \leftrightarrow A, \qquad 2 \leftrightarrow R_{\pi} \leftrightarrow B, \qquad 3 \leftrightarrow R_{3\pi/2} \leftrightarrow C,$$

then the tables are exactly the same! Therefore, it seems reasonable that we should consider them to be 'equivalent' groups.

More formally, we say that two groups G_1, G_2 are *isomorphic* (this is the word we use for 'equivalence' of group structures) if there is a mapping $f : G_1 \to G_2$ between them such that:

- f is an invertible mapping. In particular, this means that for every element $x \in G_1$, we can assign a unique element $f(x) \in G_2$. Similarly, for every element $y \in G_2$, we can assign a unique element $f^{-1}(y)$ in G_2. This gives a 'one-to-one correspondence' between the groups - our idea of 'renaming all the group elements'.

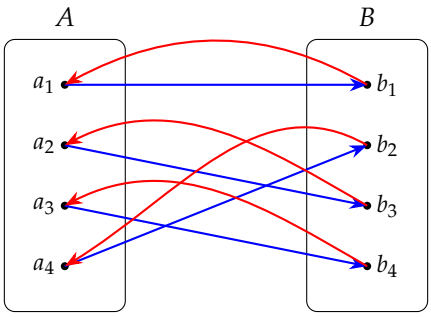

Figure 16: *An invertible function provides a one-to-one correspondence between sets. Every element of the set A is mapped to a unique element of the set B by the function f (shown in blue), and every element of B is mapped back to a unique element of A by the inverse function f^{-1} (shown in red).*

- Of course, it is not enough just to be able to rename some elements; the group tables must be the same after we have performed the renaming.

  If we have the element $x * y$ in the (x, y) position of the group table of G_1, it must be the case that in the $(f(x), f(y))$ position of the group table of G_2, we must have the renamed version of the element $x * y$. That is, we must have the key property:

$$f(x) \circ f(y) = f(x * y)$$

  for all elements x, y. We can visualise this with Fig. 17 below.

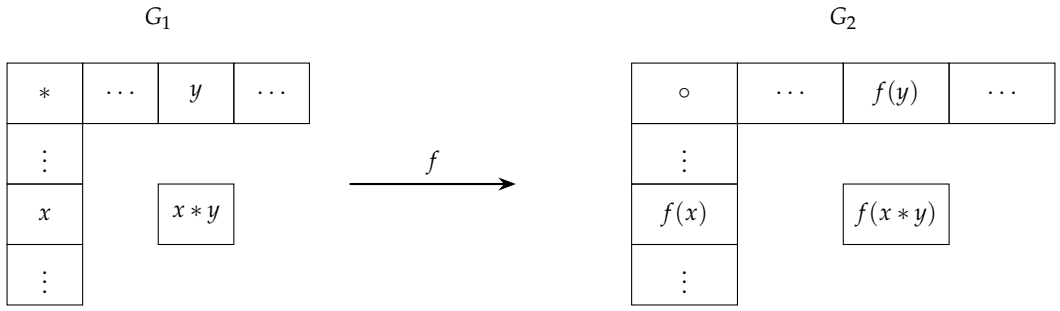

Figure 17: *An isomorphism preserves the group multiplication table. The element in the (x, y) position of the first table is $x * y$. After relabelling the elements by the bijection f, the corresponding entry in the second table must be the relabelled element $f(x * y)$, so that $f(x) \circ f(y)$ must be the same as $f(x * y)$.*

Now we have motivated and understood the idea, for clarity, let us restate this as a formal mathematical definition with the two conditions that we need to check:

> **Definition 1.5:** Let G_1, G_2 be groups with operations $*$, $\circ$ respectively. We say the two groups are *isomorphic* if there exists a function $f : G_1 \to G_2$ such that:
>
> (i) f is invertible;
>
> (ii) $f(x * y) = f(x) \circ f(y)$ for all $x, y \in G_1$.
>
> The map f is called an *isomorphism* between the groups. If two groups G_1, G_2 are isomorphic, we write $G_1 \cong G_2$.

Let's see some examples of this formal definition in action:

- Certainly it is very straightforward to check that $\mathbb{Z}_4$ and C_4 are isomorphic groups according to this definition, then: we define $f : \mathbb{Z}_4 \to C_4$ through:

$$f(0) = I, \qquad f(1) = R_{\pi/2}, \qquad f(2) = R_{\pi}, \qquad f(3) = R_{3\pi/2}.$$

  This is evidently a one-to-one correspondence, and hence invertible. We then have

$$f(x + y) = R_{(x+y)\pi/2} = R_{x\pi/2} \circ R_{y\pi/2} = f(x) \circ f(y),$$

  thus verifying the second condition. Alternatively, we can simply check that once we have performed the relabelling according to f, the group tables coincide, as we describe above. We conclude that $\mathbb{Z}_4 \cong C_4$ is an isomorphism.

- For another example, let us note that the *positive* real numbers under multiplication form a group, $\mathbb{R}^+$. We can check each of the axioms in turn:

  (G1) *Closure.* Certainly if x, y are positive reals, then their product xy is a positive real.

  (G2) *Associativity.* Multiplication of real numbers is clearly associative.

  (G3) *Identity.* The identity is clearly 1, which is a positive real number, and hence included in the set.

  (G4) *Inverses.* The inverse of x is $1/x$, since $x \cdot 1/x = 1 = 1/x \cdot x$. If x is a positive real number, then $1/x$ exists and is a positive real number, so inverses are all included in the set.

  We claim that $\mathbb{R}$, the real numbers under addition, and $\mathbb{R}^+$, the positive real numbers under multiplication, are isomorphic groups.

  We propose the isomorphism $f : \mathbb{R} \to \mathbb{R}^+$ given by:

  $$f(x) = e^x,$$

  where e^x is the standard exponential function. This is certainly invertible, since $f^{-1}(x) = \ln(x)$ is well-defined. Further, we have:

  $$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y),$$

  so the addition of real numbers is correctly translated across to multiplication of positive real numbers by the mapping f. Thus $\mathbb{R} \cong \mathbb{R}^+$ is an isomorphism.

Some general properties of isomorphisms are immediate from the definition; one we might expect is that the identity of the group G_1 must be mapped to the identity of the group G_2 by an isomorphism (we cannot 'relabel the identity' to a non-identity element!). We prove this formally as follows:

Proposition 1.6: If $f : G_1 \to G_2$ is an isomorphism, and e_1 is an identity element in G_1, then $f(e_1)$ is an identity element in G_2.

Proof: Any element in G_2 can be expressed in the form $f(x)$ for some $x \in G_1$. Hence for a generic element $f(x) \in G_2$, we have:

$$\begin{aligned} f(e_1) \circ f(x) &= f(e_1 * x) && \text{(isomorphism property (ii))} \\ &= f(x) && \text{(identity axiom of } G_1\text{)} \end{aligned}$$

Similarly, we have:

$$\begin{aligned} f(x) \circ f(e_1) &= f(x * e_1) && \text{(isomorphism property (ii))} \\ &= f(x) && \text{(identity axiom of } G_1\text{)} \end{aligned}$$

Therefore, $f(e_1)$ satisfies the properties of an identity in G_2, as required. □

Non-isomorphism of groups

We have now seen some examples of when groups *are* isomorphic. How can we prove that two groups are *not* isomorphic?

In general, this is a much more difficult task. There are many, many ways we could relabel the elements of a group G_1 as the elements of a group G_2, corresponding to many possibilities for invertible mappings $f : G_1 \to G_2$. It is very difficult to check all of them, to see that *none* of those possible relabellings could satisfy the key property $f(x * y) = f(x) \circ f(y)$.

Throughout some of the subsequent chapters, we will begin to develop some more sophisticated tools for telling whether two groups are isomorphic or not. For now though, we shall prove two of the most basic results:

- two finite groups are non-isomorphic if they have unequal size;
- if two groups are isomorphic, then they must both be Abelian, or must both be non-Abelian. That is, an Abelian group can never be isomorphic to a non-Abelian group.

The first result is almost trivial to prove:

> **Proposition 1.7:** If the group G_1, G_2 have unequal size, they are non-isomorphic.
>
> *Proof:* Suppose for a contradiction that $f : G_1 \to G_2$ is an isomorphism. Then the map f is invertible, providing a one-to-one correspondence between G_1 and G_2 as we saw in Fig. 16. Obviously this may only occur if the sets G_1, G_2 have the same size. This is a contradiction, hence G_1, G_2 could not have been isomorphic. □

This result proves that, for example, C_4 is not isomorphic to C_6 (which you probably wouldn't have expected anyway).

The second result is more involved:

> **Proposition 1.8:** If the groups G_1, G_2 are isomorphic, then G_1 is Abelian if and only if G_2 is Abelian.
>
> *Proof:* Let $f : G_1 \to G_2$ be an isomorphism. Suppose first that G_1 is Abelian. Then:
>
> $$f(y) \circ f(x) = f(y * x) = f(x * y) = f(x) \circ f(y)$$
>
> for all $x, y \in G_1$, using the isomorphism property (ii). As a result, G_2 must be Abelian, since all elements in G_2 can be expressed in the form $f(x), f(y)$ for some $x, y \in G_1$.
>
> Conversely, suppose that G_2 is Abelian. Then:
>
> $$y * x = f^{-1}(f(y * x)) = f^{-1}(f(y) \circ f(x)) = f^{-1}(f(x) \circ f(y)) = f^{-1}(f(x * y)) = x * y,$$
>
> for all $x, y \in G_1$, using the isomorphism property (ii). The result follows. □

This result proves that, for example, C_6 is not isomorphic to D_3, even though they have the same size.

Chapter 2
Basic properties of group elements

We have now seen many examples of groups, emphasising their ubiquity in mathematics. In this chapter, we shall begin to understand the advantages of studying the *abstract properties* of groups, rather than the groups themselves.

In this chapter, we shall discuss the following:

- We shall begin by proving that the identity of a group is unique (that is, it cannot have two identities), and that the inverse of an element in a group is also unique. We shall also discuss how to solve equations in groups, using left and right cancellation.
- Next, we shall investigate properties of finite group tables. We shall show that all finite group tables are *Latin squares*, meaning that every element appears exactly once in every row and column of the group table. This heavily restricts the form of group tables; we will use this property to classify finite groups with order up to and including four, showing that all such groups are either cyclic or dihedral.
- Next, we shall state and prove exponent laws for group multiplication. We shall introduce the idea of *periodic elements*, and prove the surprising fact that all elements of finite groups are periodic (that is, by raising them to a high enough power, we can eventually reach the identity). We shall also prove that the period of a group element is preserved by isomorphism, giving us a test for when two groups are *non*-isomorphic.
- Finally, we introduce the idea of *generators* and *relations* for describing a group. Here, we try to express all the elements of a group in terms of powers and products of a small subset of group elements (the *generators*). This greatly simplifies the presentation of much of the algebra we do in groups - in particular, we shall introduce generators and relations for cyclic and dihedral groups, which helps us perform computations in later chapters.

2.1 Proving properties of abstract groups

This chapter is all about learning how to *prove* things abstractly in a group. We start with some basic results: the identity of a group is unique, and the inverse of an element in a group is unique. To prove these results, we are *only allowed to use the group axioms*, and we must clearly state where we use them.

> **Proposition 2.1:** The identity of a group is unique.
>
> *Proof:* Suppose that e, f are both identity elements. Then:
>
> $$\begin{aligned} e &= e * f && (\text{since } f \text{ is an identity}) \\ &= f && (\text{since } e \text{ is an identity}) \end{aligned}$$
>
> Hence $e = f$, so the identity is indeed unique. □

Note that this proof *only* used the identity axiom for groups; it follows that any set with a (closed) binary operation that has an identity necessarily has a *unique* identity.

The fact we have proved uniqueness of an identity in *any* group means we can deduce many facts about many seemingly unrelated mathematical structures. For example, in matrix algebra, we can deduce that if a matrix A satisfies $AB = B = BA$ for all matrices B, then $A = I$.

Similarly, we can prove that the inverse of a give element in a group is unique.

> **Proposition 2.2:** The inverse of an element in a group is unique.
>
> *Proof:* Suppose that x has inverses y, z. Then:
>
> $$\begin{aligned} y &= y * e && (\text{identity axiom}) \\ &= y * (x * z) && (z \text{ is an inverse of } x) \\ &= (y * x) * z && (\text{associativity axiom}) \\ &= e * z && (y \text{ is an inverse of } x) \\ &= z && (\text{identity axiom}) \end{aligned}$$
>
> Hence $y = z$, so the inverse of x is indeed unique. □

This time, we needed to use all of the group axioms in order to prove the uniqueness of inverses. And again, we can use this fact to deduce facts about many mathematical structures. For example, in matrix algebra again, we can deduce that there is *at most* one matrix A such that $AB = I = BA$ for some fixed matrix B.

We can also think about solving equations in groups. You will see a further example in the problem set; for now, we shall show how to use the axioms to deduce the solutions of 'linear' group equations.

Proposition 2.3: Let $a, b \in G$ be fixed, given elements of a group G, and suppose that $x \in G$ is an unknown element. Then the equations:

$$a * x = b, \qquad \text{and} \qquad x * a = b$$

have unique solutions in the group.

Proof: Suppose that x satisfies $a * x = b$. Then multiplying on the left by a^{-1}, we have:

$$\begin{aligned} a^{-1} * (a * x) = a^{-1} * b \quad &\Rightarrow \quad (a^{-1} * a) * x = a^{-1} * b && \text{(associativity)} \\ &\Rightarrow \quad e * x = a^{-1} * b && \text{(inverses)} \\ &\Rightarrow \quad x = a^{-1} * b && \text{(identity)} \end{aligned}$$

So *if* there is a solution, then it is given by $x = a^{-1} * b$ (this is the *uniqueness* of a solution). Now let's assume that $x = a^{-1} * b$. Then:

$$\begin{aligned} a * (a^{-1} * b) &= (a * a^{-1}) * b && \text{(associativity)} \\ &= e * b && \text{(inverses)} \\ &= b && \text{(identity)} \end{aligned}$$

Hence, $x = a^{-1} * b$ solves the equation (this is the *existence* of a solution).

The same can be done with $x * a = b$, with unique solution $x = b * a^{-1}$; we leave this as an exercise to the reader. □

We shall shortly use this property to prove something interesting about finite group tables.

On the problem sheet, you will continue to prove properties of abstract groups; one of the most important that you shall see is the *generalised associative law*. We already know that one of the group axioms is that it does not matter where brackets are placed in the product:

$$a * b * c.$$

This generalises to n elements; it does not matter where brackets are placed in the product:

$$a_1 * a_2 * a_3 * ... * a_n.$$

Proposition 2.4: (**The generalised associative law**) In a group, all possible placements of brackets in the product:

$$a_1 * a_2 * a_3 * ... * a_n,$$

where $a_1, ..., a_n$ are group elements, leads to the same resulting group element.

Proof: By induction; see problem sheet. □

2.2 Properties of group tables

In the first section of this chapter, we proved properties that hold true in *all* groups. By restricting to finite groups, we can say more about the properties of groups.

One way we can do this is by considering the allowed structure of group tables. For example, we already know that a group needs a unique identity, so there must be one row and one column of a group table which matches the header row and header column, respectively. Without loss of generality, we usually take these to be the first row and first column respectively.

We can say more by using the 'equation solving' proposition we proved above; using this property, we can show that every group table is necessarily a *Latin square*:

> **Proposition 2.5:** (**The Latin square property**) Every group table is a *Latin square*: each element appears exactly once in each row and column.
>
> *Proof:* Let g, h be any two group elements. We shall show that h appears in row g exactly once. We seek a column x such that:
>
> $$g * x = h.$$
>
> But, by the 'equation solving' proposition from earlier, we know that this equation has a unique solution. So indeed there is exactly one column index for which h appears in row g. Similarly, every element appears exactly once in every column. □

You can readily verify that every group table we have seen so far is indeed a Latin square. Importantly, however, the converse is *not* true: not every Latin square is a group table. The smallest counterexample occurs at order five.

Remarkably, using the Latin square property, we can *classify* all possible finite groups up to order four (up to isomorphism). It turns out that the only possibilities are cyclic and dihedral groups.

> **Proposition 2.6:** The complete list of finite groups, up to isomorphism, up to and including order four is the following:
>
> - *Order 1.* C_1.
> - *Order 2.* C_2.
> - *Order 3.* C_3.
> - *Order 4.* C_4 and D_2.
>
> *Proof:* For order one, the only possible Latin square is obviously:
>
> | $*$ | e |
> |---|---|
> | e | e |
>
> This is clearly isomorphic to the cyclic group C_1, consisting only of the identity element.
>
> Similarly, for order two, the only possible Latin square (with an identity row and column) is:
>
> | $*$ | e | a |
> |---|---|---|
> | e | e | a |
> | a | a | e |
>
> This is clearly isomorphic to the cyclic group C_2, which has elements $\{I, R_\pi\}$.[10]

For order three, we can start constructing a Latin square with an identity row and column as:

$*$	e	a	b
e	e	a	b
a	a		
b	b		

Note that in the (a, a) entry, we could choose to put e or b. But if we put e, we would be forced to put b in the (a, b) entry, which would contradict the Latin square property. This implies that the completed Latin square is:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

This is clearly isomorphic to the cyclic group C_3, with $e \mapsto I$, $a \mapsto R_{2\pi/3}$ and $b \mapsto R_{4\pi/3}$, for example.

Finally, for order four, assuming an identity row and column, the Latin square must take the initial form:

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Let's now think about the position of b in the a row: it has two possibilities, either in the a column or the c column. Breaking into sub-cases then:

- If we put it in the a column, then the positions of c, e are forced in the row too, and indeed the a column. We are left with the table:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c		
c	c	e		

  Now, the positions of the remaining elements are also forced by the Latin square property. We end up with:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

  This is isomorphic to the cyclic group C_4, with $e \mapsto I$, $a \mapsto R_{\pi/2}$, $b \mapsto R_{\pi}$, $c \mapsto R_{3\pi/2}$.

- If we put b in the c column, we have two choices for filling in the remaining parts of the Latin square. Skipping some steps, we have the three possibilities:

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

  To finish, we note that the second group table represents a group that is isomorphic to D_2. Further, by swapping the b, c columns and rows in the third group table, we again get a group that is isomorphic to D_2. Finally, by swapping the b, c columns and rows in the first group table, we get a group that is isomorphic to C_4.

Technically, we still need to show that C_4 is *not* isomorphic to D_2; we shall shortly show this by considering *element orders*, however. □

We will continue to classify finite groups in the next chapter; in fact, we shall see that up to order seven, there are only cyclic and dihedral groups. Order eight is when things first begin to get interesting!

2.3 Power laws and periodicity

Have you noticed how annoying it is to continuously write $a * b$ and $x * y$, where $*$ is a group operation? From now on, let's leave it implied:

Definition 2.7: In a group G with operation $*$, if it is clear from context, we write the product $x * y$ of two elements $x, y \in G$ as:

$$xy,$$

where the $*$ is left implied. Note, we do *not* usually do this for groups where the operation is 'addition' $+$ (like the real numbers under addition, or a set of vectors under addition).

Similarly, we also introduce notation for the *powers* of a group element, involving repeated multiplication of a group element with itself.

Definition 2.8: We define the *powers* of a group element g in a group G with operation $*$ via:

$$g^n := \begin{cases} \underbrace{g * g * \ldots * g}_{n \text{ times}}, & \text{if } n > 0 \text{ is a positive integer,} \\ e, & \text{if } n = 0, \\ \underbrace{g^{-1} * g^{-1} * \ldots * g^{-1}}_{-n \text{ times}}, & \text{if } n < 0 \text{ is a negative integer.} \end{cases}$$

Note, this definition requires the expressions $g * g * \ldots * g$ and $g^{-1} * g^{-1} * \ldots * g^{-1}$ to be unambiguous; that is, we require the generalised associative property.

[10] Famously, C_2 is the most romantic group. You can find out more here: https://www.youtube.com/watch?v=p84FPXA1_Jk&list=RDp84FPXA1_Jk&start_radio=1.

This basic definition immediately implies the standard exponent laws:

Proposition 2.9: (**Exponent laws in groups**) For any integers n, m and any group element g, we have:

$$g^n g^m = g^{n+m}, \qquad (g^n)^m = g^{nm}.$$

Proof: If n, m are positive integers, in the first case we have:

$$g^n g^m = \underbrace{(g * g * ... * g)}_{n \text{ times}} * \underbrace{(g * g * ... * g)}_{m \text{ times}} = \underbrace{g * g * ... * g}_{n+m \text{ times}} = g^{n+m},$$

using generalised associativity. The other cases follow similarly. □

One interesting question we can ask about powers in groups is whether multiplying a group element by itself repeatedly eventually ends up at the identity. This is motivated by symmetry groups, for example, where performing enough of the same rotation or reflection is equivalent to doing nothing; see for example Fig. 18.

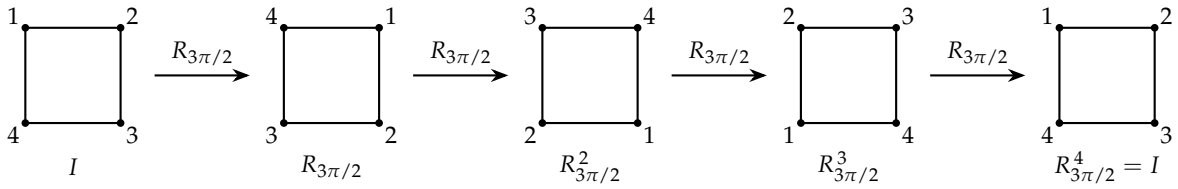

Figure 18: *Performing the rotation $R_{3\pi/2}$ on a square sufficiently many times is equivalent to doing nothing; hence the rotation $R_{3\pi/2}$ is a 'periodic' group element. In the above figure, this is shown by a sequence of $R_{3\pi/2}$ being performed multiple times to a square with vertices labelled* 1 *to* 4*.*

Making this a formal definition, we have:

Definition 2.10: Let $g \in G$ be an element of the group G, and let $e \in G$ be the identity of the group. We say that g is *periodic* if $g^n = e$ for some positive integer n. The smallest such integer is called the *period* (or more commonly, *order*) of $g \in G$.

The more common word for period is order in the mathematical literature - it is important not to get this confused with the *order* of a group, which is its size!

Some examples are the following:

- In the set of integers $\mathbb{Z}$ under addition, the only periodic element is 0. This is because:

  $$\underbrace{x + x + ... + x}_{n \text{ times}} = nx = 0$$

  if and only if $x = 0$ or $n = 0$ (not a positive integer). Note that 'powers' here correspond to adding things n times, because the group operation is *addition*, not multiplication! The order of 0 is 1.

- In the set of integers modulo 5 under multiplication, $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, all elements are periodic. The element 1 has order 1. For 2, we have:

  $$2^2 = 4, \qquad 2^3 = 3, \qquad 2^4 = 1,$$

  implying that the order of 2 is 4. Similarly, we can check that 3 has order 4, and 4 has order 2.

Surprisingly, it turns out that in a finite group, every element is periodic:

Proposition 2.11: In a finite group, every element is periodic.

Proof: Let x be any element, and consider the list:

$$x, \qquad x^2, \qquad x^3, \qquad x^4, \qquad ...$$

Since the group is finite, this list must contain only finitely many distinct entries. Hence, we must have $x^n = x^m$ for some $n < m$. Thus $x^{m-n} = e$, using the exponent laws. It follows that there is some positive integer N such that $x^N = e$; therefore, there is a least such positive integer. □

Further, the order of an element is something that is intrinsic to the element, and cannot be changed by isomorphism. This provides a useful criterion for proving that two groups are *not* isomorphic.

Proposition 2.12: Let $f : G \to H$ be an isomorphism between groups. Given any element $x \in G$, we have that x and $f(x)$ have the same order.

Proof: Let x have order n. Consider:

$$f(x^k) = f(x^{k-1})f(x) = \cdots = f(x)^k.$$

If $k < n$, then $x^k \neq e_G$, hence $f(x^k) \neq e_H$ (since an isomorphism must map the unique identity to the unique identity). However, when $k = n$, we have $f(x^n) = f(e) = e$, so $f(x)^n = e$. Thus $f(x)$ has order n. □

This is a final verification that C_4 and D_2 are not isomorphic groups; their elements have orders $\{1, 2, 4, 4\}$ and $\{1, 2, 2, 2\}$ respectively, so they cannot be isomorphic.

On the other hand, we *cannot* use this result to conclude that two groups whose elements have the same orders *are* isomorphic. The smallest counterexample happens at order 16 though, and requires a bit more machinery to construct it!

2.4 Generators and relations

The groups C_n and D_n defined in the first chapter have quite unwieldy definitions - particularly D_n, where multiplying the reflections $m_1, ..., m_n$ and the rotations requires some rather annoying geometry, for example.

This problem can be dealt with by introducing a more *algebraic* way of thinking about these groups. For example, in the cyclic group C_n:

$$C_n = \left\{ I, \qquad R_{2\pi/n}, \qquad R_{4\pi/n}, \qquad ... \qquad R_{2(n-1)\pi/n} \right\},$$

instead of writing all the elements using different symbols, we could define $r = R_{2\pi/n}$. Then all elements could be written as *powers* of r instead:

$$C_n = \left\{ r^0 = e, \qquad r, \qquad r^2, \qquad ... \qquad r^{n-1} \right\}.$$

The group multiplication becomes extremely simple now; it is just the standard exponent law:

$$r^n r^m = r^{n+m}.$$

Generators: definitions, and cyclic and dihedral examples

The above idea generalises well. Given a complicated group, we often choose a small set of elements in terms of which we write all the other elements as powers and products of these elements: this small set is called a *generating set*.

Proposition 2.13: We say that a group G has *generators* $\{g_1, ..., g_n\}$ if every element of G can be written in the form:

$$x_1^{\alpha_1} ... x_m^{\alpha_m},$$

where α_i are integers (which could be negative) and each x_i is one of $g_1, ..., g_n$.

We have just seen that the cyclic group C_n is generated by one of the rotations, $r = R_{2\pi/n}$. Similarly, we can show that D_n is generated by one of the rotations *and* one of the reflections.

Proposition 2.14: The dihedral group D_n is generated by $\{r, m\}$ where $r = R_{2\pi/n}$ and $m = m_1$.

Proof: The key algebraic relation we require is that:

$$r^{-1} m = mr. \qquad (*)$$

We saw why this was true in the first chapter; if we reflect, then rotate, this is equivalent to rotating in the opposite sense, then reflecting.

Using this relation, we note that any product of the form:

$$r^{\alpha_1} m^{\beta_1} ... r^{\alpha_n} m^{\beta_n}$$

may be transformed to the form:

$$r^{\alpha} m^{\beta}.$$

This is because if a rotation appears to the right of a reflection, it can always be moved to the left of the reflection at the cost of turning it into its inverse (which is also another rotation), using the relation $(*)$.

We now simply count how many possible elements there are of the form $r^\alpha m^\beta$. Since $r^n = e$ and $m^2 = e$, there are at most $2n$ distinct elements here. Further, if:

$$r^\alpha m^\beta = r^{\alpha'} m^{\beta'},$$

we have $r^{\alpha-\alpha'} = m^{\beta-\beta'}$. A rotation is only equal to a reflection if they are both the identity, implying that $\alpha = \alpha'$ and $\beta = \beta'$. So there are at least $2n$ distinct elements here, and indeed $\{r, m\}$ generates D_n. □

It follows that D_n can be written in the form:

$$D_n = \left\{e, \quad r, \quad r^2, \quad ... \quad r^{n-1}, \quad m, \quad rm, \quad r^2m, \quad ... \quad r^{n-1}m\right\}.$$

The first n elements are obviously the rotations (together with the 'do nothing symmetry' e), and therefore the remaining elements must be the reflections.

Having this algebraic representation of D_n can be very useful for calculations, if we remember the key relationship $r^{-1}m = mr$. For example, we can show that $r^\alpha m$ has order 2 (which we expect because it is a reflection) by calculating:

$$\begin{aligned}(r^\alpha m)^2 &= r^\alpha m r^\alpha m \\ &= r^\alpha r^{-\alpha} m^2 \qquad\qquad \text{(repeated use of } r^{-1}m = mr\text{)} \\ &= e.\end{aligned}$$

Groups generated by one element

Now we have seen the utility of generators, we might like to analyse groups in terms of them. The simplest possible case are *groups generated by one element*.

Definition 2.15: A *cyclic group* is a group which can be generated by a single element.

Unsurprisingly, the cyclic groups C_n are cyclic (hence the name). But, there is also a single infinite cyclic group, $\mathbb{Z}$.

Definition 2.16: All cyclic groups (i.e. groups generated by one element) are either isomorphic to cyclic rotation groups, C_n, or to $\mathbb{Z}$ under addition.

Proof: Let r be the generator of the group. If r has finite order n, then the elements are $\{e, r, ..., r^{n-1}\}$ and the group is isomorphic to C_n. If r has finite order, then the elements of the group are:

$$\left\{..., \quad r^{-2}, \quad r^{-1}, \quad e, \quad r, \quad r^2, \quad ...\right\},$$

which is obviously isomorphic to $\mathbb{Z}$ via the isomorphism $f(r^k) = k$. □

Group presentations

To generalise to more than one generator, we need to explain how they interact with one another. An equation constraining the multiplication of generators is called a *relation*, and we can use them to write groups in an elegant form:

> **Definition 2.17:** A *group presentation* is a representation of a group G in the form:
>
> $$G = \langle x_1, ..., x_n \mid R_1, ..., R_m \rangle ,$$
>
> where $x_1, ..., x_n$ are generators, and $R_1, ..., R_m$ are a set of constraints on the multiplication of the generators of the group. These constraints are called *relations* defining the group.

For example, we have now seen that:

- $C_n = \langle r \mid r^n = e \rangle$;
- $D_n = \langle r, m \mid r^n = e,\ m^2 = e,\ rm = mr^{-1} \rangle$.

We will not use group presentations in this text, but it is useful to know this notation as it appears fairly frequently in the mathematical literature on groups. You will examine one example of a group presentation on the Examples Sheet.

Chapter 3
Subgroup theory

We have now learned lots about the structure of general groups, and we have begun to classify all of the possible finite groups of small order (indeed, we have successfully classified all groups of orders up to and including four).

To make further progress in understanding the possible structure of groups, we now turn to a new concept: *subgroups*. Subgroups are 'smaller groups hidden inside larger groups'; understanding the possible subgroups of a group is one way of understanding the group's overall structure itself.

We shall see in this chapter that the possible subgroups of a finite group are highly constrained; the main result in this area is *Lagrange's theorem*, which says that the order of a subgroup must be a factor of the group's order. This key result will allow us to classify all groups of prime order (they are all cyclic), and allow us to classify groups of order six. We thus will know all finite groups up to order seven by the end of this chapter.

In more detail, in this chapter we shall cover the following:

- We shall introduce the definition of a subgroup, and give several examples.
- Next, we will define *cosets* of a subgroup, and explain why they *partition* the group. This is the key step in the proof of *Lagrange's theorem*, the main result in this chapter. Lagrange's theorem states that for a finite group, the order of a subgroup is a factor of the group's order. Immediately after, we deduce some simple consequences of Lagrange's theorem, namely that the order of an element in a finite group must divide the group's order.
- Next, we focus on the cyclic and dihedral groups as extended examples. We use Lagrange's theorem to classify all possible subgroups of cyclic and dihedral groups.
- We also discuss the converse of Lagrange's theorem, and give an example of why it is *false* in general. We will state and prove a partial converse to Lagrange's theorem, *Cauchy's theorem*, which guarantees the existence of subgroups of certain sizes.
- Finally, we complete the classification of small finite groups up to order seven. We do this by using Lagrange's theorem to classify all groups of prime order, and to investigate the order six case more closely.

3.1 Definition of a subgroup

As promised in the introduction to this chapter, we define a *subgroup* to be a smaller group hidden inside a larger group:

> **Definition 3.1:** Let $H \subseteq G$ be a subset of a group G. If H is a group in its own right, with respect to the same operation as the group G, then H is called a *subgroup* of G. We write $H \leq G$.

Some basic examples include the following:

- Consider the integers, rationals, reals, and complex numbers under addition. Then:
$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}.$$
- Consider the non-zero rationals, non-zero reals, and non-zero complex numbers under multiplication. Then:
$$\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*.$$
- Both C_4 and D_2 have subgroups isomorphic to C_2. One way of seeing this it to look at the group tables; we now write the group tables in terms of the generators, as per the end of the previous chapter:

$*$	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

$*$	e	r	m	rm
e	e	r	m	rm
r	r	e	rm	m
m	m	rm	e	r
rm	rm	m	r	e

  In the first table, we can spot a 'subtable' which itself is the group table of C_2; this is indicated by highlighting the rows and columns corresponding to $\{e, r^2\}$.

  In the second table, we can similarly spot a 'subtable' which itself is the group table of C_2, indicated by highlighting the rows and columns corresponding to $\{e, r\}$. However, in this case, there are multiple subgroups of size two; for example, $\{e, m\}$ would have worked equally well to produce another subgroup isomorphic to C_2. Thus, we see that subgroups of a given size are not unique (we cannot meaningfully talk about 'the C_2 subgroup of D_2', as a result).

There are also some 'obvious' subgroups of every group:

> **Definition 3.2:** Every group has the subgroup $\{e\}$, where e is the identity of the group. This subgroup is called the *trivial subgroup*.
>
> Every group G contains itself as a subgroup, G. This subgroup is called the *improper subgroup*.
>
> Subgroups which are not the identity subgroup $\{e\}$ or the whole group G are called *proper, non-trivial subgroups*.

We will see many more examples of subgroups throughout this chapter, and you will explore many more examples of subgroups on the Examples Sheet too.

3.2 Cosets and Lagrange's theorem

One of the key properties of subgroups is that they can be used to 'split up a group' into smaller, more manageable pieces. These pieces are called *cosets*.

Definition 3.3: Let $H \leq G$ be a subgroup of a group G. The *left coset of H with representative $g \in G$* is the set:

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

Similarly, the *right coset of H with representative $g \in G$* is the set:

$$Hg = \{hg : h \in H\}.$$

As some examples of left cosets, we have:

- Let $H \leq C_4$ be the subgroup $H = \{e, r^2\}$ from above. The possible left cosets are:

  $$eH = \{e, r^2\}, \qquad rH = \{r, r^2\}, \qquad r^2H = \{r^2, e\}, \qquad r^3H = \{r^3, r\}.$$

  We see that of the four left cosets, only two are distinct, since $H = r^2H$ and $rH = r^3H$. Further, all the left cosets have the same size, and if they are distinct, they are non-overlapping. We could break up C_4 as:

  $$C_4 = H \cup rH,$$

  for example.

- Let $H \leq D_2$ be the subgroup $H = \{e, r\}$ from above. The possible left cosets are:

  $$eH = \{e, r\}, \qquad rH = \{r, e\}, \qquad mH = \{m, rm\}, \qquad rmH = \{rm, m\}.$$

  Once again, of the four left cosets, only two are distinct, since $H = rH$ and $mH = rmH$. Again, the left cosets have the same size, and if they are distinct, they are non-overlapping. We could break up D_2 as:

  $$D_2 = H \cup mH.$$

This phenomonen is completely general; we prove it as follows.

Proposition 3.4: The left cosets of a subgroup $H \leq G$ of a finite group G satisfy the following properties:

(i) All left cosets have the same size.

(ii) Every element of G belongs to exactly one left coset of H; we say that the left cosets *partition* G.

Proof: (i) Let $H = \{h_1, h_2, ..., h_n\}$, and let $gH = \{gh_1, ..., gh_n\}$ be a left coset. We claim that gH has the same size as H. The only way that this could fail is if:

$$gh_i = gh_j$$

for some $i \neq j$. But then multiplying on the left by g^{-1}, we would have $h_i = h_j$, so the elements would not have been distinct in H in the first place. Hence $|H| = |gH|$ and all cosets have the same size.

(ii) Let $g \in G$ be an arbitrary element of G. Then $g \in gH$, since the identity $e \in H$, so gH contains $ge = g$. Thus every element is in *at least one* left coset.

On the other hand, suppose that $xH \cap yH$ is non-empty. Then for some elements $h_1, h_2 \in H$, we can write:

$$xh_1 = yh_2.$$

Then if $g \in xH$, for some h we can write $g = xh = xh_1h_1^{-1}h = yh_2h_1^{-1}h \in yH$. It follows that xH is completely contained in yH. Similarly, yH is completely contained in xH, and thus $xH = yH$. So two left cosets overlap if and only if they are the same coset. □

The picture of left cosets we should therefore have in our minds is that they 'cut up' a group into equal sized parcels, as shown in Fig. 19.

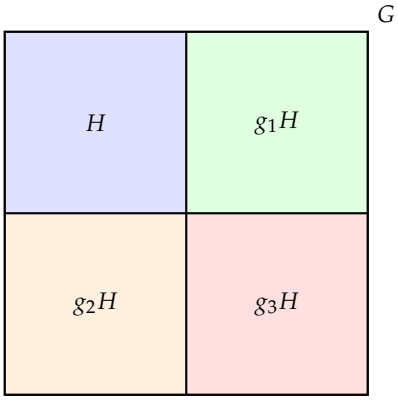

Figure 19: *The left cosets of a subgroup $H \leq G$ partition a group into subsets of equal size, covering the whole group. This is represented in the above diagram by the group G (represented as a square) being divided into four equal left cosets. The left cosets shown are H, g_1H, g_2H, and g_3H, but note that the representatives of given cosets are not unique.*

An immediate consequence of this result is the famous theorem of Lagrange:

Theorem 3.5: (**Lagrange's theorem**) In a finite group G, the order of a subgroup H is a factor of the order of the group.

Proof: Immediate from the fact that left cosets all have the same size (and $H = eH$ itself is a coset), and they partition the group. □

Lagrange's theorem places a powerful restriction on the types of subgroups that a group can have. For example, the dihedral group D_3 of a triangle can only have subgroups of size $1, 2, 3$ or 6 according to Lagrange's theorem.

An immediately useful consequence of Lagrange's theorem is the following:

Proposition 3.6: In a finite group, the order of a group element is a factor of the order of the group.

Proof: Let $g \in G$ be any element of the group G, with order n. Then:

$$\{e, \quad g, \quad g^2, \quad ..., \quad g^{n-1}\}$$

is a subgroup of G of order n. Hence n must divide the order of G, by Lagrange's theorem. □

We have already seen this is the case for some small groups, for example the orders of the elements in $C_4 = \{e, r, r^2, r^3\}$ are $\{1, 4, 2, 4\}$ respectively, and the orders of the elements in $D_2 = \{e, r, m, rm\}$ are $\{1, 2, 2, 2\}$ respectively.

3.3 Extended example: cyclic and dihedral groups

Armed with Lagrange's theorem, we can begin to understand the subgroup structure of the cyclic and dihedral groups more generally. The cyclic groups have a particularly simple subgroup structure:

Proposition 3.7: In the cyclic group C_n, there is exactly one subgroup of order m for each factor m of n, and these are all the subgroups. This subgroup is isomorphic to C_m.

Proof: Let r be a generator of C_n, so that the group can be written as:

$$C_n = \left\{e, \quad r, \quad r^2, \quad ... \quad r^{n-1}\right\}.$$

Now suppose that m is a factor of n. Then $r^{m/n}$ is an element of C_n. Further, it generates a subgroup:

$$\left\{e, \quad r^{n/m}, \quad r^{2n/m}, \quad ... \quad r^{n(m-1)/m}\right\}.$$

This is clearly isomorphic to C_m, as required. Hence, we have shown that there is at least one subgroup of size m for each factor of m of n.

By Lagrange's theorem, there can only be subgroups of order m where m is a factor of n. It remains only to show that the subgroup above is the unique subgroup of size m.

Suppose H is any subgroup of size m. If $m = 1$, then the subgroup is obviously just the identity, and hence is unique. Now suppose that $m > 1$, and let $r^k \in H$ be a non-identity element in H with k the smallest possible positive integer we can choose.

Now take any other element $r^l \in H$. Since $k < l$, we can write $l = kq + s$, for some $0 \leq s < k$ and some $q \geq 1$. Therefore, we have:

$$r^l = r^{kq+s} = r^{kq} r^s.$$

Since $r^l \in H$ and $r^{kq} = (r^k)^q \in H$, we must have $r^s = r^l r^{-kq} \in H$. But then $s = 0$ by the minimality of k. So all elements of H can be written in the form $(r^k)^q$. Thus H is a cyclic group of order m, with generator r^k. In particular, we need $r^{km} = r^n = e$, so that $k = n/m$, as required. □

Geometrically, the subgroups correspond to being able to find smaller regular polygons inscribed in larger regular polygons. For example, the group C_6 is the group of rotational symmetries of the hexagon. It has unique subgroups isomorphic to C_1, C_2, C_3 and C_6. The trivial subgroups C_1, C_6 correspond to breaking all the symmetry of the hexagon, or keeping all the symmetries of the hexagon, respectively. On the other hand, the group C_2 corresponds to being able to inscribe a straight line in the hexagon, between two of its vertices. The group C_3 corresponds to being able to inscribe a triangle in the heaxgon, between three of its vertices. See Fig. 20 for a visualisation of this.

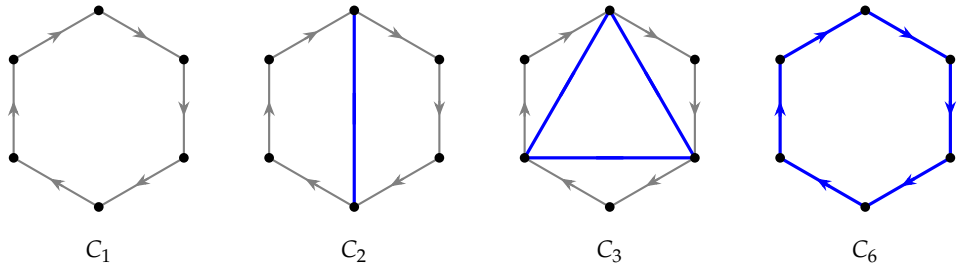

Figure 20: *The subgroups of the cyclic group C_6 correspond geometrically to regular polygons that can be inscribed in a regular hexagon using its vertices. The subgroup C_2 corresponds to an inscribed line joining opposite vertices, C_3 to an inscribed equilateral triangle, and C_6 to the hexagon itself. The trivial subgroup C_1 corresponds to the identity symmetry alone.*

Proposition 3.8: Consider the dihedral group $D_n = \{e, r, r^2, ..., r^{n-1}, m, rm, ..., r^{n-1}m\}$, written in terms of a generating rotation r and a generating reflection m. Every subgroup of D_n is one of the following:

- a cyclic group generated by $r^{n/d}$ for a factor d of n;
- a dihedral group generated by $r^{n/d}$ and $r^k m$ for a factor d of n, and $0 \leq k < n/d$ (when $d = 1$, the group is actually cyclic, and isomorphic to C_2).

Proof: If a subgroup contains no reflections, it is a subgroup of $\{e, r, r^2, ..., r^{n-1}\}$, i.e. the cyclic group C_n. This gives precisely the cyclic subgroups in the classification, using the proposition we proved above.

Now suppose that a subgroup H does contain a reflection, $r^k m \in H$, where k is the smallest non-negative integer for which this is the case. You will show on the Examples Sheet (Question 4) that $H \cap \{e, r, r^2, ..., r^{n-1}\}$ is a subgroup (the intersection of two subgroups is always a subgroup); further, this must be a cyclic subgroup, so is generated by some $r^{n/d}$ for d a factor of n. This consists of all the rotations contained in H. Now note that by closure, H needs to contain all the elements:

$$\left\{e, \quad r^{n/d}, \quad r^{2n/d}, \quad ... \quad r^{n(d-1)/d}, \quad r^k m, \quad r^{n/d+k} m, \quad ... \quad r^{n(d-1)/d+k} m\right\}.$$

Suppose now that H contains some other reflection $r^l m$, for $l > k$. Then by closure, we have that:

$$r^l m r^k m = r^{l-k}$$

is in H. This implies that $l - k = qn/d$ for some $q \geq 0$, which gives $l = qn/d + k$. Thus the only reflections contained in H are those already listed. From the list of reflections in H, we see that $0 \leq k < n/d$.

Finally, observe that this is isomorphic to a dihedral group, since $(r^{n/d})^d = e$, $(r^k m)^2 = e$ and $(r^k m) r^{n/d} = r^{-n/d}(r^k m)$, which are the defining relations of $D_{n/d}$ (or C_2 when $d = 1$). □

What do these subgroups look like concretely? Let's consider D_6, the dihedral group of the hexagon, in some detail. By the classification result, the possible subgroups are:

- The cyclic subgroups C_1, C_2, C_3, C_6 of rotations of the equilateral hexagon. These correspond to inserting inscribed polygons into a directed version of the hexagon, just as before.
- The dihedral subgroups are generated by the following combinations:
  - The trivial rotation (i.e. the identity), and each of the possible reflections $m, rm, r^2m, r^3m, r^4m, r^5m$. These give six subgroups of order two, isomorphic to C_2.
  - The 180° rotation r^3, and any of the reflections m, rm or r^2m. All of these dihedral groups are isomorphic to the dihedral group D_2.
  - The 120° rotation r^2, and either the reflection m or the reflection rm. Both of these are the dihedral groups D_3 of the triangle.
  - The 60° rotation r, and the reflection m. This is simply the full dihedral group D_6 of the hexagon again.

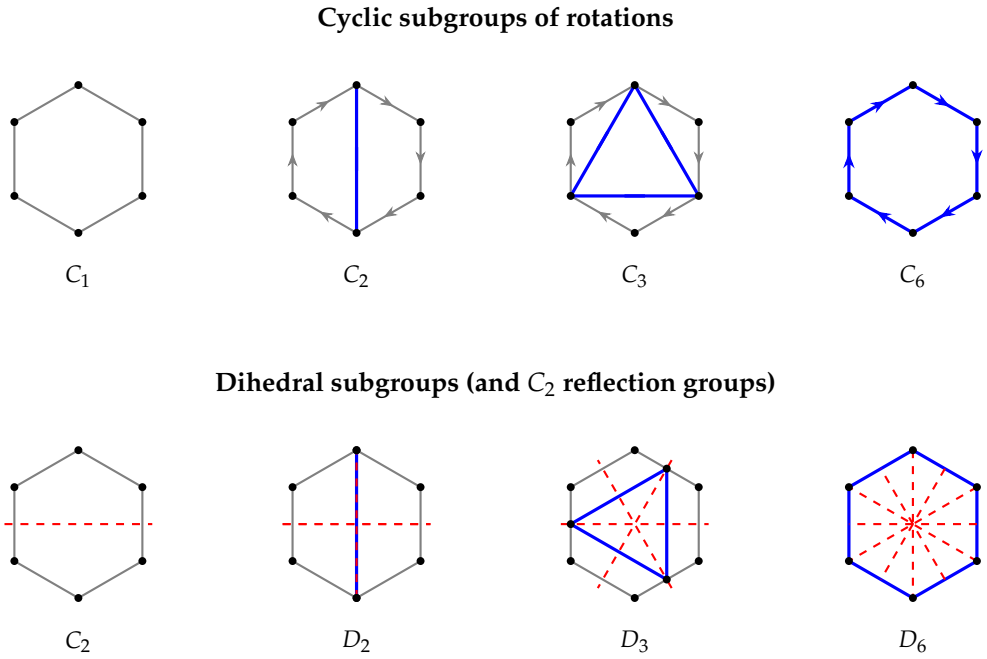

Figure 21: *The subgroups of the dihedral group D_6. The cyclic subgroups consist solely of rotations, corresponding to polygons inscribed in the directed version of the hexagon. The dihedral subgroups additionally contain reflections, indicated by dashed reflection axes. In each case we choose to use the reflection m as the generating reflection. In the first panel, this corresponds to the subgroup $\{e, m\}$. In the second panel, it corresponds to the subgroup $\{e, r^2, m, r^2m\}$. In the third panel, this corresponds to the subgroup $\{e, r, r^2, m, rm, r^2m\}$. In the final panel, the full group is the subgroup.*

3.4 A converse to Lagrange's theorem: Cauchy's theorem

So far, we have stated and proved Lagrange's theorem, which tells us that the order of any subgroup of a finite group must be a factor of the larger group's order. The *converse* of this theorem would tell us the logic works the other way around: for any factor of the larger group's order, there must be a subgroup of that order. Famously, the converse is *false* - we shall shortly see a counterexample.

Now, whilst the converse of Lagrange's theorem itself is in general false, there is a *partial* converse to Lagrange's theorem. This result is called *Cauchy's theorem*, and it says specifically that for *prime* factors of a group's order, there is always a subgroup of that order.

> **Theorem 3.9:** (**Cauchy's theorem**) Let G be a finite group. For each prime factor of the group's order, G has a subgroup of that order.
>
> *Proof:* Let p be a prime factor of the order of the finite group G. Consider the set:
>
> $$S = \left\{(x_1, ..., x_p) \ : \ x_1 x_2 ... x_p = e, \ x_i \in G\right\}$$
>
> consisting of all lists of p elements in the group whose product is the identity. First, notice that the size of this set is $|S| = |G|^p$, because there are $|G|$ choices of element for each of the p positions on the list. Therefore, p divides the size of S.
>
> Further, notice that if $(x_1, ..., x_p)$ is in the set S, then any cyclic permutation of this list is also in the set:
>
> $$(x_i, ..., x_p, x_1, ..., x_{i-1}) \in S.$$
>
> This is because $x_1 x_2 ... x_p = e$ implies $x_1 x_2 ... x_p (x_1 ... x_{i-1}) = x_1 ... x_{i-1}$, by multiplication on the right. Multiplying on the left by $(x_1 ... x_{i-1})^{-1}$, we have $x_i ... x_p x_1 ... x_{i-1} = e$.
>
> We can therefore split the set S into two parts:
>
> $$S = \left\{(x_1, ..., x_p) \ : \ x_1 x_2 ... x_p = e, \ x_i \text{ are all equal}\right\} \cup \left\{(x_1, ..., x_p) \ : \ x_1 x_2 ... x_p = e, \ x_i \text{ are not all equal}\right\}.$$
>
> The second subset here must have size a multiple of p, because of the cycling property. Since the size of S is a power of p, this implies that p divides the first subset. The first subset contains $(e, ..., e)$ so is not empty; therefore it contains some list $(x, ..., x)$ with the property that $x^p = e$ with $x \neq e$. This shows the existence of an order p element, which must generate a cyclic subgroup of order p. □

As an immediate corollary, note that this means that if p is a prime factor of the order of a finite group G, then there is an element of order p contained in the group.

Using Cauchy's theorem, we can also produce a counterexample to the converse of Lagrange's theorem:[11]

> **Proposition 3.10:** The converse of Lagrange's theorem is, in general, false.
>
> *Proof:* The smallest possible counterexample actually occurs at order 12, and is given by the chiral tetrahedral group. Suppose that the chiral tetrahedral group contains a subgroup of order six; call it H. Then by Cauchy's theorem, H must contain elements x, y of orders two and three respectively.

[11] Here, we carry out the proof using a geometric argument. It is much easier to do it algebraically, by first recognising that the chiral tetrahedral group T is isomorphic to the alternating group A_4 of permutations, which we shall see in Chapter 7. The geometric proof here also relies heavily on the idea of *conjugacy*, which is discussed in Chapter 5.

As we saw in Chapter 1, the element x of order two is necessarily a π rotation about an axis through the midpoint of two opposite edges of the tetrahedron. On the other hand, the element y of order three is necessarily a $2\pi/3$ rotation about an axis through a vertex (or a $4\pi/3$ rotation, but this is equivalent to a $2\pi/3$ in the opposite sense).

The key insight that we need is that the element of order three, y, can be thought of as permuting the axes through the midpoints of two opposite edges, as shown in Fig. 22.

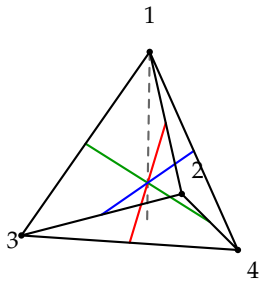

Figure 22: *The three axes through the midpoints of the tetrahedron, shown in red, green and blue, are permuted by the action of a* 120° *rotation through any symmetry axis through a vertex. For example, rotating the base face through* $2\pi/3$ *sends blue to green, green to red, then red to blue. Further rotating the base face through* $4\pi/3$ *sends blue to red, red to green, then green to blue.*

Importantly, this means that we can interpret the element $y^{-1}xy$ in the following way:

- This element first involves rotation of one of the faces. This permutes the axes through the midpoints of opposite edges.
- Next, we rotate about π through the an axis through the midpoints of opposite edges. But, given we have already swapped these axes in the first step, we are actually rotating through a *different* axis to the one we started with.
- Finally, by rotating a face in the opposite sense to the one we did originally, this restores the axes to their original configuration; albeit, having carried out a π rotation about a different axis.

Overall, $y^{-1}xy$ is a rotation by π around a different axis through midpoints of opposite signs. Similar reasoning implies that $y^{-2}xy^2$ is a rotation by π around yet another distinct axis through midpoints of opposite signs. Overall then, by closure, the subgroup H must contain all the rotations through midpoints of opposite signs.

Consider now the subset K of H given by:

$$K = \{I, R, G, B\},$$

where R, G, B are the rotations through the red, green, and blue axes in Fig. 22. By considering the transformation of the labels, it is true that $RG = B$ (a rotation about the green axis swaps $1, 3$ and $2, 4$; subsequently rotating through the red axis overall sends 1 to 4, 2 to 3, 3 to 2, and 4 to 1, equivalent to B). Overall then, we have $R^2 = I, G^2 = I$ and $RG = B$; multiplying the final relation by B on the right gives $RGB = I$. We saw on Examples Sheet 1, Question 6, that these relations imply K is a group (isomorphic to D_2).

But then $K \leq H$ is a subgroup of order four of a group of order six, which contradicts Lagrange's theorem. Hence H cannot exist, and the group indeed has no subgroup of order six. $\square$

3.5 Classification of finite groups up to order seven

Lagrange's theorem and Cauchy's theorem give us a lot of power in classifying groups. First, we can use Lagrange's theorem to easily classify all groups of prime order; indeed, all such groups are *cyclic*:

Proposition 3.11: Every group of prime order is isomorphic to a cyclic group; that is, the unique group of order p up to isomorphism is given by C_p.

Proof: Let G have order p. Then every non-identity element of G has order p, by Lagrange, since the only factors of p are 1 and p. Let $g \in G$ be any non-identity element of G. Then the elements of the group can be written as:

$$\{e, g, g^2, ..., g^{p-1}\}.$$

We cannot have $g^a = g^b$ for $a < b$, since then $g^{b-a} = e$ by the exponent laws. Therefore the group is a cyclic group of order p, isomorphic to C_p. □

We can use this fact, together with a more careful classification of groups of order six, to complete the classification of finite groups up to and including order seven:

Proposition 3.12: The complete list of finite groups, up to isomorphism, of orders five, six, and seven are:

- Order 5: C_5.
- Order 6: C_6 and D_3.
- Order 7: C_7.

Proof: Orders five and seven are done by the previous proposition, since five and seven are prime.

It remains to consider the order six case. If there is an element of order six, then the group is isomorphic to C_6. Hence, we may assume by Lagrange's theorem that the only element orders are one, two and three.

By Cauchy's theorem, there must be an element m of order two and an element r of order three. Let $H = \{e, r, r^2\}$ be the subgroup generated by r; note that m is not contained in this set, because r, r^2 both have order three. Now, consider the left cosets:

$$H, \qquad mH.$$

Since $m \notin H$, we must have that these cosets are distinct and therefore are unequal and cover the group. To finish, note that the right cosets H, Hm also partition the group, so by comparison with the left cosets, we must have $mH = Hm$, so that:

$$\{m, mr, mr^2\} = \{m, rm, r^2m\}.$$

This implies that one of the following is true:

- Case 1. $mr = rm$. In this case the group is Abelian, and rm has order six (by Examples Sheet 2, Question 11). This is a contradiction.
- Case 2. $mr = r^2m$. This is the defining relation for the dihedral group D_3. Thus the group is isomorphic to D_3. □