Introduction to Group Theory for IB Natsci Mathematicians

Oli Basquette, osb26@cam.ac.uk

Contents

1 Introduction

This set of brief notes is intended to serve as both a lightning introduction to group theory for those taking the Mathematics course in IB Natural Sciences, and a useful cramming reference for some of the annoying proofs that I can never remember but often come up in exams.

I would recommend reading this over Christmas to give yourself some exposure to group theory, since this content is only formally covered in Easter term (and you don't want to be learning it for the first time then, trust me). Feel free to email me if you want clarification on anything.

2 Fundamentals

2.1 Structure of a group

A group G is an unordered set of abstract unique elements $\{g_1, g_2, g_3, ...\}$, combined with a binary operation which we will denote by the multiplication dot $(\cdot)$, which acts on pairs of elements of G. Additionally, the set of elements and $(\cdot)$ must obey the following four properties:

1. **Closure**: For all pairs of elements x, y in G, $x \cdot y$ is also in G
2. **Associativity**: For all triplets of elements x, y, z in G, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
3. **Identity**: There exists an element I in G such that $I \cdot x = x$ for all x in G
4. **Inverse**: For all x in G, there also exists an 'inverse element' x^{-1} in G such that $x^{-1} \cdot x = I$

The 'order' of G, denoted $|G|$, is the number of elements in G. Also note that $(\cdot)$ does not necessarily obey $x \cdot y = y \cdot x$. This may be the case for some group elements, but is not a requirement. Groups in which $x \cdot y = y \cdot x$ for all x, y in G (i.e. the binary operation is 'commutative') are special and known as **Abelian groups**.

Two corollaries of these properties are useful but not obvious.
Corollary 1: If $x^{-1} \cdot x = I$ then also $x \cdot x^{-1} = I$.
Proof: Consider the quantity $Q = x^{-1} \cdot (x \cdot x^{-1})$. Then by the associative property,

$$Q = (x^{-1} \cdot x) \cdot x^{-1} = I \cdot x^{-1} = x^{-1}.$$

Let y be the inverse of x^{-1} (which exists by assumption). Then from the inverse property, $y \cdot x^{-1} = I$. But $x^{-1} = Q$, so

$$y \cdot [x^{-1} \cdot (x \cdot x^{-1})] = I$$

$$\implies (y \cdot x^{-1}) \cdot (x \cdot x^{-1}) = I$$

$$\implies I \cdot (x \cdot x^{-1}) = I$$

$$\implies \boxed{x \cdot x^{-1} = I}.$$

Corollary 2: If $I \cdot x = x$ then also $x \cdot I = x$.
Proof: From Corollary 1, $x \cdot x^{-1} = I$. Then

$$I \cdot x = x$$

$$\implies (x \cdot x^{-1}) \cdot x$$

$$\implies x \cdot (x^{-1} \cdot x) = x$$

$$\implies \boxed{x \cdot I = x}$$

In other words, while the binary operation is not necessarily commutative between two randomly chosen elements, it is when the identity is involved or when an element is combined with its inverse.

Henceforth, I may sometimes colloquially refer to the binary operation $(\cdot)$ as the 'product' for ease, but unless I'm referring to a specific named group, this is a general shorthand for 'an arbitrary binary operation'.

2.2 Brief examples and applications to symmetry

Groups can be infinite, i.e. $|G| = \infty$. An example of an infinite group is the set of natural numbers (including zero) under the operation of addition; $\{\mathbb{Z}_0, +\}$. Groups can also be finite, i.e. $|G| < \infty$, e.g. the set of natural numbers under addition mod p, in which case $|G| = p$. Spoilers for later: this group is also isomorphic to $\mathbb{C}_p$, the cyclic group of order p.

Groups can be comprised of more abstract elements. For example, the set of 90°, 180° and 270° rotations of a square around its centre forms an order-4 group under the operation of combining transformations. Join me in rotating a square in your mind (aphantasiacs may use a drawing or a square object). The square has four unique orientations, after which we end up back where we started. You can check for yourself that each of the group axioms holds. We can also add in the two reflections with axes parallel to the sides of the square, and the two reflections with axes parallel to the diagonals. It's not as easy to imagine, but you can show that this completes an order-8 group consisting of all the symmetries of the square. This is known as the dihedral group D_4.

2.3 Uniqueness of the identity

There are a few more boring properties we need to prove for completeness. Firstly, is the identity element I unique? Assume there is a second identity element I' which satisfies $I' \cdot x = x = x \cdot I'$. Now let $x = I$, then

$$I' \cdot I = I\,.$$

By the identity property of I, this implies $I' = I$, so there can only be one identity element.

2.4 Uniqueness of the inverse

What about the inverse? Can a given element have multiple distinct inverse elements? Let y and z be two postulated inverses of x. Consider the quantity $y \cdot (x \cdot z)$. Then the associative property means

$$y \cdot (x \cdot z) = (y \cdot x) \cdot z$$

But $(x \cdot z)$ and $(y \cdot x)$ are both I under our assumption that y and z are both inverses, so

$$\begin{aligned} y \cdot I &= I \cdot z \\ \implies y &= z\,. \end{aligned}$$

Hence the inverse is unique.

2.5 Inverse of a product

Consider a group with elements $\{x, y, (...), z\}$, and consider the quantity

$$P = [x \cdot y \cdot (...) \cdot z] \cdot \left[z^{-1} \cdot (...)^{-1} \cdot y^{-1} \cdot x^{-1}\right]\,.$$

By applying the associative property to each inner pair of elements in turn, we find that

$$\begin{aligned} P &= [x \cdot y \cdot (...)] \cdot (z \cdot z^{-1}) \cdot \left[(...)^{-1} \cdot y^{-1} \cdot x^{-1}\right] \\ &= [x \cdot y \cdot (...)] \cdot \left[(...)^{-1} \cdot y^{-1} \cdot x^{-1}\right] \\ &= \text{ (continued...)} \\ &= I\,. \end{aligned}$$

Hence by the uniqueness of inverses that we proved previously, this means

$$[x \cdot y \cdot (...) \cdot z]^{-1} = \left[z^{-1} \cdot (...)^{-1} \cdot y^{-1} \cdot x^{-1}\right]\,.$$

More clearly, this means that $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$, and $(x \cdot y \cdot z)^{-1} = z^{-1} \cdot y^{-1} \cdot x^{-1}$, etc.

2.6 Division law

If we have two known elements x and y, and also that $x \cdot a = y$ for some unknown element a, then a is uniquely determined. To show this, suppose that also $x \cdot b = y$ for some additional element b, then

$$y = y \implies x \cdot a = x \cdot b\,.$$

Apply x^{-1} on the left of both sides to yield $a = b$, so a is unique. This is called the division law because we can view it analogously to 'dividing' the equation $x \cdot a = y$ through by x to yield the unique element a.

2.7 Permutation law

Consider a group G, and pick one of its elements g. Now let's form the product of g with every element of G individually, and let's write this as $g \cdot G$. From the closure property, it should be obvious that every member of $g \cdot G$ belongs to G, and from the division law it's clear that each element in $g \cdot G$ is unique, so $g \cdot G$ is simply a reshuffling of G. But since groups are unordered, we can confidently write that

$$g \cdot G = G\,.$$

2.8 Order of an element

Consider a finite group G. Pick an element $g \neq I$ and consider repeatedly forming the product of g with itself. For notational convenience also write

$$\underbrace{g \cdot g \cdot g \cdot (...) \cdot g}_{n \text{ times}} \equiv g^n \,.$$

Since G is finite, and we know from the division law that each g^n is distinct from g^{n-1}, it follows that the sequence must terminate before we run out of group elements. In other words, for every element g in G, it is true that $g^p = I$ for some $1 \leq p \leq |G|$. p is what we call the 'order' of a group element; the **minimum** number of times it must be self-applied to loop back to the identity element. Don't get this mixed up with the 'order' of the group G itself, which just means $|G|$.

Let's think about the symmetry group of a square again, D_4. The rotations are each of order 4, since clearly performing the same rotation four times leaves you back where you started. The reflections are each of order 2, for hopefully obvious reasons.

Also note that this is clearly not true in general for infinite groups. Consider again the group of natural numbers under addition. Repeatedly adding a non-zero number to itself will never 'loop back' and give you zero.

2.9 Generators and cyclic groups

Let's consider a slightly modified version of the argument from the previous subsection. It's true that any element of a finite group eventually cycles back to the identity element upon repeated self-application. But this element may also cycle through several other members of the group in the process. There is no guarantee that this cycle includes every element of the group, however. For example, in D_4, it's impossible to make a reflection from just repeated rotations, no matter how hard you try.

The smallest set of elements that can generate the entire group, through repeated self-application and/or taking the product with each other, is known as the generating set S_G of the group. Let's call the elements of D_4 $\{I, r_1, r_2, r_3, m_1, m_2, m_3, m_4\}$, referring to rotations as r_i and reflections as m_i. I'll leave it as an exercise to prove to yourself that the generating set of D_4 is just $\{r_1, m_1\}$. In words, this is equivalent to saying that any of the symmetry transformations of a square can be 'factorised' into a repeated composition of a 90° rotation and a reflection about some symmetry axis. Finally note that the generating set is not unique; $\{r_2, m_3\}$, $\{r_3, m_4\}$ or any other combination of one rotation and one reflection is a valid generating set.

A cyclic group is a finite group generated by a single element, i.e. with a generating set of size 1. As an example, consider the order-4 group $\{1, i, -1, -i\}$ under the operation of complex multiplication. It's easy to see that i is a generator of the whole group;

$$\{1, i, -1, -i\} = \{i^4, i, i^2, i^3\} \,.$$

Consequently the generating set is simply $\{i\}$, and this group is considered cyclic. Importantly, it is not necessarily true that every non-identity element of a cyclic group is a generator. If you try using $-i$ as a generator instead, you'll find that it works fine, but using -1 instead generates a cyclic group of order 2, namely $\{1, -1\}$.

If we generalise the structure of this group to be the order-n roots of unity under complex multiplication, i.e.

$$G = \left\{ 1, \exp\frac{\pi i}{n}, \exp\frac{2\pi i}{n}, (...), \exp\frac{[n-1]\pi i}{n} \right\} ,$$

can you think of a condition on n that ensures every element of the group is a generator?

2.10 Group tables and common groups

Group tables are a useful way to visualise the structure of a group, and will also be important in the next sections when we talk about subgroups and mappings between groups. A group table, sometimes called a Cayley table, is a table of the products $g_2 \cdot g_1$ between pairs of elements in a group. For example, the group table for D_4 is as follows, with R representing a 90° rotation and m_i representing each reflection:

$$\begin{array}{cc|ccccccc}
 & & \multicolumn{7}{c}{\longleftarrow g_1 \longrightarrow} \\
 & I & R^2 & R & R^3 & m_1 & m_2 & m_3 & m_4 \\ \hline
 & R^2 & I & R^3 & R & m_2 & m_1 & m_4 & m_3 \\
 & R & R^3 & R^2 & I & m_4 & m_3 & m_1 & m_2 \\
\uparrow & R^3 & R & I & R^2 & m_3 & m_4 & m_2 & m_1 \\
g_2 & m_1 & m_2 & m_3 & m_4 & I & R^2 & R & R^3 \\
\downarrow & m_2 & m_1 & m_4 & m_3 & R^2 & I & R^3 & R \\
 & m_3 & m_4 & m_2 & m_1 & R^3 & R & I & R^2 \\
 & m_4 & m_3 & m_1 & m_2 & R & R^3 & R^2 & I
\end{array}$$

Drawing out a group table like this allows you to fully visualise any patterns that exist inside the group. For example, in the top left and bottom right corners we can see evidence of two copies of another group existing inside this group (see subgroups).

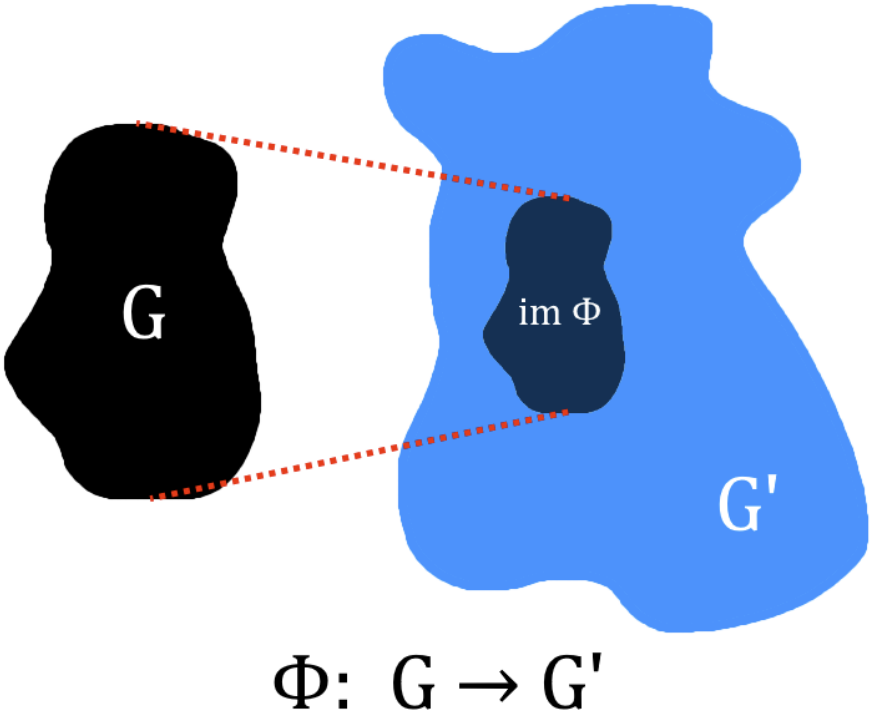
Here are some common finite groups you are likely to encounter at some point:

- $\mathbb{C}_n$, the cyclic group of order n.
- D_n, the group of symmetry transformations of a regular n-gon.
- S_4, the group of symmetry transformations of a tetrahedron.
- K_4, the 'Klein 4-group', or the group of symmetry transformations of a non-square rectangle.
- S_n, the group of permutations of n distinct objects.

3 Mappings

3.1 Homomorphism, isomorphism and abstract groups

Consider two groups G and G', with some example elements $\{x, y, z, ...\}$ and $\{x', y', z', ...\}$, and binary operations $(\cdot)$ and $(\circ)$ respectively. If we can find a mapping $\Phi : G \to G'$ that preserves the group product, i.e. $\Phi(x \cdot y) = \Phi(x) \circ \Phi(y)$ for all x, y, then this mapping is known as a **homomorphism**, and we say the groups are homomorphic. The set of elements in G' that are produced by the mapping Φ is known as the 'image' of G in G', or $\operatorname{im}\Phi$. Consult the diagram below if you need a more vibes-based explanation.



A highly sophisticated graphical depiction of a group homomorphism Φ between two groups G and G'.

A homomorphism must by definition be **injective**, i.e. every element x of G must map onto some element x' of G'. But a homomorphism is not necessarily **surjective**, i.e. not every element of G' is necessarily produced by the mapping Φ from G. If a particular homomorphism happens to be both injective (as it must be) and surjective[1], it's known as an **isomorphism**.

Isomorphisms are extremely important. If two groups are isomorphic then there is a direct one-to-one correspondance between elements of each group. For example, consider the rotational symmetry group of a square introduced in Section 2.2, which we call G. Also consider the group from Section 2.9, namely $\{1, i, -1, -i\}$ under complex multiplication, which we'll call G'. It's straightforward to show that these two small groups are isomorphic. In fact you can imagine placing a square on the complex plane and keeping track of the coordinates of one vertex as it is rotated to directly see the one-to-one correspondence between the groups. Explicitly, the isomorphism from G to

[1] note that the combination of injective and surjective has its own name; **bijective**.

G' can be written

$$\Phi : R\left(\frac{n\pi}{2}\right) \to i^n \,,$$

where $R(\theta)$ denotes an anticlockwise rotation by θ rad. If we were to draw out the group table for each of these two groups (which you are welcome to do if you like), we would see that the two groups contain the exact same multiplication structure despite containing different types of element. Therefore, from a group theorist's perspective, there is no meaningful distinction between the two groups, so we might write

$$G = G' \,.$$

This leads on to the concept of an abstract group. If we don't care about the specific nature of the elements in a group (which we rarely do in group theory), then we can lump every isomorphic group together into a single 'abstract group'. The two groups discussed above are both instances of the cyclic group of order 4, $\mathbb{C}_4$.

3.2 Properties of a homomorphism

(From this subsection onwards, I am going to stop writing the group operations $(\cdot)$ and $(\circ)$ explicitly and just write them as products instead. It should be unambiguous from context which one is needed where.)

Consider a group G with an element x, that maps to a group G' under a homomorphism Φ. Also call $\Phi(x) = x'$ for simplicity, and similarly call the identities of the two groups I and I' respectively. The following three properties are useful to note.

3.2.1 Identity maps onto identity

We know $Ix = x$ for all x in G. Then by the key homomorphism property,

$$\begin{aligned} &\Phi(I)\Phi(x) = \Phi(x) \\ \implies &\Phi(I)\, x' = x' \,, \end{aligned}$$

which means that $\Phi(I) = I'$, i.e. the identity of G maps onto the identity of G'.

3.2.2 Inverse maps onto inverse

We know $I = x^{-1}x$, so $I' = \Phi(x^{-1}x)$. By homomorphism, therefore

$$\begin{aligned} I' &= \Phi(x^{-1})\Phi(x) \\ &= \Phi(x^{-1})\, x' \,. \end{aligned}$$

This means that $\Phi(x^{-1})$ is the inverse of x'; $\Phi(x^{-1}) = (x')^{-1}$. The inverse of an element of G maps onto the inverse of the corresponding element of its image in G'.

3.2.3 Order of elements in the image

If an element x of G is of order m, i.e. $x^m = I$, then $I' = \Phi(x^m)$. By homomorphism,

$$I' = \underbrace{\Phi(x)\Phi(x)...\Phi(x)}_{m \text{ times}} = (x')^m \,.$$

$(x')^m = I'$ implies that the order of x' in G' is either m or a factor of m.

4 Permutation groups

A rearrangement of n distinct objects is called a 'permutation of degree n'. Permutations can be shown to form a group under the operation of composition (this should be fairly obvious so I'm not going to prove it explicitly). For example, let's consider a permutation θ of degree 6, which acts on six objects $a \dots f$ as follows:

$$\theta\{a\ b\ c\ d\ e\ f\} = \{b\ e\ f\ a\ d\ c\}\,.$$

Another way of writing this is $\theta = [2\ 5\ 6\ 1\ 4\ 3]$, meaning the item in position 2 moves to position 1; the item in position 5 moves to position 2, etc. With this notation, the composition of two permutations is quite intuitive. For example,

$$[4\ 5\ 3\ 6\ 2\ 1]\,[2\ 5\ 6\ 1\ 4\ 3] = [1\ 4\ 6\ 3\ 5\ 2].$$

This is nothing but the $[4^{\text{th}}, 5^{\text{th}}, 3^{\text{rd}}, 6^{\text{th}}, 2^{\text{th}}, 1^{\text{st}}]$ elements of [2 5 6 1 4 3]. Another useful concept is the decomposition of permutations into cycles. If we pick an object in the set being permuted and keep track of its position, we can always represent a permutation in terms of closed cycles. For example, let's keep track of the object in the first position when we apply the permutation $\theta = [2\ 5\ 6\ 1\ 4\ 3]$. We find that

$$\begin{aligned} &\text{object } 1 \to \text{object } 2\,, \\ &\text{object } 2 \to \text{object } 5\,, \\ &\text{object } 5 \to \text{object } 4\,, \\ &\text{object } 4 \to \text{object } 1\,. \end{aligned}$$

This is a closed cycle, (1 2 5 4). 3 and 6 haven't appeared yet, so let's now keep track of what happens to the object in position 3:

$$\begin{aligned} &\text{object } 3 \to \text{object } 6\,, \\ &\text{object } 6 \to \text{object } 3\,. \end{aligned}$$

We can therefore write $\theta = (1\ 2\ 5\ 4)(3\ 6)$, which is its cycle decomposition. Composition is quite intuitive in this notation as well, e.g.

$$[(3)(1\ 4\ 6)(2\ 5)]\,[(1\ 2\ 5\ 4)(3\ 6)] = (1)(2\ 4\ 3\ 6)(5)\,,$$

which can be found by keeping track of each element in term, as before. Note that 1-cycles such as (5) can be unambiguously left out of the decomposition, so we could write this as just (2 4 3 6).

The permutation group of degree 3, called S_3, contains these permutations:

$$\begin{aligned} I &= (1)(2)(3)\,, \\ A &= (1\ 2\ 3)\,, \\ B &= (1\ 3\ 2)\,, \\ C &= (1)(2\ 3)\,, \\ D &= (3)(1\ 2)\,, \\ E &= (2)(1\ 3)\,. \end{aligned}$$

If you look at these for a few seconds, it shouldn't be too hard to convince yourself that this group S_3 is isomorphic to the symmetry group of a triangle D_3; A and B represent 120° rotations (in which all 3 vertices are permuted), and C, D and E are the three reflections, which only swap two vertices. Physically, this isomorphism is telling us that the symmetry transformations of a triangle give us the same outcomes as if we were to permute the vertices around. This is not true for higher order regular polygons. D_4 has 8 elements while S_4 has $4! = 24$ elements, so the two cannot be isomorphic.

The 'order' of a permutation is the minimum number of times it must be self-applied to equal the identity, exactly as we defined before for the element of a general group. For the case of permutation groups, the order of a permutation is also equal to the LCM of the orders of the constituent cycles, which are themselves just equal to the length of each cycle.

5 Subgroups

5.1 Definitions and structure

A subgroup is a group within a group. In other words, it's a non-empty subset H of a group G that also obeys all the properties of a group under the same binary operation as G. Every group G contains two trivial subgroups:

1. G itself, and
2. the subgroup $\{I\}$.

Any other subgroups are called proper subgroups. For example, $\mathbb{C}_4$ is a proper subgroup of D_4; the group of rotational symmetries of a square is a group within the larger group of all the symmetries of a square.

You should check that you can convince yourself of the following assertions:

1. Cyclic groups of **prime order** have no proper subgroups.
2. Cyclic groups of **nonprime order** must contain at least one proper subgroup (this somewhat gives away the answer to the question posed at the end of Section 2.9!)

5.2 Basic subgroup theorems

Consider a group G and choose two elements x, y. Also consider a group homomorphism Φ mapping G to G', with $\Phi(x) = x'$ and $\Phi(y) = y'$.

Claim: The image $H' = \operatorname{im}\Phi$ of G in G' is a subgroup of G'.
Proof: Pick two elements a and b belonging to H'. Since $H' = \operatorname{im}\Phi$, we can write $a = x'$ and $b = y'$. We will now show each of the group axioms in turn.

1. **Closure**: $ab = x'y' = (xy)'$. xy is in G so ab is in H'.
2. **Associativity**: Obvious, inherited from the group operation of G'.

3. **Identity**: We proved earlier that I maps to I', so I' is in H'.

4. **Inverse**: $a^{-1} = (x')^{-1} = (x^{-1})'$. x^{-1} is in G so a^{-1} is in H'.

Claim: The kernel $\mathcal{K}$ of Φ (i.e. the set of elements in G that are mapped onto the identity I' of G') is a subgroup of G.
Proof: Suppose x and y belong to the kernel $\mathcal{K}$, so by definition $x' = y' = I'$. As before we will show each of the group axioms in turn.

1. **Closure**: $(xy)' = x'y' = I'I' = I'$, so xy is in $\mathcal{K}$.

2. **Associativity**: Obvious

3. **Identity**: I maps to I', so I is in $\mathcal{K}$.

4. **Inverse**: $I' = (x^{-1}x)' = (x^{-1})'x'$, but $x' = I'$, so $I' = (x^{-1})'$. Therefore x^{-1} is also in $\mathcal{K}$.

There's a hidden extra layer to this second property. Not only is the kernel of a group homomorphism a subgroup, it's a special kind of subgroup called a normal subgroup (see later).

5.3 Cyclic subgroups

Every element x of a finite group G generates a **cyclic subgroup** $H_x = \{x, x^2, x^3, (...), x^p\}$ where p is the order of the element x. If G is itself a cyclic group, then H_x may either be a trivial or proper subgroup of G depending on the nature of x.

6 Equivalence classes

In many groups, there are natural partitions we can make within the group to associate similiar elements with each other. For example, in D_4, it might seem natural to partition the group into rotations and reflections. But there are often less obvious, but equally interesting partitions we can make, so it's useful to formalise these partitions into something called 'equivalence classes'.

6.1 Equivalence relations

An equivalence relation on a set $\mathcal{S}$ is a relationship $x \sim y$ between pairs of elements x, y in $\mathcal{S}$, obeying the three properties:

1. **Reflexivity**: $x \sim x$

2. **Symmetry**: if $x \sim y$ then $y \sim x$

3. **Transitivity**: if $x \sim y$ and $y \sim z$ then $x \sim z$

An equivalence relation ($\sim$) partitions a set $\mathcal{S}$ into equivalence classes $\mathcal{C}_i$ such that:

- x and y belong to the same class if and only if $x \sim y$, and

- every element of $\mathcal{S}$ belongs to **exactly one** class.

In other words, equivalence classes are either disjoint or identical, meaning there are no overlapping elements between two distinct equivalence classes. In set-builder notation, the equivalence class containing the element a can be written $\mathcal{C}_a = \{x \in \mathcal{S} : a \sim x\}$ ('the set of elements x in $\mathcal{S}$ such that $a \sim x$').

To illustrate this, consider a set $\mathcal{S}$ with two different classes $\mathcal{C}_x$ and $\mathcal{C}_y$, containing elements x and y respectively. Suppose the two equivalence classes have an element z in common, i.e. $z \sim x$ and $z \sim y$. By symmetry,

$$z \sim x \implies x \sim z,$$

so we have $x \sim z$ and $z \sim y$. By the transitivity property, this means $x \sim y$, so $\mathcal{C}_x$ and $\mathcal{C}_y$ are the same equivalence class. This contradicts our requirement that $\mathcal{C}_x$ and $\mathcal{C}_y$ were two different equivalence classes, so $\mathcal{C}_x$ and $\mathcal{C}_y$ may not share an element z, i.e. they are disjoint.

In the following subsections, we will explore two important examples of an equivalence relation; **congruence** and **conjugacy**.

6.2 Congruence and cosets

First let's let $(\sim)$ be the congruence relation.
Definition: given x, y in a group G, $x \sim y$ (x and y are 'congruent') if $x^{-1}\,y$ belongs to some subgroup H of G.

This is equivalent to saying that $y = xh$ for some element h in H, so the elements of this equivalence class are of the form $\{xH_1, xH_2, xH_3, (...), xH_{|H|}\}$ for x in G. These equivalence classes generated by the congruence relation are called the 'cosets' of H. In fact, these are 'left cosets' of H, since we take the product with x on the left of H. The 'right cosets' would be of the form$\{H_1x, H_2x, H_3x, (...), H_{|H|}x\}$ for x in G. You can check for yourself that if we define congruence with $y\,x^{-1}$ instead of $x^{-1}\,y$, we get right cosets instead of left cosets. For notational convenience, the left coset containing x is written xH and the right coset is Hx.

Let's prove that congruence is indeed an equivalence relation.

1. **Reflexivity**: $x \sim x$ requires that $x^{-1}\,x$ belongs to H. Since $x^{-1}\,x = I$, this is obvious.

2. **Symmetry**: if $x \sim y$ then $x^{-1}\,y$ is in H by definition. Since H is a (sub)group, it must also contain $(x^{-1}\,y)^{-1} = y^{-1}\,x$, so $y \sim x$.

3. **Transitivity**: if $x \sim y$ and $y \sim z$, then by definition H contains $x^{-1}\,y$ and $y^{-1}\,z$. By closure, H also contains the product $(x^{-1}\,y)(y^{-1}\,z) = x^{-1}\,z$, so also $x \sim z$.

As an example, consider the group of the natural numbers under addition mod 8, $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Let's extract the subgroup of the even numbers, $H = \{0, 2, 4, 6\}$. It should be fairly obvious that this is a subgroup. H has two cosets; $0 + H = \{0, 2, 4, 6\}$ (the even numbers) and $1 + H = \{1, 3, 5, 7\}$ (the odd numbers). As we predicted before, these cosets are disjoint. You can try forming other cosets, e.g. $2 + H$ or $3 + H$, but you will find that these are identical to one of the two we already found. We could have predicted this as well, since the even and odd numbers together make up the entire group G, and so we must have already found all the cosets.

6.3 Lagrange's Theorem

We can use cosets to prove an important theorem in group theory, called Lagrange's theorem. Firstly observe that each left coset contains $|H|$ elements, since by the permutation law every element of xG is unique, and xH is a size-$|H|$ subset of these. By the properties of equivalence classes, we know that each member of G is in exactly one left coset. An integer number of left cosets must therefore contain all $|G|$ elements of G. This implies Lagrange's theorem: if H is a subgroup of G, then $|G|$ is a multiple of $|H|$.

Recall from section 5.3 that each element x of a finite group G generates a cyclic subgroup of size equal to the order of the element x. From Lagrange's theorem, which states that the order of this cyclic subgroup is a divisor of $|G|$, it follows that the order of each element x in G is therefore also a divisor of $|G|$.

6.4 Conjugacy and conjugacy classes

Now let's let $(\sim)$ be the conjugacy relation.
Definition: given x, y in a group G, $x \sim y$ (x and y are 'conjugate') if $y = gxg^{-1}$ for some g in G.

The equivalence classes associated with the conjugacy relation are called conjugacy classes. The conjugacy class containing the element x (the set of elements that are conjugate to x) is therefore $\{g_1xg_1^{-1}, g_2xg_2^{-1}, g_3xg_3^{-1}, (...), g_{|G|}xg_{|G|}^{-1}\}$[2].

As before, we need to prove that conjugacy is really an equivalence relation.

1. **Reflexivity**: $x \sim x$ requires that $x = gxg^{-1}$ for some g. This is clearly satisfied by $g = I$.

2. **Symmetry**: if $x \sim y$ then $y = gxg^{-1}$ by definition. By multiplying appropriately, this implies $x = g^{-1}yg = (g^{-1})y(g^{-1})^{-1}$. If we let $g^{-1} = u$, then $x = uyu^{-1}$. Since u is another element of G this implies $y \sim x$.

3. **Transitivity**: If $x \sim y$ and $y \sim z$ then by definition $y = g_1xg_1^{-1}$ and $z = g_2yg_2^{-1}$. By inserting this expression for y into the expression for z, we find $z = g_2(g_1xg_1^{-1})g_2^{-1} = (g_2g_1)x(g_1^{-1}g_2^{-1}) = (g_2g_1)x(g_2g_1)^{-1}$. Since g_2g_1 is also in G, this implies that $x \sim z$.

We now consider three additional properties of conjugacy classes.

Corollary 1: If z is in the conjugacy class containing I, the identity element, then $z = gIg^{-1}$ for some g in G, i.e. $z = gg^{-1} = I$. **So I is always in a conjugacy class by itself**.

[2] Note that all of these elements may not be unique, so in general the size of a conjugacy class is less than $|G|$, as we expect.

Corollary 2: If x is in a conjugacy class by itself, then obviously $x \sim y$ implies $y = x$. If this is true, then $y = gxg^{-1}$ implies $y = x$ for all g in G (the only element conjugate to x is itself). Therefore $x = gxg^{-1}$ for all g, i.e. $xg = gx$ for all g. **This means that x commutes with every element in the group**. By reversing the steps shown here we can also show that an element that commutes with every element of a group must be in a conjugacy class by itself (an example is always the identity element). For an Abelian group, all elements commute with each other, so all elements are in a conjugacy class by themselves.

Corollary 3: The the union of elements that are in conjugacy classes by themselves is also a group.
Proof: Consider a group G with an arbitrary element g. Consider two additional elements x and y that each occupy a conjugacy class by themselves. We now show each of the group axioms holds.

1. **Closure**: We know $xg = gx$ and $yg = gy$ since x and y are both in conjugacy classes by themselves. Therefore $(xy)g = g(xy)$, i.e. xy also commutes with every element of G and hence is in a conjugacy class by itself, so we have closure.

2. **Associativity**: Inherited from the group operation.

3. **Identity**: We proved before that I is in a conjugacy class by itself.

4. **Inverse**: $xg = gx \implies g^{-1}x^{-1} = x^{-1}g^{-1} \implies x^{-1}g = gx^{-1}$, so x^{-1} is also in a conjugacy class by itself.

As an example, consider $G = D_4$ once again. Recall that $x \sim y$ means $y = gxg^{-1}$ for some g in G. This form is reminiscent of the transformation law for a linear map; if we have a transformation matrix $\mathbf{L}$, then a linear map $\mathbf{A}$ transforms as $\mathbf{A}' = \mathbf{L}^{-1}\mathbf{A}\mathbf{L}$. We can therefore think of D_4's conjugacy classes geometrically as sets of symmetries that are equivalent, up to a change of perspective. You can check manually for yourself if you want to, but the conjugacy classes are, in the notation of section 2.10:

- $\{I\}$
- $\{R, R^3\}$ (90° rotations)
- $\{R^2\}$ (180° rotation)
- $\{m_1, m_2\}$ (reflections parallel to sides)
- $\{m_3, m_4\}$ (reflections along the diagonal)

6.5 Normal subgroups

I hinted at a special type of subgroup earlier in the notes, called a **normal** subgroup. These are defined as subgroups N of a group G that are invariant under conjugation by any element g in G, i.e. $gNg^{-1} = N$. Equivalently, normal subgroups are groups composed of the union of one of more complete conjugacy classes. The two trivial subgroups, G itself and $\{I\}$, are both technically normal subgroups.

Since $gNg^{-1} = N$, clearly the left and right cosets of a normal subgroup are equal; $gN = Ng$. I also proved earlier that the kernel $\mathcal{K}$ of a group homomorphism is a subgroup, and briefly mentioned that $\mathcal{K}$ is also a normal subgroup, which I will now prove.

Consider the kernel $\mathcal{K}$ of some homomorphism $\Phi : G \to G'$. Let x be in G and y be in $\mathcal{K}$. By definition of the kernel, this means $y' = I'$. Now observe that

$$\begin{aligned}(xyx^{-1})' &= x'y'(x^{-1})' \\ &= x'(x^{-1})' \\ &= x'(x')^{-1} \\ &= I'\end{aligned}$$

so xyx^{-1} is also in $\mathcal{K}$, hence $\mathcal{K}$ is a normal subgroup.

Normal subgroups are interesting physically. In terms of our previous analogy with transforming a linear map, we can think of them as ‘groups of closed symmetries that are unchanged under a change of perspective’. They allow us to naturally partition groups into subgroups in such a way that preserves the physical meaning and/or symmetry type of each subgroup.