MTH6106 Group Theory

Ian Morris, Semester A 2022-23*

Contents

*Based substantially on earlier lecture notes by Dr. Matt Fayers and Prof. Alexander Sodin. (September 20, 2022)

1 Basics

1.0 Informal preliminaries

In the old days, the notion of an abstract group did not exist. In those times, mathematicians thought of a group as a set of operations which can be inverted and composed.

Examples.

1. The operations that can be performed on a loose square tile: $\underline{0^\circ}$ (do nothing), $\underline{90^\circ}$ (rotate counterclockwise by 90°), $\underline{180^\circ}$, $\underline{270^\circ}$. Each of these operations can be inverted, e.g. the inverse of $\underline{270^\circ}$ is $\underline{90^\circ}$, and one can compose them, e.g. $\underline{270^\circ} \circ \underline{180^\circ} = \underline{90^\circ}$. Together, these four operations form a group called $\mathcal{C}_4$ (the cyclic group of order 4).

2. Suppose we are also allowed to reverse the tile. Then, in addition to the four operations listed above, we have four reflections: $\underline{-}$, $\underline{|}$, $\underline{/}$, $\underline{\backslash}$. Each of these is its own inverse, and we can still compose, e.g.
$$\underline{\backslash} \circ \underline{90^\circ} = \underline{|}\,, \quad \underline{90^\circ} \circ \underline{\backslash} = \underline{-}\,.$$
Thus we have a larger group with 8 elements, denoted $\mathcal{D}_8$ (the dihedial group of order 8).

3. $\{\underline{0^\circ}, \underline{90^\circ}\}$ is not a group.

In modern group theory (and in our module), one considers abstract groups which are not a priori *realised as sets of operations. Still, most (if not all) of the examples of groups we shall discuss can be naturally realised as groups of operations, so the old-fashioned point of view is still very helpful, as we shall see.*

1.1 Definitions

In this section, we recall the basic definitions relating to group theory. Most of these should be familiar to you.

Definition. A **group** is a set G, together with a binary operation $\circ$ on G, satisfying the following axioms.

G1 (closure): for every $g, h \in G$ we have $g \circ h \in G$.

G2 (associativity): for every $g, h, k \in G$ we have $(g \circ h) \circ k = g \circ (h \circ k)$.

G3 (identity): there is an element $1 \in G$ such that $1 \circ g = g = g \circ 1$ for every $g \in G$.

G4 (inverse): for every $g \in G$, there is an element g^{-1} such that $g^{-1} \circ g = 1 = g \circ g^{-1}$.

The element 1 is called the **identity element** of G. We sometimes write the identity element as id instead of 1 if we're using the number 1 for something else. (Older textbooks often use e for the identity element.)

The element g^{-1} is called the **inverse** of g.

Examples.

1. $(\mathbb{R}, +)$ is a group; $(\mathbb{R}, \times)$ is not (0 does not have an inverse), $(\mathbb{R}_{>0}, \times)$ is a group; so are $\mathcal{C}_4$ and $\mathcal{D}_8$. $(\mathbb{Z}_+, +)$ is not a group (no inverse).

2. The **trivial group** $\{1\}$ has only one element, with $1 \circ 1 = 1$.
3. A group with two elements: $\{1, x\}$. Clearly, $1 \circ 1 = 1$, $1 \circ x = x \circ 1 = x$, and x has to have an inverse, so $x \circ x = 1$. It is therefore natural to denote x by -1.
4. The set of all functions $\mathbb{R} \to \mathbb{R}$ with $\circ$ being the composition is not a group (no inverse). The set of all invertible functions (bijections) is a group.

For a small group, we can describe the group just by giving the elements and the binary operation in the form of a table (called the **Cayley table**). For example, for the group $\mathcal{C}_2 = \{1, -1\}$, the Cayley table is as follows.

	1	-1
1	1	-1
-1	-1	1

Another example of a small group is the **Klein four-group** $\mathcal{V}_4$, which has elements 1, a, b, c and group operation given by the Cayley table

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

.

Note that we cannot think of a, b, c as real or complex numbers: there are no distinct numbers $a, b, c \in \mathbb{C}$ such that $a^2 = b^2 = c^2 = 1$. So $\mathcal{V}_4$ is really an **abstract** group: it is defined simply as a list of symbols with a binary operation defined by a Cayley table.

(However, it can be realised as a set of operations. Imagine a room with two lamps; 1 *denotes doing nothing, a changes the state of the first switch, b – of the second switch, and c – of both switches. Another realisation is to exchange a and c, for example.)*

Definition. A group G is **abelian** if $g \circ h = h \circ g$ for all $g, h \in G$.

Among the groups considered so far, the only non-abelian ones were $\mathcal{D}_8$ and the group of invertible functions $\mathbb{R} \to \mathbb{R}$.

Notation.

- ◇ We usually write gh instead of $g \circ h$ if it's clear what the group operation is.
- ◇ We may write 1 as 1_G to emphasise that it is the identity element of G, if we are looking at other groups at the same time.
- ◇ Because of the associative law, we can write an expression like fgh without needing brackets.

  More generally, if $g_1, \ldots, g_r \in G$, we can write the element $g_1 \ldots g_r$ without brackets. We call this element the **product** of $g_1, \ldots, g_r$. (Be careful – in general, this product depends on the order of $g_1, \ldots, g_r$). We include the case $r = 0$, in which case we have the **empty product** which equals 1.
- ◇ We define **powers** of elements as follows. Suppose $g \in G$ and $n \in \mathbb{Z}$.
  - ◇ If $n > 0$, then g^n is just the product of n copies of g.
  - ◇ $g^0 = 1$.
  - ◇ If $n < 0$, then $g^n = (g^{-n})^{-1}$.

  Then the familiar laws
  $$g^m g^n = g^{m+n} \qquad (g^m)^n = g^{mn}$$
  hold (for all integers m and n), and we'll use these without comment.

Lemma 1.1. *Suppose G is a group.*

1. *The identity element of G is unique.*
2. *The inverse of any element of G is unique.*
3. *For any $g \in G$ we have $(g^{-1})^{-1} = g$.*
4. *(The shoes-and-socks rule) For any $f, g \in G$ we have $(fg)^{-1} = g^{-1}f^{-1}$.*

Proof.

1. Suppose $1, \widehat{1}$ are both identity elements in G. Then $1\widehat{1} = \widehat{1}$, because 1 is an identity. But also $1\widehat{1} = 1$, because $\widehat{1}$ is an identity. So $\widehat{1} = 1$.
2. Suppose g^{-1}, g^* are two different inverses for g. Then
   $$g^{-1}gg^* = 1g^* = g^*$$
   but also
   $$g^{-1}gg^* = g^{-1}1 = g^{-1},$$
   so $g^{-1} = g^*$.
3. Since $gg^{-1} = g^{-1}g = 1$, g is an inverse of g^{-1}. But inverses are unique, so g is **the** inverse of g^{-1}, i.e. $g = (g^{-1})^{-1}$.

4. We have
$$fgg^{-1}f^{-1} = f1f^{-1} = ff^{-1} = 1$$
and
$$g^{-1}f^{-1}fg = g^{-1}1g = g^{-1}g = 1$$
so $g^{-1}f^{-1}$ is an inverse of fg. But inverses are unique, so $g^{-1}f^{-1}$ is the inverse of fg, i.e. $g^{-1}f^{-1} = (fg)^{-1}$. □

Parts (3) and (4) of Lemma 1.1 each have a purely symbolic proof – this is much shorter, but doesn't really give a clear idea of **why** the statement is true. For (3) we can just say
$$(g^{-1})^{-1} = (g^{-1})^{-1}1 = (g^{-1})^{-1}g^{-1}g = 1g = g$$
and for (4) we have
$$(fg)^{-1} = (fg)^{-1}1 = (fg)^{-1}ff^{-1} = (fg)^{-1}f1f^{-1} = (fg)^{-1}fgg^{-1}f^{-1} = g^{-1}f^{-1}.$$

The next definition is very important.

Definition. Suppose G is a group and $g \in G$.

- ◇ The **order** of G (written $|G|$) is the number of elements in G (which may be ∞).
- ◇ The **order** of g (written $\mathrm{ord}(g)$) is the smallest $n > 0$ such that $g^n = 1$, or ∞ if there is no such n.

It's somewhat unfortunate that we use the word "order" in two different ways (although we shall see a kind of explanation later). Note that 1 always has order 1, and is the only element of order 1 in G.

Examples.

- ◇ Let $G = \mathcal{V}_4$. The order of G is 4. The order of $a \in \mathcal{V}_4$ is 2, because $a^1 \neq 1$ but $a^2 = 1$. Similarly $\mathrm{ord}(b) = \mathrm{ord}(c) = 2$.
- ◇ Let $G = \mathbb{R}^\times$. Then $|G| = \infty$. Also $\mathrm{ord}(-1) = 2$, and $\mathrm{ord}(2) = \infty$, because $2^n > 1$ whenever $n > 0$.
- ◇ Which elements of order 6 are there in $\mathbb{C}^\times$?

It's important to note that $\mathrm{ord}(g)$ is the **smallest** n such that $g^n = 1$; in general there will be lots of values of n for which $g^n = 1$. For example, if g has order 4, then $g^4 = 1$, but then we also get $g^8 = 1$, $g^{12} = 1$, and so on. The next lemma tells us when $g^m = 1$.

Lemma 1.2. *Suppose G is a group, and $g \in G$ with $\mathrm{ord}(g) = n < \infty$. If $m \in \mathbb{Z}$, then $g^m = 1$ if and only if n divides m.*

Proof. If $n \mid m$, write $m = nb$ with $b \in \mathbb{Z}$. Then $g^m = g^{nb} = (g^n)^b = 1^b = 1$.

If $n \nmid m$, then we can write $m = nb + r$ with $0 < r < n$. We must then have $g^r \neq 1$, since n is chosen to be the **smallest** positive integer with $g^n = 1$. Hence
$$g^m = g^{nb+r} = (g^n)^b g^r = 1^b g^r = g^r \neq 1.$$ □

This lemma can help us to pin down the order of an element. For example, suppose we have a group and an element g satisfying $g^8 = 1$. Then by definition $\mathrm{ord}(g) \leqslant 8$, but from Lemma 1.2 we can say that $\mathrm{ord}(g)$ divides 8, i.e. $\mathrm{ord}(g) = 1, 2, 4$ or 8.

1.2 Subgroups

Definition. Suppose G is a group. A **subgroup** of G is a subset $H \subseteq G$ which is also a group under the same operation.
We write $H \leqslant G$ to mean "H is a subgroup of G", and we use the symbols $<, \geqslant, >$ in the obvious way.

Examples.

- $G \leqslant G$ for any group G.
- $\{1\} \leqslant G$ for any group G.
- $\{1, a\} \leqslant \mathcal{V}_4$.
- $\mathbb{R}^\times \leqslant \mathbb{C}^\times$.
- $\mathbb{Z}_+$ is not a subgroup of $\mathbb{Z}$.
- What are the subgroups of $\mathbb{Z}$ (with addition)?

Given a group G and a subset H, how do we test whether $H \leqslant G$? It's easier than just checking whether H is a group. For example, we know that the associative law holds, because it holds in G. Also, we know that G has an identity element 1, so to check whether H has an identity, we just need to check whether $1 \in H$. A similar statement holds for inverses, so we can use the following test.

Subgroup Test. If G is a group and $H \subseteq G$, then H is a subgroup of G if it satisfies the following.

S1. H is non-empty.

S2. $gh^{-1} \in H$ for all $g, h \in H$.

1.3 Generators

Definition. Suppose G is a group and $g \in G$. The **subgroup of G generated by g** is the set of all powers of g, i.e. the set

$$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}.$$

Examples.

- Suppose $G = \mathcal{V}_4$. Then $\langle a \rangle = \{1, a\}$.
- Suppose $G = \mathbb{C}^\times$, the group of non-zero complex numbers. Then $\langle i \rangle = \{1, i, -1, -i\}$.
- Suppose $G = \mathbb{R}^\times$. Then $\langle 2 \rangle = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\}$.

The definition suggests that $\langle g \rangle$ should always be a subgroup of G. So let's prove this.

Lemma 1.3. *Suppose G is a group and $g \in G$. Then $\langle g \rangle \leqslant G$.*

Proof. Apply the Subgroup Test.

S1. $\langle g \rangle$ is non-empty because it contains $g^1 = g$.

S2. Given two elements of $\langle g \rangle$, write them as g^a and g^b, where $a, b \in \mathbb{Z}$. Then $g^a(g^b)^{-1} = g^a g^{-b} = g^{a-b} \in \langle g \rangle$, because $a - b \in \mathbb{Z}$. □

The next result provides a connection between the two different uses of the word "order".

Lemma 1.4. *Suppose G is a group and $g \in G$. Then $|\langle g \rangle| = \mathrm{ord}(g)$.*

Proof. First suppose $\mathrm{ord}(g) = \infty$. This means there is no $n > 0$ for which $g^n = 1$. Now the elements g^n for $n \in \mathbb{Z}$ must all be different, because if $g^l = g^m$ with $l < m$, then $g^{m-l} = 1$, with $m - l > 0$, a contradiction. So $\langle g \rangle$ contains infinitely many elements.

Now suppose instead that $\mathrm{ord}(g) = n < \infty$. Then we claim that $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$. Any element of $\langle g \rangle$ has the form g^m for $m \in \mathbb{Z}$; we can write $m = nb + r$ with $0 \leqslant r < n$. Then $g^m = g^{nb+r} = g^r \in \{1, g, g^2, \ldots, g^{n-1}\}$. So $1, g, \ldots, g^{n-1}$ are the only elements of $\langle g \rangle$, and they are all different, because if $g^l = g^m$ with $0 \leqslant l < m \leqslant n - 1$, then $g^{m-l} = 1$ with $0 < m - l < n$, contradicting the fact that $n = \mathrm{ord}(g)$. So $\langle g \rangle$ contains exactly n different elements. □

Now we generalise the definition above.

Definition. Suppose G is a group and $g_1, \ldots, g_r \in G$.

- ◇ The **subgroup of G generated by** $g_1, \ldots, g_r$ (written as $\langle g_1, \ldots, g_r \rangle$) is the set of all elements of G that can be written as products of elements from
$$\{g_1, \ldots, g_r, g_1^{-1}, \ldots, g_r^{-1}\}.$$
- ◇ If $\langle g_1, \ldots, g_r \rangle = G$, we say that $g_1, \ldots, g_r$ **generate** G.

n.b. when defining the elements of $\langle g_1, \ldots, g_r \rangle$, we don't have to use all of $g_1, \ldots, g_r, g_1^{-1}, \ldots, g_r^{-1}$, and we can use them more than once. So for example $g_1^2 g_2 g_1^{-1} \in \langle g_1, g_2, g_3 \rangle$.

Examples.

- ◇ Take $G = \mathcal{V}_4$. We can write every element of $\mathcal{V}_4$ in terms of a and b, since $c = ab$ and $1 = a^2$ (or in fact we could just say 1 is the empty product). So a and b generate $\mathcal{V}_4$.
- ◇ Take $G = \mathbb{R}^\times$, and consider the subgroup $\langle 1, 2, 3, 4, \ldots \rangle$. This consists of all real numbers that we can get by repeatedly multiplying and dividing by positive integers, i.e. $\{x \in \mathbb{Q} \mid x > 0\}$.
- ◇ One can generate the same subgroup using less generators, e.g. $2, 3, 5, 7, 11, \cdots$.

1.4 More about the associative law

Let's look at the associative law more closely. When groups were first studied, the associative law wasn't included as an axiom, because it was automatically true for the kinds of groups being considered: these were always groups of functions.

Suppose X is a set. Given any two functions ϕ, ψ from X to X, we define a function $\phi \circ \psi : X \to X$ by **composition**, i.e.

$$(\phi \circ \psi)(x) = \phi(\psi(x)) \qquad \text{for all } x \in X.$$

Warning. Note that we write our functions on the **left** (i.e. we write $\phi(x)$ rather than $x\phi$), so $\phi \circ \psi$ means "do ψ then ϕ". Note that many books and lecturers write their functions on the right, so they compose functions the other way round.

So we have a binary operation $\circ$ on the set of functions from X to X.

Proposition 1.5. *Suppose X is a set. Then the operation $\circ$ on the set of functions from X to X is associative.*

Proof. We need to show that

$$(\phi \circ \psi) \circ \chi = \phi \circ (\psi \circ \chi) \qquad (*)$$

for any $\phi, \psi, \chi : X \to X$. What does this mean? The two sides of $(*)$ are functions on X, so they're the same if they do the same thing to every $x \in X$. For any x we have

$$\begin{aligned}((\phi \circ \psi) \circ \chi)(x) &= (\phi \circ \psi)(\chi(x)) \\ &= \phi(\psi(\chi(x)))\end{aligned}$$

while

$$\begin{aligned}(\phi \circ (\psi \circ \chi))(x) &= \phi((\psi \circ \chi)(x)) \\ &= \phi(\psi(\chi(x)))\end{aligned}$$

so $(*)$ is true. □

This result means that a useful way to construct groups is to define them as sets of functions from a set to itself; then we get the associative law for free.

2 Examples

In this section, we give some examples which we'll use throughout the course.

2.1 Cyclic groups

Definition. Suppose $n \in \mathbb{N}$. The **cyclic group** of order n is the group

$$\mathcal{C}_n = \{1, z_n, z_n^2, \dots, z_n^{n-1}\},$$

where z_n is an element of order n.

You can think of z_n as being the complex number $e^{(2\pi i/n)}$, or just as an abstract symbol defined to have order n. Usually we will write z_n just as z is it's clear what n is.

The group operation in $\mathcal{C}_n$ is obvious: $z^a z^b = z^{a+b}$, but we have to remember that $z^n = 1$. For example, if $n = 7$ we have $z^4 z^5 = z^2$.

Definition. The **infinite cyclic group** is the group

$$\mathcal{C}_\infty = \{\dots, z_\infty^{-2}, z_\infty^{-1}, 1, z_\infty, z_\infty^2, z_\infty^3, \dots\},$$

where z_∞ is an element of infinite order.

Note that for any group G and any $g \in G$ the subgroup $\langle g \rangle$ generated by g is cyclic.

2.2 The quaternion group

Definition. The **quaternion group of order** 8 is

$$\mathcal{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

The group operation is defined by

- -1 changes the sign of everything;
- $i^2 = -1$, $j^2 = -1$, $k^2 = -1$;
- $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$.

This is one of our first examples of a non-abelian group, so we have to be careful with the order of multiplication. For example, $i(-j) = -k$, but $(-j)i = k$.

To see that $\mathcal{Q}_8$ is a group, it's quite easy to check G1, G3 and G4. But the associative law G2 is more difficult (or very boring, if you check through every single case). A clever way to check this is as follows: we can associate a 2×2 matrix over $\mathbb{C}$ to each element of $\mathcal{Q}_8$ in such a way that the group operation corresponds to matrix multiplication. Here's one way of doing this:

$$1 \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \longleftrightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \longleftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k \longleftrightarrow \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(The matrices for $-1, -i, -j, -k$ are just the negatives of these.) Now you can check that the group operation in $\mathcal{Q}_8$ does correspond to matrix multiplication, and you know that matrix multiplication is associative, so $\mathcal{Q}_8$ really is a group.

2.3 Integers modulo n

Definition. Suppose $n \geqslant 1$. Define

$$\mathcal{U}_n = \{\, i \in \{1, \ldots, n\} \mid i \text{ is coprime to } n \,\},$$

with the group operation being multiplication mod n.

These are exactly the invertible residues modulo n (which is why the group is often denoted $(\mathbb{Z}/\ltimes Z)^\times$).

For example, $\mathcal{U}_{12} = \{1, 5, 7, 11\}$, with the following Cayley table.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

We'll take it for granted that $\mathcal{U}_n$ is a group.

2.4 Matrix groups

Often we get groups consisting of $n \times n$ matrices with the group operation being matrix multiplication.

We're quite well prepared to work with groups of matrices, since we know a lot about how the group axioms apply to matrices. For example, we know already that matrix multiplication is associative. Also, we know what the identity matrix in our group must be. Finally, we know about inverses: a matrix is invertible if and only if its determinant is non-zero, and if it is, then we know how to compute the inverse.

Definition. Suppose $\mathbb{F}$ is a field and $n \in \mathbb{N}$. The **general linear group** $\mathrm{GL}_n(\mathbb{F})$ is the set of all invertible $n \times n$ matrices over $\mathbb{F}$, with the group operation being matrix multiplication.

You should remember roughly what a field is. The fields we'll use in this course are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the field $\mathbb{F}_p$ where p is a prime: this is the set $\{0, 1, \ldots, p-1\}$, with addition and multiplication mod p.

From the comments above, $\mathrm{GL}_n(\mathbb{F})$ is certainly a group. If $\mathbb{F}$ is finite, then $\mathrm{GL}_n(\mathbb{F})$ will be finite. For example, take $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$. Then $\mathrm{GL}_n(\mathbb{F})$ contains just six matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Definition. Suppose $\mathbb{F}$ is a field and $n \in \mathbb{N}$. The **special linear group** $\mathrm{SL}_n(\mathbb{F})$ is the set of all $n \times n$ matrices over $\mathbb{F}$ with determinant 1, with the group operation being matrix multiplication.

We'll occasionally see some other examples of matrix groups.

- ◇ The group of upper-triangular invertible $n \times n$ matrices. Note that if a matrix is upper-triangular, it's quite easy to check whether it's invertible – you just need all the diagonal entries to be non-zero.
- ◇ The group of upper-triangular $n \times n$ matrices with 1s on the diagonal.

If your matrix skills are rusty, then you should check as an exercise that these are subgroups of $\mathrm{GL}_n(\mathbb{F})$.

2.5 Symmetry groups of geometric objects

Definition. Suppose P is a geometric object in $\mathbb{R}^n$. A **symmetry** of P is a rigid transformation of $\mathbb{R}^n$ which fixes P. The **symmetry group** of P is the group of all symmetries of P, with the group operation being composition.

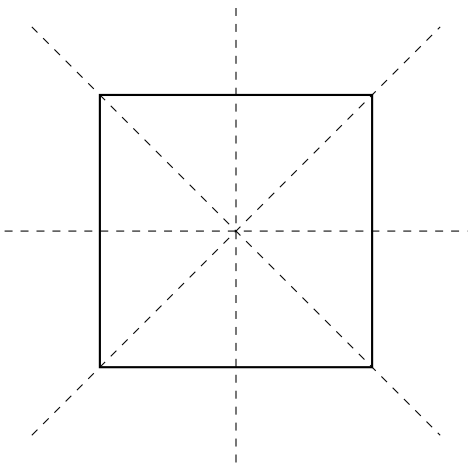
By a geometric object, I really mean any subset on $\mathbb{R}^n$, though we will usually be thinking of things like polygons or polyhedra.

By rigid transformations, we mean things like rotations, reflections and translations. (The proper term for rigid transformations is **isometries**.) We'll take the following facts for granted:

- ◇ the composition of two rigid transformations is a rigid transformation;
- ◇ the identity map on $\mathbb{R}^n$ is a rigid transformation;
- ◇ every rigid transformation has an inverse.

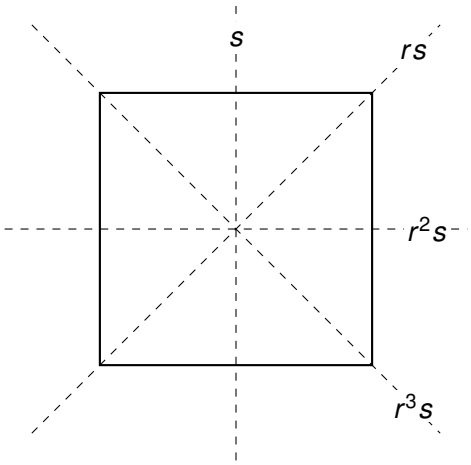
Note that these statements give us the group axioms G1, G3, G4. Axiom G2 follows from Proposition 1.5. So the symmetry group of P really is a group.

Key example. Suppose P is a square. Then the symmetry group of P contains eight elements. There are four reflections, in the following axes.



There are also four rotations about the centre of P, through $0^\circ, 90^\circ, 180^\circ, 270^\circ$. Of course, rotation through 0° is the identity element of the group.

Let's look more closely at the group operation in this group, and fix some notation that we'll use for the rest of the course. Let r denote the rotation through 90° clockwise, and let s denote the reflection in the vertical axis. Then the rotations through $0^\circ, 90^\circ, 180^\circ, 270^\circ$ are $1, r, r^2, r^3$ respectively. And the reflections are s, rs, r^2s, r^3s, as follows.



So $G = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$. r has order 4 and s has order 2, and we have $sr = r^3s$. And these relations allow us to work out the group operation completely.

In fact it's usually more convenient to write the relation $sr = r^3s$ as $sr = r^{-1}s$. Now let's generalise this example.

Definition. Suppose $n \geqslant 3$. The **dihedral group** $\mathcal{D}_{2n}$ is the symmetry group of a regular n-sided polygon.

Basic facts about $\mathcal{D}_{2n}$:

- $\mathcal{D}_{2n}$ contains exactly $2n$ elements: n reflections and n rotations;
- if we let r be the rotation through $(360/n)^\circ$ clockwise, and we fix one of the reflections s, then the rotations are $1, r, r^2, \ldots, r^{n-1}$, and the reflections are $s, rs, r^2s, \ldots, r^{n-1}s$;
- r has order n, s has order 2, and we have $sr = r^{-1}s$, and this allows us to work out the group operation completely.

We'll use the dihedral groups (especially $\mathcal{D}_8$) as a key example throughout the course. But let's have a quick look at a more complicated example.

Example. Suppose P is a cube. Then the symmetry group contains 48 elements. These are as follows.

- 24 rotations:
  - through $0^\circ, 90^\circ, 180^\circ, 270^\circ$ about an axis joining two opposite faces,
  - through $0^\circ, 180^\circ$ about an axis joining two opposite edges,
  - through $0^\circ, 120^\circ, 240^\circ$ about an axis joining two opposite vertices.

- 9 reflections:
  - three reflections in planes parallel to the faces, and
  - six reflections in planes containing two opposite edges.
- 15 **rotatory reflections**, i.e. composition of a rotation and a reflection where the plane of reflection is perpendicular to the axis of rotation.

2.6 The symmetric group

Definition. Suppose X is a set. A **permutation** of X is a bijection from X to X. Sym_X is defined to be the set of all permutations of X.

Proposition 2.1. *Sym_X is a group under composition of functions.*

Proof. We check the group axioms.

G1. Suppose $\phi, \psi \in \mathrm{Sym}_X$. Then $\phi \circ \psi$ is certainly a function from X to X, and we have to check that it is both injective and surjective.

Injective: Suppose $(\phi \circ \psi)(x) = (\phi \circ \psi)(y)$ for $x, y \in X$. This means $\phi(\psi(x)) = \phi(\psi(y))$. Since ϕ is injective, this means $\psi(x) = \psi(y)$. Since ψ is injective, this means $x = y$.

Surjective: Suppose $x \in X$. We need to show that there is $z \in X$ such that $(\phi \circ \psi)(z) = x$. Since ϕ is surjective, there is $y \in X$ such that $\phi(y) = x$. Since ψ is surjective, there is $z \in X$ such that $\psi(z) = y$. And hence

$$(\phi \circ \psi)(z) = \phi(\psi(z)) = \phi(y) = x.$$

So $\phi \circ \psi \in \mathrm{Sym}_X$.

G2. This follows from Proposition 1.5.

G3. Let id denote the identity map on X, i.e. $\mathrm{id}(x) = x$ for all $x \in X$. Given any $\phi \in \mathrm{Sym}_X$, we have

$$(\mathrm{id} \circ \phi)(x) = \mathrm{id}(\phi(x)) = \phi(x), \qquad (\phi \circ \mathrm{id})(x) = \phi(\mathrm{id}(x)) = \phi(x)$$

for all $x \in X$, so $\mathrm{id} \circ \phi = \phi = \phi \circ \mathrm{id}$. So id is an identity element in Sym_X.

G4. Suppose $\phi \in \mathrm{Sym}_X$. Since ϕ is a bijection, it has an inverse ϕ^{-1} such that

$$\phi^{-1}(\phi(x)) = x = \phi(\phi^{-1}(x))$$

for every $x \in X$. So $\phi^{-1} \circ \phi = \mathrm{id} = \phi \circ \phi^{-1}$, so ϕ^{-1} is an inverse for ϕ. ϕ^{-1} has an inverse, so is a bijection, i.e. $\phi^{-1} \in \mathrm{Sym}_X$. □

Definition. Suppose n is a positive integer. The **symmetric group** $\mathcal{S}_n$ is the group of permutations of $\{1, \ldots, n\}$.

Notation for $\mathcal{S}_n$.
- ◇ In $\mathcal{S}_n$, we write the identity element as id, not 1.
- ◇ For $f \in \mathcal{S}_n$ and $x \in \{1, \ldots, n\}$, we write $f \cdot x$ instead of $f(x)$.

We want an efficient way to write permutations. A cumbersome way is the **two-line notation**, for example

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 8 & 7 & 6 & 5 & 3 & 1 & 2 \end{pmatrix} \in \mathcal{S}_8.$$

A neater and more useful way is **disjoint cycle notation**. Here's how it works. Suppose $f \in \mathcal{S}_n$.

- ◇ Start by writing down any number x between 1 and n.
- ◇ Next to x, write $f \cdot x$, $f^2 \cdot x$, and so on.
- ◇ Continue until you return to x (but don't write x a second time). Put brackets around the number you've written. This is called a **cycle** of f.
- ◇ Write down a new x that hasn't appeared yet, and create the cycle starting from this new x in the same way.
- ◇ Continue until all the numbers from 1 to n have appeared.

For example, the permutation f above in disjoint cycle notation is

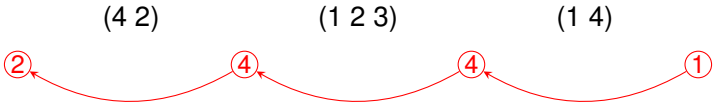
$$(1\ 4\ 6\ 3\ 7)(2\ 8)(5).$$

Disjoint cycle notation is not unique: we can change the order of the cycles, or start a cycle at a different place. And we often leave out the cycles of length 1. So

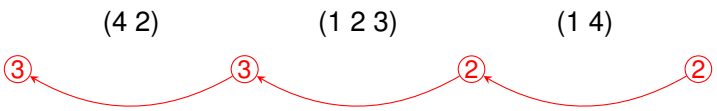
$$(8\ 2)(6\ 3\ 7\ 1\ 4)$$

is also disjoint cycle notation for the permutation f above.

Composing permutations in disjoint cycle notation is done as follows: suppose we have a product of cycles $C_1 C_2 \ldots C_r$. For each number x, we feed x in at the right, replace it with $C_r(x)$, and then replace $C_r(x)$ with $C_{r-1}(C_r(x))$, and so on. For example, suppose we have the product $f = (4\ 2)(1\ 2\ 3)(1\ 4)$. To find $f \cdot 1$, we have the following:



so $f \cdot 1 = 2$. Similarly



so $f \cdot 2 = 3$. In the same way you should find that $f \cdot 3 = 1$ and $f \cdot 4 = 4$, so $f = (1\ 2\ 3)$. It takes a bit of practice to get used to composing permutations like this.

Remark. Note that (8 2)(6 3 7 1 4) is indeed the product of the two cycles (8 2) and (6 3 7 1 4), so no confusion can occur.

Disjoint cycle notation has several advantages over two-line notation. The next two lemmas give two of them.

Lemma 2.2. *Suppose $f \in \mathcal{S}_n$ is written in disjoint cycle notation. Then f^{-1} is obtained by reversing all the cycles.*

Proof. Suppose $(a_1\ \ldots\ a_r)$ is a cycle of f. This means that

$$f \cdot a_1 = a_2, \qquad f \cdot a_2 = a_3, \qquad \ldots \quad f \cdot a_{r-1} = a_r, \qquad f \cdot a_r = a_1.$$

Applying f^{-1}, we get

$$f^{-1} \cdot a_r = a_{r-1}, \quad f^{-1} \cdot a_{r-1} = a_{r-2}, \quad \ldots \quad f^{-1} \cdot a_2 = a_1, \quad f^{-1} \cdot a_1 = a_r,$$

so $(a_r\ \ldots\ a_1)$ is a cycle of f^{-1}. If we repeat this for all the cycles of f, we get the disjoint cycle notation for f^{-1}. □

Now we consider orders. It's very well known that $|\mathcal{S}_n| = n!$, so we won't prove this. For the order of an element, we have the following.

Lemma 2.3. *Suppose $f \in \mathcal{S}_n$. Then* ord(f) *is the least common multiple of the lengths of the cycles of f.*

Proof. Suppose $(a_1\ \ldots\ a_r)$ is a cycle of f. This means that we have $f \cdot a_1 = a_2$, $f^2 \cdot a_1 = a_3$ and so on; in general, $f^m \cdot a_1 = a_{1+m}$, but the $1 + m$ has to be read modulo r.

Hence we have $f^m \cdot a_1 = a_1$ if and only if $1 + m \equiv 1 \pmod{r}$, i.e. $r \mid m$. The same thing applies to any element of any cycle. So

$$\begin{aligned} \text{ord}(f) &= \min\{m > 0 \mid f^m = \text{id}\} \\ &= \min\{m > 0 \mid f^m \cdot a = a \text{ for all } a\} \\ &= \min\{m > 0 \mid \text{every cycle length divides } m\} \\ &= \text{l.c.m.(cycle lengths of } f). \end{aligned}$$

□

Now we'll look at a very important subgroup of $\mathcal{S}_n$.

2.7 The alternating group

Definition. We call a permutation an *m*-**cycle** if it has one cycle of length m, and its other cycles all have length 1. A 2-cycle is also known as a **transposition**.

Lemma 2.4. *Every element of $\mathcal{S}_n$ can be written as a product of transpositions.*

Proof. The cycle $(a_1\ a_2\ \ldots\ a_k)$ can be written as

$$(a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k).$$

Since each permutation can be written as a product of cycles, it can therefore be written as a product of transpositions. □

Remarks.

1. This lemma is intuitively obvious: it says that you can put things in any order you want by repeatedly swapping pairs.
2. Remember that when we talk about products we include the "empty product", i.e. the product of no transpositions, which equals id. So the lemma is true even for $n = 1$ (when there are no transpositions).

Definition. Suppose $f \in \mathcal{S}_n$. Then f is **even** if it can be written as a product of an even number of transpositions, and **odd** if it can be written as a product of an odd number of transpositions.
The **alternating group** $\mathcal{A}_n$ is the set of even permutations in $\mathcal{S}_n$.

For example, (1 2 3 4) is odd, because (1 2 3 4) = (1 2)(2 3)(3 4). On the other hand, (1 2 3)(4 5 6) is even, because (1 2 3)(4 5 6) = (1 2)(2 3)(4 5)(5 6).

Lemma 2.4 tells us that every permutation is either even or odd. But at this stage it's not clear whether a permutation can be both even and odd: there might be a way of writing a permutation as a product of an even number of transpositions, and a completely different way of writing it as a product of an odd number of transpositions. In fact we'll see soon that this can't happen.

Proposition 2.5. $\mathcal{A}_n \leqslant \mathcal{S}_n$.

Proof. We apply the Subgroup Test.

S1. As remarked above, id is the product of zero transpositions. Since 0 is even, id $\in \mathcal{A}_n$, so $\mathcal{A}_n$ is non-empty.

S2. Suppose $f, g \in \mathcal{A}_n$. Then f and g can each be written as the product of an even number of transpositions, say

$$f = f_1 \ldots f_k, \qquad g = g_1 \ldots g_l,$$

where k, l are even. Then

$$fg^{-1} = f_1 \ldots f_k (g_1 \ldots g_l)^{-1} = f_1 \ldots f_k g_l^{-1} \ldots g_1^{-1}.$$

But any transposition is its own inverse, so

$$fg^{-1} = f_1 \ldots f_k g_l \ldots g_1$$

which is a product of $k + l$ transpositions. Since $k + l$ is even, fg is an even permutation. □

So we have a subgroup of $\mathcal{S}_n$, but it's not clear that it's not the whole of $\mathcal{S}_n$: could a permutation be both even and odd? Our next aim is to show that it can't. First we need a definition.

Definition. Suppose $f \in \mathcal{S}_n$. An **inversion** of f is a pair of numbers $a, b \in \{1, \ldots, n\}$ such that $a < b$ but $f \cdot a > f \cdot b$. We write $\mathrm{inv}(f)$ for the number of inversions of f.

Example. Suppose $f = (2\ 3\ 5)$. Then the inversions of f are $\{2,5\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$, so $\mathrm{inv}(f) = 4$.

We want to know how $\mathrm{inv}(g)$ changes when we multiply by transpositions.

Lemma 2.6. *Suppose $g \in \mathcal{S}_n$ and $1 \leqslant c < d \leqslant n$, and let $h = (c\ d)g$. Then $\mathrm{inv}(g)$ is even if and only if $\mathrm{inv}(h)$ is odd.*

Proof. Given any pair $\{a, b\}$, consider applying h to the numbers a and b. To do this, first we apply g to get the numbers $g \cdot a$ and $g \cdot b$ (which might or might not be in the same order as a and b) and then we apply $(c\ d)$ to the numbers $g \cdot a$ and $g \cdot b$ (which might or might not change their order). So we have $g \cdot a < g \cdot b$ if and only if $h \cdot a < h \cdot b$, except when the pair $\{g \cdot a, g \cdot b\}$ is an inversion of $(c\ d)$. So the number of pairs $\{a, b\}$ which are inversions of either g or h but not both is the number of inversions of $(c\ d)$. But we can write down all the inversions of $(c\ d)$: they are the pairs $\{c, e\}$ for $c < e \leqslant d$ and the pairs $\{e, d\}$ for $c < e < d$. So $\mathrm{inv}((c\ d)) = 2(d - c) - 1$, which is odd. So $\mathrm{inv}(h) - \mathrm{inv}(g)$ is a sum of an odd number of terms all equal to ± 1, so is odd. □

Proposition 2.7. *Suppose $f \in \mathcal{S}_n$. If f is even, then $\mathrm{inv}(f)$ is even. If f is odd, then $\mathrm{inv}(f)$ is odd. So f cannot be both even and odd.*

Proof. Consider building up f as a product of transpositions. We start from id, which has no inversions. Each time we multiply by another transposition, the number of inversions changes from even to odd or from odd to even, by Lemma 2.6. So if we have an even number of transpositions (i.e. f is an even permutation) then we end up with an even number of inversions, and if we have an odd number of transpositions, then we end up with an odd number of inversions. □

Now we'd like to be able to tell from disjoint cycle notation whether a permutation is even or odd.

Definition. Suppose $f \in \mathcal{S}_n$. Write $\mathrm{ev}(f)$ for the number of cycles of f of even length.

For example, if $f = (1\ 5\ 3\ 8)(2\ 7)(4\ 9\ 6)$, then $\mathrm{ev}(f) = 2$.

Proposition 2.8. *Suppose $f \in \mathcal{S}_n$. Then f is even if and only if $\mathrm{ev}(f)$ is even.*

Proof. As we saw earlier, a cycle of length m can be written as a product of $m - 1$ transpositions:

$$(a_1\ a_2\ \ldots\ a_m) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{m-1}\ a_m).$$

So if we write f in disjoint cycle notation and then replace each cycle with a product of transpositions like this, then each cycle of even length contributes an odd number of transpositions and vice versa. So if we want to know the total number of transpositions modulo 2, we can count 1 for each cycle of even length and 0 for each cycle of odd length, and we just get $\mathrm{ev}(f) \pmod 2$. □

We finish this section by working out the order of $\mathcal{A}_n$.

Proposition 2.9. *Suppose $n \geqslant 2$. Then $|\mathcal{A}_n| = \frac{n!}{2}$.*

Proof. Let $g = (1\ 2)$. Then we have a function

$$\begin{aligned} \phi : \mathcal{S}_n &\longrightarrow \mathcal{S}_n \\ f &\longmapsto fg. \end{aligned}$$

ϕ is a bijection, because it has an inverse (in fact, it is its own inverse).

If f is even, then fg is odd (because we've multiplied by one more transposition) and vice versa. So ϕ gives a bijection between the set of even permutations and the set of odd permutations. So the number of even permutations in $\mathcal{S}_n$ equals the number of odd permutations, i.e.

$$|\mathcal{A}_n| = |\mathcal{S}_n \setminus \mathcal{A}_n|.$$

Hence $|\mathcal{A}_n| = \frac{|\mathcal{S}_n|}{2}$. □

3 Cosets and conjugacy

3.1 Cosets

Definition. Suppose G is a group, $H \leqslant G$ and $g \in G$.
The **right coset of** H **containing** g is the set

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

The **left coset of** H **containing** g is the set

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

Example. Take $G = \mathcal{S}_3$, $H = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}$ and $g = (2\ 3)$. Then

$$Hg = \{(2\ 3), (1\ 2\ 3)\}, \qquad gH = \{(2\ 3), (1\ 3\ 2)\}.$$

Remarks.

1. H is always a right coset of itself, since

$$H1 = \{ h1 \mid h \in H \} = \{ h \mid h \in H \} = H.$$

2. We can have $Hf = Hg$ even when $f \neq g$. For example, let $G = \mathcal{C}_6 = \{1, z, z^2, z^3, z^4, z^5\}$. Then $H = \{1, z^3\}$ is a subgroup. We have $Hz = \{z, z^4\}$, and also $Hz^4 = \{z, z^4\}$. Later on, we'll see exactly when $Hf = Hg$.

Proposition 3.1. *Suppose G is a group, $H \leqslant G$ and $f, g \in G$.*

1. $|Hg| = |H|$.
2. *If $f \in Hg$, then $Hf = Hg$.*
3. *Each element of G is contained in exactly one right coset of H.*

Proof.

1. We define a map

$$\begin{aligned} \phi : H &\longrightarrow Hg \\ h &\longmapsto hg, \end{aligned}$$

and we claim that ϕ is a bijection.

Injective: Suppose $h, k \in H$ with $\phi(h) = \phi(k)$. Then $hg = kg$; multiplying both sides by g^{-1}, we get $h = k$.

Surjective: Hg is by definition the image of ϕ.

So ϕ is a bijection, so $|Hg| = |H|$.

2. Since $f \in Hg$, we can write $f = hg$ for some $h \in H$. Then we have $g = h^{-1}f$.

To show that $Hf \subseteq Hg$**:** Given an element of Hf, we can write it as kf, where $k \in H$. Then we have $kf = khg$, and this is in Hg, since $kh \in H$.

To show that $Hg \subseteq Hf$**:** Given an element of Hg, we can write it as lg, where $l \in H$. Then we have $lg = lh^{-1}f$, and this is in Hf, since $lh^{-1} \in H$.

So $Hf = Hg$.

3. Given $f \in G$, we have $f = 1f \in Hf$. If f is contained in another right coset Hg, then $Hg = Hf$, by (2). So Hf is the only right coset containing f. □

This gives us an efficient method for finding all the right cosets of a subgroup $H \leqslant G$: at each stage we choose an element $g \in G$ that hasn't yet appeared, and write out the coset Hg. We repeat until all the elements of G have appeared.

Example. Take $G = \mathcal{D}_8$ and $H = \{1, rs\}$. Then the right cosets are

$$\begin{aligned} H1 &= \{1, rs\} \\ Hr &= \{r, s\} \\ Hr^2 &= \{r^2, r^3s\} \\ Hr^3 &= \{r^3, r^2s\}. \end{aligned}$$

We know we can stop at this point because all the elements of $\mathcal{D}_8$ have appeared.

Lemma 3.2 (Coset Lemma)**.** *Suppose G is a group, $H \leqslant G$ and $f, g \in G$. Then:*

- ◇ *$Hf = Hg$ if and only if $fg^{-1} \in H$;*
- ◇ *$fH = gH$ if and only if $f^{-1}g \in H$.*

Proof. We'll prove only the first part, since the second part is very similar.

First suppose $Hf = Hg$. Then

$$f = 1f \in Hf = Hg,$$

so we can write $f = hg$ for some $h \in H$. So $fg^{-1} = h \in H$.

Conversely, suppose $fg^{-1} \in H$. Then

$$f = \underbrace{fg^{-1}}_{\in H} g \in Hg,$$

so by Proposition 3.1(2), $Hf = Hg$. □

Proposition 3.3. *If G is a group and $H \leqslant G$, then the number of right cosets of H is equal to the number of left cosets of H.*

Proof. We define a map

$$\begin{aligned} \theta : \left\{ \begin{matrix} \text{left cosets} \\ \text{of } H \end{matrix} \right\} &\longrightarrow \left\{ \begin{matrix} \text{right cosets} \\ \text{of } H \end{matrix} \right\} \\ gH &\longmapsto Hg^{-1}. \end{aligned}$$

which is we claim is a bijection. First we need to check that θ is well-defined.

- θ **is well-defined:** Suppose $f, g \in G$ and $fH = gH$. Then by the Coset Lemma, $f^{-1}g \in H$. By the Coset Lemma again, this means that $Hf^{-1} = Hg^{-1}$.
- θ **is injective:** Suppose $\theta(fH) = \theta(gH)$. Then $Hf^{-1} = Hg^{-1}$, so by the Coset Lemma $f^{-1}g \in H$. By the Coset Lemma again, $fH = gH$.
- θ **is surjective:** Given a right coset Hf, we have $Hf = \theta(f^{-1}H)$. □

Remark. It's important that we defined θ the way we did, rather than the more obvious $\theta : gH \mapsto Hg$. This would not be well-defined, since we can have $fH = gH$ but $Hf \neq Hg$.

Definition. Suppose G is a group and $H \leqslant G$. The **index** of H in G is the number of right cosets of H in G, written as $|G : H|$.

Theorem 3.4 (Lagrange's Theorem)**.** *Suppose G is a group and $H \leqslant G$. Then $|G| = |H|\,|G : H|$. In particular, if G is finite then $|H|$ divides $|G|$.*

Proof. There are $|G : H|$ right cosets of H in G, and they all have size $|H|$, by Proposition 3.1(1). So the total size of these cosets together is $|H|\,|G : H|$. By Proposition 3.1(3), each element of G lies in exactly one of these cosets, so the number of elements of G must be $|H|\,|G : H|$. □

Corollary 3.5. *Suppose G is a finite group and $g \in G$. Then* ord(g) *divides $|G|$.*

Proof. Let $H = \langle g \rangle$. Then $H \leqslant G$ and $|H| = \text{ord}(g)$, so by Lagrange's Theorem ord$(g) = |H|$ divides $|G|$. □

This corollary is very helpful in looking for subgroups of a particular order: it tells us that if we're looking for a subgroup of G of order m, this subgroup can only contain elements of order dividing m. This can often narrow down our search.

3.2 Conjugacy

Definition. Suppose G is a group and $f, g \in G$. We say that f is **conjugate** to g in G (written $f \sim_G g$) if there is $k \in G$ such that $kfk^{-1} = g$.

Example. Take $G = \mathcal{S}_3$. Then (1 2) $\sim_{\mathcal{S}_3}$ (2 3), since if k = (1 2 3) then $k(1\ 2)k^{-1}$ = (2 3). On the other hand, id $\not\sim_{\mathcal{S}_3}$ (2 3), because for any k we have $k\,\text{id}\,k^{-1}$ = id; so id is conjugate only to itself.

Lemma 3.6. *Suppose G is a group. Then $\sim_G$ is an equivalence relation.*

Proof.

- **Reflexive:** Given $g \in G$, we have $g = 1g1^{-1}$, so $g \sim_G g$.
- **Symmetric:** If $f \sim_G g$, then there $k \in G$ such that $kfk^{-1} = g$. But then we have $f = k^{-1}gk = k^{-1}g(k^{-1})^{-1}$, so $g \sim_G f$.

Transitive: Suppose we have $f, g, h \in G$ such that $f \sim_G g \sim_G h$. This means there exist $k, l \in G$ such that

$$kfk^{-1} = g, \qquad lgl^{-1} = h.$$

Combining these, we get

$$h = lkfk^{-1}l^{-1} = (lk)f(lk)^{-1},$$

so $f \sim_G h$. □

The equivalence classes under the relation $\sim_G$ are called the **conjugacy classes** of G. We may write $\mathrm{ccl}(g)$ for the conjugacy class containing g, i.e.

$$\mathrm{ccl}(g) = \left\{ kgk^{-1} \;\middle|\; k \in G \right\}.$$

Some conjugacy classes consist of just a single element; for example, the only element conjugate to 1 is 1 itself (because $k1k^{-1} = 1$ for any k), so $\{1\}$ is always a conjugacy class.

Example. Let $G = \mathcal{D}_8$. A long calculation shows that the conjugacy classes in $\mathcal{D}_8$ are

$$\{1\},\ \{r, r^3\},\ \{r^2\},\ \{s, r^2s\},\ \{rs, r^3s\}.$$

So in this case the conjugacy classes correspond to "types of symmetry":

- r and r^3 are both 90° rotations;
- r^2 is the only 180° rotation;
- s and r^2s are both reflections in axes parallel to the sides of the square;
- rs and r^3s are both reflections in diagonals of the square.

Definition. If G is a group, the **centre** of G is

$$Z(G) = \{ g \in G \mid hg = gh \text{ for all } h \in G \}.$$

Examples.

- Suppose G is abelian. Then $hg = gh$ for all g, h, so $Z(G) = G$.
- Let's find the centre of $\mathcal{Q}_8$. Certainly $1 \in Z(\mathcal{Q}_8)$, because $1g = g = g1$ for all g. Also $-1 \in Z(\mathcal{Q}_8)$, because -1 changes the sign of everything whether we multiply it from the left or the right.

  $ij \neq ji$, which means that neither i nor j is in $Z(\mathcal{Q}_8)$. Similarly we can show $-i, -j, k, -k \notin Z(\mathcal{Q}_8)$. So $Z(\mathcal{Q}_8) = \{1, -1\}$.

Proposition 3.7. *If G is a group, then $Z(G) \leqslant G$.*

Proof. We apply the Subgroup Test.

S1. For any $h \in G$ we have

$$h1 = h = 1h,$$

so $1 \in Z(G)$.

S2. Suppose $f, g \in Z(G)$. Then for any $h \in G$

$$hfg^{-1} = fhg^{-1} = fg^{-1}ghg^{-1} = fg^{-1}hgg^{-1} = fg^{-1}h,$$

so $fg^{-1} \in Z(G)$. □

Now here's the connection between conjugacy and the centre of a group.

Lemma 3.8. *Suppose G is a group and $g \in G$. Then $g \in Z(G)$ if and only if g lies in a conjugacy class by itself.*

Proof. If g lies in a conjugacy class by itself, then $hgh^{-1} = g$ for all $h \in G$, i.e. $hg = gh$ for all $h \in G$, so $g \in Z(G)$.

Conversely, if $g \in Z(G)$, then

$$\mathrm{ccl}(g) = \left\{ hgh^{-1} \;\middle|\; h \in G \right\} = \{g\}.$$ □

Example. From the example above where we found the conjugacy classes in $\mathcal{D}_8$, the only elements of $\mathcal{D}_8$ lying in a conjugacy class by themselves are 1 and r^2. So $Z(\mathcal{D}_8) = \{1, r^2\}$.

3.3 Conjugacy in $\mathcal{S}_n$

In this section, we look at conjugacy in $\mathcal{S}_n$. We start with the centre of $\mathcal{S}_n$.

Proposition 3.9. *Suppose $n \geqslant 3$. Then $Z(\mathcal{S}_n) = \{\mathrm{id}\}$.*

Proof. We know $\mathrm{id} \in Z(\mathcal{S}_n)$, so we just need to show that if $g \in \mathcal{S}_n$ and $g \neq \mathrm{id}$ then $g \notin Z(\mathcal{S}_n)$, i.e. there is some $h \in \mathcal{S}_n$ such that $gh \neq hg$.

Since $g \neq \mathrm{id}$, we can find $a \neq b \in \{1, \ldots, n\}$ such that $g \cdot a = b$. Let $c \in \{1, \ldots, n\}$ be different from a and b, and let $h = (b\ c)$. Then

$$gh \cdot a = g \cdot a = b, \qquad hg \cdot a = h \cdot b = c,$$

so $gh \neq hg$. □

Now we want a way to tell whether two elements of $\mathcal{S}_n$ are conjugate.

Definition. Suppose $f \in \mathcal{S}_n$, written in disjoint cycle notation. The **cycle type** of f is the list of the lengths of the cycles of f, written in decreasing order.

Example. In $\mathcal{S}_9$, the permutation (1 4 3)(2 8 9 6) has cycle type $(4, 3, 1, 1)$. Notice in particular that the cycle lengths must be written in decreasing order, and we include cycles of length 1 (even though we usually don't write them when we're writing down the permutation).

Proposition 3.10. *Suppose $f, g \in \mathcal{S}_n$. Then $f \sim_{\mathcal{S}_n} g$ if and only if f and g have the same cycle type.*

Proof. Suppose first that f, g are conjugate. Then there is $k \in \mathcal{S}_n$ such that $g = kfk^{-1}$.

Suppose $(a_1 \ \dots \ a_r)$ is a cycle of f. This means

$$f \cdot a_1 = a_2, \qquad f \cdot a_2 = a_3, \qquad \dots \qquad f \cdot a_r = a_1$$

which gives

$$k^{-1}gk \cdot a_1 = a_2, \qquad k^{-1}gk \cdot a_2 = a_3, \qquad \dots \qquad k^{-1}gk \cdot a_r = a_1.$$

Applying k throughout, we get

$$g \cdot (k \cdot a_1) = k \cdot a_2, \quad g \cdot (k \cdot a_2) = k \cdot a_3, \qquad \dots \qquad g \cdot (k \cdot a_r) = k \cdot a_1.$$

And this means that $(k \cdot a_1 \ \dots \ k \cdot a_r)$ is a cycle of g. So for every cycle of f, there is a corresponding cycle of g of the same length. So the list of the lengths of the cycles of f is the same as the list of the lengths of the cycles for g, i.e. f and g have the same cycle type.

Conversely, suppose f and g have the same cycle type. Then we can pair up the cycles of f with the cycles of g so that each cycle of f is paired with a cycle of g of the same length. Say we've paired up the cycle $(a_1 \ \dots \ a_r)$ of f with the cycle $(b_1 \ \dots \ b_r)$ of g; we define $k \cdot a_i = b_i$ for each i.

Then for each i we have

$$kfk^{-1} \cdot b_i = kf \cdot a_i = k \cdot a_{i+1} = b_{i+1} = g \cdot b_i. \qquad (*)$$

Doing this for every cycle, we get a function $k : \{1, \dots, n\} \to \{1, \dots, n\}$ (because every number in $\{1, \dots, n\}$ appears in exactly one cycle of f). Furthermore, k is a bijection (because every number in $\{1, \dots, n\}$ appears in exactly one cycle of g); that is, $k \in \mathcal{S}_n$. By $(*)$ we have $kfk^{-1} \cdot b = g \cdot b$ for all $b \in \{1, \dots, n\}$, so $kfk^{-1} = g$. □

The proof of Proposition 3.10 gives us the following.

How to conjugate in $\mathcal{S}_n$.

- ◇ Suppose we have f and k, and we want to write down kfk^{-1}. We just write write f in disjoint cycle notation, and then replace each number a that appears with $k \cdot a$.

  For example, suppose

  $$f = (1\ 3\ 5\ 6)(2\ 8)(4\ 9\ 7), \qquad k = (1\ 4\ 3\ 6\ 2)(5\ 8).$$

  Then in the expression $(1\ 3\ 5\ 6)(2\ 8)(3\ 9\ 4)$ we just replace 1 with 4, 3 with 6 and so on to get $kfk^{-1} = (4\ 6\ 8\ 2)(1\ 5)(3\ 9\ 7)$.

- ◇ Suppose we have f and g with the same cycle type and we want to find k such that $g = kfk^{-1}$. Write f and g in disjoint cycle notation so that the cycle lengths match up. Then for each a, find a in the disjoint cycle notation for f, and define $k \cdot a$ to be the number in the corresponding position in the disjoint cycle notation for g.

  For example, suppose

  $$f = (1\ 3\ 6\ 4)(2\ 5), \qquad g = (1\ 5)(2\ 4\ 3\ 6).$$

  We re-write g as $(2\ 4\ 3\ 6)(1\ 5)$, and then define k by mapping $1 \mapsto 2$, $3 \mapsto 4$, and so on, and we get $k = (1\ 2)(3\ 4\ 6)$.

So we've seen another advantage of using disjoint cycle notation. Let's summarise the advantages we've seen.

Advantages of using disjoint cycle notation.

- ◇ We can easily write down the inverse of a permutation. (Just reverse all the cycles.)
- ◇ We can easily write down the order of a permutation. (The l.c.m. of the cycle lengths.)
- ◇ We can easily tell whether a permutation is even or odd. (ev(f) is even or odd.)
- ◇ We can easily tell whether two permutations are conjugate. (They have the same cycle type.)

3.4 Conjugate subgroups

Definition. Suppose G is a group, $H \leqslant G$ and $g \in G$. Define

$$gHg^{-1} = \left\{ ghg^{-1} \;\middle|\; h \in H \right\}.$$

Example. Take $G = \mathcal{S}_4$ and $H = \langle (1\ 2\ 3\ 4) \rangle = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$. If $g = (1\ 2\ 3)$, then

$$gHg^{-1} = \{\mathrm{id}, (2\ 3\ 1\ 4), (2\ 1)(3\ 4), (2\ 4\ 1\ 3)\} = \langle (2\ 3\ 1\ 4) \rangle.$$

Lemma 3.11. *Suppose G is a group, $H \leqslant G$ and $g \in G$. Then gHg^{-1} is a subgroup of G.*

Proof. We apply the Subgroup Test.

S1. $1 \in H$, so $g1g^{-1} \in gHg^{-1}$, so gHg^{-1} is non-empty.

S2. Suppose we have two elements of gHg^{-1}. These can be written as ghg^{-1} and gkg^{-1}, where $h, k \in H$. We know $hk^{-1} \in H$ because H is a subgroup, so

$$(ghg^{-1})(gkg^{-1})^{-1} = ghg^{-1}gk^{-1}g^{-1} = g(hk^{-1})g^{-1} \in gHg^{-1}. \qquad \square$$

Definition. Suppose G is a group, and $H, K \leqslant G$. We say that H and K are **conjugate** if $K = gHg^{-1}$ for some $g \in G$.

Conjugacy is an equivalence relation on the set of subgroups of G.

3.5 Normal subgroups and quotient groups

Definition. Suppose G is a group and $N \leqslant G$. We say N is **normal** in G if

$$gng^{-1} \in N \qquad \text{for all } n \in N \text{ and } g \in G.$$

Notation. We write $N \trianglelefteqslant G$ to mean that N is a normal subgroup of G. We use the symbols $\trianglerighteqslant$, $\lhd$, $\rhd$ in the obvious way.

Note that if $N \trianglelefteqslant G$, then $gNg^{-1} = N$ for every $g \in G$. In other words, the only subgroup of G conjugate to N is N itself.

Example. Take $G = \mathcal{D}_8$.

- If $N = \{1, s\}$, then $N \not\trianglelefteq G$, because $rsr^{-1} = r^2 s \notin N$.
- If $N = \{1, r, r^2, r^3\}$, then $N \trianglelefteq G$: we know that $g1g^{-1} = 1$ for every g, and we saw earlier that:
  - $grg^{-1} = r$ or r^3 for every $g \in \mathcal{D}_8$,
  - $gr^2g^{-1} = r^2$ for every $g \in \mathcal{D}_8$,
  - $gr^3g^{-1} = r$ or r^3 for every $g \in \mathcal{D}_8$.

  So $gng^{-1} \in N$ for every $g \in G$ and $n \in N$.

Observe that if $N \trianglelefteq G$ and $n \in N$, then (by the definition of a normal subgroup) every element of G conjugate to n also lies in N. So we have the following way to rephrase the definition.

A subgroup is normal if and only if it is a union of conjugacy classes.

Example. Take $G = \mathcal{S}_4$ and $V = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. It takes a bit of checking to show that $V \leqslant G$, but once we know this we can see straight away that $V \trianglelefteq G$: V consists of all elements of cycle type $(1,1,1,1)$ or $(2,2)$, so is the union of two conjugacy classes in $\mathcal{S}_4$.

Checking quickly whether a subgroup is normal. Suppose we have a group G and a subgroup N. Suppose also that we have a set X of elements of G such that $G = \langle X \rangle$ and a set Y of elements of N such that $N = \langle Y \rangle$ (X and Y are called **generating sets** for G and N). Then to check that $N \trianglelefteq G$ we just need to check that $gng^{-1} \in N$ for all $g \in X$ and $n \in Y$. If X and Y are small, then this means we have much less work to do.
Returning to the second example for $\mathcal{D}_8$ above, we have $G = \langle r, s \rangle$ and $N = \langle r \rangle$. So to check that $N \trianglelefteq G$ all we need to check is that rrr^{-1} and srs^{-1} both belong to N.

The next lemma sometimes gives us a short-cut to showing that a subgroup is normal.

Lemma 3.12. *Suppose G is a group and $N \leqslant G$, and that $|G:N| = 2$. Then $N \trianglelefteq G$.*

Proof. Since $|G:N| = 2$, there are only two right cosets of N in G. Now take $g \in G$ and $n \in N$. If $g \in N$ then obviously $gng^{-1} \in N$. So suppose $g \notin N$. Then Ng is a right coset different from N. But also $gn \notin N$, so Ngn is also a coset different from N. But there is only one right coset of N different from N, so $Ngn = Ng$. So by the Coset Lemma $gng^{-1} \in N$. □

Examples.

- Returning to the case where $G = \mathcal{D}_8$ and $N = \{1, r, r^2, r^3\}$, we can see immediately from Lemma 3.12 that $N \trianglelefteq G$.
- Another example which follows immediately from Lemma 3.12 is that $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$ for all $n \geqslant 2$.

The main reason for defining normal subgroups is to define quotient groups.

Definition. Suppose G is a group and $N \trianglelefteq G$. The **quotient group** G/N is the set of all cosets of N, with group operation

$$(Ng)(Nh) = Ngh.$$

Lemma 3.13. *The group operation on G/N is well-defined.*

Proof. Suppose $g, \hat{g}, h, \hat{h} \in G$ such that $Ng = N\hat{g}$ and $Nh = N\hat{h}$. We need to show that $(Ng)(Nh) = (N\hat{g})(N\hat{h})$, i.e. $Ngh = N\hat{g}\hat{h}$.

By the Coset Lemma, we have $g\hat{g}^{-1} \in N$ and $h\hat{h}^{-1} \in N$. Write $n = h\hat{h}^{-1}$. Since $N \trianglelefteq G$, we have $gng^{-1} \in N$. So

$$(gh)(\hat{g}\hat{h})^{-1} = gh\hat{h}^{-1}\hat{g}^{-1} = gn\hat{g}^{-1} = \underbrace{gng^{-1}}_{\in N}\underbrace{g\hat{g}^{-1}}_{\in N} \in N.$$

So by the Coset Lemma $Ngh = N\hat{g}\hat{h}$. □

Proposition 3.14. *Suppose G is a group and $N \trianglelefteq G$. Then G/N is a group.*

Proof. Let's check the group axioms.

G1. Closure is easy: $(Ng)(Nh)$ is defined to be Ngh, which is a coset of N.

G2. Suppose $g, h, k \in G$. Then

$$\begin{aligned}((Ng)(Nh))(Nk) &= (Ngh)(Nk)\\ &= N(gh)k\\ &= Ng(hk) && \text{using associativity in } G\\ &= (Ng)(Nhk)\\ &= (Ng)((Nh)(Nk)).\end{aligned}$$

G3. If we let 1 denote the identity element of G, we have

$$(N1)(Ng) = N1g = Ng = Ng1 = (Ng)(N1)$$

for every g, so $N1$ is an identity element in G/N.

G4. Given $g \in G$, we have

$$(Ng^{-1})(Ng) = Ng^{-1}g = N1 = Ngg^{-1} = (Ng)(Ng^{-1})$$

so Ng^{-1} is an inverse for Ng in G/N. □

Examples.

◇ Take $G = C_6$, and $N = \{1, z^3\}$, where $z = z_6$. Then $N \leqslant G$, and in fact $N \trianglelefteq G$ (because in an abelian group every subgroup is normal). The cosets of N are

$$N1 = \{1, z^3\}, \qquad Nz = \{z, z^4\}, \qquad Nz^2 = \{z^2, z^5\}$$

so $G/N = \{N1, Nz, Nz^2\}$, with Cayley table

	$N1$	Nz	Nz^2
$N1$	$N1$	Nz	Nz^2
Nz	Nz	Nz^2	$N1$
Nz^2	Nz^2	$N1$	Nz

.

◇ For another example, take $G = \mathcal{Q}_8$ and $N = \{1, -1\}$. Then you can check that $N \trianglelefteq G$. The cosets are

$$N1 = \{1, -1\}, \qquad Ni = \{i, -i\}, \qquad Nj = \{j, -j\}, \qquad Nk = \{k, -k\}$$

and the Cayley table for G/N is as follows.

	$N1$	Ni	Nj	Nk
$N1$	$N1$	Ni	Nj	Nk
Ni	Ni	$N1$	Nk	Nj
Nj	Nj	Nk	$N1$	Ni
Nk	Nk	Nj	Ni	$N1$

Proposition 3.15. *Suppose G is a finite group and $N \trianglelefteq G$. Then $|G/N| = |G|/|N|$.*

Proof. By definition $|G/N|$ equals $|G:N|$, and by Lagrange's Theorem this equals $|G|/|N|$. □

3.6 Products of groups

In this section we introduce two constructions we'll use later.

Definition. Suppose G is a group and $H, N \leqslant G$. Define

$$HN = \{\, hn \mid h \in H,\ n \in N \}\,.$$

You might hope that if H and N are subgroups of G then so is HN. But in fact this is not the case.

Example. Take $G = \mathcal{S}_3$, $H = \{\mathrm{id}, (1\ 2)\}$ and $N = \{\mathrm{id}, (2\ 3)\}$. Then

$$HN = \{\mathrm{id}, (1\ 2), (2\ 3), (1\ 2\ 3)\}.$$

(This is not a subgroup of $\mathcal{S}_3$, as we can see straight away from Lagrange's Theorem.)

Proposition 3.16. *Suppose G is a group, $H \leqslant G$ and $N \trianglelefteq G$. Then $HN \leqslant G$. If in addition $H \trianglelefteq G$, then $HN \trianglelefteq G$.*

Proof. Apply the Subgroup Test to HN.

S1. $1 \in H$ and $1 \in N$, so $1 = 11 \in HN$.

S2. Given two elements of HN, we can write them as hm and kn for $h, k \in H$ and $m, n \in N$. Then $hk^{-1} \in H$ and $mn^{-1} \in N$, so by the normal condition $k(mn^{-1})k^{-1} \in N$ as well. So

$$(hm)(kn)^{-1} = hmn^{-1}k^{-1} = \underbrace{hk^{-1}}_{\in H}\underbrace{k mn^{-1}k^{-1}}_{\in N} \in HN.$$

Now suppose $H \trianglelefteq G$. To show that HN is normal in G we need to show that $g(hn)g^{-1} \in HN$ for all $g \in G, h \in H, n \in N$:

$$ghng^{-1} = \underbrace{ghg^{-1}}_{\in H}\underbrace{gng^{-1}}_{\in N} \in HN. \qquad \square$$

Example. Take $G = \mathcal{D}_8$, $H = \{1, rs\}$ and $N = \{1, r^2\}$. Then $N \trianglelefteq G$ (in fact N is the centre of G) and $H \leqslant G$. And

$$HN = \{1, r^2, rs, r^3s\} \leqslant G.$$

Note that if we have $N, H \leqslant G$ and $N \subseteq H$, then $HN = H$. Similarly if $N \supseteq H$, then $HN = N$.

We'll see the group HN again later when we come to the Isomorphism Theorems. But now here's a construction that works for any two groups.

Definition. Suppose G, H are groups. The **direct product** $G \times H$ is the set

$$\{(g, h) \mid g \in G,\ h \in H\}$$

with group operation

$$(g, h)(g', h') = (gg', hh').$$

It is easy to check that $G \times H$ really is a group, with identity element $(1_G, 1_H)$, and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Example. Take $G = \mathcal{C}_2$ and $H = \mathcal{C}_3$. Write z_2 as z, and z_3 as w. Then $\mathcal{C}_2 = \{1, z\}$ and $\mathcal{C}_3 = \{1, w, w^2\}$, so

$$\mathcal{C}_2 \times \mathcal{C}_3 = \{(1,1), (1,w), (1,w^2), (z,1), (z,w), (z,w^2)\},$$

with Cayley table

	$(1,1)$	$(1,w)$	$(1,w^2)$	$(z,1)$	(z,w)	(z,w^2)
$(1,1)$	$(1,1)$	$(1,w)$	$(1,w^2)$	$(z,1)$	(z,w)	(z,w^2)
$(1,w)$	$(1,w)$	$(1,w^2)$	$(1,1)$	(z,w)	(z,w^2)	$(z,1)$
$(1,w^2)$	$(1,w^2)$	$(1,1)$	$(1,w)$	(z,w^2)	$(z,1)$	(z,w)
$(z,1)$	$(z,1)$	(z,w)	(z,w^2)	$(1,1)$	$(1,w)$	$(1,w^2)$
(z,w)	(z,w)	(z,w^2)	$(z,1)$	$(1,w)$	$(1,w^2)$	$(1,1)$
(z,w^2)	(z,w^2)	$(z,1)$	(z,w)	$(1,w^2)$	$(1,1)$	$(1,w)$

3.7 The commutator subgroup

Definition. Suppose G is a group and $f, g \in G$. The **commutator** of f and g (written $[f, g]$) is the element $fgf^{-1}g^{-1}$. The **commutator subgroup** G' (also called the **derived subgroup**) is the subgroup of G generated by all the commutators in G.

(Remember: given elements $g_1, g_2, \ldots$ in a group G, the **subgroup generated by** $g_1, g_2, \ldots$ is the set of all products of $g_1, g_2, \ldots$ and their inverses, where we can take the g_is in any order and take each g_i as many times as we like. So G' is the set of all elements of the form $c_1^{\pm 1} \ldots c_r^{\pm 1}$, where $c_1, \ldots, c_r$ are commutators.)

Examples.

- ◇ Suppose G is abelian. Then for any $f, g \in G$, $[f, g] = fgf^{-1}g^{-1} = ff^{-1}gg^{-1} = 1$, so $G' = \{1\}$.
- ◇ Suppose $G = \mathcal{D}_8$. Then

$$[r, s] = rsr^{-1}s^{-1} = rsr^3s = rssr = r^2.$$

In fact, we can show that every commutator in $\mathcal{D}_8$ equals either 1 or r^2. Recalling the conjugacy classes in $\mathcal{D}_8$ from earlier, we see that every $g \in \mathcal{D}_8$ is conjugate to g, and possibly r^2g, and nothing else. So for any $f, g \in \mathcal{D}_8$, fgf^{-1} equals either g or r^2g. Hence $[f, g] = fgf^{-1}g^{-1} = gg^{-1}$ or r^2gg^{-1}, i.e. $[f, g] = 1$ or r^2. So $G' = \{1, r^2\}$.

Proposition 3.17. *Suppose G is a group. Then $G' \trianglelefteq G$.*

Proof. By definition $G' \leqslant G$, so we have to check that $knk^{-1} \in G'$ for every $k \in G$, $n \in G'$. We make two observations.

1. The inverse of any commutator is a commutator: given $f, g \in G$,

$$[f, g]^{-1} = (fgf^{-1}g^{-1})^{-1} = gfg^{-1}f^{-1} = [g, f].$$

2. Any conjugate of a commutator is a commutator: given $f, g, k \in G$,

$$\begin{aligned} k[f, g]k^{-1} &= kfgf^{-1}g^{-1}k^{-1} \\ &= kfk^{-1}kgk^{-1}kf^{-1}k^{-1}kg^{-1}k^{-1} \\ &= (kfk^{-1})(kgk^{-1})(kfk^{-1})^{-1}(kgk^{-1})^{-1} \\ &= [kfk^{-1}, kgk^{-1}]. \end{aligned}$$

Now take $k \in G$ and $n \in G'$. Then by observation 1, n can be written as

$$c_1 \dots c_r$$

where $c_1, \dots, c_r$ are commutators. Hence

$$knk^{-1} = (kc_1k^{-1}) \dots (kc_rk^{-1})$$

and by observation 2, $kc_1k^{-1}, \dots, kc_rk^{-1}$ are all commutators, so $knk^{-1} \in G'$. □

Proposition 3.18. *Suppose G is a group and $N \trianglelefteq G$. Then G/N is abelian if and only if $G' \leqslant N$.*

Proof.

$$\begin{aligned} G/N \text{ is abelian} &\iff (Nf)(Ng) = (Ng)(Nf) \quad \text{for all } f, g \in G \\ &\iff Nfg = Ngf \quad \text{for all } f, g \in G \\ &\iff fgf^{-1}g^{-1} \in N \quad \text{for all } f, g \in G \qquad \text{by the Coset Lemma.} \end{aligned}$$

So G/N is abelian if and only if N contains every commutator. But N is closed under multiplication, so if it contains every commutator, then it contains G'. □

Example. Take $G = \mathcal{Q}_8$. Then we can check that $[i, j] = -1$. So $\mathcal{Q}_8' \geqslant \{1, -1\}$. On the other hand, $\{1, -1\}$ is a normal subgroup, and $\mathcal{Q}_8/\{1, -1\}$ is abelian (we worked out its Cayley table earlier), so by Proposition 3.17 $\mathcal{Q}_8' \leqslant \{1, -1\}$. So $\mathcal{Q}_8' = \{1, -1\}$.

4 Homomorphisms

4.1 Basic definitions

Definition. Suppose G, H are groups.

- ◇ A **homomorphism** from G to H is a function $\phi : G \to H$ such that $\phi(fg) = \phi(f)\phi(g)$ for all $f, g \in G$.
- ◇ An **isomorphism** from G to H is a homomorphism which is also a bijection.
- ◇ G, H are **isomorphic** (written $G \cong H$) if there is at least one isomorphism from G to H.

Examples.

- ◇ For any groups G, H, there is a homomorphism from G to H defined by $g \mapsto 1$ for all $g \in G$. This is called the **trivial homomorphism**.
- ◇ For any group G, the identity map on G (which we'll write as id_G) is an isomorphism from G to G.
- ◇ If G is any group and $H \leqslant G$, the map $\iota : H \to G$ defined by $\iota(h) = h$ is an injective homomorphism, called the **inclusion homomorphism**.
- ◇ If G is any group and $N \trianglelefteq G$, the map $\pi : G \to G/N$ defined by $\pi(g) = Ng$ is a surjective homomorphism, called the **quotient homomorphism**.
- ◇ There is a homomorphism from $\mathrm{GL}_n(\mathbb{R})$ to $\mathbb{R}^\times$ given by $a \mapsto \det(a)$. This is surjective (assuming $n \geqslant 1$).
- ◇ There is a homomorphism (in fact, an isomorphism) from $\mathcal{U}_{10}$ to $\mathcal{U}_5$ given by $g \mapsto g \pmod 5$.
- ◇ If G is an abelian group, there is an isomorphism from G to G given by $g \mapsto g^{-1}$.

Lemma 4.1. *Suppose G, H are groups and $\phi : G \to H$ is a homomorphism. Then $\phi(1) = 1$, and $\phi(g^{-1}) = \phi(g)^{-1}$ for every $g \in G$.*

Proof.

$$\phi(1) = \phi(11) = \phi(1)\phi(1).$$

Multiplying both sides by $\phi(1)^{-1}$, we get $1 = \phi(1)$.

Now take $g \in G$. Then

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(1) = 1$$

and

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1) = 1,$$

so $\phi(g^{-1})$ is the inverse of $\phi(g)$. □

Definition. Suppose $\phi : G \to H$ is a group homomorphism. The **image** of ϕ is the set $\mathrm{im}(\phi) = \{\phi(g) \mid g \in G\}$. The **kernel** of ϕ is the set $\ker(\phi) = \{g \in G \mid \phi(g) = 1\}$.

Examples.

- ◇ Suppose $\phi : G \to H$ is the trivial homomorphism. Then $\mathrm{im}(\phi) = \{1\}$, and $\ker(\phi) = G$.
- ◇ Suppose $H \leqslant G$, and $\iota : H \to G$ is the inclusion homomorphism. Then $\mathrm{im}(\iota) = H$, and $\ker(\iota) = \{1\}$.
- ◇ Suppose $N \lhd G$ and $\phi : G \to G/N$ is the quotient homomorphism. Then $\mathrm{im}(\phi) = G/N$, and

$$\ker(\phi) = \{\, g \in G \mid \pi(g) = N1 \} = \{\, g \in G \mid Ng = N1 \} = \{\, g \in G \mid g \in N \} = N.$$

- ◇ Consider the determinant homomorphism $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$. $\mathrm{im}(\det) = \mathbb{R}^\times$, and $\ker(\det) = \mathrm{SL}_n(\mathbb{R})$.
- ◇ There is a homomorphism $\phi : \mathcal{C}_4 \to \mathcal{C}_6$ given by $z_4^a \mapsto z_6^{3a}$. Then $\mathrm{im}(\phi) = \{1, z_6^3\}$ and $\ker(\phi) = \{1, z_4^2\}$.

By definition ϕ is surjective if and only if $\mathrm{im}(\phi) = H$. We can also tell from $\ker(\phi)$ whether ϕ is injective.

Lemma 4.2. *Suppose $\phi : G \to H$ is a group homomorphism. Then ϕ is injective if and only if* $\ker(\phi) = \{1\}$.

Proof. Suppose first that ϕ is injective. If $g \in \ker(\phi)$, then $\phi(g) = 1 = \phi(1)$, so by injectivity $g = 1$. So $\ker(\phi) = \{1\}$. Conversely, suppose $\ker(\phi) = \{1\}$. If $f, g \in G$ with $\phi(f) = \phi(g)$, then

$$\phi(fg^{-1}) = \phi(f)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1,$$

so $fg^{-1} \in \ker(\phi)$, so $fg^{-1} = 1$. Multiplying both sides by g, we have $f = g$. So ϕ is injective. □

4.2 The Isomorphism Theorems

Theorem 4.3 (First Isomorphism Theorem)**.** *Suppose G, H are groups and $\phi : G \to H$ is a homomorphism. Then*

(a) $\mathrm{im}(\phi) \leqslant H$*,*

(b) $\ker(\phi) \trianglelefteq G$*, and*

(c) $G/\ker(\phi) \cong \mathrm{im}(\phi)$*.*

Proof.

(a) We apply the Subgroup Test to $\mathrm{im}(\phi)$.

S1. $1 \in G$, so $\phi(1) \in \mathrm{im}(\phi)$, so $\mathrm{im}(\phi)$ is non-empty.

S2. Given two elements of $\mathrm{im}(\phi)$, we can write them as $\phi(f)$, $\phi(g)$ for some $f, g \in G$. Then

$$\phi(f)\phi(g)^{-1} = \phi(f)\phi(g^{-1}) = \phi(fg^{-1}) \in \mathrm{im}(\phi).$$

So $\mathrm{im}(\phi) \leqslant H$.

(b) We apply the Subgroup Test to $\ker(\phi)$.

S1. $\phi(1) = 1$ by Lemma 4.1, so $1 \in \ker(\phi)$.

S2. Take $f, g \in \ker(\phi)$. Then

$$\phi(fg^{-1}) = \phi(f)\phi(g^{-1}) = \phi(f)\phi(g)^{-1} = 11^{-1} = 1,$$

so $fg^{-1} \in \ker(\phi)$.

So $\ker(\phi) \leqslant G$. Now take $g \in G$ and $n \in \ker(\phi)$. Then

$$\begin{aligned}\phi(gng^{-1}) &= \phi(g)\phi(n)\phi(g^{-1}) \\ &= \phi(g)1\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1} \\ &= 1,\end{aligned}$$

so $gng^{-1} \in \ker(\phi)$. So $\ker(\phi) \trianglelefteq G$.

(c) Define

$$\begin{aligned}\theta : \frac{G}{\ker(\phi)} &\longrightarrow \mathrm{im}(\phi) \\ \ker(\phi)g &\longmapsto \phi(g).\end{aligned}$$

We claim θ is well-defined and an isomorphism.

- θ **is well-defined:** Suppose $f, g \in G$ with $\ker(\phi)f = \ker(\phi)g$. We need to show $\phi(f) = \phi(g)$. By the Coset Lemma we have $fg^{-1} \in \ker(\phi)$. So

$$1 = \phi(fg^{-1}) = \phi(f)\phi(g^{-1}) = \phi(f)\phi(g)^{-1},$$

and this gives $\phi(f) = \phi(g)$.

- θ **is a homomorphism:** Given $f, g \in G$, we have

$$\theta\left((\ker(\phi)f)(\ker(\phi)g)\right) = \theta\left(\ker(\phi)(fg)\right) = \phi(fg) = \phi(f)\phi(g) = \theta\left(\ker(\phi)f\right)\theta\left(\ker(\phi)g\right).$$

- θ **is injective:** Suppose $f, g \in G$ with $\theta(\ker(\phi)f) = \theta(\ker(\phi)g)$. Then $\phi(f) = \phi(g)$, so $\phi(fg^{-1}) = \phi(f)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1$. So $fg^{-1} \in \ker(\phi)$, so by the Coset Lemma $\ker(\phi)f = \ker(\phi)g$.

- θ **is surjective:** Given $h \in \mathrm{im}(\phi)$, we have $h = \phi(g)$ for some $g \in G$, so $h = \theta(\ker(\phi)g) \in \mathrm{im}(\theta)$. □

Example. Consider the homomorphism $\phi : \mathcal{Q}_8 \to \mathcal{D}_8$ defined by $\phi(i) = r^2$ and $\phi(j) = s$. Then $\mathrm{im}(\phi) = \langle r^2, s\rangle = \{1, r^2, s, r^2s\}$, and $\ker(\phi) = \{1, -1\}$. Then we can see that $\mathcal{Q}_8/\ker(\phi)$ and $\mathrm{im}(\phi)$ are isomorphic from their Cayley tables, with an isomorphism given by $\ker(\phi)g \mapsto \phi(g)$. We write $K = \ker(\phi)$ in the table below.

	$K1$	Ki	Kj	Kk
$K1$	$K1$	Ki	Kj	Kk
Ki	Ki	$K1$	Kk	Kj
Kj	Kj	Kk	$K1$	Ki
Kk	Kk	Kj	Ki	$K1$

$\mathcal{Q}_8/K$

	1	r^2	s	r^2s
1	1	r^2	s	r^2s
r^2	r^2	1	r^2s	s
s	s	r^2s	1	r^2
r^2s	r^2s	s	r^2	1

$\mathrm{im}(\phi)$

Warning. We are about to prove the Second and Third Isomorphism Theorems. Some books and lecturers number these the other way round.

Theorem 4.4 (Second Isomorphism Theorem)**.** *Suppose G is a group, $H \trianglelefteq G$, $K \trianglelefteq G$ and $K \subseteq H$. Then*

(a) $K \trianglelefteq H$,

(b) $H/K \trianglelefteq G/K$, *and*

(c) $(G/K)/(H/K) \cong G/H$.

Proof.

(a) K is a subset of H which is a group under the same operation, so $K \leqslant H$. Since $K \trianglelefteq G$ we have $gkg^{-1} \in K$ for all $g \in G$ and $k \in K$. This is true in particular for $g \in H$, and hence $K \trianglelefteq H$.

(b,c) We use the First isomorphism Theorem. Define

$$\begin{aligned} \phi : \frac{G}{K} &\longrightarrow \frac{G}{H} \\ Kg &\longmapsto Hg. \end{aligned}$$

We claim ϕ is a well-defined surjective homomorphism.

- ϕ **is well-defined:** Suppose $Kf = Kg$. Then by the Coset Lemma we have $fg^{-1} \in K$. Since $K \subseteq H$, this means $fg^{-1} \in H$, so $Hf = Hg$.
- ϕ **is a homomorphism:** Take two elements of G/K, say Kf and Kg. Then

$$\begin{aligned} \phi\left((Kf)(Kg)\right) &= \phi(Kfg) \\ &= Hfg \\ &= (Hf)(Hg) \\ &= \phi(Kf)\phi(Kg). \end{aligned}$$

- ϕ **is surjective:** Any element of G/H has the form $Hg = \phi(Kg) \in \mathrm{im}(\phi)$.

Next we claim that $\ker(\phi) = H/K$. Given an element $Kg \in G/K$, we have

$$\begin{aligned} Kg \in \ker(\phi) &\iff \phi(Kg) = H1 \\ &\iff Hg = H1 \\ &\iff g \in H \qquad \text{by the Coset Lemma.} \end{aligned}$$

So

$$\ker(\phi) = \{\, Kg \mid g \in H \} = H/K.$$

So by the First Isomorphism Theorem $H/K \trianglelefteq G/K$ and

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

□

For the next isomorphism theorem, recall the product

$$HN = \{ hn \mid h \in H,\ n \in N \}.$$

Theorem 4.5 (Third Isomorphism Theorem)**.** *Suppose G is a group, $H \leqslant G$ and $N \trianglelefteq G$. Then*

(a) $N \trianglelefteq HN$,

(b) $H \cap N \trianglelefteq H$, *and*

(c) $H/(H \cap N) \cong (HN)/N$.

Proof.

(a) Certainly $N \subseteq HN$, since for each $n \in N$ we have $n = 1n \in HN$. Since $N \leqslant G$, this means that $N \leqslant HN$. Also, since $N \trianglelefteq G$, we have $gng^{-1} \in N$ for all $g \in G$. In particular, $gng^{-1} \in N$ for $g \in HN$, so $N \trianglelefteq HN$.

(b,c) We use the First Isomorphism Theorem. Define

$$\begin{aligned} \phi : H &\longrightarrow \frac{G}{N} \\ h &\longmapsto Nh. \end{aligned}$$

Then we claim ϕ is a homomorphism. Take $h, k \in H$. Then

$$\phi(hk) = N(hk) = (Nh)(Nk) = \phi(h)\phi(k).$$

Now we claim that $\mathrm{im}(\phi) = HN/N$: recall that HN/N is the set of right cosets of N in HN, i.e.

$$\{ Nhn \mid h \in H,\ n \in N \}.$$

But $Nhn = Nh$ when $n \in N$: by the Coset Lemma this is the same as saying $hnh^{-1} \in N$, which is true because N is normal. So

$$HN/N = \{ Nh \mid h \in H \} = \mathrm{im}(\phi).$$

Next we claim that $\ker(\phi) = H \cap N$:

$$\begin{aligned} \ker(\phi) &= \{ h \in H \mid \phi(h) = N1 \} \\ &= \{ h \in H \mid Nh = N1 \} \\ &= \{ h \in H \mid h \in N \} \\ &= H \cap N. \end{aligned}$$

So by the First Isomorphism Theorem $H \cap N \trianglelefteq H$ and

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

□

Example. Let $G = \mathcal{U}_{13}$, $H = \langle 4 \rangle = \{1, 4, 3, 12, 9, 10\}$ and $N = \langle 5 \rangle = \{1, 5, 12, 8\}$. Then $H \cap N = \{1, 12\}$. Write $K = H \cap N$. Then the cosets of K in H are

$$K1 = \{1, 12\}$$
$$K4 = \{4, 9\}$$
$$K3 = \{3, 10\}$$

and the cosets of N in HN are

$$N1 = \{1, 5, 12, 8\}$$
$$N4 = \{4, 7, 9, 6\}$$
$$N3 = \{3, 2, 10, 11\}.$$

You can check that H/K and HN/N are isomorphic, with an isomorphism given by mapping $Kh \mapsto Nh$ for all $h \in H$.

Notice that we did something sneaky here: we wrote down all the cosets of N in HN without having to write down all the elements of HN first. From the proof of the Third Isomorphism Theorem, HN/N is the set of all cosets Nh for $h \in H$. So we just need to write down cosets Nh until we've seen all the elements of n, and we have all the cosets of N in HN.

4.3 Automorphism groups

Throughout this section, G is a group.

Definition. An **automorphism** of G is an isomorphism from G to G. The **automorphism group** of G is the set of all automorphisms of G, written as $\mathrm{Aut}(G)$.

Proposition 4.6. $\mathrm{Aut}(G)$ *is a group under composition.*

Proof. Recall that we write Sym_G for the group of all bijections from G to G. Certainly $\mathrm{Aut}(G)$ is a subset of Sym_G, and we need to show that it is a subgroup.

S1. The identity function $\mathrm{id} : G \to G$ is an automorphism, so $\mathrm{Aut}(G)$ is non-empty.

S2. Suppose $\phi, \psi \in \mathrm{Aut}(G)$. We need to show that $\phi \circ \psi^{-1} \in \mathrm{Aut}(G)$, i.e. that $\phi \circ \psi^{-1}$ is a homomorphism. Given $f, g \in G$,

$$\begin{aligned}
\phi(\psi^{-1}(fg)) &= \phi(\psi^{-1}(\psi(\psi^{-1}(f))\psi(\psi^{-1}(g)))) \\
&= \phi(\psi^{-1}(\psi(\psi^{-1}(f)\psi^{-1}(g)))) && \text{because } \psi \text{ s a homomorphism} \\
&= \phi(\psi^{-1}(f)\psi^{-1}(g)) \\
&= \phi(\psi^{-1}(f))\phi(\psi^{-1}(g)) && \text{because } \psi \text{ is a homomorphism.}
\end{aligned}$$

So $\phi \circ \psi^{-1}$ is a homomorphism. □

Example. Take $G = \mathcal{C}_4 = \{1, z, z^2, z^3\}$. An automorphism ϕ of $\mathcal{C}_4$ is determined by what it does to z (because if $\phi(z) = h$, then $\phi(z^a) = h^a$ for all a). If we take $\phi(z) = 1$ or z^2, then we'll have $\phi(z^2) = 1$; but then ϕ is not injective, because $\phi(1) = 1$ too. So the only possibilities are $\phi(z) = z$ and $\phi(z) = z^3$. And both of these work: the first one is just the identity map, and the second is the automorphism which sends every element to its inverse.

So $\mathrm{Aut}(\mathcal{C}_4) = \{\mathrm{id}, \phi\}$, where $\phi(z) = z^3$. Observe that $\phi(\phi(z)) = \phi(z^3) = z^9 = z$, so $\phi \circ \phi = \mathrm{id}$. So $\mathrm{Aut}(\mathcal{C}_4)$ has the following Cayley table.

	id	ϕ
id	id	ϕ
ϕ	ϕ	id

Now we look at a particular type of automorphism.

Lemma 4.7. *Suppose $g \in G$, and define $\rho_g : G \to G$ by $\rho_g(h) = ghg^{-1}$. Then ρ_g is an automorphism of G.*

Proof. ρ_g is a bijection, since it has an inverse given by $h \mapsto g^{-1}hg$. ρ_g is a homomorphism, since for any $h, k \in G$,

$$\rho_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \rho_g(h)\rho_g(k). \qquad \square$$

Example. Take $G = \mathcal{Q}_8$. Then ρ_i is the automorphism given by

$$1 \longmapsto 1, \qquad -1 \longmapsto -1, \qquad i \longmapsto i, \qquad -i \longmapsto -i,$$
$$j \longmapsto -j, \qquad -j \longmapsto j, \qquad k \longmapsto -k, \qquad -k \longmapsto k.$$

Definition. An automorphism of G is called an **inner** automorphism if it has the form ρ_g for some $g \in G$. The **inner automorphism group** of G (written $\mathrm{Inn}(G)$) is the set of all inner automorphisms of G.

Now recall that $Z(G)$ denotes the centre of G, i.e.

$$Z(G) = \{\, g \in G \mid gh = hg \text{ for all } h \in G \,\}.$$

Theorem 4.8. $\mathrm{Inn}(G)$ *is a subgroup of* $\mathrm{Aut}(G)$*, and* $\mathrm{Inn}(G) \cong G/Z(G)$.

Proof. We define a map

$$\begin{aligned} \phi : G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto \rho_g. \end{aligned}$$

We claim ϕ is a homomorphism. To prove this, we have to show that $\rho_{fg} = \rho_f \circ \rho_g$ for all $f, g \in G$. Given $h \in G$, we have

$$\rho_{fg}(h) = (fg)h(fg)^{-1} = fghg^{-1}f^{-1} = \rho_f(ghg^{-1}) = \rho_f(\rho_g(h)).$$

So $\rho_{fg} = \rho_f \circ \rho_g$, and ϕ is a homomorphism.

By definition, $\mathrm{Inn}(G)$ is the image of ϕ, so $\mathrm{Inn}(G) \leqslant \mathrm{Aut}(G)$ and $\mathrm{Inn}(G) \cong G/\ker(\phi)$, by the First Isomorphism Theorem. So all we need to do is check that $\ker(\phi) = Z(G)$. For $g \in G$, we have

$$\begin{aligned} g \in \ker(\phi) &\iff \rho_g = \mathrm{id}_G \\ &\iff \rho_g(h) = h \text{ for all } h \in G \\ &\iff ghg^{-1} = h \text{ for all } h \in G \\ &\iff gh = hg \text{ for all } h \in G \\ &\iff g \in Z(G). \end{aligned}$$

□

Definition. We say that an automorphism of G is **outer** if it is not an inner automorphism.

The outer automorphisms don't give a subgroup of G, since the identity automorphism id_G is inner. But there is such a thing as the outer automorphism group of G. To define this, we need the following result.

Proposition 4.9. *Then* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof. We've already seen that $\mathrm{Inn}(G) \leqslant \mathrm{Aut}(G)$, so we need to show that for every $\phi \in \mathrm{Aut}(G)$ and $\rho \in \mathrm{Inn}(G)$ we have $\phi \circ \rho \circ \phi^{-1} \in \mathrm{Inn}(G)$. We can write ρ as ρ_g for some $g \in G$. Then for $h \in G$ we have

$$\phi(\rho_g(\phi^{-1}(h))) = \phi(g\phi^{-1}(h)g^{-1}) = \phi(g)\phi(\phi^{-1}(h))\phi(g^{-1}) = \phi(g)h\phi(g)^{-1} = \rho_{\phi(g)}(h).$$

So $\phi \circ \rho_g \circ \phi^{-1} = \rho_{\phi(g)} \in \mathrm{Inn}(G)$. □

Definition. The **outer automorphism group** of G is the quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

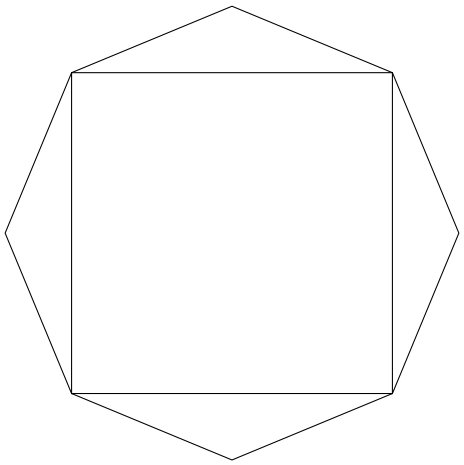
Example. Let's see an outer automorphism of $\mathcal{D}_8$. Let t denote rotation through 45° clockwise about the centre of the square, and define $\phi : \mathcal{D}_8 \to \mathcal{D}_8$ by $g \mapsto tgt^{-1}$. Then we get

$$\begin{aligned} 1 &\longmapsto 1, & r &\longmapsto r, \\ r^2 &\longmapsto r^2, & r^3 &\longmapsto r^3, \\ s &\longmapsto rs, & rs &\longmapsto r^2s, \\ r^2s &\longmapsto r^3s, & r^3s &\longmapsto s, \end{aligned}$$

so ϕ is a bijection from $\mathcal{D}_8$ to $\mathcal{D}_8$. The fact that ϕ is a homomorphism is the same as the proof of Lemma 4.7. So $\phi \in \mathrm{Aut}(G)$. ϕ cannot be an inner automorphism, because an inner automorphism maps each element to a conjugate element, whereas $\phi(s) = rs \not\sim_{\mathcal{D}_8} s$.

In fact $|\mathrm{Aut}(\mathcal{D}_8)| = 8$, and from Theorem 4.8 $|\mathrm{Inn}(\mathcal{D}_8)| = 4$. So $|\mathrm{Out}(\mathcal{D}_8)| = 2$, and hence $\mathrm{Out}(\mathcal{D}_8) = \{\mathrm{Inn}(\mathcal{D}_8)\,\mathrm{id}, \mathrm{Inn}(\mathcal{D}_8)\phi\}$.

To see where ϕ comes from, consider the following picture.



We can see that every symmetry of the square gives a symmetry of the octagon, which means that $\mathcal{D}_8 \leqslant \mathcal{D}_{16}$. In fact, $\mathcal{D}_8 \trianglelefteq \mathcal{D}_{16}$ because $|\mathcal{D}_{16} : \mathcal{D}_8| = 2$. t is an element of $\mathcal{D}_{16}$, so there is an inner automorphism of $\mathcal{D}_{16}$ which maps $g \mapsto tgt^{-1}$ for every g. ϕ is just the restriction of this inner automorphism to $\mathcal{D}_8$.

5 Actions

Actions are a very important aspect of groups. The basic idea is that we have a group and a set, and we assign to each element of the group a permutation of the set in a way which is compatible with the group operation.

5.1 Definitions

Definition. Suppose G is a group and X is a set. An **action of G on X** is a collection $\pi = (\pi_g \mid g \in G)$ of functions from X to X such that:

A1. $\pi_1 = \mathrm{id}_X$, and

A2. $\pi_f \circ \pi_g = \pi_{fg}$ for all $f, g \in G$.

Lemma 5.1. *If π is an action of G on X, then each π_g is a permutation of X.*

Proof. Given $g \in G$, we have $\pi_g \pi_{g^{-1}} = \pi_1 = \mathrm{id}_X$, and similarly $\pi_{g^{-1}} \pi_g = \mathrm{id}_X$. So π_g has an inverse, so is a bijection. □

Remark. Suppose π is an action of G on X. Then by Lemma 5.1 we have a function

$$\begin{aligned} G &\longrightarrow \mathrm{Sym}_X \\ g &\longmapsto \pi_g. \end{aligned}$$

By (A2), this function is a homomorphism. So another way an action is often defined is: a homomorphism $G \to \mathrm{Sym}_X$.

Important examples of actions.

- For any G and any X, the **trivial action** is defined by $\pi_g(x) = x$ for all g, x.
- Let $G \leqslant \mathcal{S}_n$ and $X = \{1, \ldots, n\}$. The **natural action** is defined by $\pi_g(x) = g \cdot x$.
- For any G, we have the **regular action** of G on itself, given by $\pi_g(h) = gh$.
- For any G, we have the **conjugation action** of G on itself, given by $\pi_g(h) = ghg^{-1}$.
- For any G, let X be the set of all subgroups of G. Then G acts on X by conjugation: $\pi_g(K) = gKg^{-1}$.

5.2 Orbits and stabilisers

Suppose we have an action π of G on X. We define a relation $\equiv$ on X by saying that $x \equiv y$ if there is some $g \in G$ such that $y = \pi_g(x)$.

Lemma 5.2. *$\equiv$ is an equivalence relation.*

Proof.

Reflexive: We have $\pi_1(x) = x$ for all x, so $x \equiv x$.

Symmetric: Suppose $x \equiv y$. Then there is $g \in G$ such that $\pi_g(x) = y$. Then

$$\pi_{g^{-1}}(y) = \pi_{g^{-1}}(\pi_g(x)) = \pi_1(x) = x,$$

so $y \equiv x$.

Transitive: Suppose $x \equiv y \equiv z$. Then there are $f, g \in G$ such that $\pi_g(x) = y$, $\pi_f(y) = z$. Then $\pi_{fg}(x) = \pi_f(\pi_g(x)) = z$, so $x \equiv z$. □

Definition. Suppose π is an action of a group G on a set X. The **orbits** of π are the equivalence classes under the relation $\equiv$ described above. Given $x \in X$, we write $\mathrm{Orb}(x)$ for the orbit containing x, i.e.

$$\mathrm{Orb}(x) = \{\pi_g(x) \mid g \in G\}.$$

The action π is **transitive** if there is only one orbit.

Definition. Suppose π is an action of a group G on a set X, and let $x \in X$. The **stabiliser** of x is the set

$$\mathrm{Stab}(x) = \{g \in G \mid \pi_g(x) = x\}.$$

Lemma 5.3. *Suppose π is an action of G on X, and let $x \in X$. Then* $\mathrm{Stab}(x) \leqslant G$.

Proof.

S1. $\pi_1(x) = x$, so $1 \in \mathrm{Stab}(x)$.

S2. Suppose $f, g \in \mathrm{Stab}(x)$. Then $\pi_f(x) = \pi_g(x) = x$. So

$$\pi_{fg^{-1}}(x) = \pi_f(\pi_{g^{-1}}(x)) = \pi_f(\pi_{g^{-1}}(\pi_g(x))) = \pi_f(\pi_{g^{-1}g}(x)) = \pi_f(x) = x,$$

so $fg^{-1} \in \mathrm{Stab}\, x$. □

Examples. Let's work out some examples of orbits and stabilisers.

- ◇ Take any G and X, and let π be the trivial action. Then for any $x \in X$,

$$\mathrm{Orb}(x) = \{x\}, \qquad \mathrm{Stab}(x) = G.$$

- ◇ Take $G = \mathcal{D}_8$, and let X be the set of vertices of the square, numbered $1, 2, 3, 4$ in clockwise order starting from the top right. Then G acts on X in a natural way: $\pi_g(x) = g(x)$. Taking $x = 1$, we get

$$\mathrm{Orb}(1) = \{1, 2, 3, 4\}, \qquad \mathrm{Stab}(1) = \{1, rs\}.$$

- ◇ Let G be any group, and let π be the regular action of G on G. Then any two elements $g, h \in G$ lie in the same orbit, because $\pi_{hg^{-1}}(g) = h$. So this action is transitive. $\mathrm{Stab}(h) = \{1\}$ for any $x \in G$.

- ◇ Let G be any group, and let π be the conjugation action of G on G, and let $h \in G$. Then $\mathrm{Orb}(h)$ is just the conjugacy class $\mathrm{ccl}(h)$. $\mathrm{Stab}(h)$ is called the **centraliser** of h in G; we will see more about this later.

- ◇ Let $\mathbb{F}$ be a field, and let $G = \mathrm{GL}_2(\mathbb{F})$ and $X = \mathbb{F}^2$, the set of column vectors of length 2. Let π be the multiplication action of G on X, i.e. $\pi_g(x) = gx$.

  To begin with, consider the vector $\begin{pmatrix}0\\0\end{pmatrix}$. We know that $g\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$ for every matrix g, so $\mathrm{Orb}\begin{pmatrix}0\\0\end{pmatrix} = \left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}$ and $\mathrm{Stab}\begin{pmatrix}0\\0\end{pmatrix} = G$.

  Now consider the vector $\begin{pmatrix}1\\0\end{pmatrix}$. It's easy to show that for any non-zero vector $\begin{pmatrix}a\\b\end{pmatrix}$ we can find an invertible matrix of the form $\begin{pmatrix}a & ?\\ b & ?\end{pmatrix}$, and multipliying this matrix by $\begin{pmatrix}1\\0\end{pmatrix}$ gives the vector $\begin{pmatrix}a\\b\end{pmatrix}$. So $\mathrm{Orb}\begin{pmatrix}1\\0\end{pmatrix}$ consists of all the non-zero vectors in $\mathbb{F}^2$. $\mathrm{Stab}\begin{pmatrix}1\\0\end{pmatrix}$ is the set of all invertible matrices of the form $\begin{pmatrix}1 & ?\\ 0 & ?\end{pmatrix}$.

  So this action has exactly two orbits.

Theorem 5.4 (The Orbit–Stabiliser Theorem)**.** *Suppose π is an action of G on X, and $x \in X$. Then* $|G| = |\mathrm{Orb}(x)||\mathrm{Stab}(x)|$.

Proof. Since $\mathrm{Stab}(x) \leqslant G$, we know from Lagrange's Theorem that $|G| = |G : \mathrm{Stab}(x)|\,|\mathrm{Stab}(x)|$, where $|G : \mathrm{Stab}(x)|$ is the number of left cosets of $\mathrm{Stab}(x)$ in G. So all we need to do is to construct a bijection θ from the set of left cosets of $\mathrm{Stab}(x)$ to $\mathrm{Orb}(x)$.

Define θ by

$$g\,\mathrm{Stab}(x) \longmapsto \pi_g(x).$$

θ **is well-defined:** Suppose $f, g \in G$ and $f\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$. By the Coset Lemma this means that $f^{-1}g \in \mathrm{Stab}(x)$, i.e. $\pi_{f^{-1}g}(x) = x$. Hence

$$\pi_f(x) = \pi_f(\pi_{f^{-1}g}(x)) = \pi_{ff^{-1}g}(x) = \pi_g(x).$$

θ **is injective:** Suppose $\theta(f\,\mathrm{Stab}(x)) = \theta(g\,\mathrm{Stab}(x))$, i.e. $\pi_f(x) = \pi_g(x)$. Then

$$\pi_{f^{-1}g}(x) = \pi_{f^{-1}}(\pi_g(x)) = \pi_{f^{-1}}(\pi_f(x)) = x,$$

so $f^{-1}g \in \mathrm{Stab}(x)$. So by the Coset Lemma $f\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$.

θ **is surjective:** Given an element of $\mathrm{Orb}(x)$, we can write it as $\pi_g(x)$ for some $g \in G$, and this is $\theta(g\,\mathrm{Stab}(x))$. □

Examples. We can apply the Orbit–Stabiliser Theorem to find the size of a group when we have an action that we understand.

- ◇ Let G be the symmetry group of a cube. Let x be a face of the cube, and let G act on the set of faces. This is a transitive action, because (it's easy to see that) you can get from any face to any other by applying a symmetry of the cube. So $|\mathrm{Orb}(x)| = 6$. Now think about $\mathrm{Stab}(x)$. Notice that any symmetry of the cube which fixes x gives a symmetry of x: a rotation of the cube gives a rotation of x, and a reflection of the cube gives a reflection of x. Conversely, any symmetry of x can be extended to a symmetry of the whole cube. So $\mathrm{Stab}(x)$ is isomorphic to the symmetry group of x, which is $\mathcal{D}_8$. In particular, $|\mathrm{Stab}(x)| = 8$. So by the Orbit–Stabiliser Theorem, $|G| = 6 \times 8 = 48$.

- ◇ Suppose p is a prime, and recall that $\mathbb{F}_p$ is the set $\{0, \ldots, p-1\}$ with addition and multiplication modulo p. Then $\mathrm{GL}_2(\mathbb{F}_p)$ is a finite group, and we can find its order using the Orbit–Stabiliser Theorem. Let $X = \mathbb{F}_p^2$, and consider the multiplication action of $\mathrm{GL}_2(\mathbb{F}_p)$ on X. Consider the vector $\begin{pmatrix}1\\0\end{pmatrix}$. We saw earlier that $\mathrm{Orb}\begin{pmatrix}1\\0\end{pmatrix}$ is the set of all non-zero vectors in X, so $\left|\mathrm{Orb}\begin{pmatrix}1\\0\end{pmatrix}\right| = p^2 - 1$, and $\mathrm{Stab}\begin{pmatrix}1\\0\end{pmatrix}$ is the set of all matrices $\begin{pmatrix}1 & b\\0 & d\end{pmatrix}$, where $b, d \in \mathbb{F}_p$ with $d \neq 0$. So $\left|\mathrm{Stab}\begin{pmatrix}1\\0\end{pmatrix}\right| = p(p-1)$ (because there are p choices for b and $p-1$ choices for d), and so by the Orbit–Stabiliser Theorem we get

$$|\mathrm{GL}_2(\mathbb{F}_p)| = \left|\mathrm{Orb}\begin{pmatrix}1\\0\end{pmatrix}\right| \left|\mathrm{Stab}\begin{pmatrix}1\\0\end{pmatrix}\right| = (p^2-1)p(p-1).$$

Now we consider some special cases of stabilisers.

Definition. Suppose G is a group.

- ◇ If $h \in G$, the **centraliser** of h is

$$\mathrm{C}_G(h) = \{g \in G \mid gh = hg\}.$$

- ◇ If $H \leqslant G$, the **normaliser** of H is

$$\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Proposition 5.5. *Suppose G is a group, $h \in G$ and $H \leqslant G$. Then $h \in \mathrm{C}_G(h) \leqslant G$, and $H \trianglelefteq \mathrm{N}_G(H) \leqslant G$.*

Proof. $\mathrm{C}_G(h) = \{g \in G \mid gh = hg\} = \{g \in G \mid ghg^{-1} = h\}$, so $\mathrm{C}_G(h)$ is the stabiliser of h under the conjugation action of G on G. So by Lemma 5.3 $\mathrm{C}_G(h) \leqslant G$. Similarly, $\mathrm{N}_G(H)$ is the stabiliser of H under the conjugation action of G on the set of subgroups of G, so $\mathrm{N}_G(H) \leqslant G$.

For each $h \in H$ we have $hHh^{-1} = \left\{hkh^{-1} \;\middle|\; k \in H\right\} = H$, so $H \leqslant \mathrm{N}_G(H)$. Also, for every $g \in \mathrm{N}_G(H)$ we have $gHg^{-1} = H$, so $H \trianglelefteq \mathrm{N}_G(H)$. □

Examples.

◇ Take $G = \mathcal{D}_8$. Then by the Orbit–Stabiliser Theorem,

$$|\mathcal{D}_8| = |\mathrm{ccl}(rs)||\mathrm{C}_G(rs)|,$$

so $|\mathrm{C}_{\mathcal{D}_8}(rs)| = 4$. We know $\mathrm{C}_{\mathcal{D}_8}(rs)$ contains rs (because every element commutes with itself) and r^2 (because r^2 commutes with everything), so

$$\mathrm{C}_{\mathcal{D}_8}(rs) = \{1, rs, r^2, r^3s\}.$$

◇ Take $G = \mathcal{S}_4$, and $h = (1\ 2\ 3)$. Then $\mathrm{ccl}(h)$ consists of all elements of cycle type $(3,1)$, so $|\mathrm{ccl}(h)| = 8$. So by the Orbit–Stabiliser Theorem, $|\mathrm{C}_{\mathcal{S}_4}(h)| = 4!/8 = 3$. We know $\mathrm{C}_{\mathcal{S}_4}(h)$ contains h and h^2, so

$$\mathrm{C}_{\mathcal{S}_4}(h) = \{1, h, h^2\}.$$

Lemma 5.6. *Suppose G is a finite group and $h \in G$. Then $|\mathrm{ccl}(h)|$ divides $|G|$.*

Proof. $\mathrm{ccl}(h)$ is the orbit of h under the conjugation action of G on G, so by the Orbit–Stabiliser Theorem

$$|G| = |\mathrm{ccl}(h)||\mathrm{C}_G(h)|,$$

and hence $|\mathrm{ccl}(h)|$ divides $|G|$. □

Example. In a coursework question we saw the group $\mathcal{G}_{21}$. This consists of elements a^ib^j for $i \leqslant 6$ and $j \leqslant 2$, and the group operation is given by $a^7 = b^3 = 1$ and $ba = a^2b$. With a long calculation, we can check that the conjugacy classes are

$$\{1\},\ \{a, a^2, a^4\},\ \{a^3, a^5, a^6\},$$

$$\{b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\},$$

$$\{b^2, ab^2, a^2b^2, a^3b^2, a^4b^2, a^5b^2, a^6b^2\}.$$

We see that all the conjugacy class sizes divide 21.

Theorem 5.7 (Orbit-Counting Lemma)**.** *Suppose G is a finite group, and π is an action of G on X. For each $g \in G$, define*

$$\mathrm{fix}(g) = \{\, x \in X \mid \pi_g(x) = x \,\}.$$

Then the number of orbits of π is

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{fix}(g)|.$$

Proof. Let N be the number of pairs (g, x) such that $\pi_g(x) = x$. We will work out N in two different ways.

On the one hand, if we take each $g \in G$ and count the x such that $\pi_g(x) = x$, then we get $|\mathrm{fix}(g)|$. So

$$N = \sum_{g\in G}|\mathrm{fix}(g)|.$$

On the other hand, if we take each $x \in X$ and count the the g such that $\pi_g(x) = x$, we get

$$\begin{aligned} N &= \sum_{x \in X} |\mathrm{Stab}(x)| \\ &= \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}(x)|} \qquad \text{by the Orbit–Stabiliser Theorem.} \end{aligned}$$

Equating these two expressions for N, we get

$$\sum_{g \in G} |\mathrm{fix}(g)| = \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}(x)|},$$

i.e.

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)| = \sum_{x \in X} \frac{1}{|\mathrm{Orb}(x)|}.$$

We want to split up this last sum into the different orbits. So let $Y_1, \ldots, Y_r$ be the orbits. Then

$$\sum_{x \in X} \frac{1}{|\mathrm{Orb}(x)|} = \sum_{i=1}^{r} \sum_{x \in Y_i} \frac{1}{|Y_i|} = \sum_{i=1}^{r} \frac{|Y_i|}{|Y_i|} = \sum_{i+1}^{r} 1 = r,$$

i.e. the number of orbits. □

Example. The Orbit-Counting Lemma can be used to count colourings. Suppose P is a square, and we colour the vertices of the square using three colours. Then there are $3^4 = 81$ possible colourings. But now suppose we say that two colourings are equivalent if we can transform one into the other by applying a symmetry of the square; how many colourings are there up to equivalence?

The group $\mathcal{D}_8$ acts on the 81 basic colourings in a natural way, and the question is really asking how many orbits this action has. So we use the Orbit-Counting Lemma:

$\lvert\mathrm{fix}(1)\rvert = 81$	(the identity fixes everything)
$\lvert\mathrm{fix}(r)\rvert = 3$	(all the vertices must have the same colour)
$\lvert\mathrm{fix}(r^2)\rvert = 9$	(opposite vertices must have the same colour)
$\lvert\mathrm{fix}(r^3)\rvert = 3$	(all the vertices must have the same colour)
$\lvert\mathrm{fix}(s)\rvert = 9$	(the top two vertices must be the same colour, and so must the bottom two)
$\lvert\mathrm{fix}(rs)\rvert = 27$	(the top-left and bottom-right vertices must be the same colour)
$\lvert\mathrm{fix}(r^2s)\rvert = 9$	(the left-hand vertices must be the same colour, and so must the right-hand ones)
$\lvert\mathrm{fix}(r^3s)\rvert = 27$	(the top-right and bottom-left vertices must be the same colour).

So by the Orbit-Counting Lemma, the number of orbits is

$$\frac{81 + 3 + 9 + 3 + 9 + 27 + 9 + 27}{8} = 21.$$

The next lemma reduces the amount of work we have to do in applying the Orbit-Counting Lemma.

Lemma 5.8. *Suppoe π is a action of G on X. If f and g are conjugate elements of G, then* $|\mathrm{fix}(f)| = |\mathrm{fix}(g)|$.

Proof. We need to construct a bijection from fix(f) to fix(g). Take $k \in G$ such that $kfk^{-1} = g$. Suppose $x \in \text{fix}(f)$. Then we claim that $\pi_k(x) \in \text{fix}(g)$:

$$\pi_g(\pi_k(x)) = \pi_{kfk^{-1}}(\pi_k(x)) = \pi_{kf}(x) = \pi_k(\pi_f(x)) = \pi_k(x).$$

Similarly if $x \in \text{fix}(g)$, then $\pi_{k^{-1}}(x) \in \text{fix}(f)$. So we have a function

$$\begin{aligned} \theta : \text{fix}(f) &\longrightarrow \text{fix}(g) \\ x &\longmapsto \pi_k(x). \end{aligned}$$

θ is a bijection, because it has in inverse $x \mapsto \pi_{k^{-1}(x)}$. □

6 Simple groups and composition series

6.1 Simple groups

Definition. Suppose G is a group. G is **simple** if $G \neq \{1\}$ and G has no normal subgroups except for G and $\{1\}$.

The idea of simple groups is that they are the basic building blocks from which bigger groups can be built. If G is a group and $\{1\} < N \lhd G$, then we can break G up into two smaller groups N and G/N, and if we understand these smaller groups then we understand a lot about G. A simple group is one which can't be broken down in this way. This is a bit like prime numbers being the building blocks from which all positive integers are built.

Examples. Let's look at some of the groups we know and see whether they're simple.

- ◇ If p is prime, then the cyclic group $\mathcal{C}_p$ is simple, by Lagrange's Theorem.
- ◇ If n is composite, say $n = ab$, then $\mathcal{C}_n$ is not simple: it has a normal subgroup $\langle z^a \rangle$.
- ◇ $\mathcal{D}_{2n}$ is not simple: the subgroup $\langle r \rangle$ has index 2, so is normal.
- ◇ $\mathcal{S}_n$ is not simple if $n \geqslant 3$, since $\mathcal{A}_n$ is a normal subgroup.

So in fact simple groups are hard to find. The abelian case is easy to deal with.

Proposition 6.1. *Suppose G is an abelian group. Then G is simple if and only if G is finite and $|G|$ is a prime number p, in which case $G \cong \mathcal{C}_p$.*

Proof. Since G is abelian, every subgroup of G is normal, so G is simple if and only if if has no subgroups except G and $\{1\}$.

Suppose G is finite and $|G|$ is prime. Then by Lagrange's Theorem the only subgroups of G are $\{1\}$ and G, so G is simple. If we take $g \neq 1 \in G$, then $\mathrm{ord}(g)$ divides p, so $\mathrm{ord}(g) = p$, so $G = \{1, g, \ldots, g^{p-1}\} \cong \mathcal{C}_p$.

Now suppose G is finite and $|G| > 1$ and is not prime. Take $g \neq 1 \in G$, and let $a = \mathrm{ord}(g)$. Then $\langle g \rangle$ is a subgroup of G of order a. If $a < |G|$, then $\{1\} \neq \langle g \rangle < G$, so G is not simple. If $a = |G|$, write $a = bc$ with $b, c > 1$. Then $\mathrm{ord}(g^b) = c$, so $\{1\} \neq \langle g^b \rangle < G$, so G is not simple.

Now suppose G is infinite, and take $g \neq 1$ in G. If $\mathrm{ord}(g) < \infty$, then $\langle g \rangle$ is finite, so $\{1\} \neq \langle g \rangle < G$ and G is not simple. If $\mathrm{ord}(g) = \infty$, then $\{1\} \neq \langle g^2 \rangle < \langle g \rangle \leqslant G$, so G is not simple. □

6.2 Simplicity of the alternating groups

In this section we'll prove that the alternating group $\mathcal{A}_n$ is simple provided $n \geqslant 5$. This is not true when $n = 4$: consider the subgroup

$$V = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

We saw earlier that V is a normal subgroup of $\mathcal{S}_4$; since it's contained in $\mathcal{A}_4$, it must also be a normal subgroup of $\mathcal{A}_4$. V comprises all the elements of $\mathcal{A}_4$ of cycle type $(1,1,1,1)$ or $(2,2)$. So the remaining eight elements of $\mathcal{A}_4$ all have cycle type $(3,1)$.

In fact V is the only normal subgroup of $\mathcal{A}_4$ apart from $\{\mathrm{id}\}$ and $\mathcal{A}_4$. To prove this, we start by considering actions. Recall that the **natural action** of $\mathcal{S}_n$ on $\{1,\dots,n\}$ is defined by $\pi_g(x) = g \cdot x$. We can apply this for any subgroup of $\mathcal{S}_n$ as well. Recall also that this action is **transitive** if the only orbit is $\{1,\dots,n\}$.

Lemma 6.2. *Suppose $\{\mathrm{id}\} \neq N \trianglelefteqslant \mathcal{A}_n$. Then the action of N on $\{1,\dots,n\}$ is transitive.*

Proof. Take $g \in N$ with $g \neq \mathrm{id}$. Take $a \in \{1,\dots,n\}$ with $g \cdot a \neq a$, and write $b = g \cdot a$. Then a and b lie in the same orbit. Now given any other number $c \in \{1,\dots,n\}$, we claim that c also lies in this orbit. Let $k = (a\ b\ c)$. Then $kgk^{-1} \in N$ because $N \trianglelefteqslant \mathcal{A}_n$. And

$$kgk^{-1} \cdot b = kg \cdot a = k \cdot b = c,$$

so $c \in \mathrm{Orb}(b)$. So $\mathrm{Orb}(b)$ contains every element of $\{1,\dots,n\}$. □

Now let's apply this in the case $n = 4$.

Proposition 6.3. *The only normal subgroups of $\mathcal{A}_4$ are $\{\mathrm{id}\}$, $\mathcal{A}_4$ and V.*

Proof. Suppose $N \trianglelefteqslant \mathcal{A}_4$ and $N \neq \{\mathrm{id}\}$. Then by Lemma 6.2 the action of N on $\{1,2,3,4\}$ is transitive. So by the Orbit–Stabiliser Theorem $|N|$ is divisible by 4. In particular, $|N| \geqslant 4$. So if $N \neq V$, then contains an element of $\mathcal{A}_4 \setminus V$, so N contains a 3-cycle. Now by Corollary 3.5 $|N|$ is divisible by 3, so $|N|$ is divisible by 12, so $N = \mathcal{A}_4$. □

Now we can look at $\mathcal{A}_n$ for $n \geqslant 5$. We'll use induction, and we'll regard $\mathcal{A}_{n-1}$ as a subgroup of $\mathcal{A}_n$ (we just extend any permutation f of $\{1,\dots,n-1\}$ to a permutation of $\{1,\dots,n\}$ by setting $f \cdot n = n$). So given $N \leqslant \mathcal{A}_n$, we can think about the group $N \cap \mathcal{A}_{n-1}$.

Lemma 6.4. *Suppose $n \geqslant 5$ and $\{\mathrm{id}\} \neq N \trianglelefteqslant \mathcal{A}_n$. Then $N \cap \mathcal{A}_{n-1} \neq \{\mathrm{id}\}$.*

Proof. The natural action of N on $\{1,\dots,n\}$ is transitive, so we can find $g \in N$ such that $g \cdot n = 1$. Observe that if $h \in \mathcal{A}_n$, then $ghg^{-1}h^{-1} \in N$, because $g \in N$ and $hg^{-1}h^{-1} \in N$. We will choose h so that $ghg^{-1}h^{-1} \in \mathcal{A}_{n-1}$ and $ghg^{-1}h^{-1} \neq \mathrm{id}$. We consider two cases.

1. Suppose $g \cdot 1 = n$. Choose $a \neq 1, n$ such that $g \cdot a \neq a$ (there must be such an a, since otherwise $g = (1\ n)$, but this doesn't lie in $\mathcal{A}_n$). Let $b = g \cdot a$, and then choose $c \neq 1, a, b, n$. Let $h = (1\ n)(b\ c) \in \mathcal{A}_n$. Then

   $$ghg^{-1}h^{-1} \cdot n = ghg^{-1} \cdot 1 = gh \cdot n = g \cdot 1 = n,$$

   so $ghg^{-1}h^{-1} \in \mathcal{A}_{n-1}$. Also,

   $$ghg^{-1}h^{-1} \cdot c = ghg^{-1} \cdot b = gh \cdot a = g \cdot a = b,$$

   so $ghg^{-1}h^{-1} \neq \mathrm{id}$.

2. Suppose $g \cdot 1 \neq n$. Let $a = g^{-1} \cdot n$. Then $a \neq 1$. Choose $b, c \neq 1, a, n$, and let $h = (1\ b\ c)$. Then
$$ghg^{-1}h^{-1} \cdot n = ghg^{-1} \cdot n = gh \cdot a = g \cdot a = n.$$
So $\mathrm{id} \neq ghg^{-1}h^{-1} \in N \cap \mathcal{A}_{n-1}$. Also,
$$ghg^{-1}h^{-1} \cdot b = ghg^{-1} \cdot 1 = gh \cdot n = g \cdot n = 1,$$
so $ghg^{-1}h^{-1} \neq \mathrm{id}$. □

Examples. We give examples to illustrate the above proof. Suppose $N \trianglelefteq \mathcal{A}_6$.

- ◇ Suppose $g = (1\ 6)(2\ 4\ 3\ 5) \in N$. We set $h = (1\ 6)(4\ 5)$. Then $ghg^{-1}h^{-1} = (2\ 3)(4\ 5) \in N \cap \mathcal{A}_5$.
- ◇ Suppose $g = (1\ 2\ 6)(4\ 3\ 5) \in N$. We set $h = (1\ 3\ 4)$. Then $ghg^{-1}h^{-1} = (1\ 4\ 2\ 5\ 3) \in N \cap \mathcal{A}_5$.

Now we need a similar lemma just for the case $n = 5$.

Lemma 6.5. *Suppose $N \trianglelefteq \mathcal{A}_5$. Then $N \cap \mathcal{A}_4 \neq V$.*

Proof. Suppose $N \cap \mathcal{A}_4 = V$. Then $(1\ 2)(3\ 4) \in N$, so
$$(3\ 4\ 5)(1\ 2)(3\ 4)(3\ 4\ 5)^{-1} = (1\ 2)(4\ 5) \in N.$$
Also,
$$(1\ 2\ 3\ 4\ 5)(1\ 2)(3\ 4)(1\ 2\ 3\ 4\ 5)^{-1} = (2\ 3)(4\ 5) \in N.$$
Hence
$$(1\ 2)(4\ 5)(2\ 3)(4\ 5) = (1\ 2\ 3) \in N$$
so $N \cap \mathcal{A}_4$ contains elements not in V, a contradiction. □

Now we can prove the main theorem of this section.

Theorem 6.6. *For $n \geqslant 5$, $\mathcal{A}_n$ is simple.*

Proof. We use induction on n. So if $n \geqslant 6$ assume the theorem is true for $\mathcal{A}_{n-1}$.

Suppose $\{\mathrm{id}\} \neq N \trianglelefteq \mathcal{A}_n$. We need to show that $N = \mathcal{A}_n$. First we claim that $N \cap \mathcal{A}_{n-1} = \mathcal{A}_{n-1}$. From the Third Isomorphism Theorem, we know that $N \cap \mathcal{A}_{n-1} \trianglelefteq \mathcal{A}_{n-1}$. Using Proposition 6.3 and the induction hypothesis, the only normal subgroups of $\mathcal{A}_n$ are $\{\mathrm{id}\}$, $\mathcal{A}_n$ and (if $n = 5$) V. By Lemma 6.4 $N \cap \mathcal{A}_{n-1} \neq \{\mathrm{id}\}$, and by Lemma 6.5 if $n = 5$ then $N \cap \mathcal{A}_4 \neq V$. So the only possibility is that $N \cap \mathcal{A}_{n-1} = \mathcal{A}_{n-1}$.

Now consider the natural action of N on $\{1, \ldots, n\}$, and look at the orbit and stabiliser of n. By Lemma 6.2 $\mathrm{Orb}(n) = \{1, \ldots, n\}$. Also, $\mathrm{Stab}(n) = N \cap \mathcal{A}_{n-1} = \mathcal{A}_{n-1}$. So by the Orbit–Stabiliser Theorem
$$\begin{aligned} |N| &= |\mathrm{Orb}(n)||\mathrm{Stab}(n)| \\ &= n \times \frac{(n-1)!}{2} \\ &= \frac{n!}{2} \\ &= |\mathcal{A}_n|, \end{aligned}$$
so $N = \mathcal{A}_n$. □

6.3 Composition series

Now we'll look at groups which are not simple, and how they can be broken down into simple groups.

Definition. Suppose G is a group. A **normal series** of length r for G is a series

$$G_0 \rhd G_1 \rhd \cdots \rhd G_r,$$

where $G_0 = G$ and $G_r = \{1\}$.
This series is called a **composition series** if G_i/G_{i+1} is simple for each i.

Examples.

- If $G = \{1\}$, then G has a composition series

  $$\{1\}$$

  of length 0.

- If G is simple, then G has a composition series

  $$G \rhd \{1\}$$

  of length 1.

- If $G = \mathcal{C}_{12}$, then G has a composition series

  $$\mathcal{C}_{12} \rhd \langle z^2 \rangle \rhd \langle z^4 \rangle \rhd \{1\}$$

  of length 3. To see that this is a composition series, look at the order of the quotient of any two consecutive groups in the series:

  $$\left|\frac{\mathcal{C}_{12}}{\langle z^2 \rangle}\right| = \frac{12}{6} = 2, \qquad \left|\frac{\langle z^2 \rangle}{\langle z^4 \rangle}\right| = \frac{6}{3} = 2, \qquad \left|\frac{\langle z^4 \rangle}{\{1\}}\right| = \frac{3}{1} = 3.$$

  In each case we have a prime number, and by Lagrange's Theorem any group of prime order is simple.

- If $G = \mathcal{D}_8$, then G has a composition series

  $$\mathcal{D}_8 \rhd \langle r \rangle \rhd \langle r^2 \rangle \rhd \{1\}$$

  of length 3.

- If $G = \mathcal{S}_n$ for $n \geqslant 5$, then G has a composition series

  $$\mathcal{S}_n \rhd \mathcal{A}_n \rhd \{\mathrm{id}\}$$

  of length 2.

The next lemma gives another way to think about composition series.

Lemma 6.7. *Suppose G is a group and $N \lhd G$. Then G/N is simple if and only if there is no K such that $N < K \lhd G$.*

Proof. First suppose G/N is not simple, and take M such that $\{N1\} < M \lhd G/N$. Let $K = \{k \in G \mid Nk \in M\}$. Then we claim that $N < K \lhd G$. This involves several steps.

- $N \leqslant K$, because if $k \in N$ then $Nk = N1 \in M$.
- $N \neq K$, because if we take a coset $Nk \in M$ with $Nk \neq N1$ then $k \in K$ but $K \notin M$.
- $K \leqslant G$, by the Subgroup Test:

  S1. $N1 \in M$ because M is a subgroup of G/N, so $1 \in K$;

  S2. if $h, k \in K$. Then $Nh, Nk \in M$, so $N(hk^{-1}) = (Nh)(Nk)^{-1} \in M$, so $hk^{-1} \in K$.
- K is normal in G, because if $g \in G$ and $k \in K$, then $Nk \in M$, so

$$N(gkg^{-1}) = (Ng)(Nk)(Ng)^{-1} \in M,$$

  so $gkg^{-1} \in K$.
- $K \neq G$, because if we take $g \in G$ such that $Ng \notin M$, then $g \notin K$.

Conversely, suppose there is K with $N < K \lhd G$. Then $\{1\} < K/N \lhd G/N$, so G/N is not simple. □

Lemma 6.7 tells us that a composition series is a normal series which is as **refined** as possible, i.e. we can't squeeze another normal subgroup in between any two consecutive terms.

Corollary 6.8. *Every finite group has a composition series.*

Proof. Suppose G is a finite group and take a normal series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$$

with r as big as possible. (There must be a maximum possible r, since $|G| > |G_1| > \cdots > |G_{r-1}| > 1$, which means that $r \leqslant |G|$ for any normal series.) Now for each i there cannot be a group K with $G_i \rhd K \rhd G_{i+1}$ (otherwise we would be able to make a longer normal series by inserting K). So by Lemma 6.7 G_i/G_{i+1} is simple for each i, so our series is actually a composition series. □

Note that not every group has a composition series. For example, consider the infinite cyclic group $G = \mathcal{C}_\infty = \{\ldots, z^{-1}, 1, z, z^2, \ldots\}$. If this has a composition series $\mathcal{C}_\infty \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd \{1\}$, then in particular G_{r-1} is a simple subgroup of $\mathcal{C}_\infty$. But in fact $\mathcal{C}_\infty$ has no simple subgroups. To see this, suppose H is a simple subgroup of $\mathcal{C}_\infty$. Then $H \neq \{1\}$, so there is some $g \in H$ with $g \neq 1$. But then $\mathrm{ord}(g) = \infty$, so H is infinite. But by Proposition 6.1 there are no infinite abelian simple groups.

Theorem 6.9 (Jordan–Hölder Theorem)**.** *Suppose G is a group, and that G has two composition series*

$$G_0 \rhd G_1 \rhd \cdots \rhd G_r \qquad \text{and} \qquad H_0 \rhd H_1 \rhd \cdots \rhd H_s \rhd \{1\}.$$

Then $r = s$ and the groups

$$\frac{G_0}{G_1}, \ldots, \frac{G_{r-1}}{G_r}$$

are isomorphic to the groups

$$\frac{H_0}{H_1}, \ldots, \frac{H_{r-1}}{H_r}$$

in some order.

We won't give a full proof of the Jordan–Hölder Theorem.

Proof of the Jordan–Hölder Theorem in the case $r = 2$ (omitted in lectures, and non-examinable). The assumption $r \geqslant 2$ means that G is not trivial and not simple, and hence $s \geqslant 2$. We consider two cases.

- ◇ Suppose $G_1 = H_1$. Because $r = 2$, G_1 is simple. So H_1 is simple, so $s = 2$ (because there can't be a group H_2 with $H_1 \rhd H_2 > \{1\}$). So the two composition series are actually the same.

- ◇ Suppose $G_1 \neq H_1$. Then we claim that $G_1 \cap H_1 = \{1\}$ and $G_1 H_1 = G$.

  To see that $G_1 \cap H_1 = \{1\}$, recall from the Third Isomorphism Theorem that $G_1 \cap H_1 \trianglelefteqslant G_1$. Because G_1 is simple, this means that $G_1 \cap H_1 = \{1\}$ or G_1. But if $G_1 \cap H_1 = G_1$, then $G_1 \subseteq H_1$. But then $G_1 \lhd H_1 \lhd G$, contradicting the fact that G/G_1 is simple. So $G_1 \cap H_1 = \{1\}$.

  To see that $G_1 H_1 = G$: from the Third Isomorphism Theorem $G_1 \trianglelefteqslant G_1 H_1 \trianglelefteqslant G$. Since G/G_1 is simple, this means that $G_1 H_1 = G_1$ or G. But if $G_1 H_1 = G_1$, then $H_1 \subseteq G_1$, which gives $H_1 \lhd G_1 \lhd G$, contradicting the fact that G/H_1 is simple. So $G_1 H_1 = G$.

  Now by the Third Isomorphism Theorem

  $$\frac{G}{H_1} = \frac{G_1 H_1}{H_1} \cong \frac{G_1}{G_1 \cap H_1} = G_1$$

  and

  $$H_1 = \frac{H_1}{G_1 \cap H_1} \cong \frac{G_1 H_1}{G_1} = \frac{G}{G_1}.$$

  In particular, H_1 is simple, which means that $s = 2$. And the two factors in the series $G \rhd G_1 \rhd \{1\}$ are the same as the factors in the series $G \rhd H_1 \rhd \{1\}$ but the other way round. □

In view of the Jordan–Hölder Theorem, we can make the following definition.

Definition. Suppose G is a group and G has a composition series. The **composition length** of G is the length of any composition series for G, and the **composition factors** of G are the simple groups $G_0/G_1, \ldots, G_{r-1}/G_r$ in any composition series for G.

Examples.

- ◇ If $G = \{1\}$, then G has no composition factors.

- ◇ If G is simple, then the only composition factor of G is G.
- ◇ If $G = \mathcal{C}_{12}$, then we saw that the quotients in a composition series for G have orders $2, 2, 3$. Since any group of order p (for p a prime) is isomorphic to $\mathcal{C}_p$, the composition factors of $\mathcal{C}_{12}$ are $\mathcal{C}_2, \mathcal{C}_2, \mathcal{C}_3$. (Note that when we list the composition factors of a group, factors can appear more than once.)
- ◇ If $G = \mathcal{S}_n$ for $n \geqslant 5$, then the composition factors of G are $\mathcal{C}_2$ and $\mathcal{A}_n$.

7 *p*-groups

7.1 Finite *p*-groups

For the rest of Section 7, p is a prime number, and we'll only consider **finite** groups.

Definition. A ***p*-group** is a group whose order is a power of p.

Examples.

- ◇ The cyclic group $\mathcal{C}_{p^r}$ is a p-group for any r.
- ◇ $\mathcal{V}_4$ is a 2-group.
- ◇ $\mathcal{D}_{2^r}$ is a 2-group for any r.
- ◇ Let

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F}_p \right\}.$$

Then H is a subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$. Clearly $|H| = p^3$, so H is a p-group.

To construct lots more example, recall the **direct product** $G \times H$ from Section 3.6. If G and H are p-groups, then so is $G \times H$, so this enables us to construct lots of p-groups.

7.2 Classification of *p*-groups

Classification of all the groups of order p^n for given p, n is an important topic in group theory. Here we give a very brief taste. First we need a lemma.

Lemma 7.1. *Suppose G is a p-group and $G \neq \{1\}$. Then $Z(G) \neq \{1\}$.*

Proof. If we add up the sizes of all the conjugacy classes in G, then we get $|G|$, which is divisible by p. Since $\{1\}$ is a conjugacy class whose size is not divisible by p, there must be at least one more conjugacy class whose size is not divisible by p. So take an element $h \neq 1$ such that $p \nmid |\mathrm{ccl}(h)|$. Recall that

$$|G| = |\mathrm{ccl}(h)||\mathrm{C}_G(h)|.$$

Since $|G|$ is a power of p, this means that $|\mathrm{ccl}(h)|$ is a power of p. The only power of p not divisible by p is $p^0 = 1$. So $|\mathrm{ccl}(h)| = 1$, which means that $h \in Z(G)$. So $Z(G) \neq \{1\}$. □

Now let's look at small p-groups. We start with groups of order p.

Lemma 7.2. *Suppose G is a group of order p. Then $G \cong \mathcal{C}_p$.*

Proof. Take an element $g \neq 1$ in G. Then by Corollary 3.5 g has order p. So $\langle g \rangle$ is a subgroup of G of order p, so $G = \langle g \rangle \cong \mathcal{C}_p$. □

Now we move on to groups of order p^2.

Proposition 7.3. *Suppose G is a group of order p^2. Then G is isomorphic to $\mathcal{C}_{p^2}$ or $\mathcal{C}_p \times \mathcal{C}_p$.*

Proof. By Corollary 3.5, the order of any element of G is 1, p or p^2. If there is an element h of order p^2, then $G = \langle g \rangle \cong \mathcal{C}_{p^2}$. So suppose there is no element of order p^2; then every element apart from 1 has order p.

By Lemma 7.1 we can find an element $h \neq 1$ in $Z(G)$. Let $H = \langle h \rangle$; then H is a normal subgroup of G of order p.

Now take $k \in G \setminus H$, and let $K = \langle k \rangle$. Then $H < HK \leqslant G$, so by Lagrange's Theorem $HK = G$. So

$$G = \left\{ h^i k^j \;\middle|\; 0 \leqslant i, j < p \right\}$$

with $\mathrm{ord}(h) = \mathrm{ord}(k) = p$ and $kh = hk$. So we can define an isomorphism from G to $\mathcal{C}_p \times \mathcal{C}_p$ by $h^i k^j \mapsto (z^i, z^j)$. □

Proposition 7.4. *There are exactly five groups of order p^3 up to isomorphism. If $p = 2$, they are*

$$\mathcal{C}_8, \quad \mathcal{C}_4 \times \mathcal{C}_2, \quad \mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2, \quad \mathcal{D}_8, \quad \mathcal{Q}_8.$$

Sketch proof for $p = 2$. The order of any element of G must be $1, 2, 4$ or 8.

- ◇ If there is an element g of order 8, then $G = \langle g \rangle \cong \mathcal{C}_8$. So assume there are no elements of order 8.
- ◇ Now consider the case where every element of H has order 1 or 2, i.e. $g^{-1} = g$ for all $g \in G$. In this case we claim first of all that G is abelian: if $f, g \in G$, then

  $$fg = (fg)^{-1} = g^{-1} f^{-1} = gf.$$

  Now take an element $h \neq 1$, then an element $k \notin \{1, h\}$, then an element $l \notin \{1, h, k, hk\}$. Then the elements $h^a k^b l^c$ for $a, b, c \in \{0, 1\}$ are different, so

  $$G = \left\{ h^a k^b l^c \;\middle|\; a, b, c \in \{0, 1\} \right\},$$

  and the fact that G is abelian and $\mathrm{ord}(h) = \mathrm{ord}(k) = \mathrm{ord}(l) = 2$ determines the group operation. We get an isomorphism

  $$\begin{aligned} G &\longrightarrow \mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2 \\ h^a k^b l^c &\longmapsto (g^a, g^b, g^c). \end{aligned}$$

- ◇ Now assume that there are no elements of order 8, and that there is an element h of order 4. Then we have a subgroup

  $$H = \langle h \rangle = \{1, h, h^2, h^3\}.$$

  Let k be an element not in this subgroup. Then $H1$ and Hk are two different cosets of H, so we have eight different elements

  $$1, h, h^2, h^3, k, hk, h^2 k, h^3 k$$

of G. Since $|G| = 8$, these are all the elements of G. To work out the group operation, we just need to know what k^2 and kh are.

$H \trianglelefteq G$, since $|G:H| = 2$. So $khk^{-1} \in H$. $\mathrm{ord}\left(khk^{-1}\right) = \mathrm{ord}(h) = 4$, so $khk^{-1} = h$ or h^3, i.e. $kh = hk$ or $kh = h^3k$.

Now consider k^2. This must equal one of the above eight elements, but can't equal h^ik for any i, since then we would have $k = h^i$, a contradiction. So $k^2 \in H$. Furthermore, since k has order 2 or 4, k^2 has order 1 or 2, so $k^2 = 1$ or h^2.

So we have four possibilities, and enough information to work out the group completely in each case.

- ◇ If $k^2 = 1$ and $kh = hk$, then $G \cong \mathcal{C}_4 \times \mathcal{C}_2$.
- ◇ If $k^2 = h^2$ and $kh = hk$, then again $G \cong \mathcal{C}_4 \times \mathcal{C}_2$.
- ◇ If $k^2 = 1$ and $kh = h^3k$, then $G \cong \mathcal{D}_8$ (with $h \leftrightarrow r$, $k \leftrightarrow s$).
- ◇ If $k^2 = h^2$ and $kh = h^3k$, then $G \cong \mathcal{Q}_8$ (with $h \leftrightarrow i$, $k \leftrightarrow k$). □

Example. Let

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F}_2 \right\}.$$

Then G s a group of order 8, so must be isomorphic to one of the groups in Proposition 7.4. Let's follow the proof above to find out which one.

G is non-abelian, because for example

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So H can't have any elements of order 8 (because then H would be isomorphic to $\mathcal{C}_8$, which is abelian). Also, H must have elements of order 4 (because otherwise H would be isomorphic to $\mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2$, which is abelian). In fact by trial and error we can find an element of order 4, say

$$h = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$H = \langle h \rangle = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Now take an element $k \notin H$, say

$$k = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$k^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad kh = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = h^3k.$$

So now we have an isomorphism $G \cong \mathcal{D}_8$ determined by $h \mapsto r$ and $k \mapsto s$.

7.3 Simple p-groups and composition factors

Next we'll consider **simple** p-groups, and work out the composition factors of a p-group.

Proposition 7.5. *Suppose G is a p-group and $G \neq \{1\}$. Then G has a normal subgroup of order p. Hence the only simple p-group is $\mathcal{C}_p$.*

Proof. By Lemma 7.1 we can find an element $h \neq 1$ in $Z(G)$. By Corollary 3.5 $\mathrm{ord}(h)$ is a power of p, say p^a. Then $h^{p^{a-1}}$ has order p, so $\langle h^{p^{a-1}} \rangle$ is a subgroup of order p. This subgroup is normal, because $h \in Z(G)$.

So if $|G| > p$ then G is not simple. So G can only be simple if $|G| = p$, in which case $G \cong \mathcal{C}_p$. □

Corollary 7.6. *Suppose G is a group and $|G| = p^n$. Then the composition factors of G are $\underbrace{\mathcal{C}_p, \ldots, \mathcal{C}_p}_{n \text{ copies}}$.*

Proof. Take a composition series $G_0 \rhd \ldots \rhd G_r$ for G. Because every subgroup and quotient of a p-group is a p-group, the groups

$$\frac{G_0}{G_1}, \ldots, \frac{G_{r-1}}{G_r}$$

are p-groups. But these groups are simple, so by Proposition 7.5 $G_i/G_{i+1} \cong \mathcal{C}_p$ for every i. Since

$$\left|\frac{G_0}{G_1}\right| \times \cdots \times \left|\frac{G_{r-1}}{G_r}\right| = |G| = p^n,$$

we have $r = n$, so the composition factors are n copies of $\mathcal{C}_p$. □

7.4 p-subgroups

In this section we consider the following question: given a finite group G and an integer m dividing $|G|$, must G have a subgroup of order m? The general answer is no: $\mathcal{A}_4$ does not have a subgroup of order 6. But we'll specialise to the case where m is a prime power.

Definition. Suppose G is a finite group and p is a prime, and write the order of G as $p^a b$, where $p \nmid b$. A **Sylow p-subgroup** of G is a subgroup of order p^a.

Examples.

- ◇ If $|G| = p^a$, then G is a Sylow p-subgroup of G.
- ◇ If $p \nmid |G|$, then $\{1\}$ is a Sylow p-subgroup of G.
- ◇ Take $G = \mathcal{C}_{100}$. Then $|G| = 2^2 \times 5^2$.
  So $\langle g^{25} \rangle$ is a Sylow 2-subgroup, and $\langle g^4 \rangle$ is a Sylow 5-subgroup.
- ◇ Take $G = \mathcal{S}_3$. Then $|G| = 2 \times 3$.
  So $\langle (1\ 2) \rangle$ is a Sylow 2-subgroup, and $\langle (1\ 2\ 3) \rangle$ is a Sylow 3-subgroup.

- ◇ Take $G = \mathcal{D}_{12}$. Then $|G| = 2^2 \times 3$.

  So $\langle r^3, s\rangle$ is a Sylow 2-subgroup, and $\langle r^2\rangle$ is a Sylow 3-subgroup.

- ◇ Take $G = \mathrm{GL}_2(\mathbb{F}_p)$. Then $|G| = p \times (p-1)(p^2-1)$. So a Sylow p-subgroup of G must have order p. An example of such a subgroup is

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{F}_p \right\}.$$

We want to prove that every group has a Sylow p-subgroup. First we need a little lemma.

Lemma 7.7. *Suppose p is a prime and $n = p^a b$, where $p \nmid b$. Then $\binom{n}{p^a}$ is not divisible by p.*

Proof. Not given. This won't be examinable, but you might like to prove it for yourself – it's not very hard, it's just not group theory. □

Theorem 7.8 (Sylow's Theorem 1)**.** *Suppose G is a finite group and p is a prime. Then G has at least one Sylow p-subgroup.*

Proof. Write $|G|$ as $p^a b$ where $p \nmid b$. Let X be the set of all subsets of G of size p^a. We have an action π of G on X by left multiplication:

$$\pi_g\{s_1, \ldots, s_{p^a}\} = \{gs_1, \ldots, gs_{p^a}\}.$$

By Lemma 7.7, $|X| = \binom{p^a b}{p^a}$ is not divisible by p, so there must be an orbit Y for π such that $|Y|$ is not divisible by p. Let $S = \{s_1, \ldots, s_{p^a}\} \in Y$, and let $P = \mathrm{Stab}(S)$. Then $P \leqslant G$ by Lemma 5.3, and by the Orbit–Stabiliser Theorem we have $|Y||P| = |G| = p^a b$. Since $|Y|$ is not divisible by p, this means $|P|$ is divisible by p^a.

Now we claim that $|P| \leqslant p^a$. To see this, suppose $g \in P$. Then g fixes the set $S = \{s_1, \ldots, s_{p^a}\}$, i.e.

$$\{gs_1, \ldots, gs_{p^a}\} = \{s_1, \ldots, s_{p^a}\}.$$

In particular $gs_1 \in \{s_1, \ldots, s_{p^a}\}$, so $gs_1 = s_i$ for some i, so $g = s_i s_1^{-1}$. This applies for every $g \in P$, so $P \subseteq \{s_1 s_1^{-1}, \ldots, s_{p^a} s_1^{-1}\}$, and hence $|P| \leqslant p^a$.

So $P \leqslant G$, $|P|$ is divisible by p^a and $|P| \leqslant p^a$. So $|P| = p^a$, and P is a Sylow p-subgroup of G. □

Example. Let $G = \mathcal{U}_9 = \{1, 2, 4, 5, 7, 8\}$, and $p = 3$. G is small enough that we can easily find a subgroup of order 3, but let's follow the proof of Sylow's Theorem 1.

Let X be the set of 3-subsets of $\mathcal{U}_9$. For this example only, we'll write the set $\{a, b, c\}$ as abc. We have $|X| = \binom{6}{3} = 20$, which isn't divisible by 3. Let's find the orbits, to find an orbit of size not divisible by 3.

$$\begin{aligned}
\mathrm{Orb}(124) &= \{124, 248, 478, 125, 157, 578\} \\
\mathrm{Orb}(127) &= \{127, 245, 148, 158, 457, 278\} \\
\mathrm{Orb}(128) &= \{128, 247, 458, 145, 257, 178\} \\
\mathrm{Orb}(127) &= \{147, 258\}
\end{aligned}$$

So we have an orbit $Y = \{147, 258\}$ whose size is not divisible by 3. Let $H = 147$, and let $P = \mathrm{Stab}(H)$. Then $P = \{1, 4, 7\}$, which is a Sylow 3-subgroup of $\mathcal{U}_9$.

Notation. Suppose G a finite group. Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G, and let $\mathrm{n}_p(G)$ denote the number of Sylow p-subgroups of G.

Example. Take $G = \mathcal{D}_{10}$. Then a Sylow 5-subgroup is a subgroup of order 5. One such subgroup is $\langle r \rangle$. In fact, this is the only example: the elements of $\mathcal{D}_{10} \setminus \langle r \rangle$ all have order 2, so cannot be contained in a subgroup of order 5. So a subgroup of order 5 is contained in $\langle r \rangle$, so must be $\langle r \rangle$. So $\mathrm{n}_5(\mathcal{D}_{10}) = 1$.

Now consider Sylow 2-subgroups of $\mathcal{D}_{10}$. Such a subgroup has order 2, so consists of 1 together with an element of order 2. So $\mathrm{n}_2(\mathcal{D}_{10})$ is simply the number of elements of order 2 in $\mathcal{D}_{10}$, which is 5.

Now we consider conjugacy. If $P \in \mathrm{Syl}_p(G)$ and $g \in G$, then $gPg^{-1} \leqslant G$ and $|gPg^{-1}| = |P|$, so gPg^{-1} is also a Sylow p-subgroup of G.

Hence we have an action of G of G on $\mathrm{Syl}_p(G)$ by conjugation:

$$\pi_g(P) = gPg^{-1}.$$

As a special case: if P is the only Sylow p-subgroup of G, then $P \trianglelefteq G$.

The next part of Sylow's theorems says that this action is transitive, i.e. all the Sylow p-subgroups are conjugate. This needs a bit of set-up. Recall that f $N \leqslant G$ then the **normaliser** of N is defined as

$$\mathrm{N}_G(N) = \{ g \in G \mid \ gNg^{-1} = N \},$$

and that $N \trianglelefteq \mathrm{N}_G(N)$.

Proposition 7.9. *Suppose G is a finite group and $P, Q \in \mathrm{Syl}_p(G)$ with $gQg^{-1} = Q$ for every $g \in P$. Then $P = Q$.*

Proof (non-examinable). The condition that $gQg^{-1} = Q$ for all $g \in P$ says that just says that $P \leqslant \mathrm{N}_G(Q)$. So we have $P \leqslant \mathrm{N}_G(Q)$ and $Q \trianglelefteq \mathrm{N}_G(Q)$. So by Proposition 3.16 we get $Q \trianglelefteq PQ \leqslant \mathrm{N}_G(Q)$, and by the Third Isomorphism Theorem

$$\frac{PQ}{Q} \cong \frac{P}{P \cap Q}.$$

Hence

$$\left| \frac{PQ}{Q} \right| = \left| \frac{P}{P \cap Q} \right|,$$

i.e.

$$\frac{|PQ|}{|Q|} = \frac{|P|}{|P \cap Q|}.$$

If we let $|G| = p^a b$ with $p \nmid b$, then $|P| = |Q| = p^a$. Since $P \cap Q \leqslant Q$, we have $|P \cap Q| = p^d$ for some $d \leqslant a$. So $|PQ| = p^a p^{a-d}$. So by Lagrange's Theorem p^{a-d} divides b. So we must have $p^{a-d} = 1$, i.e. $d = a$. So $|P| = |P \cap Q| = |Q|$, and so $P = P \cap Q = Q$. □

Theorem 7.10 (Sylow's Theorem 2)**.** *Suppose G is a finite group and p is a prime. Then all the Sylow p-subgroups of G are conjugate.*

Theorem 7.11 (Sylow's Theorem 3)**.** *Suppose G is a finite group, and p is a prime, and write $|G| = p^a b$, where $p \nmid b$. Then $n_p(G) \equiv 1 \pmod{p}$, and $n_p(G) \mid b$.*

Proof of Sylow's Theorems 2 and 3 (non-examinable). G acts by conjugation on $\mathrm{Syl}_p(G)$; we'll refer to an orbit for this action as a **G-orbit**. If we take $P \in \mathrm{Syl}_p(G)$, then P also acts on $\mathrm{Syl}_p(G)$ by conjugation. We'll refer to an orbit for this action as a **P-orbit**.

By the Orbit–Stabiliser Theorem, the size of any P-orbit divides $|P| = p^a$, so must be a power of p. So the size of any P-orbit is either 1 or divisible by p. Now $gPg^{-1} = P$ for every $g \in P$, so $\{P\}$ is a P-orbit of size 1. By Proposition 7.9 the only P-orbit of size 1 is $\{P\}$, since if $\{Q\}$ is a P-orbit, then $hQh^{-1} = Q$ for every $h \in P$, so $P = Q$. So all the P-orbits except $\{P\}$ have size divisible by p. Hence the total size of all the orbits, i.e. $n_p(G)$, is congruent to 1 modulo p.

Since $P \leqslant G$, if two elements of $\mathrm{Syl}_p(G)$ lie in the same P-orbit then they lie in the same G-orbit. So every P-orbit is contained in a G-orbit, so every G-orbit is a union of P-orbits. So if we let Y be the G-orbit containing P, then from the last paragraph $|Y| \equiv 1 \pmod{p}$, and for every other G-orbit Z we have $|Z| \equiv 0 \pmod{p}$. But if there is a G-orbit $Z \neq Y$, then we can take $\hat{P} \in Z$ and repeat the above argument with $\hat{P}$ in place of P, and we find that $|Z| \equiv 1 \pmod{p}$; contradiction. So Y is the only G-orbit, i.e. all the Sylow p-subgroups of G are conjugate.

So $\mathrm{Orb}(P) = \mathrm{Syl}_p(G)$, so by the Orbit–Stabiliser Theorem

$$|G| = |\mathrm{Syl}_p(G)||\mathrm{N}_G(P)|.$$

Now $P \leqslant \mathrm{N}_G(P) \leqslant G$, and we have $|P| = p^a$, $|G| = p^a b$, so by Lagrange's Theorem $|\mathrm{N}_G(P)| = p^a c$ for some $c \mid b$. So

$$n_p(G) = |\mathrm{Syl}_p(G)| = \frac{|G|}{|\mathrm{N}_G(P)|} = \frac{p^a b}{p^a c} = \frac{b}{c}$$

which divides b. □

Remark. Sylow's Theorem 2 shows that if $P \in \mathrm{Syl}_p(G)$ and $P \trianglelefteq G$, then P is the only Sylow p-subgroup of G (because any other Sylow p-subgroup would have to be conjugate to P). In particular, if G is abelian, then (since all subgroups of an abelian group are normal) G has a unique Sylow p-subgroup.

Sylow's Theorem 3 can be useful for classifying groups of a given order.

Example. We can show that C_{15} is the only group of order 15 up to isomorphism. To do this, suppose G is a group of order 15. Then $n_3(G) \equiv 1 \pmod{3}$ and $n_3(G) \mid 5$, so $n_3(G)$ must be 1, i.e. there is only one subgroup $P < G$ of order 3. P contains two elements of order 3, and in fact these are the only elements in G of order 3, since if $g \in G$ with $\mathrm{ord}(g) = 3$, then $\langle g \rangle$ is a subgroup of G of order 3, so must be P, i.e. $g \in P$.

Similarly $n_5(G) = 1$, and this means that G contains only four elements of order 5. We know G has only one element of order 1, and elements of G have order 1, 3, 5 or 15. So there must be eight elements of order 15. So let g be an element of order 15. Then $\langle g \rangle$ is a subgroup of order 15, so $G = \langle g \rangle \cong C_{15}$.

Sylow's Theorem 3 is also useful in the search for finite simple groups.

Examples.

- ◇ Suppose G is a group of order 20; then we claim that G cannot be simple. $n_5(G) \equiv 1 \pmod 5$ and $n_5(G) \mid 4$, so $n_5(G) = 1$. So G has only one Sylow 5-subgroup P, so $P \lhd G$, and therefore G is not simple.

- ◇ For a more complicated example, suppose G is a group of order 12; again we claim that G cannot be simple. $n_3(G) \equiv 1 \pmod 3$ and $n_3(G) \mid 4$, so $n_3(G) = 1$ or 4. If $n_3(G) = 1$ then (as in the example above) G has a normal Sylow 3-subgroup, so is not simple. So assume instead that $n_3(G) = 4$. Then G has four subgroups of order 3, each of which contains two elements of order 3, so G contains eight elements of order 3. But now consider Sylow 2-subgroups: such a subgroup has order 4, and cannot contain any element of order 3. But there are only four elements whose order is not 3, so only one possible Sylow 2-subgroup. So G has a normal Sylow 2-subgroup, so again cannot be simple.