MAS114: Numbers and Groups, Semester 2

Module Information

- **Contact details.** Dr Sam Marsh (Room G9, Hick Building).
- **Office hour.** FILL THIS IN HERE: , or see the course website. No appointment necessary, just drop in.
- **Webpage.** `http://sam-marsh.staff.shef.ac.uk/mas114` (also found through MOLE).
- **Discussion board.** Unless you are contacting me about personal matters, please ask questions on the discussion board instead of emailing (found via the website).
- **Tutorial class.** In the tutorial class you will receive a brief demonstration from your tutor and be set interesting problems related to the material in the course. Worksheets from the classes will appear on the course webpage.
- **Extra exercises.** In addition to the tutorial class worksheets, there is a booklet of extra exercises. Worked solutions to these exercises appear on the course webpage. You should work on these exercises in your own time.
- **Homework and online tests.** The online tests from Semester 1 continue. Additionally, one written homework question will be due in at each problem class. The written homework is important as it helps you to develop skills in presenting coherent arguments — or *proofs* — among other things. It will be returned to you with feedback.

- **Mathematics at degree-level.** Degree-level pure mathematics has a different emphasis from the subject you learnt at school. Roughly summarised, ideas, reasons and methods are seen as more important than answers. Getting used to this takes practise and effort. With this in mind, I ask you to
  - spend time outside of lectures understanding the material,
  - puzzle over the problem booklet (even when it feels like you're getting nowhere),
  - hand in the homeworks,
  - ask for help from me and the tutors,
  - do your best to finish the course having grown as a mathematician.

References

[1] C.R. Jordan and D.A. Jordan, *Groups*, Newnes, Elsevier, 1994, ISBN 0-340-61045-X.

An excellent recommended, but not compulsory, text book covering all of the material from course. A [1] appearing in the notes refers to this book.

Introduction

The main object of study this semester will be an abstract mathematical object known as a *group*, and we will be studying *group theory*.

If this sounds scary, don't worry: you will find that you are already familiar with some groups. That is, some of the mathematical objects you have used regularly are examples of groups.

As an overview of what's to come, we introduce the notion of a group by listing four so-called *group axioms*. In other words, we give four properties

that a group obeys; anything that satisfies these four properties will be a group, and the theory that we develop will apply to it.

In this way we can prove things about a whole range of seemingly unconnected objects all in one go.

Have you met approaches like this already?

You will see that, roughly speaking, when you have dealt with a collection (or set) of things, with a rule for combining any two of them to get a third, you have probably been dealing with a group.

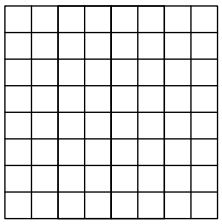
Numbers and addition? Numbers and multiplication? Are these groups? For which numbers? You will be able to answer these questions by the end of the course!

1 Orbits, Functions and Symmetries

1.1 Colouring problems and orbits

At the start of MAS114, you asked

How many squares are there on a chessboard?



Of course, counting only single 1×1 squares there are 64, but including things like the 3×3 squares hidden within the grid, we get a bigger number, namely 204 $(= 64 + 49 + 36 + 25 + 16 + 9 + 4 + 1)$.

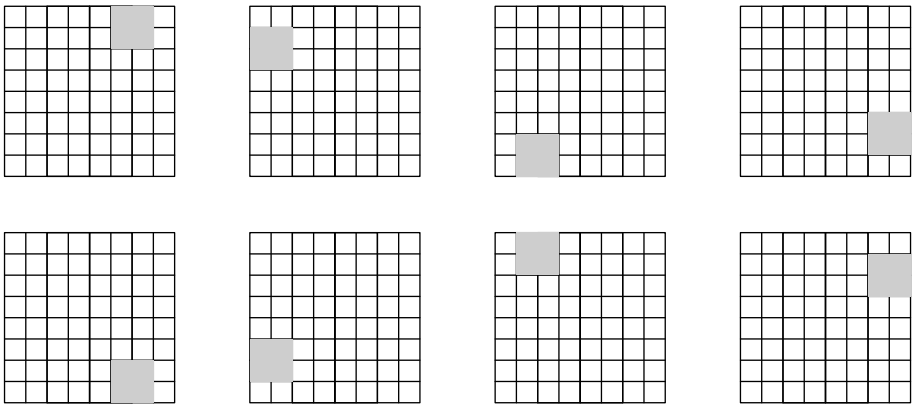
Problem 1.1. Let's change the question again, taking account of symmetry.

Suppose that on a square glass tile is drawn an 8×8 square grid, and that there is to be a blue square of any size coloured in, using the grid-lines as edges. In how many ways can this be done?

> We will regard, for example, all four tiles in which a 1×1 corner square is blue as 'the same', as they can be obtained from each other by rotation or by reflection (turning the tile over). We say that these four tiles are in the same *orbit*.

So the answer to our problem is clearly the number of different orbits. Is this $204/4 = 51$?

That would be true if all orbits had four elements. But, of course, it's not that simple. It's easy to find a tile that's in an orbit on its own (draw one!) and there are orbits of eight tiles, for example the eight tiles with 2×2 blue squares shown below.



Clearly the problem is hard! We will return to this type of problem later in the course, when the *Orbit-counting Theorem* will be available. For now, we settle for the answer to the corresponding problem for a 3×3 and 4×4 grid.

For a 3×3 grid,

Thus there are 5 orbits, as shown in the table:

	no. of orbits	no. of elements in each orbit	total
1×1	3	4,4,1	9
2×2	1	4	4
3×3	1	1	1
total	5	—	14

.

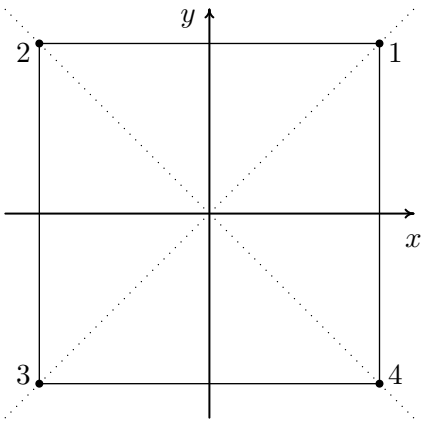
For a 4×4 grid, taking no account of symmetry, there are $16+9+4+1 = 30$ glass tiles patterned with a blue square. Introducing symmetry, and using the applet on the course website or pen and paper, you should be able to convince yourself that there are 8 orbits altogether, as shown in the table.

	no. of orbits	no. of elements in each orbit	total
1×1	3	4,8,4	16
2×2	3	4,1,4	9
3×3	1	4	4
4×4	1	1	1
total	8	—	30

.

1.2 Symmetries of the square

Definition 1.2. Consider a square in the xy-plane with centre at the origin and with sides parallel to the x and y axes.



r_0 = rotation through 0
r_1 = rotation through $\pi/2$
r_2 = rotation through π
r_3 = rotation through $3\pi/2$
s_1 = reflection in x-axis
s_2 = reflection in diagonal $y = x$
s_3 = reflection in y-axis
s_4 = reflection in diagonal $y = -x$

Listed above are eight functions on the plane which, although they may move the individual points in the square, leave the square occupying its original position.

The rotations are taken to be anticlockwise.

These eight functions are called the *symmetries* of the square.

If we apply these symmetries to a tile from Problem 1.1, we obtain the other tiles in the same orbit.

1.3 Functions

The symmetries of the square are examples of *functions* and we recall the following basic language and notation for handling them.

Most of this has been covered in MAS110 or Semester 1 of MAS114.

Domains, codomains and ranges

Definitions 1.3. Below, A and B are non-empty sets.

- A *function* (or *mapping*) $f : A \to B$ assigns, for each $a \in A$, a unique element $f(a)$ of B.
- The set A is called the *domain* of f and B is the *codomain* of f.
- The *range* or *image* of f is the set

$$f(A) = \{b \in B : b = f(a) \text{ for some } a \in A\}$$

of all things 'hit' by the function.

The range may or may not be all of the codomain.

Example 1.4.

Composition of functions

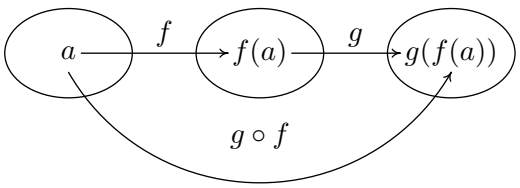
Definitions 1.5. Again, A, B, C and D denote non-empty sets.

- Two functions $f : A \to B$ and $g : C \to D$ are *equal* when $A = C$, $B = D$ and $f(a) = g(a)$ for all $a \in A$; that is, when they have the same domain and codomain and give the same value on each element of the domain.

- Let $f : A \to B$ and $g : B \to C$ be functions. The *composite* $g \circ f$ is the function $A \to C$ such that, for all $a \in A$,

$$g \circ f(a) = g(f(a)).$$

We can picture this as below.



Sometimes we omit the symbol $\circ$ and just write gf.

- If f and g map from A to A, then we can form both $g \circ f$ and $f \circ g$ (which are both functions $A \to A$). We say that f and g *commute* if $g \circ f = f \circ g$.

Example 1.6. Let $f : \mathbb{R} \to \mathbb{R},\ f(x) = x + 1$ and $g : \mathbb{R} \to \mathbb{R},\ g(x) = x^2$.

To show that $f \circ g \neq g \circ f$ we demonstrate one *specific* value of x at which they differ. This is proof by counter-example.

Observing that $x^2 + 2x + 1$ looks like a different function to $x^2 + 1$ is not good enough, as it's still possible that these two expressions would give the same output for each value of x in the domain. The point is, now we've shown that they don't!

Example 1.7.

Because functions don't always commute, remember that, to work out $g \circ f$, first apply f, then apply g.

Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions.

Then $g \circ f : A \to C$ so we can form the composite $h \circ (g \circ f) : A \to D$. Also, $h \circ g : B \to D$ so we can form $(h \circ g) \circ f : A \to D$.

Thus we have two functions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ from A to D.

Proposition 1.8 (Associative law for composition of functions)**.** *With f, g and h as above, $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof. Both $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are functions from A to D. Both send an arbitrary element $a \in A$ to $h(g(f(a)))$. Thus $h \circ (g \circ f) = (h \circ g) \circ f$. □

The associative law allows us to omit brackets, and write simply $h \circ g \circ f$ or hgf without ambiguity.

Identity functions and inverses

Definitions 1.9. Let A and B denote non-empty sets.

- The function from A to A which sends each element $a \in A$ to itself is called the *identity function* on A and is written id_A. In other words, $\mathrm{id}_A : A \to A$ and $\mathrm{id}_A(a) = a$ for all $a \in A$.

  Suppose $f : A \to B$ and we compose with an identity function. What do we get? That is, what are $f \circ \mathrm{id}_A$ and $\mathrm{id}_B \circ f$?

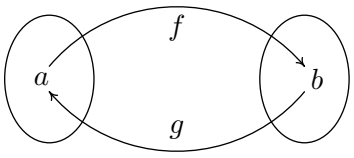
- If $f : A \to B$ is a function, then an *inverse* for f is a function $g : B \to A$ such that

  $$g \circ f = \mathrm{id}_A \text{ and } f \circ g = \mathrm{id}_B .$$

  That is, for all $a \in A$ and all $b \in B$, $g(f(a)) = a$ and $f(g(b)) = b$.

Here f 'undoes' g, and vice versa.

We say a function is *invertible* if it has an inverse.



Note that the definition of inverse is symmetric: if g is an inverse for f then f is an inverse for g.

Examples 1.10. The following are pairs of inverse functions.

1. $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = 3x$ and $g(x) = \frac{1}{3}x$ for all $x \in \mathbb{R}$.
2. $A = \mathbb{R}$, $B = \{x \in \mathbb{R} : x > 0\}$, $f : A \to B$ given by $f(x) = e^x$ for all $x \in A$, and $g : B \to A$ given by $g(x) = \ln(x)$ for all $x \in B$.
3. For any non-empty set A, the identity function id_A is an inverse for itself.

1.4 Rotations and reflections

Rotations and reflections in 2-dimensional space are examples of functions, where the domain and codomain both consist of all points $P = (x, y)$ where $x, y \in \mathbb{R}$.

> The set of all such points is written $\mathbb{R}^2$ and is called the *Euclidean (or x, y) plane.*

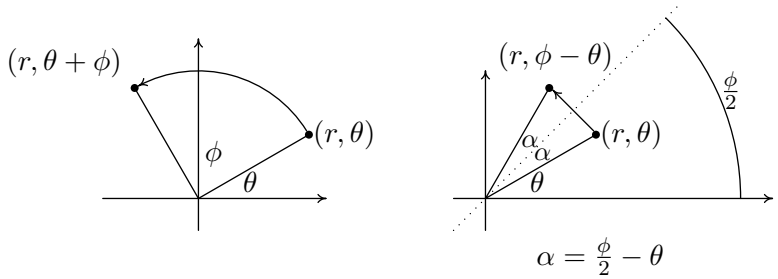
Each point (x, y) in $\mathbb{R}^2$ can also be written in polar coordinates (r, θ)

That is, two (non-zero) points are the same if and only if they have the same distance from the origin and arguments differing by a multiple of 2π.

Let $\phi \in \mathbb{R}$. Using polar coordinates, we define two functions $\mathrm{rot}_\phi : \mathbb{R}^2 \to \mathbb{R}^2$ and $\mathrm{ref}_\phi : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$\begin{aligned} \mathrm{rot}_\phi((r,\theta)) &= (r, \phi + \theta) \\ \mathrm{ref}_\phi((r,\theta)) &= (r, \phi - \theta) \end{aligned}$$

for all $(r,\theta) \in \mathbb{R}^2$. [1]



The effect of rot_ϕ is to rotate each point through the angle ϕ anticlockwise about 0. The effect of ref_ϕ is to reflect each point in the line making an angle of $\frac{\phi}{2}$ with the x-axis.

Where does the point $(1,0)$ *get sent under* rot_ϕ *and* ref_ϕ*?*
Is there any ambiguity in that question?

[1] We often don't bother with two sets of brackets, and write just $\mathrm{rot}_\phi(r,\theta)$ and $\mathrm{ref}_\phi(r,\theta)$ for clarity.

Here are some points to note.

- rot_0 is the identity function $\mathrm{id}_{\mathbb{R}^2}$, but ref_0 (which is reflection in the x-axis) is not.
- rot_α and rot_β can be equal when $\alpha \neq \beta$ and similarly for ref:

$$\mathrm{rot}_\alpha = \mathrm{rot}_\beta \iff \alpha = \beta + 2n\pi \text{ for some } n \in \mathbb{Z} \quad (1)$$
$$\text{and } \mathrm{ref}_\alpha = \mathrm{ref}_\beta \iff \alpha = \beta + 2n\pi \text{ for some } n \in \mathbb{Z}. \quad (2)$$

- In Section 1.2, we looked at the symmetries of the square, with rotations $r_0, \ldots, r_3$ and reflections $s_1, \ldots, s_4$. Using our new notation,

$$r_0 = \mathrm{rot}_0,\ r_1 = \mathrm{rot}_{\pi/2},\ r_2 = \mathrm{rot}_\pi,\ r_3 = \mathrm{rot}_{3\pi/2},$$
$$s_1 = \mathrm{ref}_0,\ s_2 = \mathrm{ref}_{\pi/2},\ s_3 = \mathrm{ref}_\pi \text{ and } s_4 = \mathrm{ref}_{3\pi/2}\,.$$

  Note. Remember that, for ref_ϕ, the angle between the line of reflection and the x-axis is $\phi/2$, not ϕ, so for example reflection in the diagonal $y = x$ is $\mathrm{ref}_{\pi/2}$ because the angle between the line of reflection and the x-axis is $\pi/4$.

Composing rotations and reflections

As rotations and reflections are functions, we can compose them. What do we get? Clearly $\mathrm{rot}_\alpha \mathrm{rot}_\beta = \mathrm{rot}_{\alpha+\beta}$: the combined effect of rotation through two angles is rotation through their sum. Less obvious is the composite $\mathrm{ref}_\alpha \mathrm{ref}_\beta$.

To calculate this, let $(r, \theta) \in \mathbb{R}^2$ be any point. Then

Hence $\mathrm{ref}_\alpha \mathrm{ref}_\beta = \mathrm{rot}_{\alpha-\beta}$. In particular, two reflections give a rotation.

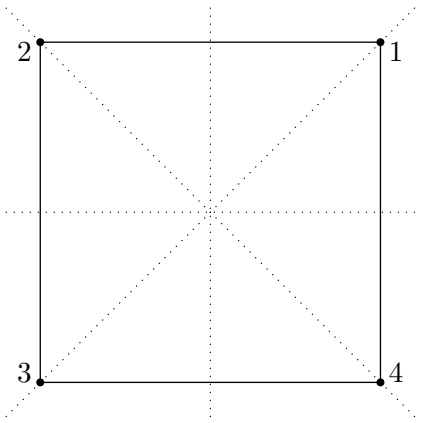
Similar calculations show that $\mathrm{rot}_\alpha \mathrm{ref}_\beta = \mathrm{ref}_{\alpha+\beta}$ and $\mathrm{ref}_\alpha \mathrm{rot}_\beta = \mathrm{ref}_{\alpha-\beta}$. The four rules for composing rot/ref can be summarized in a table.

$\mathrm{rot}_\alpha \mathrm{rot}_\beta$	$=$	$\mathrm{rot}_{\alpha+\beta}$
$\mathrm{ref}_\alpha \mathrm{ref}_\beta$	$=$	$\mathrm{rot}_{\alpha-\beta}$
$\mathrm{rot}_\alpha \mathrm{ref}_\beta$	$=$	$\mathrm{ref}_{\alpha+\beta}$
$\mathrm{ref}_\alpha \mathrm{rot}_\beta$	$=$	$\mathrm{ref}_{\alpha-\beta}$

Are rot_θ *and* ref_θ *invertible? If so, what are their inverses? (Think about the geometry or the formulae, noting that* $\mathrm{rot}_0 = \mathrm{id}_{\mathbb{R}^2}$*.)*

1.5 Dihedral and orthogonal groups

The dihedral group, D_4



$r_0 = \mathrm{rot}_0$
$r_1 = \mathrm{rot}_{\pi/2}$
$r_2 = \mathrm{rot}_\pi$
$r_3 = \mathrm{rot}_{3\pi/2}$
$s_1 = \mathrm{ref}_0$
$s_2 = \mathrm{ref}_{\pi/2}$
$s_3 = \mathrm{ref}_\pi$
$s_4 = \mathrm{ref}_{3\pi/2}$

The eight symmetries of the square form one of the basic examples of a *group*, the group D_4 of symmetries of the square. (D stands for dihedral.) It has the following four important properties.

(i) *Closure.* If f and g are in D_4 then so is the composite fg.

For example, consider $r_1 s_3$. From the general rules, this must be a reflection. To find out which one, follow vertex (corner) 1 of the square. Now, s_3 sends 1 to 2, and r_1 sends 2 to 3, so $r_1 s_3$ sends 1 to 3. Therefore $r_1 s_3$ must be the reflection sending 1 to 3, which is s_4.

Similarly, $s_3 r_1$ is the reflection sending 1 to itself, so $s_3 r_1 = s_2$. Alternatively, we can use the rot/ref formulae:

We can complete a so-called *Cayley table* showing the combinations in D_4. We rewrite r_0 as e; see (iii) below.

D_4	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_2	s_3	s_4	s_1
r_2	r_2	r_3	e	r_1	s_3	s_4	s_1	s_2
r_3	r_3	e	r_1	r_2	s_4	s_1	s_2	s_3
s_1	s_1	s_4	s_3	s_2	e	r_3	r_2	r_1
s_2	s_2	s_1	s_4	s_3	r_1	e	r_3	r_2
s_3	s_3	s_2	s_1	s_4	r_2	r_1	e	r_3
s_4	s_4	s_3	s_2	s_1	r_3	r_2	r_1	e

The composite fg is entered in the row labelled f and the column labelled g.

(ii) *Associativity.* $(fg)h = f(gh)$ for all $f, g, h \in D_4$.

This follows since elements of D_4 are functions, so the associative law for composition of functions, Proposition 1.8, applies.

(iii) *Neutral element.* The element $e = \mathrm{rot}_0$ has the property that $ef = f = fe$ for all symmetries $f \in D_4$. That is, composing with rot_0 leaves every symmetry unchanged.

We call this element a *neutral* or *identity* element for D_4.

(iv) *Inverses.* For each element $f \in D_4$ there is an element $g \in D_4$, called the *inverse* of f, such that $fg = e = gf$.

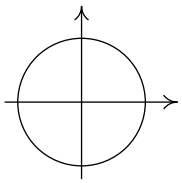
Notice that 6 elements of D_4 are their own inverses: they satisfy $f^2 = e$. The remaining two elements are r_1 and r_3, which are inverses of each other.

Observations. From the Cayley table, we see that $r_2 s_1 = s_1 r_2$, so r_2 and s_1 commute, but $r_1 s_1 \neq s_1 r_1$, so r_1 and s_1 do not.

Also notice the *Latin square* property: each element of D_4 appears exactly once in each row and exactly once in each column.

Are there more pairs of elements of D_4 which commute or more which don't?

THE ORTHOGONAL GROUP, O_2



In contrast to the square, the unit circle has infinitely many symmetries, all the rotations rot_θ and all the reflections ref_θ where $\theta \in \mathbb{R}$.

As for the square, these symmetries form a group, called O_2 or the group of symmetries of the circle. (O stands for orthogonal.)

We cannot draw up a Cayley table for O_2 because it is infinite. However, like with D_4, the same four important properties hold:

(i) *closure* holds because of the rot/ref formulae,
(ii) *associativity* holds by Proposition 1.8,
(iii) $e = \mathrm{rot}_0$ is *neutral*, and
(iv) each ref_α is its own *inverse* and each rot_α has *inverse* $\mathrm{rot}_{-\alpha}$.

1.6 Inverting functions

Given a function $f : A \to B$, we can ask whether or not it has an inverse, $g : B \to A$. Perhaps we'd try to create such an inverse by

$$\text{for any } b \in B, \text{ let } g(b) = a \text{ where } a \in A \text{ is mapped by } f \text{ to } b. \qquad (3)$$

But this can fail for two reasons.

Luckily, some familiar definitions help.

Surjectivity, injectivity and bijectivity

Definitions 1.11. Let $f : A \to B$ be a function.

- We say that f is *surjective* or a *surjection* if, for each $b \in B$, there exists at least one element $a \in A$ such that $f(a) = b$.

  That is, if everything gets hit at least once. Can you rephrase this in terms of the range and codomain?

- We say that f is *injective* or an *injection* if whenever $a_1,\ a_2 \in A$ are such that $f(a_1) = f(a_2)$ then $a_1 = a_2$.

  That is, if two different elements of the domain can't go to the same element of the codomain. Or, equivalently, if nothing gets hit more than once.

- A function which is both injective and surjective is said to be *bijective* or a *bijection.*

  Bijections are the function for which everything gets hit precisely once.

Notice that f is bijective if and only if for each $b \in B$ there is a unique element $a \in A$ such that $f(a) = b$.

Example 1.12. Let's look at how injectivity and surjectivity of functions given by the rule $f(x) = x^2$ depend on the domain and codomain.

Proving surjectivity

To show that a function $f : A \to B$ is surjective we must demonstrate that for each $b \in B$ there exists $a \in A$ such that $f(a) = b$. Often, rough work is needed to find an expression for a in terms of b; the proof then involves showing that the formula works.

Example 1.13. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be the function such that $f(x, y) = (y, x + y)$ for all $(x, y) \in \mathbb{R}^2$. We show that f is surjective.

Example 1.14. Let $A = \mathbb{R}\backslash\{0\}$, $B = \mathbb{R}$, and let $f(a) = a - \frac{1}{a}$ for $a \in A$. Again, we show that f is surjective.

Proof. Let $b \in \mathbb{R}$ and put $a = \dfrac{b + \sqrt{b^2+4}}{2}$. Note that $b^2 + 4 > 0$ so $\sqrt{b^2+4}$ is a real number, so $a \in \mathbb{R}$. Also $a \neq 0$, otherwise $b = -\sqrt{b^2+4}$ and $b^2 = b^2 + 4$, which is impossible. Hence $a \in A$. Now,

$$\begin{aligned} f(a) = a - \frac{1}{a} &= \frac{b + \sqrt{b^2+4}}{2} - \frac{2}{b + \sqrt{b^2+4}} \\ &= \frac{b + \sqrt{b^2+4}}{2} - \frac{2(b - \sqrt{b^2+4})}{b^2 - (b^2+4)} \\ &= \frac{b + \sqrt{b^2+4}}{2} + \frac{b - \sqrt{b^2+4}}{2} \\ &= b. \end{aligned}$$

Hence f is surjective. □

We could have used the other value for a here, and all would have worked fine. In fact, using these ideas we see that f is not injective: putting $b = 0$ we get $a = \pm 1$ and find that $f(1) = 0 = f(-1)$.

Sometimes, as in the next example, for a given $b \in B$, there may be infinitely many choices for $a \in A$ with $f(a) = b$.

Example 1.15. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be the function such that $f(x, y) = x + y$ for all $(x, y) \in \mathbb{R}^2$. We show that f is surjective.

Let $b \in \mathbb{R}$. Then $f(x, y) = b$ whenever $x + y = b$. In particular, let $a = (b, 0) \in \mathbb{R}^2$. Then $f(a) = b$. Thus f is surjective.

We could just as well have taken $a = (0, b)$ or $a = (1, b - 1)$
or any one of infinitely many possibilities.

Proving injectivity

To show that a function $f : A \to B$ is not injective is easy: we give a clear counter-example by finding two different elements $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, e.g. $f(1) = f(-1)$ shows that $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$ is not injective.

Below are two proofs that particular functions $f : A \to B$ *are* injective.

Example 1.16. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be given by $f(x, y) = (y, x + y)$ for all $(x, y) \in \mathbb{R}^2$. We show that f is injective.

Example 1.17. Let $A = \mathbb{R}\backslash\{0\}$ and $f : A \to \mathbb{R}$ be $f(a) = \frac{1+a}{a}$.

In this last example, is f surjective? See what happens if you try to prove surjectivity, being very careful of division by zero.

Bijective functions

Theorem 1.18. *A function $f : A \to B$ has an inverse if and only if f is bijective.*

Proof. For the 'if' part, suppose that f is bijective. For each $b \in B$, let $g(b)$ be the unique element $x \in A$ with $f(x) = b$ (such an element exists since f is bijective). This defines a function $g : B \to A$ such that $f(g(b)) = b$ for all $b \in B$ and $g(f(a)) = a$ for all $a \in A$. Thus g is an inverse of f.

For the 'only if' part, suppose that f has an inverse $g : B \to A$. For surjectivity, let $b \in B$ and set $a = g(b) \in A$. Then $f(a) = f(g(b)) = f \circ g(b) = \mathrm{id}_B(b) = b$. Thus f is surjective. For injectivity, let $a_1, a_2 \in A$ be such that $f(a_1) = f(a_2)$. Applying g to both sides, $g(f(a_1)) = g(f(a_2))$. But $g \circ f = \mathrm{id}_A$, so $\mathrm{id}_A(a_1) = \mathrm{id}_A(a_2)$ and hence $a_1 = a_2$. Therefore f is injective and, as it is also surjective, it is bijective. □

Remark 1.19 (Uniqueness of inverse)**.** The inverse of a bijective function $f : A \to B$ is unique. To see this, let $g : B \to A$ and $h : B \to A$ be inverses of f. Then, for any $b \in B$, $f(g(b)) = b = f(h(b))$. But f is injective, so $g(b) = h(b)$. Thus h and g are the same function, so the inverse of f is unique.

The inverse of a bijective function f is written $f^{-1} : B \to A$.

Corollary 1.20. *The inverse f^{-1} of a bijective function f is bijective.*

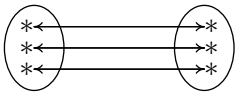
Proof. Since f is an inverse for f^{-1}, it follows that f^{-1} has an inverse, so is bijective by Theorem 1.18. □

Corollary 1.21. *Let $f : A \to B$ and $g : B \to C$ be bijective functions. Then gf is bijective and $(gf)^{-1} = f^{-1}g^{-1}$.*

1.7 Countability

Pairing

A bijective function between two sets pairs off the elements of the two sets.



It follows that if A is a finite set and there is a bijective function $f : A \to B$ then A and B have the same number of elements.

We will generalize this idea to sets which may be infinite, and think of two sets A and B as having the same size if and only if there is exists a bijective function $f : A \to B$; in other words, A and B have the same size if and only if the elements of A can be paired with the elements of B.

Example 1.22. Recall that $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$. The set of even positive integers is $2\mathbb{N} = \{2, 4, 6, 8, 10, \ldots\}$. This appears to be smaller than $\mathbb{N}$ because we have left out infinitely many elements $1, 3, 5, 7, 9, \ldots$. However we can pair off elements of $\mathbb{N}$ with those of $2\mathbb{N}$:

$$\begin{array}{cccccccccccc} \mathbb{N}: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots \\ 2\mathbb{N}: & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & \ldots \end{array}$$

Thus these two infinite sets should be thought of as having the same size, as discussed above. The pairing-off is done by the bijective function $f : \mathbb{N} \to 2\mathbb{N}$, with $f(n) = 2n$ for all $n \in \mathbb{N}$.

Countability

Definition 1.23. A set A is *countable* if there is a bijection $f : \mathbb{N} \to A$.

That is, the countable sets are the ones which are the same size as the natural numbers.

If A is countable, with $f : \mathbb{N} \to A$ a bijective function, then by surjectivity, $f(1), f(2), \ldots, f(n), \ldots$ is a list of all the elements of A and, by injectivity, the list has no repetitions. Writing $a_i = f(i)$ for $i \in \mathbb{N}$, it follows that $A = \{a_1, a_2, \ldots, a_n, \ldots\}$, where the elements a_i are all distinct.

Conversely, if the set A can be expressed in the form $\{a_1, a_2, \ldots, a_n, \ldots\}$, where the elements a_i are all distinct, then A is countable because there is a bijective function $f : \mathbb{N} \to A$ given by the rule $f(n) = a_n$ for all $n \in \mathbb{N}$.

$$\begin{array}{cccccccccccc} \mathbb{N}: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots \\ A: & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & \ldots \end{array}$$

Demonstrating countability. To show that a set A is countable, there are two options:

1. construct an explicit bijective function $f : \mathbb{N} \to A$ (such as the bijection $\mathbb{N} \to 2\mathbb{N}$ given by $f(n) = 2n$), or
2. write A in the form $\{a_1, a_2, \ldots, a_n, \ldots\}$, where the elements a_i are all distinct, making it clear why every element of A will occur somewhere in the list.

The second method is acceptable, and often easier!

Example 1.24. Consider $\mathbb{Z}$, which we might be tempted to think is larger than $\mathbb{N}$. In fact, we can show $\mathbb{Z}$ is countable.

Of course, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, but this doesn't demonstrate countability as the list is open-ended at both ends. Instead, write

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\},$$

which demonstrates countability by the second method above.

(Alternatively, a bijection $f : \mathbb{N} \to \mathbb{Z}$ is given by the rule

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even,} \\ \frac{1-n}{2} & \text{if } n \text{ is odd.)} \end{cases}$$

Example 1.25. Now consider the set $\mathbb{Q}$ of all rational numbers (fractions) which, at first sight, appears much larger than $\mathbb{N}$. The elements of $\mathbb{Q}$ can be presented in an infinite array, with numbers with denominator j on the jth row:

To obtain a listing of $\mathbb{Q}$ in the form $\{q_1, q_2, q_3, \ldots\}$, follow the indicated path, deleting repetitions (such as $\frac{2}{2} = \frac{1}{1}$ and $\frac{2}{4} = \frac{1}{2}$). Thus

$$\mathbb{Q} = \{ \qquad\qquad\qquad\qquad \},$$

demonstrating that it is a countable set.

You may now be thinking that all infinite sets are countable, in which case there would be little point in defining countability. The idea that some infinite sets could be larger than others is recent (in terms of the history of mathematics) and originates in the work of Georg Cantor (1845-1918).

Theorem 1.26 (Cantor)**.** $\mathbb{R}$ *is not countable.*

Proof. Suppose $\mathbb{R} = \{a_1, a_2, a_3, a_4, a_5, \ldots\}$ is countable. We shall show, for a contradiction, that there is a real number r not in our list. This is done in terms of the decimal expansions of the elements a_i.

□

This proof is known as Cantor's diagonal argument, for obvious reasons. It's easy to understand, but very non-trivial!

2 Permutations

Notice that a bijective function from a non-empty set X to itself rearranges or *permutes* the elements of X.

Definitions 2.1. A bijective function $f : X \to X$ is called a *permutation* of X. The set of all permutations of X will be denoted by S_X.

An element of S_X is a bijective function from X to itself.

We will mainly be in the set of permutations of $X = \{1, 2, \ldots, n\}$, and will write S_n rather than S_X in this case.

From here on, when discussing S_n, we will assume $n \geq 2$.

Permutation notation

To specify a permutation $\alpha \in S_n$ (that is, a shuffling of the numbers $1, \ldots, n$), we write $1, 2, \ldots n$ in a row and below each i we write $\alpha(i)$. For example, the permutation in S_5 which reverses the order of $1, 2, 3, 4, 5$ is

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

The identity function on $\{1, 2, \ldots, n\}$ is a permutation in S_n:

$$\mathrm{id}(= \mathrm{id}_n = \mathrm{id}_{S_n}) = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Theorem 2.2. *Let $n \in \mathbb{N}$. The number of permutations in S_n is $n!$.*

Proof. Each of the numbers from 1 to n must appear exactly once in the bottom row representing a permutation α.

□

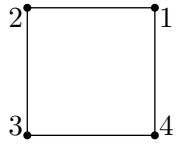
Example 2.3. The 6 elements of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Permutations arising from symmetries

Example 2.4. Consider the two ways of labelling a square below.



1	2	3
4	5	6
7	8	9

Each symmetry of the square will perform a permutation of the vertices (left) or the 9 numbered squares (right).

For example, r_1 performs the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ on the vertices and the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix}$ on the nine squares.

We will return to this later.

Group properties of S_X

The set S_X of all permutations of the non-empty set X satisfies the same four group properties as did D_4 and O_2 (see Section 1.5).

- *Closure* holds by Corollary 1.21. That is, $\alpha\beta \in S_X$ for all $\alpha, \beta \in S_X$ since the composition of two bijections is again a bijection.
- *Associativity* holds by Proposition 1.8. That is, $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ for all $\alpha, \beta, \gamma \in S_X$ by the associative law for composition of functions.
- id_X is a *neutral element* in S_X.
- Each $\alpha \in S_X$ has *inverse* $\alpha^{-1} \in S_X$ by Theorem 1.18 and Corollary 1.20.

Example 2.5. In S_4, let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$.

Similarly

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

Note that $\beta\alpha \neq \alpha\beta$. In other words, α and β do not commute.

Can you find elements of S_4 that do commute?

Definitions 2.6 (Powers)**.** For $\alpha \in S_X$, we write $\alpha\alpha$ (that is, α done twice) as α^2, $\alpha\alpha\alpha$ as α^3, etc. α^{-2} means $(\alpha^{-1})^2$, which, by Corollary 1.21, is equal to $(\alpha^2)^{-1}$. Similarly, $\alpha^{-3} = (\alpha^{-1})^3$, and so on.

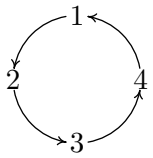
What would you expect α^0 to be?

With α as in Example 2.5, $\alpha^2 = \begin{pmatrix} & \\ & \end{pmatrix}$ and $\alpha^{-1} = \begin{pmatrix} & \\ & \end{pmatrix}$.

Finding inverses is easy: turn upside-down then reorder!

2.1 Cycles and decompositions

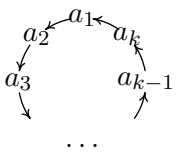
The permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ is an example of a 4-*cycle*.



Definition 2.7. Let n be a positive integer. Let $a_1, a_2, \ldots a_k$ be k *distinct* elements of $\{1, 2, \ldots, n\}$. The permutation $\alpha \in S_n$ such that

$$\alpha(a_1) = a_2,\ \alpha(a_2) = a_3,\ \ \ldots\ ,\ \alpha(a_{k-1}) = a_k \text{ and } \alpha(a_k) = a_1,$$

and $\alpha(a) = a$ if a is not in the list $a_1, \ldots, a_k$, is called a *cycle of length* k, or a k-*cycle*. It is written $(a_1\ a_2\ \ldots\ a_{k-1}\ a_k)$.



For example, $(1\ 6\ 3\ 4) = \begin{pmatrix} & & & & & \\ & & & & & \end{pmatrix}$ is a 4-cycle in S_6.

As 2 and 5 do not appear, they are sent to themselves.

Remarks 2.8.

1. In general, a k-cycle can be written in k different ways, each with the same *cyclic order*; for example,

$$(1\ 6\ 3\ 4) = (6\ 3\ 4\ 1) = (3\ 4\ 1\ 6) = (4\ 1\ 6\ 3).$$

2. Let $\alpha = (a_1\ a_2\ \ldots\ a_k)$ be a k-cycle. We can think of α as moving each a_i one place anticlockwise round the circle (see the diagram above). Similarly, α^2 moves each a_i two places round the circle, and so on.

In particular, k is the least positive integer with $\alpha^k = \mathrm{id}$.

Also α^{-1} moves each a_i one place clockwise round the circle; thus

$$\alpha^{-1} = \alpha^{k-1} = (a_k \ldots a_2\ a_1).$$

3. A cycle of length 1, e.g. (3), is the identity permutation in disguise.

Counting cycles

Example 2.9. How many 5-cycles $(a\ b\ c\ d\ e)$ are there in S_5?

> Of course, each 5-cycle can be expressed in 5 different ways (see Remark 2.8(i)) so the number of 5-cycles is actually $120/5 = 24$.

Similarly the number of 4-cycles in S_5 is $(5 \times 4 \times 3 \times 2)/4 = 30$, the number of 3-cycles in S_5 is $(5 \times 4 \times 3)/3 = 20$, and the number of 2-cycles in S_5 is $(5 \times 4)/2 = 10$. The only 1-cycle in S_5 is id.

The remaining 35 elements of S_5 are not cycles. They include, for example, (1 2 3)(4 5) and (1 2)(3 4).

Cycle decomposition

Definition 2.10. A set of cycles is called *disjoint* if no number appears in more than one of them. A *cycle decomposition* of a permutation α is an expression of α as a product of disjoint cycles.

For example, in Example 2.4, the permutation

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix}$$

of the 9 squares given by the rotation r_1 has cycle decomposition

This gives a much better feel for the effect of the permutation than the two row notation.

Algorithm 2.11. There is a simple algorithm to find a cycle decomposition for any permutation. For example, let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 1 & 12 & 6 & 5 & 2 & 10 & 7 & 8 & 11 & 9 & 3 \end{pmatrix}.$$

Starting with 1 (the smallest number), we see that α sends $1 \mapsto 4$. Then α sends $4 \mapsto 6$ and $6 \mapsto 2$. But then α sends 2 back to 1, which completes a cycle (1 4 6 2).

Next, find the smallest number not already appearing (in this case 3), and do the same thing to get the 2-cycle (3 12). Continuing in this way, we get

$$\alpha = (1\ 4\ 6\ 2)(3\ 12)(5)(7\ 10\ 11\ 9\ 8).$$

See [1, pp22,23] for a fuller description.

Example 2.12. Find a cycle decomposition of $\alpha = (2\ 4)(1\ 2\ 3)(4\ 5)(1\ 2)(3\ 4\ 5)$.

If you think we're already done, re-read the definition of disjoint!

In working out where α sends 1, we apply the five cycles in turn, beginning with the one on the right hand end, because

compositions of functions are applied right to left.

Transpositions

Definition 2.13. A cycle $(i\ j)$ of length 2 is called a *transposition*. Note that $(i\ j) = (j\ i)$ and $(i\ j)^2 = \mathrm{id}$. An *adjacent* transposition is one of the form $(i\ i+1)$, e.g. $(4\ 5)$.

A transposition swaps, or transposes, two numbers.

Algorithm 2.14. Any cycle can be expressed as a product of transpositions using either of the following formulas.

$$(a_1\ a_2\ a_3\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k) \quad (4)$$

$$(a_1\ a_2\ a_3\ \ldots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\ldots(a_1\ a_2) \quad (5)$$

See [1, pp24,25] for more discussion of these formulas.

Using these and Algorithm 2.11, we can write any permutation $\alpha \in S_n$ as a product of transpositions. For the example in 2.11, using formula 4,

$$\begin{aligned} \alpha &= (1\ 4\ 6\ 2)(3\ 12)(5)(7\ 10\ 11\ 9\ 8) \\ &= \end{aligned}$$

or, using formula 5, $\alpha = (1\ 2)(1\ 6)(1\ 4)(3\ 12)(7\ 8)(7\ 9)(7\ 11)(7\ 10)$.

Uniqueness of cycle decompositions

Note 2.15. The cycle decomposition $\alpha_1\alpha_2\ldots\alpha_s$ of a permutation α is unique except that

1. disjoint cycles commute, so the order of the cycles can be changed e.g. to $\alpha_2\alpha_1\ldots\alpha_s$;
2. each cycle can be written in different ways, each with the same cyclic order;
3. cycles of length 1 can be deleted from the product.

For example, with α as in 2.11, both of the cycle decompositions

$$(1\ 4\ 6\ 2)(3\ 12)(5)(7\ 10\ 11\ 9\ 8) \text{ and } (12\ 3)(11\ 9\ 8\ 7\ 10)(6\ 2\ 1\ 4)$$

are valid, and essentially the same. However,

there is no uniqueness in the expression for a permutation as a product of transpositions.

We've already seen this in Algorithm 2.14, with two different such expressions for the same permutation. Also, one sole transposition can be rewritten as a product of more than one transposition; for example

$$(1\ 4) = (3\ 4)(2\ 3)(1\ 2)(2\ 3)(3\ 4), \quad \text{or} \quad (2\ 4) = (1\ 2)(1\ 4)(1\ 2).$$

These are examples of general formulas: if $j > i$ then

$$(i\ j) = (j-1\ j)\dots(i+1\ i+2)(i\ i+1)(i+1\ i+2)\dots(j-1\ j) \tag{6}$$

and, if $b, c \neq 1$ then

$$(b\ c) = (1\ b)(1\ c)(1\ b). \tag{7}$$

Formula (6) *looks nasty, but is easy! It's just the general version of identities like* $(3\ 6) = (5\ 6)(4\ 5)(3\ 4)(4\ 5)(5\ 6)$.

In both formulas, the number of factors on the right hand side is odd; this will be important later. (For more on formula (6), see [1, p25].)

2.2 Parity

In mathematics, *parity* is a word used to discuss oddness and evenness.

Definition 2.16. A permutation α in S_n is said to be *even* (respectively *odd*) if it can be written as a product of an even (respectively odd) number of transpositions.

For the example in Algorithm 2.14, α is even, being a product of 8 transpositions.

Remarks 2.17.

1. Every permutation in S_n can be written as a product of transpositions, by Algorithm 2.14, so must be even or odd.
2. The identity permutation is even (because, for example, $\mathrm{id} = (1\ 2)(1\ 2)$).
3. Any transposition is odd (because it's the product of just *one* transposition).

4. The formula (4) shows that cycles of even length are odd and cycles of odd length are even.

5. We shall show in Section 5 that no permutation can be both even and odd. In the meantime we shall assume this result.

Parity-based arguments turn out to be useful in lots of places.

The 15-puzzle

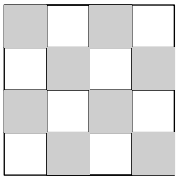
Suppose we're given the configuration on the left. Can we rearrange to get the configuration on the right?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

$\longmapsto$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Let's imagine the squares of the underlying 4×4 grid coloured alternately light and dark:



1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

$\longmapsto$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Each move is a transposition in S_{16}, and the outcome needed corresponds to the permutation (14 15), which is odd.

Now, each move changes the shade of the blank square. If the puzzle is possible, the blank square begins dark and ends up dark. Thus there would

have to be an even number of moves, so (14 15) would have to be even; a contradiction! Therefore the puzzle is impossible.

Parity of products

If α is a product of k transpositions and β is a product of l transpositions then $\alpha\beta$ is a product of $k + l$ transpositions.

Hence the rules for combining even and odd permutations by composition are the same as for combining even and odd integers by addition. They are summarized in the table

	even	odd
even	even	odd
odd	odd	even

.

Definition 2.18. The *sign* of a permutation α, written $\text{sgn}(\alpha)$, is defined to be $+1$ if α is even and -1 if α is odd.

> For example, if $\alpha = (1\ 4)(4\ 6)(6\ 2)(3\ 12)(7\ 10)(10\ 11)(11\ 9)(9\ 8)$, then α is even and $\text{sgn}(\alpha) = 1$.

Discussing signs instead of parity is useful, as the rules in the earlier table can be summarized by

$$\text{sgn}\,(\alpha\beta) = \text{sgn}\ \alpha\,\text{sgn}\ \beta. \tag{8}$$

Notes 2.19. 1. If we know the sign of α, then what is the sign of α^{-1}? Well, using (8), $\text{sgn}(\alpha)\,\text{sgn}(\alpha^{-1}) = \text{sgn}(\alpha\alpha^{-1}) = \text{sgn}\,\text{id} = 1$ and so

$$\text{sgn}(\alpha^{-1}) = \frac{1}{\text{sgn}\,\alpha} = \text{sgn}\,\alpha \quad (\text{as } \text{sgn}\,\alpha = \pm 1).$$

2. We shall see in Section 8 that half of the permutations in S_n are even and half are odd; that is, there are $n!/2$ of each.

   (For an alternative proof, see [1, p77, proof of Theorem 2], where $|A_n|$ denotes the number of even permutations in S_n.)

Look back at Example 2.3. What can you say about how the permutations are laid out, in terms of parity?

Example 2.20. In S_4, there are $4!/2 = 12$ elements of each parity.

The even elements are id, eight 3-cycles, and three products $(i\ j)(k\ l)$ of two disjoint transpositions.

The odd elements are six 4-cycles and six transpositions.

Orders of permutations

Definition 2.21. The *order* of a permutation $\alpha \in S_n$ is the least positive integer m such that $\alpha^m = \mathrm{id}$.

> In other words, the order is the minimum number of times α has to be performed for every element of $\{1, 2, \ldots, n\}$ to revert to itself.

We observed in 2.8(ii) that cycles of length k have order k.

Example 2.22. What is the order m of $\alpha = (1\ 2\ 3)(5\ 6)$?

As disjoint cycles commute, $\alpha^k = (1\ 2\ 3)^k(5\ 6)^k$ for all positive integers k.

Similarly $(1\ 2\ 3\ 4)(5\ 6)$ has order 4.

These examples illustrate a general rule for the order of a permutation α in terms of the lengths of the cycles in its cycle decomposition.

Proposition 2.23. *Let $\alpha \in S_n$. Then the order of α is the least common multiple of the lengths of the cycles appearing in the cycle decomposition for α.*

Proof. Consider any $1 \leq i \leq n$. If i appears in the cycle decomposition in a cycle of length k, then $\alpha^m(i) = i$ whenever m is a multiple of k. Hence $\alpha^m(i) = i$ for *every* $1 \leq i \leq n$ when m is a multiple of the length of each cycle. Thus, the order of α is the least such common multiple, as claimed. □

This applies nicely to our examples above!

3 Groups and subgroups

3.1 Key definitions

We now reach the key part of the module, where we introduce the notion of a *group*. In doing so we will make precise some of the notions we introduced in Section 1.

Definition 3.1. Let A be a non-empty set. A *binary operation* $\odot$ on A is a rule which, for each ordered pair (a, b) of elements of A, determines a unique element $a \odot b$ of A.

Equivalently, a binary operation is a function
$$\odot : A \times A \to A.$$

When $\odot$ is a binary operation on the set A we often say that A is *closed under* $\odot$; that is, $a \odot b \in A$ for all $a, b \in A$.

The word 'ordered' in the definition is important, because $a \odot b$ may not be the same as $b \odot a$.

The good news is, you already know of lots of examples.

Examples 3.2.

1. Addition, $+$, is a binary operation on each of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
2. Multiplication, $\times$, is a binary operation on each of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

3. Composition of functions, $\circ$, is a binary operation on the set S_X of permutations of the non-empty set X: see Section 2.

4. For each positive integer m, addition and multiplication modulo m are binary operations on the set $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

   Remember that addition and multiplication modulo m is easy! For example, in $\mathbb{Z}_{11}$, $\overline{7} + \overline{9} = \overline{5}$ and $\overline{4} \times \overline{8} = \overline{10}$.

5. Let $n \in \mathbb{N}$. Then matrix multiplication (see MAS111) is a binary operation on the set of all $n \times n$ real matrices.

We are now able to state the key definition of the course.

Definition 3.3. A non-empty set G is a *group* under $\odot$ (more formally, $(G, \odot)$ is a group) if the following four axioms hold.

G1 (*Closure*): $\odot$ is a binary operation on G. That is, $a \odot b \in G$ for all $a, b \in G$.

G2 (*Associativity*): $(a \odot b) \odot c = a \odot (b \odot c)$ for all $a, b, c \in G$.

G3 (*Neutral element*): There is an element $e \in G$ such that, for all $g \in G$,

$$e \odot g = g = g \odot e$$

Such an element is called a *neutral* or *identity* element for G.

G4 (*Inverses*): For each element $g \in G$ there is an element $h \in G$ such that

$$g \odot h = e = h \odot g.$$

Such an element h is called an *inverse* of g.

The above definition is so important to the rest of the course that it needs to be learnt, and understood, pretty much word-for-word!

Before we look at some examples, an important related property a group may have is the following.

Definition 3.4. A group G is said to be *abelian* if $a \odot b = b \odot a$ for every $a, b \in G$.[2]

That is, a group is abelian if the binary operation commutes.

What distinctive feature does an abelian group's Cayley table have?

3.2 Examples of groups

Groups of numbers under addition

Examples 3.5. The familiar sets $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ and $\mathbb{Z}$ are all abelian groups under addition. We demonstrate this for $\mathbb{Z}$; the other proofs are similar.

Proof that $(\mathbb{Z}, +)$ *is an abelian group.* We check the group axioms hold.

□

Note. $\mathbb{N} = \{1, 2, 3, \ldots\}$ is not a group under $+$ since it has no neutral element: if $e \in \mathbb{N}$ is such that $a + e = a = e + a$ for all $a \in \mathbb{N}$ then $e = 0 \notin \mathbb{N}$. Also, $\mathbb{N}$ has no inverses under addition.

[2]The concept was named after Niels Henrik Abel (1802-1829), one of the founders of group theory. And there's no typing error: he died young of tuberculosis.

So whilst most sets of numbers do work as groups under addition, we must be careful as there are cases which don't.

Groups of numbers under multiplication

Examples 3.6. The sets $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{Z}$ are *not* groups under multiplication. The axioms G1, G2 and G3 all hold, but G4 fails as 0 has no inverse.

However, $\mathbb{C}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ and $\mathbb{Q}\backslash\{0\}$ are all abelian groups under multiplication. Sketching the proof, for G1 we use the fact that $xy \neq 0$ whenever $x \neq 0$ and $y \neq 0$; G2 holds for all numbers under multiplication; for G3 the neutral element is 1; for G4 the inverse of x is $\frac{1}{x}$.

> **Note.** The set of non-zero integers, $\mathbb{Z}\backslash\{0\}$, is not a group under $\times$ since G4 fails: 2 is not invertible (as $\frac{1}{2} \notin \mathbb{Z}\backslash\{0\}$). Notice, however, that two elements of $\mathbb{Z}\backslash\{0\}$ do have inverses: 1 and -1.

But here's a trick! The set $\{1, -1\}$ (that is, those elements of $\mathbb{Z}$ which do have inverses) *is* a group under multiplication.

Groups of functions under composition

Examples 3.7. The following are groups of functions under composition, with the appropriate identity function as the neutral element.

You should be able to write down convincing proofs of all of these, referencing the group axioms.

1. The dihedral group D_4 of symmetries of the square (see Section 1.5). Note that D_4 is not abelian because, for example, $r_1 s_1 \neq s_1 r_1$.
2. The orthogonal group $O_2 = \{\mathrm{rot}_\phi : \phi \in \mathbb{R}\} \cup \{\mathrm{ref}_\phi : \phi \in \mathbb{R}\}$ of symmetries of a circle (Section 1.5). Again, O_2 is not abelian because, for example, $\mathrm{rot}_{\frac{\pi}{2}}\,\mathrm{ref}_0 \neq \mathrm{ref}_0\,\mathrm{rot}_{\frac{\pi}{2}}$.

3. For any non-empty set X, the set S_X of all permutations of X (see Section 2). In particular, for any positive integer n, the set S_n of all permutations of $\{1, 2, \ldots, n\}$, is a group, called the *nth symmetric group*.

   Note that S_n is not abelian if $n > 2$ because $(1\ 2)(1\ 3) = (1\ 3\ 2)$ and $(1\ 3)(1\ 2) = (1\ 2\ 3)$, which are different. However, S_2, which just consists of the elements id and $(1\ 2)$, *is* abelian.

Groups under modular arithmetic

Examples 3.8. With care, we can use modular arithmetic to form groups.

1. For each positive integer m, $\mathbb{Z}_m$ is an abelian group under addition modulo m. Axioms G1 and G2 are easy. For G3 and G4, the neutral element is $\overline{0}$ and the inverse of $\overline{a}$ is $\overline{m-a}$.

   For example, in $\mathbb{Z}_6$ under addition, $\overline{4}$ has inverse $\overline{2}$ because $\overline{4} + \overline{2} = \overline{6} = \overline{0}$.

   The Cayley table for $(\mathbb{Z}_5, +)$ is below.

$(\mathbb{Z}_5, +)$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

2. For multiplication modulo m, axioms G1-G3 all hold ($\overline{1}$ is neutral) but $\overline{0}$ has no inverse, so $\mathbb{Z}_m$ is *not* a group under multiplication.

   Perhaps we can throw away $\overline{0}$*...*

3. The following tables display $\times$ modulo 5 on $\mathbb{Z}_5 \backslash \{\overline{0}\}$ and $\times$ modulo 6 on $\mathbb{Z}_6 \backslash \{\overline{0}\}$.

$\times$mod5	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\times$mod6	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

What can we deduce from this? Well, the one on the left looks like a group: certainly, $\overline{1}$ seems to be acting as a neutral element, and every row and column contains $\overline{1}$, so every element has an inverse. The one on the right is clearly *not* a group: $\overline{3}$ has no inverse, for example, and it is not closed ($\overline{0}$ appears within the grid).

The following proposition gives half of the story.

Proposition 3.9. *If p is prime then $\mathbb{Z}_p\backslash\{\overline{0}\}$ is an abelian group under multiplication modulo p.*

Proof. For G1, if a and b are not divisible by p (that is, non-zero mod p), then so is ab, so $\mathbb{Z}_p\backslash\{\overline{0}\}$ is closed under multiplication. For G2, multiplication of numbers is associative so, for $a, b, c \in \mathbb{Z}$,

$$\overline{a}\ (\overline{b}\ \overline{c}) = \overline{a}\ (\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}\ \overline{c} = (\overline{a}\ \overline{b})\ \overline{c}.$$

For G3, the neutral element is $\overline{1}$. For G4, inverses are given by Euclid's algorithm: if p is prime and $\overline{a} \in \mathbb{Z}_p\backslash\{\overline{0}\}$ then the highest common factor of a and p is 1, so $sa + tp = 1$ for some integers s, t (see Semester 1). Then $sa \equiv 1 \bmod p$ and $\overline{s}\ \overline{a} = \overline{1}$ in $\mathbb{Z}_p\backslash\{\overline{0}\}$. That is, $\overline{s}$ is an inverse for $\overline{a}$. □

Note. For small primes, inverses are better found by inspection or trial-and-error as an alternative to Euclid's Algorithm. In $\mathbb{Z}_5\backslash\{\overline{0}\}$, for example, $\overline{1}$ and $\overline{4}$ are their own inverses (each square to give $\overline{1}$) and $\overline{2}$ and $\overline{3}$ are inverses of each other (as $\overline{2} \times \overline{3} = \overline{1}$).

How do the inverses pair up in $\mathbb{Z}_7\backslash\{\overline{0}\}$?

Notice that, in $\mathbb{Z}_p\backslash\{\overline{0}\}$ under multiplication, the element $\overline{p-1}$ is always its own inverse because

$$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \bmod p,$$

so $\overline{p-1}^2 = \overline{1}$.

We saw that $\mathbb{Z}_6\backslash\{\overline{0}\}$ is not a group under multiplication, and similarly $\mathbb{Z}_m\backslash\{\overline{0}\}$ is not a group under multiplication whenever m is composite (not prime).

But here's another trick! The set $\{\overline{1}, \overline{5}\}$ (the elements that do have inverses in $\mathbb{Z}_6\backslash\{\overline{0}\}$) is a group under multiplication mod 6. There is a similar group under multiplication modulo m for any m, formed by taking the elements $\overline{a}$ where a is coprime to m; for example $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ is a group under multiplication modulo 8.

Groups of matrices

Examples 3.10. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix with real entries. Recall that its *determinant*, $\det A$, is the number $ad - bc$. Also A is invertible if and only if $\det A \neq 0$, and when that's the case its inverse is given by

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

The invertible 2×2 matrices with real entries form a group under matrix multiplication, called the *general linear group* $GL_2(\mathbb{R})$ (see [1, p32] for the proof).[3] The neutral element is the identity matrix I_2.

Groups of matrices over general fields

In the above example, $\mathbb{R}$ can be replaced by any *field*, that is a non-empty set F with two binary operations $+$ and $\times$ such that

- F is an Abelian group under $+$ (with neutral element 0);

[3] In fact, for any $n \geq 2$, the invertible $n \times n$ matrices with real entries form a group under multiplication, denoted $GL_n(\mathbb{R})$. However, in this course we shall only look at the case where $n = 2$.

- $F\backslash\{0\}$ is an Abelian group under $\times$ (with neutral element 1);
- $a(b+c) = ab + ac$ for all $a, b, c \in F$ (the *distributive* law).

Important examples of fields are $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ and the finite fields $\mathbb{Z}_p$, where p is prime.

Note 3.11 (Inverses and determinants)**.** For 2×2 matrices with entries in F, determinants and inverses are calculated as before. For example, the matrix

$$B = \begin{pmatrix} \overline{4} & \overline{3} \\ \overline{1} & \overline{3} \end{pmatrix}$$

over $\mathbb{Z}_7$ has determinant $\det B = \overline{4}\,\overline{3} - \overline{3}\,\overline{1} = \overline{12} - \overline{3} = \overline{9} = \overline{2} \in \mathbb{Z}_7$. Similarly, a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

over F is invertible if and only if $\det A \neq 0$, with inverse given by

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Example 3.12. For the matrix $B = \begin{pmatrix} \overline{4} & \overline{3} \\ \overline{1} & \overline{3} \end{pmatrix}$ over $\mathbb{Z}_7$ above,

$$B^{-1} =$$

If you're confused here, remember we're working in $\mathbb{Z}_7$, so $\overline{2}^{-1} = \overline{4}$ since $\overline{2}\,\overline{4} = \overline{1}$. Also, negative entries get 'wrapped around' since we are working modulo 7.

Definition 3.13. For any field F, the invertible 2×2 matrices over F form the *general linear group* $GL_2(F)$.

For example, the matrix $\begin{pmatrix} \overline{4} & \overline{3} \\ \overline{1} & \overline{3} \end{pmatrix}$ over $\mathbb{Z}_7$ is in $GL_2(\mathbb{Z}_7)$ and $\begin{pmatrix} i & 1 \\ 1+i & -i \end{pmatrix}$ is in $GL_2(\mathbb{C})$.

3.3 Developing group theory

First steps

We now do our first steps in abstract group theory. The plan is to see what the axioms entail without looking at any group in particular. In this way, the results will apply to *all* groups.

Definition 3.14. The *order* of a group G, written $|G|$, is the number of elements in G. This is either infinite or a positive integer.

> For example, $|D_4| = 8$, $|S_n| = n!$ and $|GL_2(\mathbb{R})| = |O_2| = \infty$.
> For $m \in \mathbb{N}$, $|\mathbb{Z}_m| = m$ and, if p is prime, $|\mathbb{Z}_p \backslash \{\overline{0}\}| = p - 1$.

Note 3.15. As we've seen, we often write ab instead of $a \odot b$ (particularly when the binary operation is multiplication or composition). However, when the binary operation is addition we include the $+$ sign and say that the group is in *additive notation.*

Note 3.16 (Consequences of the axioms)**.** Throughout, G denotes a group.

(i) Uniqueness of neutral element. Suppose that G has two neutral elements e and f. Then $ef = e$ since f is neutral, and $ef = f$ since e is neutral. Thus $f = e$ and so the neutral element of G is unique.

> The neutral element is sometimes written e_G to emphasise which group is involved. In additive notation, it is written as 0.

(ii) Uniqueness of inverses. Suppose that $g \in G$ has two inverses h and k. Then $h = he = h(gk) = (hg)k = ek = k$. Thus the inverse of g is unique.

> The inverse of g is denoted by g^{-1}. However, in additive notation we write $-g$ for obvious reasons.

(iii) Cancellation laws. Let $g, h, k \in G$ and suppose that $gh = gk$. Then $g^{-1}(gh) = g^{-1}(gk)$, so $h = k$. That is,

$$gh = gk \Rightarrow h = k.$$

In other words, in groups one can cancel on the left. Similarly,

$$hg = kg \Rightarrow h = k,$$

which is cancellation on the right.

There is no general law which says
$gh = kg \Rightarrow h = k$**, so be careful!**

(iv) Latin square property. If G is finite it has a Cayley table, as we have seen for D_4 in Section 1.5. In this Cayley table, any element $g \in G$ appears precisely once in each row and each column. This property is the *Latin square property*, observed earlier for D_4.

To see that this holds, let h be any element of G. The element g will appear in the row for h whenever we can find an element $x \in G$ such that $hx = g$. But this equation has precisely one solution, namely $x = h^{-1}g$ (by multiplying on the left by h^{-1}). Thus g appears in the row for h precisely once, namely in the column for $h^{-1}g$ (see the table below).

A similar argument shows that g appears in the column for h for precisely once, namely in the row for gh^{-1}.

Latin square property for a finite group G

G	h	$h^{-1}g$
h		g
gh^{-1}	g	

(v) Omission of brackets. The associative law allows us to write abc or longer expressions like $ab^{-1}cdab$ without ambiguity. In additive notation we can write $a + b + c$ without brackets.

(vi) Inverses of products. Let $g, h \in G$. Then $(gh)^{-1} = h^{-1}g^{-1}$. The proof is identical to the corresponding result for bijective functions (Corollary 1.21), namely checking that $(gh)h^{-1}g^{-1} = e = h^{-1}g^{-1}(gh)$.

This law generalizes, using induction, to

$$(g_1 g_2 \dots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \dots g_1^{-1}.$$

(vii) Powers. Let $g \in G$. Then $gg \in G$ and is written g^2. For an arbitrary positive integer n we define

$$g^n = \underbrace{gg \dots g}_{n \text{ times}}, \quad g^0 = e \quad \text{and} \quad g^{-n} = (g^{-1})^n.$$

With these definitions, for any integers $m, n \in \mathbb{Z}$ we have the familiar laws for indices:

$$g^m g^n = g^{m+n} \quad \text{and} \quad (g^m)^n = g^{mn}.$$

In additive notation, for $n \geq 1$, we instead define

$$ng = \underbrace{g + g + \dots + g}_{n \text{ times}}, \quad 0g = 0 \quad \text{and} \quad (-n)g = n(-g).$$

3.4 Subgroups and the subgroup criterion

Definition 3.17. Let G be a group. A subset H of G is a *subgroup* of G if H is a group using the same binary operation as G.

> For example, D_4 (the group of symmetries of a square) is a subgroup of O_2 (the group of symmetries of the circle). Also, $(\mathbb{R}\backslash\{0\}, \times)$ is a subgroup of $(\mathbb{C}\backslash\{0\}, \times)$. We'll see plenty more examples.

In any group G, the singleton subset $\{e\}$ is a subgroup known as the *trivial subgroup*; any other subgroup is called *non-trivial*.

Any group G is a subgroup of itself; any other subgroup is called a *proper subgroup*.

Lemma 3.18. *Let G be a group, and let H be a subgroup of G. Then $e_H = e_G$; that is, H inherits its neutral element from G.*

Proof.

□

Theorem 3.19 (The Subgroup Criterion)**.** *Let G be a group and H be a subset of G. Then H is a subgroup of G if and only if the following three conditions hold.*

SG1: $H \neq \emptyset$.

SG2: $gh \in H$ *for all* $g, h \in H$.

SG3: $h^{-1} \in H$ *for all* $h \in H$.

For a group in additive notation, SG2 and SG3 become

SG2*:* $a + b \in H$ *for all* $a, b \in H$ *and* ***SG3****:* $-a \in H$ *for all* $a \in H$.

Proof. ($\Leftarrow$) Suppose that H is a subset of G satisfying SG1-3. We show that H is a group, and hence a subgroup of G, by verifying the group axioms.

($\Rightarrow$) Conversely, suppose that H is a subgroup of G. In particular, axioms G1-4 hold for H. We show that SG1, SG2 and SG3 hold.

This finishes the proof. □

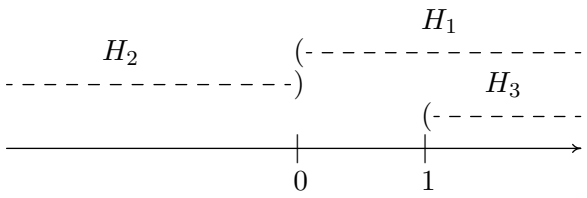
3.5 Subgroup examples

We're about to use the subgroup criterion to uncover lots of examples of subgroups. Look out for the following as we go along.

- To prove that a subset is a subgroup involves verifying SG1, SG2 and SG3 carefully.
- To prove that a subset is *not* a subgroup requires a clear counter-example to one of SG1, SG2 or SG3.
- SG1 (that is, non-emptiness) is often demonstrated using the identity element.
- It's good practice to have a concluding sentence.

Examples 3.20. Consider the following subsets of $\mathbb{R}\backslash\{0\}$, considered as a group under multiplication.

- $H_1 := \{x \in \mathbb{R} : x > 0\}$ (the set of positive real numbers);
- $H_2 := \{x \in \mathbb{R} : x < 0\}$ (the set of negative real numbers);
- $H_3 := \{x \in \mathbb{R} : x > 1\}$.



It's easy to see H_1 satisfies SG1, 2 and 3, so is a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$.

Why not write down a justification (i.e. proof) of this?

As $-1 \in H_2$ but $1 = (-1)(-1) \notin H_2$, SG2 fails for H_2, so H_2 is not a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$.

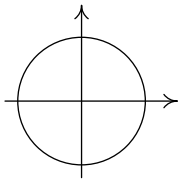
H_3 satisfies SG1 and SG2 but SG3 fails: $2 \in H_3$ but $2^{-1} \notin H_3$. Thus H_3 is not a subgroup of $(\mathbb{R}\backslash\{0\}, \times)$.

Example 3.21 (Alternating group)**.** For $n \geq 2$, let $G = S_n$ and let A_n be the set of all the even permutations in S_n. Thus, for $\alpha \in S_n$, we have $\alpha \in A_n \iff \operatorname{sgn} \alpha = 1$.

Thus A_n is a subgroup of S_n. It is called the *alternating group*. By earlier comments, $|A_n| = n!/2$.

The set of odd permutations *do not* form a subgroup of S_n, as SG2 fails: $(1\ 2)$ is odd but $(1\ 2)(1\ 2) = \mathrm{id}$ is even.

Example 3.22 (Special orthogonal group)**.** In O_2, let $H = \{\mathrm{rot}_\phi : \phi \in \mathbb{R}\}$ (the set of all rotations of the circle).



SG1: SG1 holds because $\mathrm{rot}_0 \in H$, so $H \neq \emptyset$.

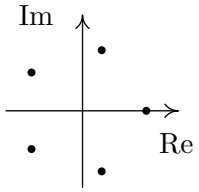
SG2: Let $\mathrm{rot}_\alpha, \mathrm{rot}_\beta \in H$. Then $\mathrm{rot}_\alpha \mathrm{rot}_\beta = \mathrm{rot}_{\alpha+\beta} \in H$, so SG2 holds.

SG3: If $\mathrm{rot}_\alpha \in H$ then $(\mathrm{rot}_\alpha)^{-1} = \mathrm{rot}_{-\alpha} \in H$, so SG3 holds.

Thus H is a subgroup of O_2. It is denoted by SO_2 and is called the *special orthogonal group.*

The set of reflections $\{\mathrm{ref}_\phi : \phi \in \mathbb{R}\}$ of the circle is not a subgroup of O_2 as it fails SG2: $\mathrm{ref}_0 \mathrm{ref}_0 = \mathrm{rot}_0$, for example.

Example 3.23 (Roots of unity)**.** Fix a positive integer n and, in $\mathbb{C}\backslash\{0\}$ under multiplication, let $U_n = \{z \in \mathbb{C} : z^n = 1\}$, the set of all complex nth roots of unity.



Thus, by the subgroup criterion, U_n is a subgroup of $(\mathbb{C}\backslash\{0\}, \times)$. It is called the *group of nth roots of unity.*

$$U_1 = \{1\},\ U_2 = \{1, -1\},\ U_3 = \{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\},$$

$$U_4 = \{1, i, -1, -i\}, \ldots, U_n = \{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}\}, \ldots.$$

What's the order of U_n? (If you can't answer, you probably need to recap the definition of 'order').

The next example involves a group with addition as the binary operation, so uses the *additive* version of the subgroup criterion.

Example 3.24. Fix a positive integer n and, in $\mathbb{Z}$ under addition, let $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\}$. For example, $5\mathbb{Z} = \{\ldots, -15,\ -10,\ -5,\ 0,\ 5,\ 10,\ 15, \ldots\}$.

SG1: SG1 holds because $0 \in n\mathbb{Z}$, so $n\mathbb{Z} \neq \emptyset$.

SG2: For SG2 let $a, b \in n\mathbb{Z}$. Thus $a = np$ and $b = nq$ for some integers p, q. Then $a + b = n(p + q) \in n\mathbb{Z}$.

SG3: If $a \in n\mathbb{Z}$, then $a = np$ for some $p \in \mathbb{Z}$, so $-a = n(-p) \in n\mathbb{Z}$.

By the additive version of the subgroup criterion, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Example 3.25 (The special linear group)**.** Let F be a field (such as $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ or $\mathbb{Z}_p$ for some prime number p). In the general linear group $GL_2(F)$, let

$$SL_2(F) = \{A \in GL_2(F) : \det A = 1\}$$

be the set of all invertible 2×2 matrices over F with determinant 1.

Thus $SL_2(F)$ is a subgroup of $GL_2(F)$. It is called the *special linear group over* F.

For example, $A = \begin{pmatrix} \overline{4} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix}$ and $B = \begin{pmatrix} \overline{3} & \overline{5} \\ \overline{1} & \overline{2} \end{pmatrix}$ are elements of $SL_2(\mathbb{Z}_7)$ as are the product $AB = \begin{pmatrix} \overline{5} & \overline{6} \\ \overline{2} & \overline{4} \end{pmatrix}$ and the inverses $A^{-1} = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{4} \end{pmatrix}$ and $B^{-1} = \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{6} & \overline{3} \end{pmatrix}$.

Why? Look at their determinants!

Example 3.26 (S_{n-1} inside S_n)**.** Let $G = S_n$ (for $n \geq 2$) and let

$$H = \{\alpha \in S_n : \alpha(n) = n\}.$$

By the subgroup criterion, H is a subgroup of S_n. Notice that its elements fix n and permute $\{1, 2, \ldots, n-1\}$, so H acts like a copy of S_{n-1} inside S_n.

Groups of symmetries

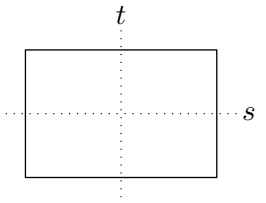
Here we deal with symmetries of shapes in $\mathbb{R}^2$.

Definition 3.27. Let A be a geometrical figure in $\mathbb{R}^2$ with centre at the origin and let f be a rotation or reflection in the orthogonal group O_2. The set $f(A) = \{f(a) : a \in A\}$ is called the *image* of A. If $f(A) = A$ then f is said to be a *symmetry* of A.

> The set of all symmetries of A is a subgroup of O_2 (why not prove this as an exercise?) and is called the *group of symmetries* of A.

We have already met the groups of symmetries of the circle (O_2 itself), the square (D_4) and, on the problem sheets, the equilateral triangle (D_3).

Example 3.28 (Klein's 4-group)**.** The group K of symmetries of a non-square rectangle has four elements $e = \mathrm{rot}_0$, $r = \mathrm{rot}_\pi$, $s = \mathrm{ref}_0$, and $t = \mathrm{ref}_\pi$. Each element is its own inverse and the group is abelian.



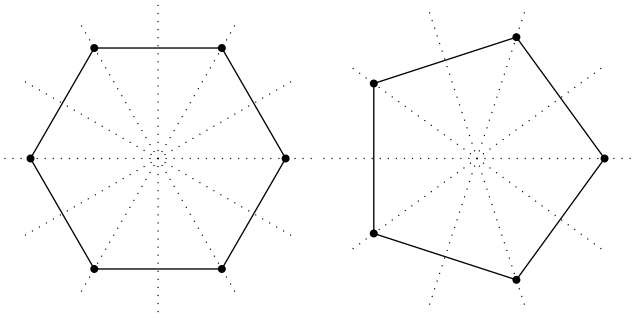
K	e	r	s	t
e	e	r	s	t
r	r	e	t	s
s	s	t	e	r
t	t	s	r	e

This group is called *Klein's 4-group.*

Surely the adjective 'non-square' is being pedantic, isn't it?

Example 3.29 (The dihedral groups)**.** The group of symmetries of a regular n-sided polygon (or n-gon) is called the *dihedral group* and is denoted D_n.

What are the symmetries of a regular n-gon? Some pictures, below, may help. You should find that D_n has order $2n$.



Example 3.30. In the group of symmetries of a geometrical figure A, consider the subset consisting of the rotations of A.

For example, for the square we get $\{e, \mathrm{rot}_{\frac{\pi}{2}}, \mathrm{rot}_{\pi}, \mathrm{rot}_{\frac{3\pi}{2}}\}$ and for the circle we get, of course, SO_2.

With the help of the following theorem, we show that the rotations of A always form a subgroup of the group of symmetries of A.

Theorem 3.31 (Intersections of subgroups)**.** *If H and K are subgroups of a group G then the intersection $H \cap K$ is a subgroup of G.*

Proof. As usual, we check SG1, SG2 and SG3 hold. As in the proof of the subgroup criterion, e_G is an element of both H and K,so $H \cap K \neq \emptyset$ and SG1 holds. Let $a, b \in H \cap K$. Both H and K satisfy the subgroup criterion so $ab \in H$, $a^{-1} \in H$, $ab \in K$ and $a^{-1} \in K$. Therefore $ab \in H \cap K$ and $a^{-1} \in H \cap K$. Thus $H \cap K$ satisfies SG2 and SG3. Hence, by the subgroup criterion, $H \cap K$ is a subgroup of G. □

Corollary 3.32 (Rotation groups)**.** *Let A be a geometrical figure in $\mathbb{R}^2$ with centre at the origin. Then the set of rotations of A forms a group under composition.*

Proof. Let $G = O_2$, $K = SO_2$ (the group of all rotations) and H be the group of symmetries of a figure A. Then H and K — and hence $H \cap K$ — are subgroups of O_2, with $H \cap K$ consisting of all rotations which are symmetries of A. Thus the set of rotations of A forms a group under composition. □

The group of rotations of A is called the *rotation group* of A.

3.6 Products and isomorphisms

Direct products

Definition 3.33. Let G and H be groups. The *cartesian product* $G \times H$ consists of all ordered pairs (g, h), where $g \in G$ and $h \in H$.

We define a binary operation on $G \times H$ componentwise, by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \quad \text{for all } g_1, g_2 \in G \text{ and } h_1, h_2 \in H.$$

For example, in $D_4 \times D_4$, $(s_1, r_2)(s_2, r_1) = (r_3, r_3)$.

> With this binary operation, $G \times H$ is a group called the *direct product* of G and H. The group axioms are checked in [1, p46] (or check them yourself!). The neutral element is (e_G, e_H) and the inverse of (g, h) is (g^{-1}, h^{-1}).

When G and H are in additive notation, the binary operation in $G \times H$ is given by $(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$ for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

As an example, if G and H are just the real number, $\mathbb{R}$, under addition, then $G \times H$ is $\mathbb{R}^2$ under componentwise addition. So, for example, $(2, 4) + (1, 1) = (3, 5)$.

Note 3.34 (Orders of direct products)**.** If either G or H is infinite then $|G \times H| = \infty$ and if both are finite then $|G \times H| = |G||H|$, there being $|G|$ choices for the first component and, for each of these, $|H|$ choices for the second.

Hopefully you've realised that direct products are easy.
That is, suppose you had to guess how things work: you'd probably have got it right!

Isomorphism

The groups D_3 and S_3 are in some sense "the same". That is, if we label the elements of D_3 in the usual way, and we label the elements of S_3 by

$$\text{id},\ \rho_1 = (1\ 2\ 3),\ \rho_2 = (1\ 3\ 2),\ \sigma_1 = (1\ 2),\ \sigma_2 = (1\ 3) \text{ and } \sigma_3 = (2\ 3)$$

then the Cayley tables have exactly the same structure.

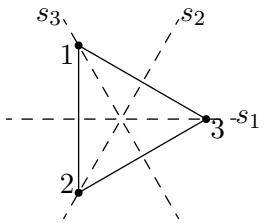
$\mathbf{D_3}$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_2	s_3	s_1
r_2	r_2	e	r_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r_2	r_1
s_2	s_2	s_1	s_3	r_1	e	r_2
s_3	s_3	s_2	s_1	r_2	r_1	e

$\mathbf{S_3}$	id	ρ_1	ρ_2	σ_1	σ_2	σ_3
id	id	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_1	ρ_1	ρ_2	id	σ_2	σ_3	σ_1
ρ_2	ρ_2	id	ρ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	id	ρ_2	ρ_1
σ_2	σ_2	σ_1	σ_3	ρ_1	id	ρ_2
σ_3	σ_3	σ_2	σ_1	ρ_2	ρ_1	id

We will shortly see that these two groups are *isomorphic*, which will be a precise way of expressing such a situation.

Was this just a coincidence?

Consider the labelled triangle below.



Each symmetry $g \in D_3$ permutes the vertices of the equilateral triangle. Let $f(g) \in S_3$ be the corresponding permutation of the vertices of the triangle.

In this way,

$$f(e) = \mathrm{id}, f(r_1) = \rho_1, f(r_2) = \rho_2,$$
$$f(s_1) = \sigma_1,\ f(s_2) = \sigma_2,\ f(s_3) = \sigma_3.$$

Then f is a bijective function $D_3 \to S_3$ and the Cayley table for S_3 is obtained from that of D_3 by applying f throughout. This property can be summarised by the statement $f(xy) = f(x)f(y)$ for all $x, y \in D_3$.

D_3	y
x	xy

S_3	$f(y)$
$f(x)$	$f(xy)$ $= f(x)f(y)$

Definitions 3.35. With the above in mind, we make the following definitions.

- Let G and H be groups and $f : G \to H$ be a function. Then f is said to be a *homomorphism* if $f(xy) = f(x)f(y)$ for all $x, y \in G$.
- A homomorphism which is bijective is called an *isomorphism*.
- We say that two groups G and H are *isomorphic* and write $G \cong H$ if there is an isomorphism $f : G \to H$.

For example, $D_3 \cong S_3$, because the function $f : D_3 \to S_3$ specified above is a bijective homomorphism, i.e. an isomorphism.

Example 3.36. For D_4 and S_4, the situation is different. There is a homomorphism $f : D_4 \to S_4$ where, for each $g \in D_4$, $f(g)$ is the permutation of the vertices corresponding to g.

Here f is injective but not surjective.

Not surprising, really! As $|D_4| = 8$ and $|S_4| = 24$, a function $D_4 \to S_4$ can never be surjective.

Although D_4 is not isomorphic to S_4 it is isomorphic to a subgroup of S_4, namely the range or image, $f(D_4)$, consisting of the permutations hit by f:

$$\begin{aligned} f(D_4) &= \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), \\ &\quad (1\ 4)(2\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)\}. \end{aligned}$$

Examples 3.37. The group $\mathbb{Z}_4$ under addition, the rotation group of the square, the group U_4 of 4th roots of unity and the group $\mathbb{Z}_5\backslash\{\overline{0}\}$ under multiplication are all isomorphic, as can be seen from their Cayley tables:

+mod4	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

	e	r_1	r_2	r_3
e	e	r_1	r_2	r_3
r_1	r_1	r_2	r_3	e
r_2	r_2	r_3	e	r_1
r_3	r_3	e	r_1	r_2

U_4	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

×mod5	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$

.

It would be easy to write down isomorphisms between any two of these groups (like in the example above). But instead we'll wait until after the next chapter.

4 Cyclic Groups

Consider three of the groups from Example 3.37: the rotation group $\{e, r_1, r_2, r_3\}$ of the square, the group $U_4 = \{1, i, -1, -i\}$ of 4th roots of unity and the group $\mathbb{Z}_5\backslash\{\overline{0}\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ under multiplication modulo 5.

- In each case there is an element g such that $g^4 = e$ and the four elements of the group are $e,\ g,\ g^2$ and g^3.

  (For the rotation group of the square, we take $g = r_1$; in U_4, we take $g = i$; in $\mathbb{Z}_5\backslash\{\overline{0}\}$, we take $g = \overline{2}$.)

- Other powers repeat these four elements in a cyclic pattern. Going forwards,

  $$g^4 = e, g^5 = g, g^6 = g^2, g^7 = g^3, \ldots$$

  and backwards,

  $$g^{-1} = g^3 \text{ (because } gg^3 = e = g^3g), g^{-2} = g^2, g^{-3} = g$$

  and so on.

The fourth group in Example 3.37, $\mathbb{Z}_4$, was in additive notation and the elements are all *multiples* of $\overline{1}$.

These four groups are examples of *cyclic groups*.

Definitions 4.1. Let G be a group and $g \in G$.

- We let $\langle g \rangle$ denote the set $\{g^n : n \in \mathbb{Z}\}$ of all powers of g. It is easy to see (with the subgroup criterion) that $\langle g \rangle$ is a subgroup of G called the *cyclic subgroup generated by* g.
- A group G is said to be *cyclic* if $G = \langle g \rangle$ for some $g \in G$; that is, if G consists of the powers of one of its elements g.

Have you understood this? It's not hard, so keep looking at it until you have!

Note 4.2. If H is a subgroup of G containing g then, by SG2 and SG3, H contains all powers of g, and so $\langle g \rangle \subseteq H$. In this sense, $\langle g \rangle$ is the smallest subgroup of G containing g.

4.1 Examples of cyclic groups

Example 4.3. In $\mathbb{R}\backslash\{0\}$ under multiplication,

$$\langle 2\rangle = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\} \text{ and } \langle -1\rangle = \{1, -1\}.$$

Example 4.4. From above, the group U_4 is cyclic, generated by i. In general, the group U_n of nth roots of unity is cyclic, generated by $e^{\frac{2\pi i}{n}}$. That is, $U_n = \{1,\ \omega,\ \omega^2, \ldots,\ \omega^{n-1}\}$ where $\omega = e^{\frac{2\pi i}{n}}$.

Example 4.5. From above, the rotation group of the square is cyclic, generated by $\mathrm{rot}\frac{\pi}{2}$. In general, the rotation group of the regular n-gon is cyclic, generated by $\mathrm{rot}\frac{2\pi}{n}$.

Example 4.6. From above, the group $\mathbb{Z}_5\backslash\{\overline{0}\}$ is cyclic, generated by $\overline{2}$. In general, when p is prime, the group $\mathbb{Z}_p\backslash\{\overline{0}\}$ is cyclic but the proof of this is beyond the scope of this module and $\overline{2}$ is not always a generator.

> For example, consider $\mathbb{Z}_7\backslash\{\overline{0}\}$. Here $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{1}$ and the powers of $\overline{2}$ then repeat. Thus $\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}\}$, so $\overline{2}$ does not generate $\mathbb{Z}_7\backslash\{\overline{0}\}$. However, $\langle\overline{3}\rangle = \{\overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}, \overline{1}\} = \mathbb{Z}_7\backslash\{\overline{0}\}$, and so $\mathbb{Z}_7\backslash\{\overline{0}\}$ is cyclic, generated by $\overline{3}$.

Notice that, for a group in additive notation, $\langle g\rangle$ consists of all *multiples* of g; that is, $\langle g\rangle = \{ng : n \in \mathbb{Z}\}$.

Example 4.7. In $\mathbb{Z}$ under addition, let $m \in \mathbb{Z}$ and consider the subgroup

$$\langle m\rangle = \{nm : n \in \mathbb{Z}\} = \{\ldots, -2m, -m,\ 0,\ m,\ 2m, \ldots\}.$$

This is the same subgroup that we called $m\mathbb{Z}$ in Example 3.24. In particular $\langle 1\rangle = \{\ldots, -2, -1,\ 0,\ 1,\ 2, \ldots\} = \mathbb{Z}$, so $(\mathbb{Z}, +)$ is cyclic with generator 1.

Example 4.8. From the earlier discussion, $\mathbb{Z}_4$ under addition is cyclic, generated by $\overline{1}$. Of course, this works more generally: for any m, $\mathbb{Z}_m$ under addition is cyclic, generated by $\overline{1}$. That is, every element $\overline{j}$ has the form $\overline{1} + \ldots + \overline{1}$ (j terms).

4.2 Orders of elements

Earlier we saw the definition of the order of a group. We use the same word to denote a different concept, but one which, we will find, is related.

Definition 4.9. For an element g of a group G, we define the *order* of g to be the least positive integer n such that $g^n = e$, if such an integer exists, and to be infinite if no such integer exists.

Examples 4.10.

1. In $\mathbb{R}\backslash\{0\}$ under multiplication, 2 has order ∞ (since there is no positive integer n with $2^n = 1$) and -1 has order 2.
2. In $\mathbb{C}\backslash\{0\}$ under multiplication, i has order 4 and $e^{\frac{2\pi i}{n}}$ has order n.
3. In the orthogonal group O_2, $\mathrm{rot}\,\frac{2\pi}{n}$ has order n, and every reflection has order 2.
4. The order of any permutation α is the least common multiple of the lengths of the cycles in the cycle decomposition of α: see Proposition 2.23. For example, (1 2 3 4 5) has order 5 and (1 2)(3 4 5 6) has order 4.
5. From the calculations in 4.6, $\overline{2}$ has order 4 in $\mathbb{Z}_5\backslash\{\overline{0}\}$ whereas, in $\mathbb{Z}_7\backslash\{\overline{0}\}$, $\overline{2}$ has order 3 and $\overline{3}$ has order 6.

Theorem 4.11. *Let G be a group and let $g \in G$ have finite order n. Let $m \in \mathbb{Z}$. Then*

1. *$g^m = g^r$, where r is the remainder on division of m by n;*
2. *$g^m = e$ if and only if m is a multiple of n;*
3. *the order of $\langle g \rangle$ is the same as the order of g.*

Remark 4.12. Part (iii) says the two versions of the word *order*, namely the order of the element g and the order of the subgroup $\langle g \rangle$, coincide.

Proof.

□

Examples 4.13. We can now work out large powers in groups.

1. Because i has order 4 in $\mathbb{C}\backslash\{0\}$, $i^{6011} = i^{6008+3} = i^3 = -i$.
2. Because $\overline{3}$ has order 6 in $\mathbb{Z}_7\backslash\{\overline{0}\}$, $\overline{3}^{6011} = \overline{3}^5 = \overline{5}$.
3. Today is ..... and 3^{6011} days from now it will be .....

If a group element g has infinite order, the elements of $\langle g\rangle$ are

$$\ldots,\ g^{-3},\ g^{-2},\ g^{-1},\ e,\ g,\ g^2,\ g^3, \ldots.$$

No two of these are equal, for if $g^i = g^j$ with $j > i$ then $g^{j-i} = e$, a contradiction to the fact that g has infinite order. Thus the order of the cyclic subgroup $\langle g\rangle$ is infinite and equal to the order of g in this case also.

> An example is given by the element 2 in $\mathbb{R}\backslash\{0\}$, where $\langle 2\rangle = \{\ldots \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \ldots\}$ is infinite.

In summary, whether finite or not,

the order of an element $g \in G$ is the same as the order of the subgroup $\langle g\rangle$.

4.3 More theory on cyclic groups

Proposition 4.14. *Let G be a finite group of order n. Then G is cyclic if and only if G has an element of order n.*

Proof. Suppose G has an element g of order n. Then, by Theorem 4.11(iii), the cyclic group $\langle g \rangle$ has n distinct elements, and so these must be all the elements of G. Thus $G = \langle g \rangle$ is cyclic.

Conversely if G has no element of order n then, for any $g \in G$, $|\langle g \rangle|$ is not equal to n, so $\langle g \rangle$ cannot be G. It follows that G is not cyclic. □

Another 'if and only if' proof with two arguments, as always!

Example 4.15. In Example 3.28, we looked at Klein's 4-group, the group of symmetries of a non-square rectangle, $K = \{e, r, s, t\}$, where $r = \mathrm{rot}_\pi$, $s = \mathrm{ref}_0$ and $t = \mathrm{ref}_\pi$.

Here r, s and t all have order 2 and e has order 1. No element has order 4, so K is not cyclic. Its cyclic subgroups are $\langle r \rangle = \{e, r\}$, $\langle s \rangle = \{e, s\}$, $\langle t \rangle = \{e, t\}$ and $\langle e \rangle = \{e\}$.

Theorem 4.16. *Every cyclic group G is abelian.*

Proof. Let $G = \langle g \rangle$ (where $g \in G$) and let $a, b \in G$. There exist $m, n \in \mathbb{Z}$ such that $a = g^m$ and $b = g^n$. Then

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba.$$

Thus $ab = ba$ for all $a, b \in G$ and so G is abelian. □

> For example, the dihedral group D_4, which is not abelian, cannot be cyclic. But, be careful! The converse to Theorem 4.16 is false; there are abelian groups which are not cyclic (Klein's 4-group is one example).

Example 4.17. Let g be a group element of order 12. What is the order of g^8?

Theorem 4.18. *Let g be a group element of finite order n, and let $m \in \mathbb{Z}$ be a positive integer. Then the order of g^m is $\frac{l}{m}$, where l is the l.c.m. of m and n. In particular, if m is a factor of n then the order of g^m is $\frac{n}{m}$.*

Proof. Let k be the order of g^m. Then k is the least positive integer such that $g^{mk} = e$. But, by Theorem 4.11(ii), mk must be a multiple of n. Hence mk must be the l.c.m. of m and n and so $k = \frac{l}{m}$. □

Remark 4.19. There is an alternative formula for the order of g^m above, namely $\frac{n}{h}$, where h is the h.c.f. of m and n. This is valid because it is always true that $mn = hl$.

4.4 Subgroups of cyclic groups

Theorem 4.20 (Subgroups of cyclic groups are cyclic)**.** *Let $G = \langle g \rangle$ be a cyclic group and let H be a subgroup of G. Then H is cyclic.*

Proof.

□

If this seems hard, then focus on the key idea in the proof:
any subgroup H of a cyclic group $G = \langle g \rangle$ is cyclic,
generated by the smallest positive power of g in H.

Example 4.21. Find all the subgroups of a cyclic group $G = \langle g \rangle$ of order 6 (such as U_6, $\mathbb{Z}_7 \backslash \{\overline{0}\}$ or the rotation group of a regular hexagon).

Solution.

So the *distinct* subgroups of G are $\langle g^1 \rangle = G$, of order 6, $\langle g^2 \rangle$, of order 3, $\langle g^3 \rangle$, of order 2 and $\langle g^6 \rangle = \{e\}$, of order 1. Note that 1, 2, 3, 6 are the positive factors of 6.

The above is an example of a general result: let $G = \langle g \rangle$ be cyclic group of order n and let $d_1, d_2, \ldots, d_k$ be a list of the positive divisors of n. Then $\langle g^{d_1} \rangle$, $\langle g^{d_2} \rangle$, $\ldots, \langle g^{d_k} \rangle$ are all the subgroups of G and these have orders $\frac{n}{d_1}$, $\frac{n}{d_2}, \ldots,$ $\frac{n}{d_k}$ respectively (which is a list of the positive divisors of n in reverse order). For more details, see [1].

4.5 Isomorphisms between cyclic groups

Let $G = \langle g \rangle$ and $H = \langle h \rangle$ be cyclic groups of the *same order* (that is, with the same number of elements or, equivalently, such that the elements g and h have the same order).

Then there is a bijection $f : G \to H$ given by the rule $f(g^i) = h^i$ for any integer i. (This is true whether the order of G and H is finite or infinite.)

Proposition 4.22. *With $G = \langle g \rangle$ and $H = \langle h \rangle$ as above, the function $f : G \to H$ given by $f(g^i) = h^i$ is an isomorphism of groups.*

Proof. We've already determined that f is bijective, so it remains to show that f is a homomorphism. For all $g^i, g^j \in G$,

$$f(g^i g^j) = f(g^{i+j}) = h^{i+j} = h^i h^j = f(g^i) f(g^j).$$

Thus f is a homomorphism, and hence an isomorphism. □

The key point to remember is

cyclic groups of the same order are isomorphic.

For example, the rotation group of the regular n-gon is isomorphic to the group U_n of nth roots of unity.

Now's a good time to look back at the end of Section 3!

5 Group Actions

At the beginning of Section 2 we saw how elements of D_4 permute the vertices of a square. Given $g \in D_4$ and a vertex x of the square, let $g * x$ denote the vertex to which g sends x. This is an example of a *group action*.

Definition 5.1. A group G *acts* on a non-empty set X if, for each $g \in G$ and each $x \in X$, there is an element $g * x \in X$ such that

GA1: $e * x = x$ for all $x \in X$,
GA2: $g * (h * x) = (gh) * x$ for all $g, h \in G$ and all $x \in X$.

Here the group G shuffles around the elements of the set X.

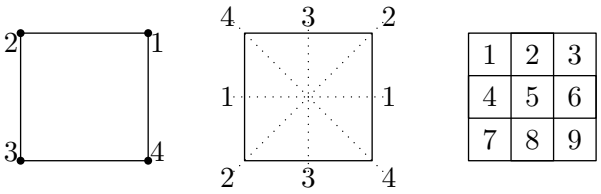
5.1 Examples of groups actions

Most of our examples will be of the following form. Suppose that G is a group of functions and X is a non-empty set with $f(x) \in X$ for all $f \in G$ and $x \in X$. Then G acts on X by the rule $f * x = f(x)$. To see this, we check GA1 and GA2.

GA1: $e_G * x = \mathrm{id} * x = \mathrm{id}(x) = x$ for all $x \in X$.

GA2: $g * (h * x) = g * (h(x)) = g(h(x)) = (gh)(x) = (gh) * x$
for all $g, h \in G$ and all $x \in X$.

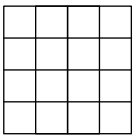
Examples 5.2. Consider the three labelled squares below.



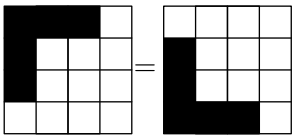
- The group D_4 of symmetries of the square acts on the four vertices of the square (left-hand picture). For example, $r_3 * 2 = 1$.

- The group D_4 also acts on the four axes of symmetry of the square, numbered above (middle picture). For example, $r_1 * 1 = 3$.
- Thirdly, D_4 acts on the nine squares in the right-hand picture above. For example $s_2 * 1 = 9$.

Example 5.3. The group D_4 also acts on the set X of all n^{16} ways of colouring the pattern



with n colours, e.g. r_1*



.

We'll use this idea later to count the number of essentially different colourings of grids.

Example 5.4. The group S_n acts on $\{1, 2, \ldots, n\}$ by the rule $\alpha * i = \alpha(i)$ for $1 \leq i \leq n$ and $\alpha \in S_n$. For example, $(1\ 5\ 6) * 1 = 5$.

Example 5.5. Another important action of S_n is on the set of polynomials in n variables $x_1, x_2, \ldots, x_n$ with real coefficients by the rule

$$\alpha * p(x_1, x_2, \ldots, x_n) = p(x_{\alpha(1)}, x_{\alpha(2)}, \ldots, x_{\alpha(n)})$$

for all $\alpha \in S_n$ and such polynomials p. For more detail, see [1, p74].

All that's happening is α shuffles the variables.

The alternating polynomial

Definition 5.6. For $n \geq 2$, the *alternating polynomial* a_n (in variables $x_1, \ldots, x_n$) is the product of all polynomials of the form $x_i - x_j$ with $i < j$.

For example,

$$\begin{aligned} a_4 = (x_1 - x_2) &\times (x_1 - x_3) \times (x_1 - x_4) \\ &\times (x_2 - x_3) \times (x_2 - x_4) \\ &\times (x_3 - x_4), \end{aligned}$$

and, in general,

$$\begin{aligned} a_n = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) &\ldots (x_1 - x_n) \\ (x_2 - x_3)(x_2 - x_4) &\ldots (x_2 - x_n) \\ &\ddots \ \vdots \\ &(x_{n-1} - x_n). \end{aligned}$$

Every permutation sends a_n either to a_n or $-a_n$ (see the proof of Theorem 5.7 below). For example,

$$\begin{aligned} (2\ 3) * a_4 = (x_1 - x_3) &(x_1 - x_2) (x_1 - x_4) \\ &(x_3 - x_2) (x_3 - x_4) \\ &(x_2 - x_4) = -a_4. \end{aligned}$$

Indeed, it's easy to see that if $\tau = (i\ i+1)$ is an adjacent transposition, then

$$\tau * a_n = -a_n \text{ and } \tau * (-a_n) = a_n.$$

The factor $x_i - x_{i+1}$ becomes $x_{i+1} - x_i$ and other factors are unchanged, though they appear in a different order.

Theorem 5.7. *No permutation in S_n can be both even and odd.*

Proof. As above, any adjacent transposition sends a_n to $-a_n$ and $-a_n$ to a_n. By formula (6) in Note 2.15, any transposition is a product of an odd number of adjacent transpositions and so must also send a_n to $-a_n$ and $-a_n$ to a_n. An even permutation is a product of an even number of transpositions and so it must send a_n to a_n whereas an odd permutation sends a_n to $-a_n$. Hence no permutation can be both even and odd. □

5.2 Orbits, stabilizers and related concepts

Given a group action, there are a number of important collections that we need names for.

Definitions 5.8. Let G be a group acting on a non-empty set X.

- For any $x \in X$, the *orbit* of x is the set

$$\mathrm{orb}(x) = \{y \in X : y = g * x \,\text{for some}\, g \in G\}.$$

  This consists of all elements of X that can be obtained from x by applying elements of G.

- The *stabilizer* of x is the set

$$\mathrm{stab}(x) = \{g \in G : g * x = x\}.$$

  This consists of those elements of G that stabilize x (send it to itself).

- For each $y \in \mathrm{orb}(x)$, the *sending set* $\mathrm{send}_x(y)$ is given by

$$\mathrm{send}_x(y) = \{g \in G : g * x = y\}.$$

  This consists of those elements of G that send x to y. Notice that $\mathrm{send}_x(x) = \mathrm{stab}(x)$.

- For each $g \in G$, the *fixed set* of g is the subset

$$\mathrm{fix}(g) = \{x \in X : g * x = x\}.$$

  This consists of those elements of X that are fixed by g.

Theorem 5.9. *Let G be a group acting on a non-empty set X and let $x \in X$. Then* $\mathrm{stab}(x)$ *is a subgroup of G.*

Proof. We use the subgroup criterion.

SG1:

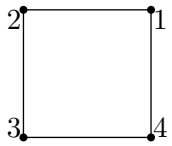
SG2:

SG3:

□

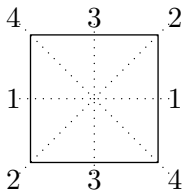
Examples of orbits, stabilizers, fixed and sending sets

Example 5.10. For the action of D_4 on the vertices (see Example 5.2),



These sending sets are examples of what we will call *left cosets* (in Section 7). They divide the group D_4 into non-overlapping subsets of the same size.

Example 5.11. For the action of D_4 on axes in Example 5.2,



The stabilizers are subgroups of D_4, both isomorphic to Klein's 4-group.

The sending sets for axis 1 again divide the group D_4 into non-overlapping subsets of the same size:

$$\text{send}_1(1) = \{e, r_2, s_1, s_3\} \text{ and } \text{send}_1(3) = \{r_1, r_3, s_2, s_4\}.$$

Of course, $\text{send}_1(2)$ and $\text{send}_1(4)$ are empty, as 2 and 4 don't lie in the orbit of 1.

Example 5.12. For the action of D_4 on the nine squares in Example 5.2, the orbits divide the set of 9 squares into non-overlapping subsets:

1	2	3
4	5	6
7	8	9

$$\text{orb}(1) = \{1, 7, 9, 3\}, \text{orb}(2) = \{2, 4, 8, 6\}, \text{orb}(5) = \{5\}.$$

The stabilizers of all except the center square are cyclic groups of order 2:

$$\text{stab}(1) = \{e, s_4\} = \text{stab}(9), \quad \text{stab}(2) = \{e, s_3\} = \text{stab}(8),$$

$$\text{stab}(3) = \{e, s_2\} = \text{stab}(7), \quad \text{stab}(4) = \{e, s_1\} = \text{stab}(6).$$

The odd one out is $\text{stab}(5) = D_4$. The fixed subsets are:

$$\text{fix}(e) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\text{fix}(r_1) = \text{fix}(r_2) = \text{fix}(r_3) = \{5\},$$

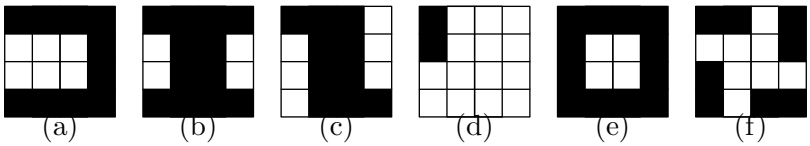
$$\text{fix}(s_1) = \{4, 5, 6\}, \quad \text{fix}(s_3) = \{2, 5, 8\},$$

$$\text{fix}(s_2) = \{3, 5, 7\}, \quad \text{fix}(s_4) = \{1, 5, 9\}.$$

It would be easy to have lost the thread slightly at this point. Are you happy with the above examples? If not, recap the definitions! The concepts aren't hard, and the names are well chosen.

Example 5.13. As in Example 5.3, consider D_4 acting on the set X of colourings of a 4×4 grid with 2 colours. For each of the shown colourings x, we work out

1. the number of elements, $|\operatorname{orb}(x)|$, in the orbit of x;
2. the stabilizer $\operatorname{stab}(x)$.



(a) (b) (c) (d) (e) (f)

The answers are:

(a) $|\operatorname{orb}(x)| = 4$, $\operatorname{stab}(x) = \{e, s_1\}$.
(b) $|\operatorname{orb}(x)| = 2$, $\operatorname{stab}(x) = \{e, r_2, s_1, s_3\}$.
(c) $|\operatorname{orb}(x)| = 4$, $\operatorname{stab}(x) = \{e, r_2\}$.
(d) $|\operatorname{orb}(x)| = 8$, $\operatorname{stab}(x) = \{e\}$.
(e) $|\operatorname{orb}(x)| = 1, \operatorname{stab}(x) = D_4$.
(f) $|\operatorname{orb}(x)| = 2$, $\operatorname{stab}(x) = \{e, r_1, r_2, r_3\}$.

The stabilizers give a rough measure of symmetry in the colouring.

Example 5.14. For the action of S_n on $\{1, 2, \ldots, n\}$ in Example 5.4, $\operatorname{orb}(i) = \{1, 2, \ldots, n\}$ for all i because for each i and j there exists a permutation α with $\alpha(i) = j$ (e.g. the transposition $(i\ j)$).

As in Example 3.26, the stabilizers are copies of S_{n-1}; in particular $\operatorname{stab}(n)$ is precisely the subgroup considered there.

Why? This should be clear with a bit of thought!

Example 5.15. For the alternating polynomial a_n, it follows from the proof of Theorem 5.7 that $\operatorname{orb}(a_n) = \{a_n, -a_n\}$ and that $\operatorname{stab}(a_n) = A_n$ (the subgroup of all even permutations from Example 3.21).

What does $\mathrm{send}_{a_n}(-a_n)$ *consists of?*

Example 5.16. In Example 5.5, we let S_3 act on polynomials in x_1, x_2 and x_3. There we had $p = x_1x_2 + x_3$.

5.3 The orbit-counting theorem

For the action of D_4 on coloured grids, if the pattern can be turned over (e.g. a glass tile) colourings in the same orbit for D_4 are essentially the same and the number of essentially different colourings is the number of orbits for the action.

This terminology matches up perfectly with Problem 1.1!

If the pattern cannot be turned over (e.g. a ceramic floor tile) the number of essentially different colourings is the number of orbits for the action of the rotation group of the square. In either case, the answer is given by the next theorem.

Theorem 5.17 (The orbit-counting theorem)**.** *Let G be a finite group acting on a non-empty finite set X and let n be the number of orbits. Then*

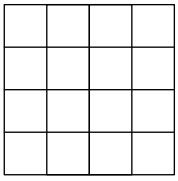
$$n = \frac{1}{|G|} \sum_{g \in G} |\operatorname{fix}(g)|.$$

This will be proved in Section 8. For now, we just check that it works for the action of D_4 on the 9 squares of Example 5.12. Using the fixed subsets listed there, the formula tells us that the number of orbits is

$$\frac{1}{|D_4|} \sum_{g \in D_4} |\operatorname{fix}(g)| = \frac{9+1+1+1+3+3+3+3}{8} = \frac{24}{8} = 3,$$

which is what we found earlier.

Example 5.18. In how many essentially different ways can the shown square glass tile, which can be turned over, be coloured (i) using n colours; (ii) so that there are 12 blue regions and 4 red regions?



Solution.

Remarks 5.19. Here are some comments about such calculations.

- *Sometimes a fixed set can be empty.* For example, if in (ii) above we had 3 red and 13 blue then $|\operatorname{fix}(g)| = 0$ for $g = r_1, r_2, r_3, s_1, s_3$ but $|\operatorname{fix}(s_2)| = |\operatorname{fix}(s_4)| = (4 \times 6) + 4 = 28$ ((any one of A-D and any one of E-J are red) or (three of A-D are red)) and the number of essentially different colourings is

$$\frac{1}{8}(\ {}_{16}C_3 + 28 + 28) = \frac{616}{8} = 77.$$

- *If the pattern cannot be turned over, we use the Orbit-Counting Theorem with G being the rotation group of the square,* $\{e, r_1, r_2, r_3\}$; then the answers are

  (i) $\frac{1}{4}(n^{16} + n^8 + 2n^4)$;

  (ii) $\frac{1}{4}(1820 + 4 + 4 + 28) = \frac{1856}{4} = 464$.

For other examples of colouring problems, see [1, pp124-127].

These colouring problems are easy to get the hang of, but make sure you lay your solutions out clearly!

6 Equivalence Relations

Definition 6.1. A *relation* R on a set A is a non-empty subset of the cartesian product[4] $A \times A$.

So a relation is just a collection of ordered pairs of elements of A.

Rather than specifying a subset R of $A \times A$, it is usual to give a rule for when $(a, b) \in R$. We write aRb rather than $(a, b) \in R$ and read this as 'a is related to b (under the relation R)'.

Often a symbol such as $\sim$ or $\bowtie$ is used in place of the letter R.

We clearly need some examples!

Examples 6.2. 1. Define a relation R on the real numbers $\mathbb{R}$ by specifying that, for real numbers a and b,

$$aRb \iff a \geq b.$$

(That is, a is related to b if and only if $a \geq b$.)

2. Define a relation R on the plane, $\mathbb{R}^2$, by specifying that, for points p and q in $\mathbb{R}^2$,

$$pRq \iff \begin{array}{l} p \text{ and } q \text{ are the same distance} \\ \text{from the origin } (0, 0). \end{array}$$

One of the most important relations is congruence modulo n, introduced in Semester 1. We will use the following, precise definition.

Definition 6.3. Let n be a positive integer. We define a relation called *congruence modulo n* on the set of integers, $\mathbb{Z}$, by specifying that, for integers a and b,

$$aRb \iff a - b \text{ is divisible by } n.$$

For this relation, aRb is written $a \equiv b \bmod n$. For example, $17 \equiv 2 \bmod 5$ and $-39 \equiv 3 \bmod 7$.

[4] Recall that $A \times A$ is the set of all ordered pairs (a, b) with $a \in A$ and $b \in A$.

6.1 Equivalence relations

Definitions 6.4. A relation R on a set A is said to be

- *reflexive* if aRa for all $a \in A$;
- *symmetric* if whenever $a, b \in A$ with aRb, then bRa;
- *transitive* if whenever $a, b, c \in A$ with aRb and bRc, then aRc.

A relation R is an *equivalence relation* if it is reflexive, symmetric and transitive.

Examples 6.5. In Example 6.2(i),

In Example 6.2(ii), R is reflexive, symmetric and transitive and hence is an equivalence relation.

Theorem 6.6. *Congruence modulo the positive integer n is an equivalence relation on $\mathbb{Z}$.*

Proof.

□

Equivalence classes

Definition 6.7. If R is an equivalence relation on a set A then, for each $a \in A$, the *equivalence class* of a is the set

$$\overline{a} = \{b \in A : bRa\}$$

of all elements of A related to a under R.

> For the relation on $\mathbb{R}^2$ in Example 6.2(ii), if $p \in \mathbb{R}^2$ then the equivalence class of p is the collection of all points the same distance from the origin as p; that is, the circle through p with centre $(0, 0)$.

What does this mean for the equivalence class of $(0, 0)$*?*

Example 6.8. When doing modular arithmetic we have been using the overline notation $\overline{a}$ to distinguish it from ordinary arithmetic. But this notation can also be used for equivalence classes for congruence modulo n. We will see later that these two ideas match up. For now, let's look equivalence classes for congruence modulo 5:

$$\begin{aligned}
\overline{0} &= \{b \in \mathbb{Z} : b - 0 \text{ is divisible by } 5\} &&= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},\\
\overline{1} &= \{b \in \mathbb{Z} : b - 1 \text{ is divisible by } 5\} &&= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},\\
\overline{2} &= \{b \in \mathbb{Z} : b - 2 \text{ is divisible by } 5\} &&= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},\\
\overline{3} &= \{b \in \mathbb{Z} : b - 3 \text{ is divisible by } 5\} &&= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},\\
\overline{4} &= \{b \in \mathbb{Z} : b - 4 \text{ is divisible by } 5\} &&= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

Other classes repeat these; for example, $\overline{5} = \overline{0}$, $\overline{6} = \overline{1}$, $\overline{7} = \overline{2}$,..., $\overline{-1} = \overline{4}$, ...

Theorem 6.9. *Let R be an equivalence relation on a set A and let $a, b \in A$. Then $\overline{a} = \overline{b}$ if and only if aRb.*

Proof. For the 'if' part, suppose that aRb. We must show that $\overline{a} = \overline{b}$. Let $c \in \overline{a}$. Then cRa and, by hypothesis, aRb so, by transitivity, cRb. Therefore $c \in \overline{b}$. This holds for any $c \in \overline{a}$, so $\overline{a} \subseteq \overline{b}$.

We need the reverse inclusion. But this follows easily as, by symmetry, we have bRa and we can use the same argument to get $\overline{b} \subseteq \overline{a}$. Hence $\overline{a} = \overline{b}$.

For the 'only if' part, suppose that $\overline{a} = \overline{b}$. Since R is reflexive, aRa and so $a \in \overline{a}$. As $\overline{a} = \overline{b}$, we must have $a \in \overline{b}$; that is, aRb. □

Another 'if and only if' proof: as always, two directions needed!

6.2 Partitions

Definition 6.10. A *partition* of a non-empty set A is given by a collection of non-empty subsets A_i of A such that

- $\bigcup_i A_i = A$, and
- $A_i \cap A_j = \emptyset$ whenever $A_i \neq A_j$.

(That is, each element of A belongs to at least one A_i and no element belongs to two different A_is.)

The name is appropriate: picture a set being split up into smaller collections by drawing boundaries, or partitions. The above definition is the formal, mathematical way of writing that down.

For example, the five displayed equivalence classes of $\equiv \bmod 5$ in Example 6.8 form a partition of $\mathbb{Z}$.

Theorem 6.11. *Let R be an equivalence relation on a set A.*

1. *The union of the equivalence classes for R is equal to A.*
2. *If $a, b \in A$ then either $\overline{a} = \overline{b}$ or $\overline{a} \cap \overline{b} = \emptyset$.*
3. *The equivalence classes for R form a partition of A.*

Proof.

Finally, 3 is immediate from 1 and 2. □

6.3 Modular arithmetic revisited

Let $n > 1$ be an integer. Following Example 6.8, we now have a more formal definition than before of the set $\mathbb{Z}_n$.

Definition 6.12. The set of all equivalence classes of congruence modulo n is denoted $\mathbb{Z}_n$.

We need to show this matches up with our previous understanding of $\mathbb{Z}_n$. Firstly, note that if $m \in \mathbb{Z}$ then $m \equiv r \bmod n$, where r is the remainder on division of m by n, so that $\overline{m} = \overline{r}$ for some $0 \leq r < n$ by Theorem 6.9. Hence

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

These n classes are distinct, because if $0 \leq i < j < n$ then $0 < j - i < n$ so that n cannot divide $j - i$. Hence $j \not\equiv i \bmod n$ and, by Theorem 6.9, $\overline{i} \neq \overline{j}$.

So $\mathbb{Z}_n$ has precisely n distinct elements and the notation agrees with that used for $\mathbb{Z}_n$ earlier in the module. For example,

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

where

$$\begin{aligned}
\overline{0} &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},\\
\overline{1} &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},\\
\overline{2} &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},\\
\overline{3} &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},\\
\overline{4} &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\},
\end{aligned}$$

(the 5 classes displayed in Example 6.8).

7 Cosets and Lagrange's Theorem

Definition 7.1. Let G be a group and H be a subgroup of G. Let g be an element of G. We call the set $gH = \{gh : h \in H\}$ a *left coset of* H in G.

Take everything in H and multiply on the left by g. Easy!

Example 7.2. Let $H = \{e, s_2\} = \langle s_2 \rangle$, the cyclic subgroup of $G = D_4$ generated by s_2. The left cosets of H in D_4 can be calculated using the Cayley table for D_4 in Section 1.5.

$$\begin{array}{rcccc}
eH & = & \{ee, es_2\} & = & \{e, s_2\}, \\
s_2H & = & \{s_2e, s_2s_2\} & = & \{s_2, e\} = eH, \\
r_1H & = & \{r_1e, r_1s_2\} & = & \{r_1, s_3\}, \\
s_3H & = & \{s_3e, s_3s_2\} & = & \{s_3, r_1\} = r_1H, \\
r_2H & = & \{r_2e, r_2s_2\} & = & \{r_2, s_4\}, \\
s_4H & = & \{s_4e, s_4s_2\} & = & \{s_4, r_2\} = r_2H, \\
r_3H & = & \{r_3e, r_3s_2\} & = & \{r_3, s_1\}, \\
s_1H & = & \{s_1e, s_1s_2\} & = & \{s_1, r_3\} = r_3H.
\end{array}$$

This example illustrates much of the general theory we will prove. Points to note are:

- H itself appears as the left coset eH.
- For all g, $g \in gH$ (because $g = ge$).
- Whenever $b \in aH$, the left cosets bH and aH are equal.(For example, $s_1 \in r_3H$ and $s_1H = r_3H$.)
- The distinct left cosets form a partition of the group G. That is, every element of G appears in precisely one of the distinct left-cosets.
- Each left coset contains 2 elements, the same number as H.
- $|G| = m|H|$, where $m = 4$ is the number of different left cosets of H in G.

In the above example, the distinct left cosets of H form a partition of the group G. We will see that this is always true because left cosets turn out to be equivalence classes of an equivalence relation.

Equivalence modulo H

Definition 7.3. Let G be a group, let H be a subgroup of G and let $a, b \in G$. We say that a *is equivalent to* b *modulo* H, and write $a \equiv b \bmod H$, if and only if $b^{-1}a \in H$.

> For a group in additive notation, the condition $b^{-1}a \in H$ becomes $a - b \in H$. Congruence modulo n is a special case, in additive notation, of equivalence mod H with $G = \mathbb{Z}$ and $H = n\mathbb{Z}$.

Theorem 7.4. *Let G be a group and let H be a subgroup of G. Then equivalence modulo H is an equivalence relation on G. Further, for any $a \in G$, the equivalence class $\overline{a}$ of a under equivalence mod H is the left coset aH.*

Proof. We need to show that equivalence modulo H is reflexive, symmetric and transitive. For reflexivity, let $a \in G$. Then $a^{-1}a = e \in H$ and so $a \equiv a \bmod H$.

For symmetry, let $a, b \in G$ be such that $a \equiv b \bmod H$. Then $b^{-1}a \in H$ so, by SG3, $a^{-1}b = (b^{-1}a)^{-1} \in H$, and hence $b \equiv a \bmod H$.

For transitivity, let $a, b, c \in G$ be such that $a \equiv b \bmod H$ and $b \equiv c \bmod H$. Then $b^{-1}a \in H$ and $c^{-1}b \in H$; therefore, by SG2, $c^{-1}a = c^{-1}bb^{-1}a \in H$ and hence $a \equiv c \bmod H$.

For the statement about equivalence classes, let $a \in G$ and take any $c \in G$. Then $c \in \overline{a} \iff c \equiv a \bmod H \iff a^{-1}c \in H \iff a^{-1}c = h$ for some $h \in H$ $\iff c = ah$ for some $h \in H \iff c \in aH$. Thus $\overline{a} = aH$. □

Corollary 7.5. *Let G and H be as above, and let $a, b \in G$. Then*

1. *$bH = aH$ if and only if $a^{-1}b \in H$;*
2. *if $b \in aH$ then $bH = aH$.*

Proof. (i) By Theorem 6.9, $\overline{b} = \overline{a}$ if and only if $b \equiv a \bmod H$. But $\overline{a} = aH$ and $\overline{b} = bH$. Hence $bH = aH$ if and only if $b \equiv a \bmod H$, that is, if and only if $a^{-1}b \in H$.

(ii) Let $b \in aH$. Then $b = ah$ for some $h \in H$. Thus $a^{-1}b = h \in H$ and so, using part (i), $bH = aH$. □

In Example 7.2, the four left cosets each had two elements, the same number as H itself. This is always true, as we now show.

Theorem 7.6. *Let G be a group with a subgroup H and let $g \in G$. Then $|gH| = |H|$; that is, the size of gH is the same as the size of H.*

Proof.

□

Above, f pairs up elements of H with elements of gH by muliplying on the left by g.

7.1 Lagrange's Theorem

We are now in a position to prove the first substantial result of group theory.

Theorem 7.7 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then the order of G is a multiple of the order of H. More precisely, $|G| = m|H|$ where m is the number of distinct left cosets of H in G.*

Proof. The left cosets of H in G, being the equivalence classes of an equivalence relation (Theorem 7.4), form a partition of G (Theorem 6.11) and so each element of G is in exactly one of them. Each equivalence class has $|H|$ elements (Theorem 7.6) and so $|G| = m|H|$. □

Lagrange's Theorem is widely applicable, and has many implications.

Theorem 7.8. *Let G be a finite group and let $a \in G$. Then*

1. *the order of G is a multiple of the order of a;*

2. $a^{|G|} = e$.

Proof. Note first that the order of a must be finite; if not, $\langle a \rangle$ would be an infinite subgroup of the finite group G, which is impossible. Let the order of a be m.

1. Then the cyclic subgroup $\langle a \rangle$ of G has order m by Theorem 4.11(iii) and, by Lagrange's Theorem, the order of G is a multiple of m.
2. By (i), m divides $|G|$, say $|G| = mq$ for some $q \in \mathbb{N}$. Then

$$a^{|G|} = a^{mq} = (a^m)^q = e^q = e. \qquad \square$$

Theorem 7.9. *Let p be a prime number and let G be a group of order p.*

1. The only subgroups of G are G and $\{e\}$.

2. G is cyclic.

Proof. (i) Let H be a subgroup of G. By Lagrange's Theorem, the order of H must be a factor of p. Since p is prime the only possibilities are $|H| = p$, in which case $H = G$, and $|H| = 1$, in which case $H = \{e\}$.

(ii) Let $g \in G$ with $g \neq e$. Let $H = \langle g \rangle$ be the cyclic subgroup generated by g. Since $g \neq e$ we know that $H \neq \{e\}$ and so, by (i), $H = G$. That is, $G = \langle g \rangle$ is cyclic. $\square$

Fermat's Little Theorem

We now give an alternative proof of Fermat's Little Theorem (Semester 1 of MAS114) which is important in number theory and cryptography and can be proved very quickly by applying ideas of order to the group $\mathbb{Z}_p \backslash \{\overline{0}\}$.

Theorem 7.10 (Fermat's Little Theorem)**.** *Let p be a prime number and let a be an integer. If p does not divide a then $a^{p-1} \equiv 1 \bmod p$.*

Proof.

$\square$

Remember that there's a corollary 'For any integer a, $a^p \equiv a \bmod p$' which was proved in Semester 1.

8 The Orbit-Stabilizer Theorem

In this final section, we prove two results about group actions. We work first towards a theorem linking orbits and stabilizers, and we'll finish with a proof of the orbit-counting theorem, which we stated and used earlier but weren't quite in a position to prove.

Orbits as equivalence classes

Let G be a group acting on a set X. Define a relation $\sim$ on X as follows: for $x, y \in X$,

$$x \sim y \iff x = g * y \text{ for some } g \in G.$$

For example, for the action of D_4 on the 9 squares in Example 5.2, $1 \sim 7$ and $2 \sim 4$ but $1 \not\sim 2$.

1	2	3
4	5	6
7	8	9

Proposition 8.1. *Let G be a group acting on a set X. Then the relation on X defined by*

$$x \sim y \iff x = g * y \text{ for some } g \in G$$

is an equivalence relation.

Proof.

□

Corollary 8.2. *Let G act on a set X, and consider the relation as defined above. If $a \in X$ then the equivalence class $\overline{a}$ is the same as the orbit* $\mathrm{orb}(a)$. *Hence the orbits of the group action form a partition of X.*

Proof. For $a \in X$, $\overline{a} = \{b \in X : b = g * a \,\text{for some}\, g \in G\} = \mathrm{orb}(a)$. The final remark follows since equivalence classes always partition a set. □

So the orbits for a group action partition a set.

For example, the action of D_4 on the 9 squares partitions $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ into three sets: $\{1, 3, 7, 9\}$, $\{2, 4, 6, 8\}$, $\{5\}$.

8.1 The orbit-stabilizer theorem

We are now within reach of the orbit-stabilizer theorem. First we will need a result about the sending sets $\mathrm{send}_x(y)$ for a group action.

Theorem 8.3. *Let G be a group acting on a non-empty set X. Let $x \in X$ and let $H = \mathrm{stab}(x)$. Take any $g \in G$ and put $y = g * x$. Then* $\mathrm{send}_x(y) = gH$.

That is, the elements of G which send x to $g * x$ coincide precisely with the left coset $g\,\mathrm{stab}(x)$. This sounds plausible, as elements of $g\,\mathrm{stab}(x)$ are of the form gh, where h sends x to itself, so will send x to $g * x$.

Proof. Let $k \in gH$. Then $k = gh$ for some $h \in \text{stab}(x)$. Using GA2, $k * x = (gh) * x = g * (h * x) = g * x = y$, (since $h * x = x$) and so k sends x to y; that is, $k \in \text{send}_x(y)$. Therefore $gH \subseteq \text{send}_x(y)$.

For the reverse inclusion, let $k \in \text{send}_x(y)$. Then $k * x = y = g * x$. We'll show that $g^{-1}k \in \text{stab}(x)$, from which the result will follow. Indeed, using GA2 and GA1,

$$g^{-1}k * x = g^{-1} * (k * x) = g^{-1} * (g * x) = (g^{-1}g) * x = e * x = x.$$

Hence $g^{-1}k \in \text{stab}(x)$ and so $k = g(g^{-1}k) \in g\,\text{stab}(x) = gH$. Thus $\text{send}_x(y) \subseteq gH$, and we have the reverse inclusion. □

Notice that this is another proof which shows that two sets are equal by showing each is included in the other.

The following is another substantial result of the course. We present a version for finite groups; for a corresponding statement for infinite groups, see [1].

Theorem 8.4 (The Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on a non-empty set X and let $x \in X$. Then*

$$|\,\text{orb}(x)| \times |\,\text{stab}(x)| = |G|.$$

Proof.

□

Examples of the orbit-stabilizer theorem

Example 8.5. Recall that S_3 acts on $\{1,2,3\}$ by the rule $\alpha * x = \alpha(x)$. For this action, $\mathrm{orb}(1) = \{1,2,3\}$ and $\mathrm{stab}(1) = \{\mathrm{id}, (2\ 3)\}$. In accordance with the orbit-stabilizer theorem,

$$|\operatorname{orb}(1)| \times |\operatorname{stab}(1)| = 2 \times 3 = 6 = |S_3|.$$

Example 8.6. With the action of D_4 on the vertices of the square (Example 5.10), $\mathrm{orb}(1) = \{1,2,3,4\}$ and $\mathrm{stab}(1) = \{e, s_2\}$. Again,

$$|\operatorname{orb}(1)| \times |\operatorname{stab}(1)| = 4 \times 2 = 8 = |D_4|,$$

as expected from the orbit-stabilizer theorem.

Examples 8.7. Many examples are given by the action of D_4 on colourings of a 4×4 square grid as in Example 5.13, where there are cases with

(d) $|\operatorname{orb}(x)| = 8$, $|\operatorname{stab}(x)| = 1$;
(a),(c) $|\operatorname{orb}(x)| = 4$, $|\operatorname{stab}(x)| = 2$;
(b),(f) $|\operatorname{orb}(x)| = 2$, $|\operatorname{stab}(x)| = 4$;
(e) $|\operatorname{orb}(x)| = 1$, $|\operatorname{stab}(x)| = 8$.

In all cases, $|\operatorname{orb}(x)| \times |\operatorname{stab}(x)| = 8 = |D_4|$.

Examples 8.8. For the action of S_n on the set of polynomials in n variables, the alternating polynomial a_n has $\mathrm{orb}(a_n) = \{a_n, -a_n\}$ and $\mathrm{stab}(a_n)$ is the alternating group A_n of all even permutations in S_n: see Example 5.15.

By the orbit-stabilizer theorem,

$$n! = |S_n| = |\operatorname{orb}(a_n)||\operatorname{stab}(a_n)| = 2 \times |A_n|.$$

Therefore, as claimed earlier,

$$|A_n| = n!/2.$$

Orbits and stabilizers for infinite groups

Notice that the function $f : \mathrm{orb}(x) \to \{g\,\mathrm{stab}(x) : g \in G\}$ in the proof of the orbit-stabilizer theorem given by $f(y) = \mathrm{send}_x(y)$ exists and is bijective even when G is not a finite group. The final example explores this idea for the infinite group O_2.

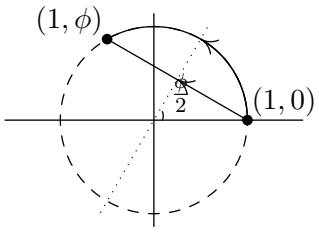
Example 8.9. The orthogonal group O_2 of symmetries of the circle acts on $\mathbb{R}^2$ by rotation and reflection. In polar coordinates,

$$\mathrm{rot}_\phi * (r, \theta) = (r, \phi + \theta), \quad \mathrm{ref}_\phi * (r, \theta) = (r, \phi - \theta)$$

for all $(r, \theta) \in \mathbb{R}^2$.

Consider the point $P = (1, 0)$. The orbit of P is the unit circle and $\mathrm{stab}(P) = \{e, \mathrm{ref}_0\}$. A typical element of $\mathrm{orb}(P)$ is, in polar coordinates, $(1, \phi)$. As both rot_ϕ and ref_ϕ send P to $(1, \phi)$, the bijection between $\mathrm{orb}(P)$ and $\{g\,\mathrm{stab}(P) : g \in G\}$ is given by

$$(1, \phi) \longleftrightarrow \{\mathrm{rot}_\phi, \mathrm{ref}_\phi\}.$$



Why not check that $\{\mathrm{rot}_\phi, \mathrm{ref}_\phi\}$ *is indeed the left coset* $\mathrm{rot}_\phi H$*, where* $H = \{e, \mathrm{ref}_0\}$*, by using the rot/ref formulae?*

8.2 Proving the Orbit-Counting Theorem

We can now prove the Orbit-Counting Theorem used in Section 5 to solve colouring problems.

Theorem 8.10 (The Orbit-Counting Theorem)**.** *Let G be a finite group acting on a non-empty finite set X and let n be the number of orbits. Then*

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

Proof. (In [1, pp119-120], the proof is illustrated by references to the action of D_4 on the 9 squares, our Examples 5.2 and 5.12.)

□

End of course! If you enjoyed this material then there is more group theory to be taken at Level 2. If you didn't, then there are plenty of other options...

Good luck with the exam!