4. Groups and Symmetry

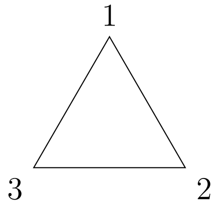
Most algebraic objects are mathematicians attempt to unify and generalise some type of object. Rings, which we will meet next, are the generalisation of a “number system” like $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ or $\mathcal{M}_n(\mathbb{R})$. Vector spaces generalise the idea of Euclidean vectors. Groups, the object of this chapter, are mathematicians’ attempt to formalise the idea of *symmetry*.

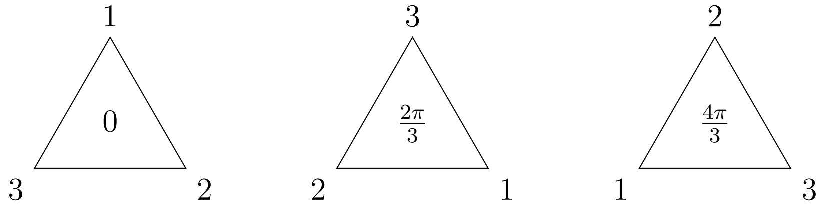
If you want to formalise something, say symmetry, you have two (realistically more) options:

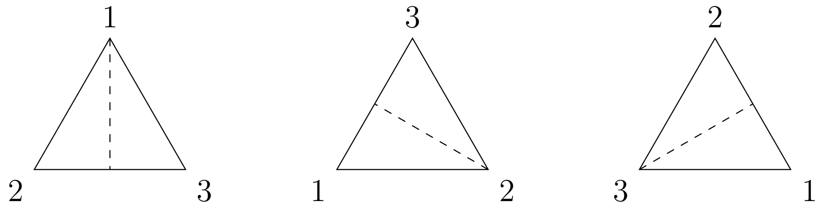
- *the physicist method:* collect all of the examples of symmetry you can find, and come up with a (complicated) framework for considering all of them;
- *the algebraic method:* define a new object called *a symmetry group*, which behaves like the things you intuitively define a symmetry to be. Then if a few things which you originally thought might be a symmetry turn out not to form a symmetry group, then maybe they weren’t the same type of symmetry to start with. This is the approach that we will be following.

§4.1. What is a group?

A group is the set of symmetries of an object. As we don’t quite know what that means, let’s consider some examples. To start with, let’s consider the symmetries of a triangle. Usually, we would think of a triangle as having 3 rotational symmetries (rotating by $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ and 2π) and three reflective symmetries (one through each diagonal). Let’s draw a diagram of each of these. Note that I have labelled the vertices, to make it easier to keep track of the changes.







The top row are our rotational symmetries, by 0, $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$ respectively. The bottom row are our reflections, with the lines of reflection marked. Importantly, notice that our rotation by 0 (or equivalently by 2π) appears to do nothing - it leaves the triangle unchanged. But it still is a symmetry. After applying each symmetry, some things are the same - for example, there is a still a line connecting vertices 1 and 2, 2 and 3, and 3 and 1, and the triangle formed is still equilateral. But some things are different - notably, the positions of each of the vertices. That can now give us some idea about what “a symmetry” is - it’s a transformation of an object that preserves some, but not all, of the structure of that object. If we wanted to preserve more structure (say, that the vertices had to be labelled clockwise), we would have fewer symmetries (here, only the rotations). If we wanted to preserve less structure (say, that all of the vertices has distinct labels), we would have a few more symmetries. But generally, our intuition can tell us which symmetries are helpful.

Let’s take another example - shuffling. You may have heard a mathematician describe a function like

$$f\left(x,y,z\right) = \frac{xy^2}{z} + \frac{x^2y}{z} + \frac{yz^2}{x} + \frac{y^2z}{x} + \frac{xz^2}{y} + \frac{x^2z}{y}$$

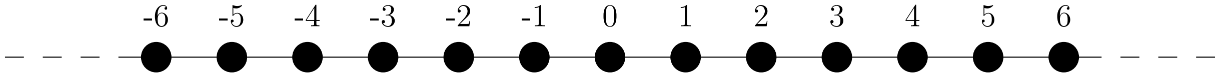
as a *symmetric* function, because

$$f(x,y,z) = f(x,z,y) = f(z,y,x) = f(y,x,z) = \cdots$$

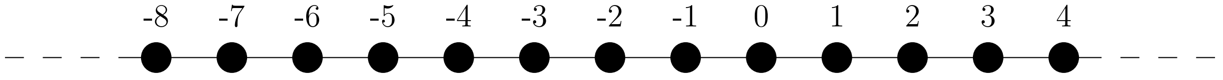
That is, the function is the same, regardless of which input is which, so the *structure* of the output is preserved under the *transformation* of shuffling the inputs. The symmetries of this function are then the same as the “symmetries” of shuffling 3 objects. It might be a little strange to think of shuffling as symmetric, but it does fit our general idea of a transformation that preserves some structure. In the spirit of generality, then, we will count it. Hence the symmetries of a deck of cards are the ways of shuffling 52 objects. Again, we count leaving the cards as they are (or any complicated shuffle that doesn’t end up changing the order of the cards) as being a valid shuffle.

Let’s take one last example, which might be a weirder one still. $\mathbb{Z}$ feels like it must be “translationally symmetric” in some way - that is, we can shift the number line to the left or right and it will look more or less the same. There will still be the integers, each spaced one unit apart, in ascending order going left-to-right. The only difference, just like in our triangles, is that which number each point is labelled with is different.

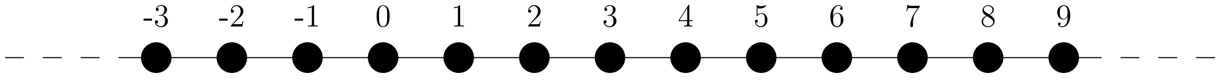
Consider this number line:



After shifting two to the right, we get

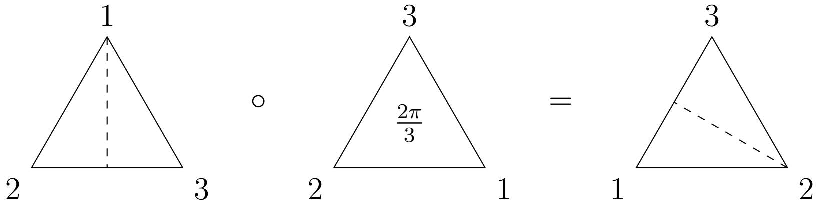


You can see that, by our slightly abstracted definition, this is definitely a symmetry. Similarly, so is shifting to the right by 3 units.



We can label these by looking at where 0 gets moved to. When shifting 2 units right, 0 ended up under what used to be 2. We can call that the *additive symmetry of 2 on* $\mathbb{Z}$. Similarly, shifting 3 units left was the *additive symmetry of -3 on* $\mathbb{Z}$. But now consider what would happen if you shifted 3 units left, then 2 units right. The net result would be 1 shift to the left - the additive symmetry of -1. Said equivalently, $-3 + 2 = -1$. This is a major discovery. *The additive symmetries of* $\mathbb{Z}$ *are the same as the numbers in* $\mathbb{Z}$ *acting under addition.* Hence, we can describe the symmetries of $\mathbb{Z}$ with the elements of $\mathbb{Z}$. That makes $\mathbb{Z}$ a group, even though it isn't immediately apparent that $\mathbb{Z}$ is a set of symmetries.

In the same way as we could "add" the symmetries of $\mathbb{Z}$ to get a new symmetry, we can combine symmetries of a triangle to get a new symmetry. For example,



Notice that we read from right-to-left, like with function composition. That is, if we first we rotate by $\frac{2\pi}{3}$, and then reflect through the vertical axis, the result is the same as if we had just reflected through the second axis. You can probably also fairly easily intuit that composing two shuffles, i.e. shuffling twice, gives another shuffle.

So what properties do we want from symmetries? Well, beyond what a symmetry actually *is*, we want them to behave nicely when combined with each other. In particular:

- We want composition of symmetries to be a binary operation on the set of symmetries, so that composing any two symmetries gets us a new one.
- We want there to be an identity (the symmetry of doing nothing).

What else do we reasonably expect from symmetries? It seems sensible that we should be able to reverse any symmetry, whether by unshuffling, rotating back, reflecting back, etc. Hence

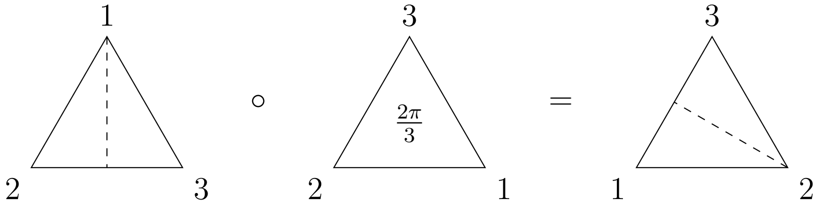
- We want every element to have an inverse.

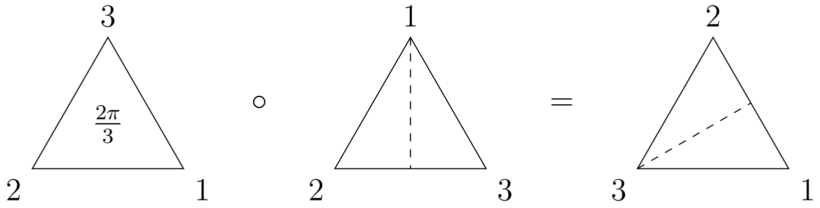
Some more thinking should tell us that we want one more thinking.

- Composition should be associative.

Question 4.1.1. Convince yourself of this by considering the above examples.

Do we want composition to be commutative? Addition over $\mathbb{Z}$ certainly is, but consider our triangles again (reading right-to-left, remember):





Apparently, we don't need commutivity to have a nice symmetry group. Now there's just one step left before full abstraction. We've developed the idea of a symmetry in the abstract, now let's let go of the need for us to understand what our symmetries are acting on.

§4.1.i. The axiomatic definition

Definition 4.1.2. A **group** $(G, \star)$ is a set G equipped with a binary operation $\star$, such that:

(i) $\star$ is associative: $a \star (b \star c) = (a \star b) \star c$;

(ii) there is an identity $e \in G$: $e \star a = a \star e = a$;

(iii) every element has an inverse: $a \star a^{-1} = a^{-1} \star a = e$.

When the operation is clear from context, it is common to write G for the group $(G, \star)$, and to write ab for $a \star b$. Some people include closure as a fourth axiom: that $a \star b \in G$ for any $a, b \in G$. We included this in our definition of $\star$ being a binary operation, but it is still important to note if you're checking if something is a group.

Definition 4.1.3. Let $(G, \star)$ be a group. If $\star$ is commutative, we call the group **abelian**, after Norwegian mathematician Niels Abel.

> **Remark 4.1.4** (On our intuition) — Think about what we've done here. First, we came up with the rules that anything we consider to be a "symmetry" should follow. Now, we have said that *anything* that follows those rules is a group, whether or not we understand it as being a symmetry. Sometimes, as in $\mathbb{Z}$, a bit more thought will reveal the elements of G to be the symmetries of some object. It turns out that G will always be a symmetry of *something*, but it won't necessarily be interesting or helpful.

One definition that will be helpful to know now, even if we don't deal with it just yet.

Definition 4.1.5. Let $(G, \star)$ be a group. If G is finite, we call $|G|$ the **order** of $(G, \star)$. If G is infinite, we say $(G, \star)$ is of infinite order.

Here's a few examples, before we prove some basic facts.

Example 4.1.6 (Additive groups)

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are all abelian groups. You can think of these as the translational symmetries of the respective sets, as we saw with $\mathbb{Z}$. $(\mathbb{N}, +)$ is not a group, as 1 doesn't have an inverse.

Example 4.1.7 (Multiplicative groups)

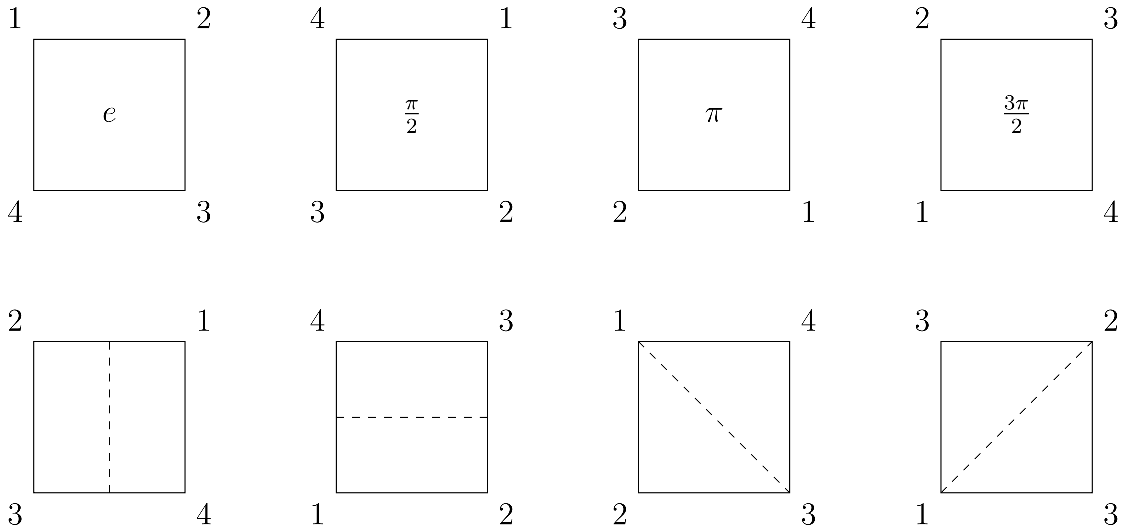
$(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$ and $(\mathbb{Q} \setminus \{0\}, \times)$ are all abelian groups, denoted $\mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^*$ respectively. [Why do we need to remove 0?] $(\mathbb{Z} \setminus \{0\}, \times)$ is not a group, as 2 does not have in inverse. These are symmetries under scaling for $\mathbb{R}$ and $\mathbb{Q}$, and symmetry under *both* scaling and rotation for $\mathbb{C}$. [Think about multiplication by 2 vs by i].

Example 4.1.8 (Matrix groups)

$(\mathcal{M}_n(\mathbb{R}), +)$ is an abelian group, again a higher-dimensional analogue of translation. $\mathrm{GL}_n(\mathbb{R})$, the **$n$th general linear group**, is the (non-abelian) group of invertible $n \times n$ real matrices under multiplication. If you remember how matrices represent transformations, you can see why this is a symmetry of $\mathbb{R}^n$ - almost every point moves under the transformation, but a lot of structure is preserved, such as the location of the origin, and the dimension of space. $\mathrm{SL}_n(\mathbb{R})$, is the (non-abelian) group invertible $n \times n$ matrices with determinant 1 (if you know what that means). This preserves the additional structure of area.

Example 4.1.9 (Dihedral groups)

For $n \geq 3$, D_{2n} is the group of symmetries of a regular n-gon is a group under composition. For example, we saw D_6 earlier, and I've drawn out D_8 below. It is always non-abelian. These are called the **dihedral groups**.



Example 4.1.10 (Symmetric groups)

The permutations of $\{1, 2, \ldots, n\}$ is a group, called S_n. It is non-abelian for $n \geq 3$. They are called the **symmetric groups** - a very unhelpful name. You also usually just say "S n" in practice. Below is an example composition in S_4. Don't worry if it looks very complicated - we'll find a way to do it more easily later.

$$\begin{tikzcd}
\alpha & = & 1 \arrow[rr, bend left] & 2 \arrow[l, bend left] & 3 \arrow[l, bend left] & 4 & = & 2 & 3 & 1 & 4 \\
\beta & = & 1 & 2 \arrow[r, bend left] & 3 \arrow[r, bend left] & 4 \arrow[ll, bend left] & = & 1 & 4 & 2 & 3 \\
\alpha \circ \beta & = & 1 \arrow[rr, bend left] & 2 \arrow[l, bend left] & 3 \arrow[l, bend left] & 4 & \circ & 1 & 2 \arrow[r, bend left] & 3 \arrow[r, bend left] & 4 \arrow[ll, bend left] \\
 & = & 1 \arrow[rr, bend left] & 2 \arrow[l, bend left] & 3 \arrow[l, bend left] & 4 & \circ & 1 & 4 & 2 & 3 \\
 & = & 1 \arrow[rr, bend left] & 4 \arrow[l, bend left] & 2 \arrow[l, bend left] & 3 \\
 & = & 4 & 2 & 1 & 3
\end{tikzcd}$$

Example 4.1.11 (Circle group)

$S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is a group under multiplication. This represents the infinite rotational symmetries of a circle, and is called the **circle group**. You might also see this written $\mathbb{T}$.

Example 4.1.12 (Modular groups)

Recall $\mathbb{Z}_n$, the set of equivalence classes of $\mathbb{Z}$ under congruence modulo n. Then $(\mathbb{Z}_n, +)$ forms an abelian group for any n, where $+$ is defined by $\overline{a} + \overline{b} = \overline{a+b}$.E.g., in $\mathbb{Z}_8$, $\overline{6} + \overline{5} = \overline{3}$. This is the symmetry of anything that repeats in n steps. If this all seems confusing, don't worry - we will look at it in more detail soon.

For prime p, it turns out that $(\mathbb{Z}_p \setminus \{\overline{0}\}, \times)$ forms a group denoted $\mathbb{Z}_p^*$, where $\overline{a} \times \overline{b} = \overline{ab}$. This follows from Proposition 2.4.18 (Invertibility in $\mathbb{Z}_n$), as for any $x \in \mathbb{Z}_p^*$, $\text{hcf}(x, p) = 1$. As said however, we haven't yet proven that. It's a bit harder to see at first glance what this is the symmetry of.

Example 4.1.13 (Other matrix groups)

The **special orthogonal group** SO(2) is the set of matrices of the form

$$\left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in [0, 2\pi) \right\}$$

under matrix multiplication. This is symmetry of $\mathbb{R}^2$ under rotation.

The **affine group** Aff($\mathbb{R}$) is the set of matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\}$$

under matrix multiplication. There is a natural way to interpret this is the symmetry under translation of a plane in $\mathbb{R}^3$ that doesn't pass through the origin. I may make you show that at some point.

Question 4.1.14 (Trig function and matrix review)**.** Check that $SO(2)$ and $\mathrm{Aff}(\mathbb{C})$ are closed under matrix multiplication.

Question 4.1.15 (A hint of isomorphism)**.** Have a think about the link between SO(2) and S^1? Hold on to this thought - we will return to it.

Let's look at a couple of sets of basic facts about groups.

Proposition 4.1.16 (Arithmetic works)

Let G be a group. Then the following hold:

(i) The identity e of G is unique.

(ii) Inverses are unique.

(iii) (Cancellation law). Let $a, x, y \in G$. If $ax = ay$, then $x = y$.

(iv) For any $a, b \in G$, we can solve the equation $ax = b$ for $x \in G$.

(v) For any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We proved (i) for a general set in Proposition 2.4.10 (Identity is unique). You should have proven (ii) in Exercise 2.4.22 (Inverses are unique). But in case you didn't, I'll do it here for the special case of groups.

- Fix $x \in G$, and suppose that for $a, b \in G$, $ax = xa = e$ and $bx = xb = e$. Then, by associativity,
$$a = ae = a(xb) = (ax)b = eb = b.$$

(iii) is an incredibly useful result.

$$ax = ay \implies a^{-1}ax = a^{-1}ay \implies x = y.$$

Notice that the same argument also gives $xa = ya \implies x = y$. (iv) is also very nice. We can just see that $x = a^{-1}b$ by associativity

$$a(a^{-1}b) = (a^{-1}a)b = b.$$

(v) is simple to check.

Question 4.1.17. Prove (v).

□

(iii) and (iv) are perhaps most naturally phrased as one result.

Corollary 4.1.18 (Multiplicative maps)

Fix $a \in G$. Then the map given $x \mapsto ax$ is a bijection. This map is often called **left multiplication by a**.

Proof. (iii) above proved injectivity, and (iv) proved surjectivity. □

We also define powers for groups.

Definition 4.1.19. Let $(G, \star)$ be a group. For $n \in \mathbb{Z}$, we write

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

Proposition 4.1.20 (Powers work as expected)
For any $g \in G$, and for any $m, n \in \mathbb{Z}$:

(i) $(g^{-1})^{-1} = g$;

(ii) $(g^{-1})^n = g^{-n}$;

(iii) $g^m g^n = g^{m+n}$;

(iv) $(g^m)^n = g^{mn}$.

Proof. Irritatingly fiddly to write down, but obvious. The "proofs" from AS Maths actually work as proofs here. □

Remark 4.1.21 ($\mathbb{Z}_n$) — Note that for $g = \overline{x} =\in \mathbb{Z}_n$,

$$g^k = \overline{x}^k = \underbrace{\overline{x} + \cdots + \overline{x}}_{k \text{ times}} = \overline{kx},$$

for positive k, with a similar result if k is negative. In summary,

$$\overline{x^k} \neq \overline{x}^k = \overline{kx}.$$

Exercise 4.1.22 (Group identification)
Which of the following are groups?

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

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

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

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

Exercise 4.1.23 (Compulsory - product groups)

Let $(G, \star_G)$ and $(H, *_H)$ be groups. We define the **product group** $(G \times H, \circ)$ by

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \star_G g_2, h_1 *_H h_2).$$

Consider $\mathbb{Z}_2 \times \mathbb{Z}_2 = (\mathbb{Z}_2)^2$. What shape is this the symmetry group of?

§4.2. Symmetric groups and symmetry groups

I think the best way to really get to grips with group theory is to play around with some groups. Possibly the most important types of groups are S_n.

§4.2.i. Symmetric groups

Let's formally define S_n.

Definition 4.2.1. Let X be set. A bijection from $X \to X$ is called a **permutation** of X.

Definition 4.2.2. Fix $n \in \mathbb{N}$. Then the ***n*th symmetric group** S_n is the group of permutations of $\{1, \dots, n\}$ under function composition.

It's always important to actually check that things are groups.

Proposition 4.2.3 (Symmetric groups)

For any n, S_n is a group.

Proof. The identity function id is bijective, so $\text{id} = e \in S_n$. Let $\varphi \in S_n$. As φ is a bijection, φ^{-1} is well-defined and $\varphi^{-1} \in S_n$. Function composition is associative in general by Proposition 2.4.7 (Function composition is associative), so in particular it is here. THe group is also closed, as clearly the composition of two bijections is a bijection. Hence S_n satisfies all of the group axioms. □

Example 4.2.4 (S_3)

Let's list all of the elements of S_3.

- There will be the identity: $(1, 2, 3) \mapsto (1, 2, 3)$.
- There are three ways of swapping two elements: $(1, 2, 3) \mapsto (2, 1, 3), (3, 2, 1), (1, 3, 2)$.
- There are two ways of cycling the elements: $(1, 2, 3) \mapsto (2, 3, 1), (3, 1, 2)$.

§4.2.ii. Notations

Traditionally, we use Greek letters ρ, σ, τ for permutations. Suppose $\sigma \in S_5$, and it acts by

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

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

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

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

> **Question 4.2.5.** Write $\sigma : (1, 2, 3, 4, 5) \mapsto (3, 2, 5, 1, 4)$ and $\tau : (1, 2, 3, 4, 5) \mapsto (4, 3, 2, 1, 5)$ and their inverses in cycle notation.

> **Question 4.2.6.** Show that any 2-cycle is it's own inverse. Are any other cycles their own inverses?

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

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

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

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

However, the real advantage of this method is that it makes composition very easy. Using just cycle notation, it can take a while to work out what $\tau \circ \sigma$ should be, but with two-line notation it's very easy. I won't explain how to do it, but I'll show you an example. It should speak for itself.

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

> **Question 4.2.7.** If $\sigma : (1, 2, 3, 4, 5) \mapsto (3, 2, 5, 1, 4)$ and $\tau : (1, 2, 3, 4, 5) \mapsto (4, 3, 2, 1, 5)$ then find $\tau \circ \sigma$ and $\sigma \circ \tau$ by using two-line notation.

Here are two facts.

Proposition 4.2.8 (Symmetric groups)

(i) The order of S_n is $|S_n| = n!$.

(ii) S_n is non-abelian for $n \geq 3$.

Proof. (i) We have n choices for where n maps to, $n-1$ for where 2 maps to, etc. [A different way of approaching this: there are $n!$ ways of ordering the second row in two-line notation.]

(ii) For $n \geq 3$, $(1\,2)$ and $(1\,3)$ are in S_n. But

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

Hence S_n is non-abelian for $n \geq 3$.

□

OPTIONAL - more cycle notation

We were very unrigorous when we defined cycle notation. We neither showed that the cycle notation necessarily exists, nor is unique, for any given permutation. It fairly obviously is true, so if you want to skip this section, feel free. But I'm too much of a purist to not offer you a guided tour of the proof.

Definition 4.2.9. Let $(a_1 \cdots a_m)$ and $(b_1 \cdots b_n)$ be cycles. If $a_i \neq b_j$ for all i, j then the two cycles are called **disjoint**.

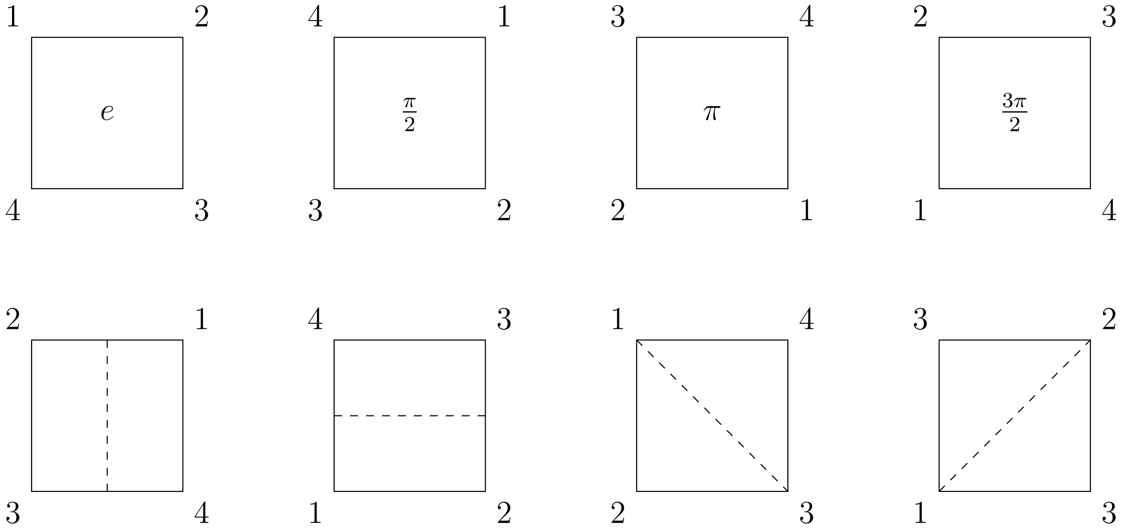
Lemma 4.2.10 (Cycle notation)

Disjoint cycles commute, and any $\sigma \in S_n$ can be written uniquely as a composition of disjoint cycles.

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

§4.2.iii. Dihedral groups

Consider the symmetries of a regular n-gon. As in the triangle, we have $2n$ symmetries: n rotations, and n reflections. You saw them for $n = 3$ earlier, so here's $n = 4$:



These form a group called D_{2n}, the **dihedral group of order $2n$**.

How do we know that they are all of the symmetries? The easiest way to understand this is in terms of permutations of the vertices. We can, for example, write the rotation by π in D_8 as the permutation

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

Now, for a permutation to represent a symmetry of an n-gon, we need the vertices to still be labelled in order, either clockwise or anticlockwise. That is, for some k, either

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ k & k+1 & \cdots & k-2 & k-1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ k & k-1 & \cdots & k+2 & k+1 \end{pmatrix}.$$

We can see that permutations of the first type correspond to rotations (with $k = 1$ giving our identity e), and permutations of the second type correspond to reflections.

Proposition 4.2.11 (Order of D_{2n})
As the name suggests, $|D_{2n}| = 2n$.

Proof. There are n choices for k (as above), and two symmetries for each k. Hence $2n$ total symmetries. □

Using our techniques from symmetric groups, we can find inverses. Let's do it with cycle notation. A rotation of k clockwise has the inverse of a rotation $n - k$ clockwise:

$$\begin{pmatrix} 1 & k & 2k & \cdots & n-k \end{pmatrix}^{-1} = \begin{pmatrix} 1 & n-k & \cdots & 2k & k \end{pmatrix}.$$

Any reflection is it's own inverse:

$$\begin{aligned} \left(\begin{pmatrix} 1 & k \end{pmatrix} \begin{pmatrix} 2 & k-1 \end{pmatrix} \cdots \begin{pmatrix} n & k+1 \end{pmatrix}\right)^{-1} &= \begin{pmatrix} 1 & k \end{pmatrix}^{-1} \begin{pmatrix} 2 & k-1 \end{pmatrix}^{-1} \cdots \begin{pmatrix} n & k+1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & k \end{pmatrix} \begin{pmatrix} 2 & k-1 \end{pmatrix} \cdots \begin{pmatrix} n & k+1 \end{pmatrix}. \end{aligned}$$

This should match up with our intuitions.
We define

$$r = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix} = \text{ rotation by } \frac{2\pi}{n}$$

and

$$f = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & n & \cdots & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix} \begin{pmatrix} 2 & n \end{pmatrix} \begin{pmatrix} 3 & n-2 \end{pmatrix} \cdots = \text{ reflection that fixes 1.}$$

> **Question 4.2.12.** Show that every rotation can be written in the form r^k for $k = 1, \dots, n$, with $r^n = e$.

That covers the n rotations. Then the reflection that sends 1 to k is $r^{k-1}f$:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k & k+1 & \cdots & k-1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & n & \cdots & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & n & \cdots & 2 \\ k & k-1 & \cdots & k+1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & \cdots & n \\ k & k-1 & \cdots & k+1 \end{pmatrix}$$

Again, this should agree with your geometric intuition - a reflection is the same as turning the shape over (flipping it) and then rotating. Hence we can write

$$D_{2n} = \left\{e, r, r^2, \dots, r^{k-1}, f, rf, \dots, r^{k-1}f\right\}.$$

That is, the symmetries of a regular n-gon are the n rotations, and n reflections; or equivalently, n rotations, and n sets of a flip followed by a rotation.

> **Remark 4.2.13** (Morals) — There was quite a lot of algebra in that section - congratulations on getting through it. However, most of it boiled down to showing that our algebraic structure D_{2n} actually does a good job of representing the symmetries of a regular n-gon.
>
> Soon, we will have developed enough tools in group theory to make this sort of grunt work much easier - in fact, I could have compressed all of this into about 5 lines had I put it at the end of this chapter. However, that isn't the point. By spending a long time looking at these groups that you should have a strong intuition for already, you got the opportunity to work with a nicely behaved group, to build your intuition about the algebra.

Exercise 4.2.14 (To flip before or after)

Show that $r^k f = f r^{n-k}$.

§4.3. Subgroups and isomorphism

§4.3.i. Ignoring the set

Consider our two constructions of D_{2n}:

$$\left\{e, r, r^2, \dots, r^{n-1}, f, rf, r^2f, \dots, r^{n-1}f\right\}$$

and

$$\left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}, \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & \cdots & n \\ 3 & 4 & \cdots & 1 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & n & \cdots & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 1 & \cdots & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & \cdots & n \\ 3 & 2 & \cdots & 4 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix} \right\}$$

But we defined a group $(G, \star)$ as depending on the set G! So if the underlying set is different, these actually aren't the same group. But they act the same (they both represent the symmetries of a regular n-gon), and clearly anything that we prove about one group is also true about the other. In fact, it is almost as though the groups are the same except with renamed elements. Algebra gives us a word for this relation: isomorphism.

Definition 4.3.1. Let $(G, \star_G)$ and $(H, *_H)$ be groups. If $\varphi : G \to H$ is a bijection which satisfies

$$\varphi(g_1 \star_G g_2) = \varphi(g_1) *_H \varphi(g_2) \qquad \text{for every } g_1, g_2 \in G$$

we say it is an **isomorphism** (Greek for *same form*). If there is an isomorphism between two groups G and H we say they are **isomorphic** and write $G \cong H$.

Remark 4.3.2 (Preserving group structure) — The condition $\varphi(g_1 \star_G g_2) = \varphi(g_1) *_H \varphi(g_2)$ is sometimes called "preserving group structure". It says that it doesn't matter whether you take the product of the inputs or the outputs - the result is the same.

It should be relatively clear how this is a "renaming" function. It is a bijection, so we can pair each element in H with a distinct element in G, and it preserves group structure, so the operations behave the same.

Exercise 4.3.3 (Compulsory)

Let $\varphi : G \to H$ be an isomorphism. Show that φ^{-1} is also an isomorphism, so that $G \cong H \iff H \cong G$. Hence show that isomorphism is an equivalence relation.

We generally then only consider groups *up to isomorphism.* D_{2n} is the name of any group isomorphic to $\{e, r, \ldots, r^{n-1}, f, rf, \ldots, r^{n-1}f\}$, regardless of what we call the elements. The trivial group is any group with only one element (as they must be isomorphic). Some isomorphisms are a bit less trivial.

Example 4.3.4 (Easy examples of isomorphisms)

(a) $\mathbb{Z} \cong 2\mathbb{Z}$ with the isomorphism $x \mapsto 2x$.

(b) Clearly $G \times H \cong H \times G$.

(c) For any G, $G \cong G$ by $g \mapsto g$.

(d) Sometimes we have more exciting isomorphisms $G \to G$. For example, $x \mapsto -x$ is an isomorphism $\mathbb{Z} \to \mathbb{Z}$.

(e) $(\mathbb{R}, +) \cong (\mathbb{R}^{>0}, \times)$ by $x \mapsto e^x$. That means that anything we can prove about adding reals is equivalent to statement about multiplying positive reals.

Example 4.3.5 (Modular isomorphism)

We can see that $\mathbb{Z}_6 \cong \mathbb{Z}_7^*$ with $\varphi(\overline{x}) = \overline{3^x}$. It is a bijection:

$$\left(\overline{3^0}, \overline{3^1}, \overline{3^2}, \overline{3^3}, \overline{3^4}, \overline{3^5}\right) = \left(\overline{1}, \overline{3}, \overline{9}, \overline{27}, \overline{81}, \overline{243}\right) = \left(\overline{1}, \overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}\right).$$

It also preserves the group structure, as

$$\varphi\left(\overline{a} + \overline{b}\right) = \varphi\left(\overline{a+b}\right) = \overline{3^{a+b}} = \overline{3^a} \times \overline{3^b}.$$

It turns out that for any prime p, $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^*$, but proving that will have to wait until later.

Exercise 4.3.6 (Dihedral and symmetric groups.)

Show that $D_6 \cong S_3$ but that for $n \geq 4$, $D_{2n} \ncong S_n$.

Exercise 4.3.7 (Circle groups)

In Exercise 4.1.15 (A hint of isomorphism) you should have realised that

$$S^1 = \{z \in \mathbb{C} : |z| = 1\} \quad \text{and} \quad \mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in [0, 2\pi) \right\}$$

where in a sense "the same", as both represent all possible rotations of $\mathbb{R}^2$; equivalently, they are the the rotational symmetries of a circle. Show that $S^1 \cong \mathrm{SO}(2)$ by constructing an explicit isomorphism.

§4.3.ii. Subgroups

We analysed the elements of D_{2n} as elements of S_n. This is actually very common! We define a subgroup analogously to a subset.

Definition 4.3.8. Let $(G, \star)$ be a group. If $H \subseteq G$ forms a group $(H, \star)$ *with the same operation as* G, we say that $(H, \star)$ is a **subgroup** of $(G, \star)$, and write $H \leq G$.

Example 4.3.9 (Examples of subgroups)

(a) $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, which is also isomorphic to $\mathbb{Z}$.

> **Question 4.3.10.** Show that if $H < G$ is a proper subgroup such that $G \cong H$, then both G and H are infinite.

(b) D_{2n} is a subgroup of S_n for any n by thinking of it as a permutation of vertices.

(c) The subset $\{\sigma \in S_n : \sigma(1) = 1\}$ is a subgroup of S_n, which is isomorphic to S_{n-1}.

(d) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ and $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.

(e) S^1 is a subgroup of $\mathbb{C}^*$.

(f) $\mathrm{SL_n}(\mathbb{R})$, $\mathrm{SO}(2)$, and $\mathrm{Aff}(\mathbb{R})$ are all subgroups of $\mathrm{GL}_n(\mathbb{R})$, but none are subgroups of each other.

(g) For any group G, $\{e\}$ and G are the **trivial** subgroups.

Note that some things that might look like subgroups aren't!

Example 4.3.11 (Non-examples of subgroups)

(a) $(\mathbb{Z}, \times)$ isn't a subgroup of $\mathbb{Q}^*$, as it isn't a group.

(b) $\mathbb{Z}_n$ isn't a subgroup of $\mathbb{Z}$, as elements are different.

There's a very nice way of checking if something is a subgroup.

Proposition 4.3.12 (Subgroup test)

Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if H is non-empty and whenever $x, y \in H$ then $x^{-1}y \in H$.

Proof. ($\Rightarrow$) Suppose $H \leq G$. Then clearly H is non-empty as $e \in H$, and $x^{-1}y \in H$ for each $x, y \in H$, as H is group so closed under inverses and products.
($\Leftarrow$) Suppose H is non-empty, and for each $x, y \in H$, $x^{-1}y \in H$.

- As H is non-empty, pick some $x \in H$. Then $x^{-1}x = e \in H$. Thus H has an identity.
- For any $x \in H$, $x^{-1}e = x^{-1} \in H$, so H has inverses.
- The operation is the same as in G so is associative (associativity is inherited from G).
- For any $x, y \in H$, $x^{-1} \in H$ so $(x^{-1})^{-1}y = xy \in H$, so H is closed under the operation.

Thus H is a group, so a subgroup of G. □

Proposition 4.3.13 (Combining subgroups)

Let G be a group, and let $H, K \leq G$ be subgroups. Then:

(i) $H \cap K$ is a subgroup;

(ii) $H \cup K$ is not necessarily a subgroup;

(iii) $HK = \{hk : h \in H, k \in K\}$ is not necessarily a subgroup;

(iv) if G is abelian, then HK is a subgroup.

Proof. (i) As H, K are groups, $e \in H$ and $e \in K$, so $e \in H \cap K$. Also, if $x, y \in H$ then $x^{-1}y \in H$ by the subgroup test, similarly if $x, y \in K$ then $x^{-1}y \in K$. Hence if $x, y \in H \cap K$ then $x^{-1}y \in H \cap K$ so $H \cap K$ passes the subgroup test.

(ii) Should be fairly easy.

> **Question 4.3.14.** Come up with a counterexample to prove (ii).

(iii) Let $G = S_3$, $H = \{e, (1\,2)\}$ and $K = \{e, (1\,3)\}$. Clearly $H, K \leq G$. Then $(1\,2)(1\,3) = (1\,3\,2) \in HK$ but $(1\,3\,2)^{-1} = (1\,2\,3) \notin HK$, so HK is not a group.

(iv) Suppose G is abelian. As H, K are groups, $e \in H$ and $e \in K$, so $ee = e \in HK$. Suppose $x, y \in HK$. Then there are $h_x, h_y \in H$ and $k_x, k_y \in K$ such that $h_x k_x = x$ and $h_y k_y = y$. Hence

$$x^{-1}y = (h_x k_x)^{-1} h_y k_y = k_x^{-1} h_x^{-1} h_y k_y = h_x^{-1} h_y k_x^{-1} k_y.$$

But $h_x^{-1}h_y \in H$ and $k_x^{-1}k_y \in K$ by the subgroup test, so $x^{-1}y = (h_x^{-1}h_y)(k_x^{-1}k_y) \in HK$, and HK passes the subgroup test.

□

We can use (i) to define the most important type of subgroup.

Definition 4.3.15. Let G be a group and $S \subseteq G$ be a subset of G. We define the **subgroup generated by S**, written $\langle S \rangle$, by

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

That is, $\langle S \rangle$ is the intersection of all subgroups of G containing S.

If you have studied groups before, you may have forgotten that that is actually how you define generated subgroups (or you may actually never have met it, and had another definition). That's because of the following result.

Proposition 4.3.16 (The smallest subgroup)

Let G be a group and $S \subseteq G$ a subset. Then

(i) $\langle S \rangle$ is a subgroup;

(ii) if $H \leq G$ is a subgroup with $S \subseteq H$ then $\langle S \rangle \leq H$.

The usual way of stating (ii) is that $\langle S \rangle$ is the smallest subgroup containing S.

Proof. (i) e must be in every subgroup of G, so $e \in \langle S \rangle$. By similar logic to (i) in the previous proposition, if $x, y \in \langle S \rangle$, then x, y are in every subgroup containing S. The subgroup tests then tells us that $x^{-1}y$ is in all of those subgroups, so $x^{-1}y \in \langle S \rangle$. Hence $\langle S \rangle$ passes the subgroup test.

(ii) For any such H, we must have $\langle S \rangle \subseteq H$ from the definition. As both are subgroups of G, we have $\langle S \rangle \leq H$.

□

Remark 4.3.17 (Notation) — We typically write $\langle a, b, \ldots, z \rangle$ rather than $\langle \{a, b, \ldots, z\} \rangle$ for obvious aesthetic reasons.

Remark 4.3.18 (The box analogy) — One way to think of $\langle S \rangle$ is as follows. Put all of the elements of S (as well as their inverses) in a box, and shake it around, until you end up with all of the possible products of elements. So if $S = \{s_1, s_2, \ldots\}$ just $s_3 \in \langle S \rangle$, but so is $s_4s_7s_1$ and $s_2s_3^{-1}s_5s_7s_11^{-1}s_13^{-1}\cdots$. All of these are necessary (by closure) for $\langle S \rangle$ to be a group, but we also aren't forming any extra elements that aren't necessary for $\langle S \rangle$ to be a group.

Exercise 4.3.19 (Making the box rigorous)

We can make that analogy rigorous. Show that $\langle S \rangle$ is the group formed by the set

$$\{x : x \text{ is a finite product of elements of } S \text{ and their inverses.}\}.$$

§4.3.iii. A hint of cyclic groups

In particular, the subgroups generated by a single element are nice.

Proposition 4.3.20 (Subgroups generated by a single element)
Let G be a group and $g \in G$. Then

$$\langle g \rangle = \left\{ g^k : k \in \mathbb{Z} \right\}.$$

In particular, if there is an $n \in \mathbb{Z}$ such that $g^n = e$, then

$$\langle g \rangle = \left\{ e, g, g^2, \ldots, g^{n-1} \right\}.$$

Proof. Clearly, $g^k \in \langle g \rangle$ for any k by closure, and so $\left\{ g^k : k \in \mathbb{Z} \right\} \subseteq \langle g \rangle$. Also, $\left\{ g^k : k \in \mathbb{Z} \right\}$ is a subgroup of G, as $g^0 = e$, and $(g^m)^{-1} g^n = g^{n-m}$, so it passes the subgroup test. But by Proposition 4.3.16 (ii) (The smallest subgroup), that means $\langle g \rangle \leq \left\{ g^k : k \in \mathbb{Z} \right\}$. Thus by double inclusion they are equal.

> **Question 4.3.21.** Show that the second result follows from the first.

□

Alternatively, we could have used Exercise 4.3.19 (Making the box rigorous) above.

We can tell that $\langle g \rangle$ is probably a very easy group to work with. Hence, in true mathematical fashion, we give groups of that type a name.

Definition 4.3.22. Let G be a group. If there is a $g \in G$ such that $\langle g \rangle = G$, we call G a **cyclic group**.

It turns out that there actually aren't very many cyclic groups!

Proposition 4.3.23 (Cyclic groups are $\mathbb{Z}_n$)
Let G be a cyclic group.

(i) If $|G| = n$ is finite, then $G \cong \mathbb{Z}_n$.

(ii) If G is infinite, then $G \cong \mathbb{Z}$.

Sketch of proof. If $G = \langle g \rangle$ is finite, then we must have

$$\langle g \rangle = \left\{ e, g, g^2, \ldots, g^{n-1} \right\}.$$

But then we can check $\varphi(\overline{x}) = g^x$ is an isomorphism $\mathbb{Z}_n \to G$. If G is infinite, then $\varphi(x) = g^x$ is also an isomorphism. □

> **Question 4.3.24.** Feel free to fill in the details on that proof - the result should be obvious as it is, however.

There are a lot of uses for cyclic groups, some of which we will meet later. But first, a quick overview of an area of group theory which actually isn't very well understood.

§4.3.iv. Group presentations

In a similar vein to set-builder notation, we have "group-builder notation", called a group presentation. To motivate it, I will give a slightly different definition of a generated subgroup.

Definition 4.3.25. Let G be a group, and $S \subseteq G$ a subset. Then the **subgroup generated by S** $\langle S \rangle$ is the set of elements of G that can be written as a finite product of the elements of S and their inverses.

Exercise 4.3.26 (Equivalent definitions)
Show that this definition is equivalent to the definition I gave earlier.

Now, clearly $D_6 \cong \langle r, f \rangle$. But so is D_8. In fact, for any n, $D_{2n} \cong \langle r, f \rangle$, just for different r, f. This is very confusing. Thus, when context isn't clear (notice that I didn't specify which group $\{r, f\}$ was a subset of), we specify the properties of the generators. Thus we have the **group presentations**

$$D_6 \cong \left\langle r, f : r^3 = f^2 = e,\, rf = fr^2 \right\rangle$$

while

$$D_8 \cong \left\langle r, f : r^4 = f^2 = e,\, rf = fr^3 \right\rangle.$$

We can now write any group as a generated group, just by specifying how the generators behave. For example

$$\mathbb{Z}_{10} = \left\langle x : x^{10} = e \right\rangle.$$

But notice that we could also have written

$$\mathbb{Z}_{10} = \left\langle a, b : a^2 = b^5 = e,\, ab = ba \right\rangle.$$

Clearly, group presentations are not unique. A famous example is D_{2n}:

$$D_{2n} \cong \left\langle r, f : r^n = f^2 = e,\, rf = fr^{-1} \right\rangle \cong \left\langle x, y : x^2 = y^2 = (xy)^n = e \right\rangle.$$

> **Question 4.3.27.** To see why this is equivalent, set $x = f$, $y = rf$.

Actually, determining whether two presentations are isomorphic is undecidable. In fact, it is undecidable to even determine if a group is *finite* from its presentation. It does make for some good problems though!

Exercise 4.3.28 (Group presentations)
Find the groups which are isomorphic to each of these presentations.

(a) $\langle p, q : p^2 = q^2 = e,\, pqp = qpq \rangle$.

(b) $\langle x, y : a^2 = b^2 = e,\, ab = ba \rangle$.

(c) $\langle g, h : gh = hg \rangle$.

(d) $\langle a, b, c : ab = c^2a^4,\, bc = ca^6,\, ac = ca^8,\, c^{2018} = b^{2019} \rangle$.

§4.4. Homomorphisms

Lagrange's theorem is one of the most important facts in group theory. You may have noticed it when looking at examples of subgroups earlier.

Theorem 4.4.1 (Lagrange's theorem)
Let G be a finite group, and $H \leq G$ a subgroup. The $|H|$ divides $|G|$.

This quite a surprising result! We will prove it at the end of this chapter, but it might take a bit of motivating.

§4.4.i. Homomorphisms

Recall the definition of an isomorphism: a bijection $\varphi : G \to H$ which preserves group structure by $\varphi(x)\varphi(y) = \varphi(xy)$. You might be wondering what happens if we don't insist on a bijection, but just look at any function that preserves group structure. For example, if $\varphi : G \to H$ is injective, then it's as though there is a copy of G embedded in H. This gives us the definition of a homomorphism.

Definition 4.4.2. Let $(G, \star_G)$ and $(H, *_H)$ be groups. Then $\varphi : G \to H$ is a **homomorphism** if it satisfies

$$\varphi\left(g_1 \star_G g_2\right) = \varphi\left(g_1\right) *_H \varphi\left(g_2\right) \quad \text{for any } g_1, g_2 \in G.$$

Remark 4.4.3 — Note that isomorphisms are then just bijective isomorphisms.

These also have a lot of nice properties. A couple of facts should be obvious.

Proposition 4.4.4 (Homomorphisms preserve inverses)
Let G, H be groups, and $\varphi : G \to H$ a homomorphism. Then for any $g \in G$,

$$\varphi(g^{-1}) = \varphi(g)^{-1}.$$

In particular, $\varphi(e_G) = \varphi(e_H)$.

Proof. First, note that for any $g \in G$,

$$\varphi(g) = \varphi(e_G g) = \varphi(e_G)\varphi(g),$$

so $\varphi(e_G) = e_H$. Then

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H \implies \varphi(g)^{-1} = \varphi(g^{-1}).$$

□

Question 4.4.5. Show that for any homomorphism φ, $\varphi(g^n) = \varphi(g)^n$.

Example 4.4.6 (Examples of homomorphisms)

(a) For any groups G, H, $g \mapsto e_H$ is a homomorphism.

(b) For any groups G, H, $G \times H \to G$ by $(g, h) \to g$ is a surjective homomorphism.

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

(d) The map $\mathbb{Z} \to \mathbb{Z}$ by $x \mapsto 10x$ is an injective homomorphism.

(e) There is an injective homomorphism $S_n \to S_{n+1}$: we can treat any permutation of $\{1, 2, \dots, n\}$ as a permutation of $\{1, 2, \dots, n, n+1\}$ which leaves $n+1$ fixed.

Exercise 4.4.7 (Square homomorphisms)
For which groups G is $g \mapsto g^2$ a homomorphism?

Homomorphisms are very useful, not only because they preserve group structure: they also let us find new groups and subgroups!

Proposition 4.4.8 (Images are a group)
Let G, H be groups, and $\varphi : G \to H$ a homomorphism. Then $\operatorname{Im}\varphi \leq H$ is a subgroup.

Proof. We apply the subgroup test.

- As in Proposition 4.4.4 (Homomorphisms preserve inverses) above, $\varphi(e_G) = e_H$ so $e_H \in \operatorname{Im}\varphi$.
- Suppose $x, y \in \operatorname{Im}\varphi$. Then there are $a, b \in G$ such that $\varphi(a) = x$, $\varphi(b) = y$. But then
$$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) = x^{-1}y,$$
so $x^{-1}y \in \operatorname{Im}\varphi$.

□

In fact, pre-images of a subgroup also form a group!

Theorem 4.4.9 (Pre-images form a group)
Let G, H be groups, and $\varphi : G \to H$ a homomorphism. Let $N \leq H$ be a subgroup. The $\varphi^{\text{pre}}(N)$ is a subgroup of G.

Proof. We apply the subgroup test.

- $\varphi(e_G) = e_H \in N$ so $e_G \in \varphi^{\text{pre}}(N)$.
- Suppose $x, y \in \varphi^{\text{pre}}(N)$. Then let $\varphi(x) = m$ and $\varphi(y) = n$, so
$$\varphi(x^{-1}y) = \varphi(x^{-1})\varphi(y) = \varphi(x)^{-1}\varphi(y) = m^{-1}n.$$
As $m^{-1}n \in N$ by closure, $x^{-1}y \in \varphi^{\text{pre}}(N)$.

□

No matter which H we choose, we always have $\{e\} \leq H$. That suggests that it's pre-image might be especially useful. It is.

Definition 4.4.10. Let G, H be groups, and $\varphi : G \to H$ a homomorphism. We define the **kernel** of φ as

$$\ker \varphi = \varphi^{\text{pre}}(e_H) = \{g \in G : \varphi(g) = e_H\}.$$

Corollary 4.4.11 (Kernels form a subgroup)

$\ker \varphi$ is a group, for any homomorphism φ.

Proof. Apply Theorem 4.4.9 (Pre-images form a group) with $N = \{e_H\}$. □

Exercise 4.4.12 (If you know matrices)

Consider the determinant map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$. Show that det is a homomorphism. What is $\ker \det$?

We have a rough intuition about what it means for a homomorphism $\varphi : G \to H$ to be injective: it means that there is a copy of G inside H. That actually makes the first part of the following result fairly obvious.

Exercise 4.4.13 (Compulsory - Kernels of injective homomorphisms)

Let $\varphi : G \to H$ be a homomorphism. Show that $\ker \varphi = \{e\}$ if and only of φ is injective. This is one indicator of how important the kernel is.

But what if we have a surjective homomorphism? These are a bit harder to picture, so let's take an example. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$ by $\varphi(x) = \overline{x}$, which is clearly a homomorphism. One natural question you could ask, to get a picture of the homomorphism, is where does each element of $\mathbb{Z}$ map to. In other words, what are the pre-images? If you excuse some sloppy notation, we get

$$\begin{aligned}
\ker \varphi = \varphi^{\text{pre}}\left(\overline{0}\right) &= \{\ldots, -20, -10, 0, 10, 20, 30, \ldots\} = 10\mathbb{Z} \\
\varphi^{\text{pre}}\left(\overline{1}\right) &= \{\ldots, -19, -9, 1, 11, 21, 31, \ldots\} = 1 + 10\mathbb{Z} \\
\varphi^{\text{pre}}\left(\overline{2}\right) &= \{\ldots, -18, -8, 2, 12, 22, 32, \ldots\} = 2 + 10\mathbb{Z} \\
&\vdots \\
\varphi^{\text{pre}}\left(\overline{8}\right) &= \{\ldots, -12, -2, 8, 18, 28, 38, \ldots\} = 8 + 10\mathbb{Z} \\
\varphi^{\text{pre}}\left(\overline{9}\right) &= \{\ldots, -11, -1, 9, 19, 29, 39, \ldots\} = 9 + 10\mathbb{Z}.
\end{aligned}$$

Let's try another example. Let's try the homomorphism $\psi : D_{12} \to D_6$ by reducing the power of r mod 3. For example, $\psi(rf) = rf$, $\psi(r^5) = r^2$ and $\psi(r^4 f) = rf$. Then what are our pre-images?

$$\ker \psi = \psi^{\text{pre}}(e) = \left\{e, r^3\right\} = \left\langle r^3 \right\rangle \text{ recalling we're in } D_{12} \text{ here.}$$

$$\begin{aligned}\psi^{\text{pre}}\left(r\right) &= \left\{r, r^4\right\} = r\left\langle r^3\right\rangle \\ \psi^{\text{pre}}\left(r^2\right) &= \left\{r^2, r^5\right\} = r^2\left\langle r^3\right\rangle \\ \psi^{\text{pre}}\left(f\right) &= \left\{f, r^3 f\right\} = f\left\langle r^3\right\rangle \\ \psi^{\text{pre}}\left(rf\right) &= \left\{rf, r^4 f\right\} = rf\left\langle r^3\right\rangle \\ \psi^{\text{pre}}\left(r^2 f\right) &= \left\{r^2 f, r^5 f\right\} = r^2 f\left\langle r^3\right\rangle .\end{aligned}$$

Let's map $\theta : \mathbb{R} \to \mathbb{R}$ where $\theta(x)$ is the fractional part of x. For example, $\theta(2.34) = 0.34$, $\theta(5) = 0$, and $\theta(\pi) = \pi - 3$. This has pre-images of the form

$$\theta^{\text{pre}}(x) = \{\dots, -2 + x, -1 + x, x, 1 + x, 2 + x, \dots\} = x + \mathbb{Z}.$$

One final example. Let's map $\lambda : S_3 \to S_2$ by $\lambda(\sigma) = (12)$ if σ is a 2-cycle, and $\lambda(\sigma) = e$ else.

> **Question 4.4.14.** Check that this is a surjective homomorphism by noting that $S_3 \cong D_6$ and $S_2 \cong \mathbb{Z}_2$, and the homomorphism is equivalent to the mapping $\lambda : D_6 \to \mathbb{Z}_2$ by choosing whether the symmetry is a reflection or rotation.

Let's check our pre-images!

$$\begin{aligned}\ker\lambda = \lambda^{\text{pre}}(e) &= \{e, (123), (132)\} = \langle(123)\rangle \\ \lambda^{\text{pre}}(\,(12)\,) &= \{(12), (13), (23)\} = (12)\left\langle(123)\right\rangle .\end{aligned}$$

It seems natural to introduce a name for this type of pre-image.

Definition 4.4.15. Let G be a group, and $H \leq G$ a subgroup. Then the **left cosets** of H are the sets of the form

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

where $g \in G$. We can define right cosets Hg similarly. We write the set of left cosets G/H.

Example 4.4.16 (Cosets of (12))

Let $G = S_3$ and $H = \langle(12)\rangle = \{e, (12)\}$. Then the left cosets are

$$\begin{aligned}eH = (12)H &= \{e, (12)\} \\ (13)H = (123)H &= \{(13), (123)\} \\ (23)H = (132)H &= \{(23), (132)\}.\end{aligned}$$

Notice that $|G| = 6$, $|H| = 2$ and $|G/H| = 3$.

Example 4.4.17 (Cosets of S^1)

Let $G = \mathbb{C}^*$ and $H = S^1$. The left cosets of H are

$$wH = wS^1 = \{z \in \mathbb{C}^* : |w| = |z|\}.$$

That is, the left coset wS^1 is the circle around the origin containing w. Hence, we can write the set of concentric circles in $\mathbb{C}$ as $\mathbb{C}^*/S^1$.

Example 4.4.18 (Cosets of $\mathbb{Z}$)

Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ for some n. Then the set of left cosets of H is $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ (although as sets - we haven't got an operation for $\mathbb{Z}/n\mathbb{Z}$).

Let $G = \mathbb{Z}_{12}$ and $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \cong \mathbb{Z}_4$. Then the left cosets of H are

$$\begin{gathered}\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}\\ \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\}\\ \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\}.\end{gathered}$$

> **Question 4.4.19.** Find the left cosets if $H \cong \mathbb{Z}_3$.

Again, notice that $|G| = |G/H| \times |H| = 12$.

Remark 4.4.20 (Quotient groups) — Noticing that $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ as sets should raise the question "when is there a natural operation to turn G/H into a group?" It turns out that there often is, but not necessarily. Working out when there is will be the first thing we tackle when we return to groups.

Notice that we sometimes have $g_1H = g_2H$ even if $g_1 \neq g_2$. Thankfully, we can characterise when this happens.

Lemma 4.4.21 (Coset equality lemma)

Let $H \leq G$ and $g, k \in G$. Then

$$gH = kH \iff g^{-1}k \in H.$$

Proof. ($\Rightarrow$). Suppose $gH = kH$. As $e \in H$, $k \in kH = gH$. Thus there is a $h \in H$ such that $k = gh \iff g^{-1}k = h \in H$.
($\Leftarrow$). Suppose that $g^{-1}k \in H$, so let $h_0 = g^{-1}k$. Then $kH = gh_0H \subseteq gH$. Also, $gH = kh_0^{-1}H \subseteq kH$, so by double inclusion, $gH = kH$. □

Notice that $g \sim k \iff gH = kH \iff g^{-1}k \in H$ is an equivalence relation on G. (It is clearly symmetric and reflexive, and slightly-less-clearly transitive.) That motivates the following lemma.

Lemma 4.4.22 (Cosets partition G)

Let $H \leq G$. Then G/H is a partition of G.

Proof. As noted above, $\sim$ defined by $g \sim k \iff gH = kH$ is an equivalence relation. Thus note:

$$\begin{aligned}\overline{g} &= \{k : g \sim k\} = \{k : g^{-1}k \in H\} = \{k : g^{-1}k = h \text{ for some } h \in H\}\\ &= \{k : k = gh \text{ for some } h \in H\} = gH.\end{aligned}$$

Hence the equivalence classes are the left cosets, giving our result by Theorem 2.2.21 (Equivalence classes ARE partitions). □

Also, looking at our examples, it looks like we should have $|gH| = |H|$ for any g. This is also fairly easy to prove.

Lemma 4.4.23 (Cosets are equinumerous)
For any group G, any subgroup $H \leq G$, and any $g \in G$, $|H| = |gH|$.

Proof. For any g, the map $\varphi : H \to gH$ by $\varphi(h) = gh$ is a bijection. It is injective by Proposition 4.1.16 (Cancellation law), and surjective by the definition of gH. Hence $|H| = |gH|$. □

Now Lagrange's theorem is a trivial result!

Theorem 4.4.24 (Lagrange's theorem)
Let G be a finite group. For any subgroup $H \leq G$, $|H|$ divides $|G|$.

Proof. Use the above lemmas to show $|G| = |G/H| \times |H|$. □

§4.4.ii. Order of an element

There are a few trivial corollaries of Lagrange's theorem. First, let us define the worst named term in group theory.

Definition 4.4.25. Let G be a group, and $g \in G$. Suppose that there is an $n \in \mathbb{N}$ such that $g^n = e$. Then we say that the **order** of g, written $o(g)$, is the *smallest* such n. If no such n exists, we say that g is of infinite order.

> **Question 4.4.26.** What can we say if $o(g) = 1$?

There are a lot of very obvious facts, that I legally have to prove for you.

Proposition 4.4.27 (Order of finite groups)
Let G be a finite group, and $g \in G$. Then $o(g)$ is finite.

Proof. Consider the sequence $g, g^2, g^3, \ldots$. As G is finite, some element must repeat; suppose $g^i = g^j$, where $i < j$. Then $g^{j-i} = e$, so there is an n such that $g^n = e$. Hence there is a smallest such n, which is the order. □

Here's the most important use of element orders, and the reason they have that name. To check your understanding, I've left it as an exercise.

Exercise 4.4.28 (Orders and cyclic subgroups)
Let G be a group, and $g \in G$. Show that $|\langle g \rangle| = o(g)$.

Then we get the four cornerstone results of element orders.

Proposition 4.4.29 (Element orders)

Let G be a finite group and $g \in G$.

(i) $g^n = e$ if and only if $o(g) \mid n$.

(ii) $o(g) \mid |G|$.

(iii) $g^{|G|} = e$.

(iv) $o(g^k) \mid o(g)$.

Proof. (i) Suppose $n = ko(g)$. Then

$$g^n = \left(g^{o(g)}\right)^k = e^k = e.$$

Suppose $g^n = e$. Then we can find $q, r \in \mathbb{Z}$ with $0 \leq r < o(g)$ such that $n = qo(g) + r$ by Exercise 2.2.25 (The division algorithm). Then

$$g^r = g^{n-qo(g)} = g^n \left(g^{o(g)}\right)^q = ee^q = e,$$

so the minimality of $o(g)$ means that $r = 0$. Hence $n = qo(g)$.

(ii) $\langle g \rangle \leq G$, so apply Lagrange's theorem.

(iii) Apply (i) and (ii).

> **Question 4.4.30.** Check that $\langle g^k \rangle \leq \langle g \rangle$ and apply Lagrange's theorem.

□

Exercise 4.4.31 (Homomorphisms and order)

Let φ be a homomorphism. Show that $o(\varphi(g))$ divides $o(g)$. What happens if φ is bijective, and why is it obvious?

§4.5. Classification of finite groups

One of the biggest areas of study of group theory is the classification of groups. Image you know some information about a group G - say that it has order 10, and only 1 self-inverse element. Can you uniquely identify the group (up to isomorphism)? It turns out that in this case you can: $G \cong \mathbb{Z}_2 \times \mathbb{Z}_5$. What if it was order 20? Then it's much harder to tell.

In general, answering the question "how much information is needed to determine a group" is very difficult. We've already seen that group presentations aren't the way to go. However, there are some instances in which we can do very well. Most of these facts rely on Lagrange's theorem, and clever arguing about subgroups. We will stick to finite groups as they are much easier to handle. Also, to show why each theorem is interesting, I will also state (almost) everything in terms of symmetry.

We have already seen one very simply theorem.

Proposition 4.5.1 (Cyclic groups are $\mathbb{Z}_n$)
Let G be a cyclic group.

(i) If $|G| = n$ is finite, then $G \cong \mathbb{Z}_n$.

(ii) If G is infinite, then $G \cong \mathbb{Z}$.

We have two easy conditions for when we can state that a group is cyclic.

Proposition 4.5.2 (Elements of order $|G|$)
Let G be a finite group and $g \in G$. If $o(g) = |G| = n$, then $G \cong \mathbb{Z}_n$.

Remark 4.5.3 — Suppose an object has n symmetries. Suppose we pick one symmetry, and repeat it's action $n-1$ times. If we still haven't gotten back to where we started, then the only symmetries of the object are rotations about the same axis (or a higher dimensional analogue).

Proof. Consider $\langle g \rangle \leq G$. As $|\langle g \rangle| = o(g) = |G|$, we have $\langle g \rangle = G$, so G is cyclic. □

For this next one, we just need to know $|G|$.

Proposition 4.5.4 (Groups of prime order)
Let G be a group with $|G| = p$ prime. Then $G \cong \mathbb{Z}_p$.

Remark 4.5.5 — Suppose an object has a prime number of symmetries. Then they must be rotations about a fixed axis.

Proof. As $|G| = p \geq 2$, there is a non-identity element g. But by Lagrange's theorem, $o(g) \neq 1$ must divide p, so $o(g) = p = |G|$, so $G \cong \mathbb{Z}_p$. □

Proposition 4.5.6 (Cauchy's theorem)
Let G be a group with $|G| = 2n$. Then G contains a self-inverse element.

Remark 4.5.7 — Technically, Cauchy's theorem states that, for any prime p which divides $|G|$, G has an element of order p. We aren't quite ready to prove that yet, however.

I really like this proof.

Proof. Define the relation $\sim$ on G by $x \sim y$ if $x = y$ or $x = y^{-1}$. Clearly $\sim$ is symmetric, reflexive and transitive, so it is an equivalence relation. Then $\overline{x} = \{x\}$ if x is self-inverse, and $\overline{x} = \{x, x^{-1}\}$ else.
Suppose there are k equivalence classes of size 2, and m of size 1. As the equivalence classes partition G,

$$2k + m = |G| = 2n.$$

But then m must be even. As $\overline{e} = \{e\}$, $m \geq 1$ so by evenness $m \geq 2$. Then there must be at least one other self-inverse element. □

These next two have much trickier proofs, that are far more reminiscent of most classification proofs.

§4.5.i. Self-inverse groups

Theorem 4.5.8 (Self-inverse groups)

Let G be a group with every element self-inverse; that is, for all $g \in G$, $g^2 = e$. Then $G \cong (\mathbb{Z}_2)^n$ for some n.

Remark 4.5.9 — I'll leave this one up to you - which objects can you think of whose symmetry group is $(\mathbb{Z}_2)^n$?

The steps of the proof we will use are as follows:

- Prove that G is abelian.
- Show that, for any subgroup H and $g \in G \setminus H$, $K = H \cup gH$ is a subgroup.
- Show $K \cong H \times \mathbb{Z}_2$.
- Show $G \cong (\mathbb{Z}_2)^n$.

This may not be the most efficient proof - I came up with it myself.

Proof. Suppose $x, y \in G$. Then

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$

so G is abelian.

Let H be any subgroup of G, and fix any $g \in G \setminus H$. Let $K = H \cup gH$, and we apply the subgroup test.

- First, $e \in H$ so $e \in K$.
- Suppose $x, y \in K$. Then $x = g^{a_1}h_1$, $y = g^{a_2}h_2$ where $h_1, h_2 \in H$ and $a_1, a_2 \in \{0, 1\}$. Then

  $$x^{-1}y = xy = g^{a_1}h_1g^{a_2}h_2 = g^{a_1+a_2}h_1h_2$$

  as G abelian. But $g^{a_1+a_2} \in \langle g \rangle = \{e, g\}$ and $h_1h_2 \in H$ by closure, so either $x^{-1}y = gh_1h_2 \in gH$ or $x^{-1}y = h_1h_2 \in H$. Hence $x^{-1}y \in K$.

Thus by the subgroup test, $K \leq G$.

Note that as $g \in G \setminus H$, $gh \notin H$ for all $h \in H$. Hence $k \in K$ can be uniquely written in the form $k = g^a h$ where $a \in \{0, 1\}$ and $h \in H$. Thus define

$$\varphi : K \to H \times \mathbb{Z}_2 \text{ by } \varphi\left(g^a h\right) = \left(h, \overline{a}\right).$$

We can check that φ is a homomorphism:

$$\varphi\left(g^{a_1}h_1g^{a_2}h_2\right) = \varphi\left(g^{a_1+a_2}h_1h_2\right) = \left(h_1h_2, \overline{a_1 + a_2}\right) = \left(h_1, \overline{a_1}\right)\left(h_2, \overline{a_2}\right) = \varphi\left(g^{a_1}h_1\right)\varphi\left(g^{a_2}h_2\right).$$

We can see that $\ker\varphi = \{e\}$ so φ is injective by Exercise 4.4.13 (Kernels of injective homomorphisms). Also, φ is surjective as any $(h, \overline{a}) \in H \times \mathbb{Z}_2$ gets mapped to by $g^a h$. Hence φ is bijective and so an isomorphism. Thus $K \cong H \times \mathbb{Z}_2$.

Finally, we proceed by induction on $|G|$. If $|G| = 1$, then

$$G = \{e\} \cong (\mathbb{Z}_2)^0 .$$

Suppose $|G| > 1$, and that for any group A with $1 \leq |A| \leq |G|$, and $x^2 = e$ for all $x \in A$, there is an n_A such that $A \cong (\mathbb{Z}_n)^{n_A}$.
Then let $H < G$ be a maximal proper subgroup; that is, a subgroup of the largest possible order. (This must exist as $|H| < |G|$, so there are only finitely many possible values of $|H|$.) Fix any $g \in G \setminus H$, and consider $\langle g, H\rangle$. As $H \subseteq \langle g, H\rangle$, and $g \in \langle g, H\rangle$, $|H| < |\langle g, H\rangle|$. Thus, by the maximality of H, $\langle g, H\rangle = G$. As G is abelian,

$$\langle g, H\rangle = \{g^r h : r \in \mathbb{Z},\, h \in H\} = \{h : h \in H\} \cup \{gh : h \in H\} = H \cup gH.$$

Thus $G = H \cup gH \cong H \times \mathbb{Z}_2$. But by our inductive hypothesis, $H \cong (\mathbb{Z}_2^{n_H})$, so we get

$$G \cong H \times \mathbb{Z}_2 = (\mathbb{Z}_2)^{n_H} \times \mathbb{Z}_2 \cong (\mathbb{Z}_2)^{n_H+1} .$$

□

§4.5.ii. Groups of order 2p - approach 1

We can use that result to prove this next one, which is one of my favourites.

Theorem 4.5.10 (Groups of order $2p$)
Let G be a group with $|G| = 2p$, $p \geq 3$ prime. Then either $G \cong \mathbb{Z}_{2p}$ or $G \cong D_{2p}$.

Remark 4.5.11 — Suppose an object has $2p$ symmetries. Then these either correspond the the symmetries of a p-gon, or the rotations of a $2p$-gon.

Proof. Suppose G is not cyclic. We then want to prove that $G \cong D_{2p}$.
By Lagrange's theorem, the possible orders of an element in G are $1, 2, p$ $2p$. We then have two easy cases to consider.

(a) If G has an element of order $2p$, G is cyclic by Proposition 4.5.2 (Elements of order $|G|$).

(b) If G only has elements of order 1, $G = \{e\}$ so $|G| = 1 \neq 2p$.

(c) If G has only elements of order 1 and 2, by Theorem 4.5.8 (Self-inverse groups), $G \cong (\mathbb{Z}_2)^n$ for some n. But then $|G| = 2^n$, but we know $|G| = 2p$, $p \geq 3$, so this is a contradiction.

Thus, G must have an element y of order p but no element of order $2p$. Also, by Proposition 4.5.6 (Cauchy's theorem), G has an element x of order 2.
By Propostion 4.4.29 (iv) (Element orders), $o(y^k) \,|\, o(y) = p$ for all k. Thus, as p is prime, $o(y^k) = p$ so long as $y^k \neq e$. Thus, by considering the orders of elements,

$$x \notin \langle y\rangle = \{e, y, y^2, \ldots, y^{p-1}\}.$$

Thus, by Lemma 4.4.22 (Cosets partition G), and the fact that $|\langle y\rangle| = |x\,\langle y\rangle| = p$,

$$G = \langle y\rangle \cup x\,\langle y\rangle = \{e, y, y^2, \ldots, y^{p-1}, x, xy, xy^2, \ldots, xy^{p-1}\}.$$

Now, consider the element yx. Clearly $yx \notin \langle y \rangle$ as $x \notin \langle y \rangle$, so $yx \in x \langle y \rangle$. Thus there is a $1 \leq j < p$ such that $yx = xy^j$. Then

$$(yx)^2 = (yx)(xy^j) = y^{j+1}.$$

Hence for any k,

$$(yx)^{2k} = y^{k(j+1)} \in \langle y \rangle , \quad (yx)^{2k+1} = y^{k(j+1)}yx = y^{kj+k+1}x \notin \langle y \rangle .$$

Thus yx must have even order as $e \in \langle y \rangle$. In particular, we get that $o(yx) = 2$ so $j = p - 1$. Hence $yx = xy^{p-1}$, and we have the presentation for G

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

□

§4.5.iii. Optional - Groups of order 2p - approach 2

There is another proof of this result. The last way was the one I was taught, so is probably the best. This a method I concocted myself (although it is inspired by a proof I saw elsewhere). It requires a lemma, which I will leave as a nice exercise.

Exercise 4.5.12 (Size of HK)

Let G be a finite group, and $H, K \leq G$ be subgroups. Show that

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

where as before $HK = \{hk : h \in H,\ k \in K\}$.

Hint: show that each element of HK can be written in the form hk in exactly $|H \cap K|$ ways. Hence there are $|HK|\,|H \cap K|$ products of the form hk.

Theorem 4.5.13 (Groups of order $2p$)

Let G be a group with $|G| = 2p$, $p \geq 3$ prime. Then either $G \cong \mathbb{Z}_{2p}$ or $G \cong D_{2p}$.

Remark 4.5.14 — Suppose an object has $2p$ symmetries. Then these either correspond the the symmetries of a p-gon, or the rotations of a $2p$-gon.

Proof. As before, suppose G is not cyclic. We then want to prove that $G \cong D_{2p}$. By the same reasoning as before, G must have an element y of order p but no element of order $2p$. Note

$$|\langle y \rangle| = \left|\{e, y, y^2, \ldots, y^{p-1}\}\right| = p < |G| .$$

Thus we have an $x \in G \setminus \langle y \rangle$, so that $\langle x \rangle \neq \langle y \rangle$. By Lemma 4.4.22 (Cosets partition G),

$$G = \langle y \rangle \cup x \langle y \rangle = \{e, y, y^2, \ldots, y^{p-1}, x, xy, xy^2, \ldots, xy^{p-1}\} = \langle x, y \rangle .$$

Recall that by Proposition 4.3.13 (i) (Combining subgroups), $\langle x \rangle \cap \langle y \rangle$ is a subgroup of $\langle y \rangle$. Thus by Lagrange's theorem, $|\langle x \rangle \cap \langle y \rangle|$ divides $|\langle y \rangle| = p$, so $|\langle x \rangle \cap \langle y \rangle| = 1$ or p. But as $\langle x \rangle \neq \langle y \rangle$, we must have $|\langle x \rangle \cap \langle y \rangle| = 1$. By Exercise 4.5.12 (Size of HK),

$$|\langle x \rangle \langle y \rangle| = \frac{|\langle x \rangle|\,|\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = |\langle x \rangle|\,|\langle y \rangle| = p\,|\langle x \rangle| .$$

But we need $|\langle x\rangle \langle y\rangle| \le |G| = 2p$, so $|\langle x\rangle| \le 2$. As $x \ne e$, we get $|\langle x\rangle| = o(x) = 2$. Hence, for any $x \notin \langle y\rangle$, $o(x) = 2$. Also, for any such x, $xy \notin \langle y\rangle$, so $o(xy) = 2$. Hence

$$xy = (xy)^{-1} = y^{-1}x^{-1} = y^{-1}x,$$

so G has presentation

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

□

One fun other exercise about HK:

Exercise 4.5.15 (Product of disjoint subgroups)
Let G be an abelian group, and $H, K \le G$ be subgroups. If $H \cap K = \{e\}$, then $HK \cong H \times K$.

§4.5.iv. Small groups

Notice that we now have enough to list almost all of the groups of order less than 12.

- Order 1: only $\{1\}$
- Order $2, 3, 5, 7, 11$: only $\mathbb{Z}_p$
- Order $6, 10$: only $\mathbb{Z}_{2p}$ and D_{2p} (note $S_3 \cong D_6$)
- Order $4, 8, 9$: unknown.

Orders 8 and 9 are hard to prove. It turns out that there are only two groups of order 9, $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$, but 5 of order 8:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad D_8, \quad Q_8,$$

where

$$Q_8 = \left\langle a, b : a^4 = b^4 = e,\ a^2 = b^2,\ ba = a^3 b \right\rangle.$$

Order 4, however, we can easily crack.

Proposition 4.5.16 (Groups of order 4)
The only groups of order 4 are $\mathbb{Z}_4$ and $\mathbb{Z}_3 \times \mathbb{Z}_2$.

Note that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is often called the **Klein 4-group** and written V_4 or K_4.

> **Question 4.5.17.** Explain why V_4 is the symmetry group of a rectangle by interpreting it as the subgroup $V_4 \le D_8$.

> **Remark 4.5.18 —** Suppose an object has 4 symmetries. Then it either has the symmetry group of a rectangle, or the rotational symmetry group of a square.

Proof. Let G be a group of order 4. The possible orders of a non-identity element are 2 or 4.

- Suppose there is an element of order 4. Then G is cyclic, so $G \cong \mathbb{Z}_4$.

- Suppose that all non-identity elements are order 2. Then by Theorem 4.5.8 (Self-inverse groups), $G \cong (\mathbb{Z}_2)^n$, so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

□

9 is nearly not too bad. We will prove a general result for groups of order p^2 when we return to groups, but here is a challenge if you want it.

Exercise 4.5.19 (Groups of order p^2)
Let G be an abelian group of order p^2. Show that either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

There are a lot of ways of solving this one. One neat way ususes Exercise 4.5.15 (Product of disjoint subgroups) if you did that one, but you can find a lot of other ways too.

Remark 4.5.20 (Groups of order p^2) — You can actually show fairly quickly that any group of order p^2 is abelian, but it requires a few concepts that I didn't feel were right to introduce yet.

§4.6. Final exercises

§4.6.i. Some group-based exercises

These are just some results that are sort-of required to prove for yourself in a first course in groups. I don't make the rules, they're nice results. Hints are found at the end of the chapter.

Exercise 4.6.1 (Easy - Cayley's theorem)
Let G be a finite group. Then there is an n such that $G \leq S_n$. (Strictly speaking, there is an n such that G is isomorphic to a subgroup of S_n).

Exercise 4.6.2 (Middle - Cyclic subgroups)
Let G be a cyclic group, and $H \leq G$ a subgroup. Then H is cyclic.

Question 4.6.3 (Subgroups of $\mathbb{Z}$)**.** Find two ways of showing that the only subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$.

Exercise 4.6.4 (Hard - Elements of prime order)
Let p be a prime and G a finite group. Then the number of elements of G of order p is a multiple of $p - 1$.

Question 4.6.5 (Groups of order 35)**.** Deduce that a group of order 35 has an element of order 5 and an element of order 7.

Exercise 4.6.6 (Symmetry groups)
Find the proper (i.e. rotational) symmetry groups of a tetrahedron, and of a cube.

Exercise 4.6.7 (Intro to representation theory)
Let G be a finite group. Show that there is an n such that G is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

§4.6.ii. Some fun exercises

I like these. You can too. No hints for these though.

Exercise 4.6.8 (Geometric homomorphisms)
Show that there are 5 homomorphisms $\mathbb{Z}_5 \to \mathbb{C}^*$, but only 2 $D_{10} \to \mathbb{C}^*$, even though $\mathbb{Z}_5 < D_{10}$.

Exercise 4.6.9 (Fibonacci fun)
Let p be a prime, and $F_1 = F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$ be the Fibonacci sequence. Prove that $F_{2p(p^2-1)}$ is divisible by p.

Exercise 4.6.10 (Bob's a loser)
Alice and Bob got abducted by aliens to be experimented on. As a twisted version of a doctor's sticker, they each got an object with exactly 1000 symmetries. However, Bob was a whiny bitch during the procedures, so the aliens removed one, but only one, of his symmetries.

Bob claims that his and Alice's objects are entangled, so that whenever Alice performs a transformation on her object, his also transforms in a predictable way. Show that Bob is full of shit: his object doesn't transform when she transforms hers.

Exercise 4.6.11 (Very hard)
There are n markers, each with one side white and the other side black. In the beginning, these n markers are aligned in a row so that their white sides are all up. In each step, if possible, we choose a marker whose white side is up (but not one of the outermost markers), remove it, and flip the closest marker to the left of it and also reverse the closest marker to the right of it.
Prove that if $n \equiv 1 \pmod 3$, it's impossible to reach a state with only two markers remaining. (In fact the converse is true as well.)

§4.6.iii. Hints for final exercises

- Cayley's theorem: consider the map $a \mapsto ga$ for some $g \in G$.

- Cyclic subgroups: Let $G = \langle g \rangle$, and define $n = \min \left\{ k > 0 : g^k \in H \right\}$.
- Elements of prime order: define $S = \{g \in G : o(g) = p\}$ and define $\sim$ on S by $g \sim h \iff \langle g \rangle = \langle h \rangle$.
- Symmetry groups: no hint.
- Intro to representation theory: consider Cayley's theorem.