4. Groups and Symmetry

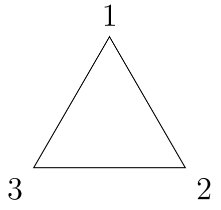
Most algebraic objects are mathematicians attempt to unify and generalise some type of object. Rings, which we will meet next, are the generalisation of a “number system” like $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ or $\mathcal{M}_n(\mathbb{R})$. Vector spaces generalise the idea of Euclidean vectors.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

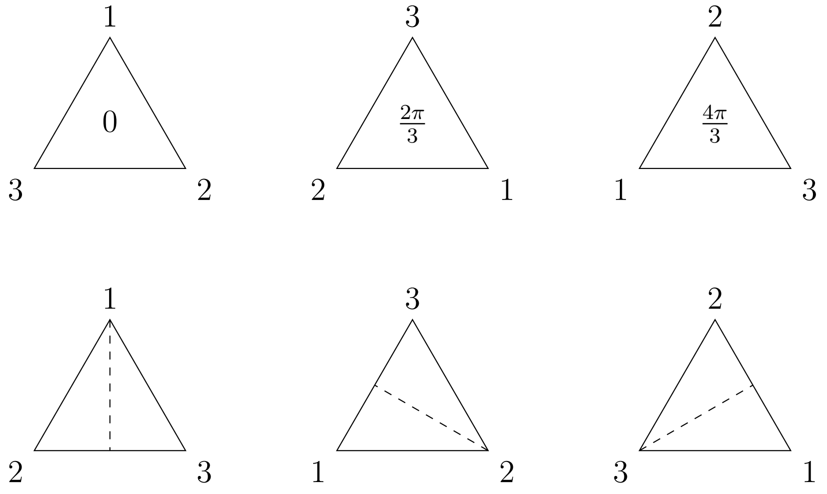
If you want to formalise something, say symmetry, you have two (realistically more) options:

- *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

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

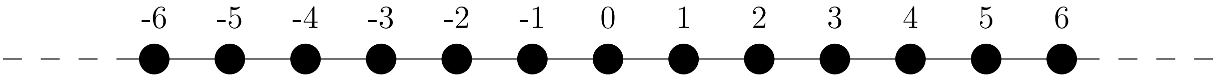
as a *symmetric* function, because

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

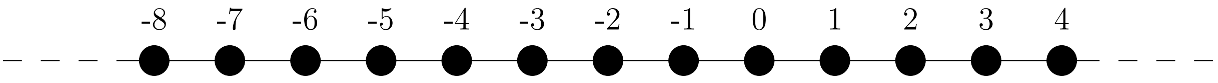
That is, the function is the same, regardless of which input is which, so the *structure* of the output is preserved under the *transformation* of shuffling the inputs. The symmetries of this function are then the same as the "symmetries" of shuffling 3 objects. It might be a little strange to think 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.

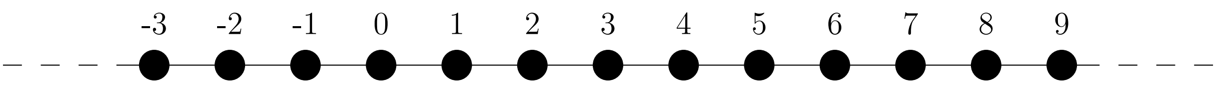
Consider this number line:



After shifting two to the right, we get

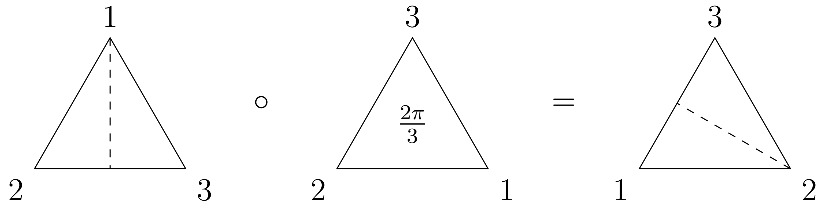


You can see that, by our slightly abstracted definition, this is definitely a symmetry. Similarly, so is shifting to the right by 3 units.



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

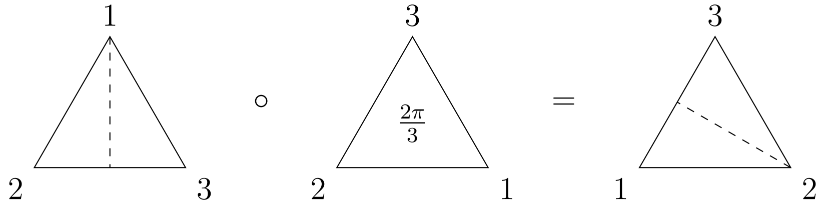
- We want every element to have an inverse.

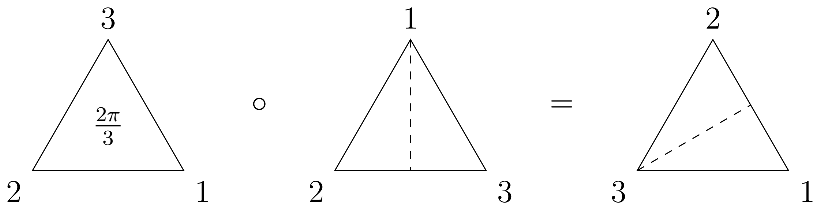
Some more thinking should tell us that we want one more thinking.

- 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)

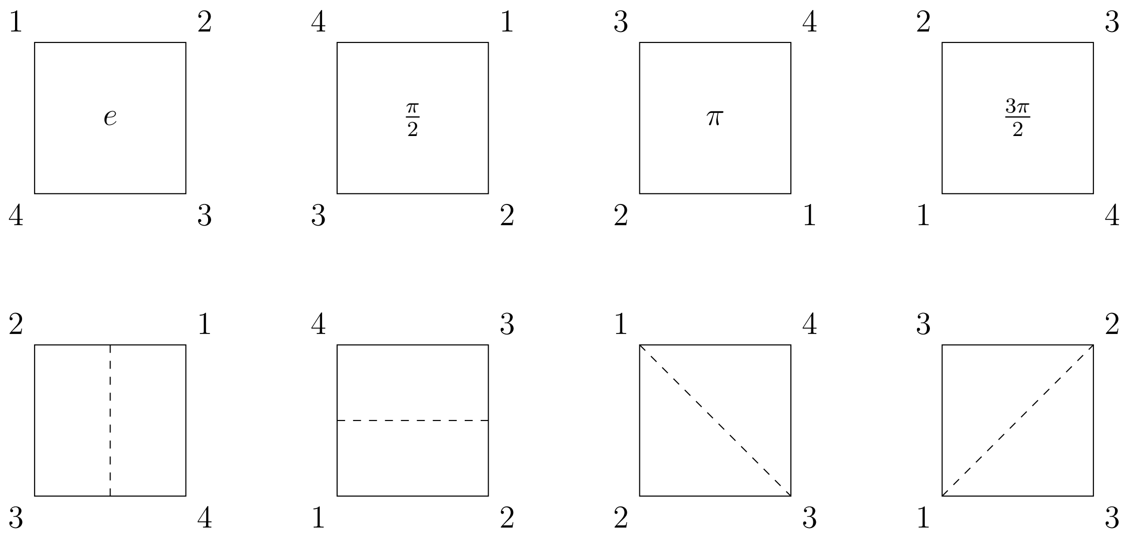
$(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$ and $(\mathbb{Q} \setminus \{0\}, \times)$ are all abelian groups, denoted $\mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^*$ respectively. [Why do we need to remove 0?] $(\mathbb{Z} \setminus \{0\}, \times)$ is not a group, as 2 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.

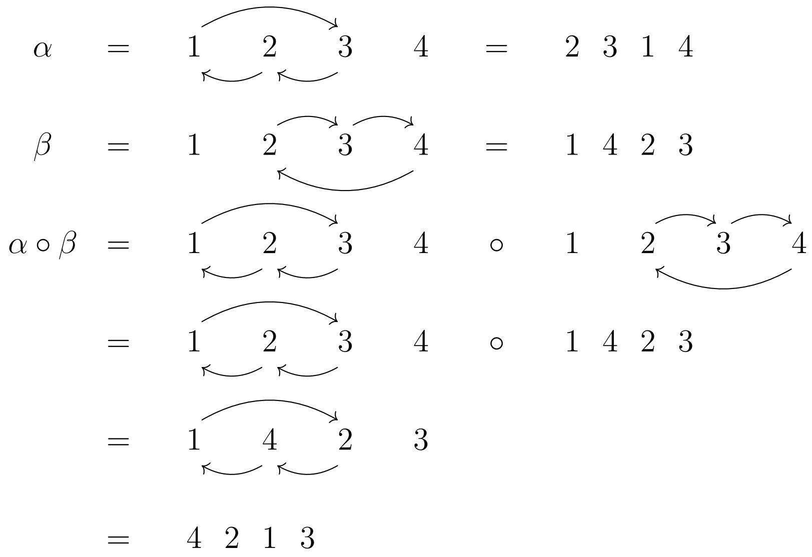
Example 4.1.9 (Dihedral groups)

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.


α = 1 2 3 4 = 2 3 1 4
β = 1 2 3 4 = 1 4 2 3
$\alpha \circ \beta$ = 1 2 3 4 ∘ 1 2 3 4
= 1 2 3 4 ∘ 1 4 2 3
= 1 4 2 3
= 4 2 1 3

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 $x \in \mathbb{Z}_p^*$, $\mathrm{hcf}(x, p) = 1$. 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.