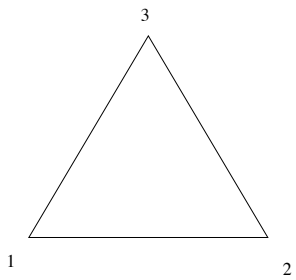
Chapter 1

The idea of a group

One of our goals in this class is to make precise the idea of symmetry, which is important in math, other parts of science, and art. Something like a square has a lot of symmetry, but circle has even more. But what does this mean? One way of expressing this is to a view a *symmetry of a given shape as a motion which takes the shape to itself.* Let us start with the example of an equilateral triangle with vertices labelled by $1, 2, 3$.



We want to describe all the symmetries, which are the motions (both rotations and flips) which takes the triangle to itself. First of all, we can do nothing. We call this I, which stands for identity. In terms of the vertices, I sends $1 \to 1$, $2 \to 2$ and $3 \to 3$. We can rotate once counterclockwise.

$$R_+ : 1 \to 2 \to 3 \to 1.$$

We can rotate once clockwise

$$R_- : 1 \to 3 \to 2 \to 1.$$

We can also flip it in various ways

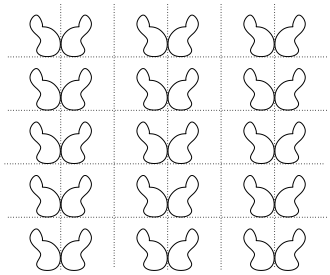
$$F_{12} : 1 \to 2, 2 \to 1, 3 \text{ fixed}$$

$$F_{13} : 1 \to 3, 3 \to 1, 2 \text{ fixed}$$

$$F_{23} : 2 \to 3, 3 \to 2, 1 \text{ fixed}$$

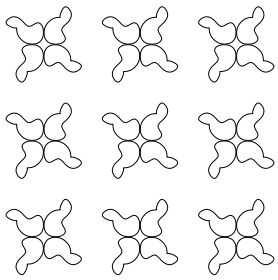
We will say more about this example and generalizations for regular polygons later. In the limit, as the number of vertices go to infinity, we get the circle. This has infinitely many symmetries. We can use any rotation about the center, or a reflection about a line through the center.

Another example which occurs in classical art and design (mosaics, wallpaper....) and two dimensional crystals is a repetetive pattern in the plane such as the one drawn below.



We imagine this covering the entire plane; the grid lines are not part of the pattern. Then there are infinitely many symmetries. We can translate or shift all the "ducks" up or down by one square, or left or right by two squares. We can also flip or reflect the pattern along vertical lines.

Here is another pattern below.



This has translational symmetries as before, but no flipping symmetries. Instead, if the plane is rotated by 90° about any point where four ducks meet, the pattern is preserved. One might ask can we replace four by five, or some arbitrary number of, ducks and still get an infinitely repeating symmetric pattern as above? The answer surprisingly is no. We will prove this later.

The study of symmetry leads to an algebraic structure. To simplify things, let us ignore flips and consider only rotational symmetries of a circle C of radius r. To simplify further, let us start with the limiting case where $r \to \infty$. Then C becomes a line L, and rotations correspond to translations. These can be described precisely as follows. Given a real number $x \in \mathbb{R}$, let $T_x : L \to L$

denote the symmetry which takes a point p on L and moves it by a distance x to the right if $x > 0$, fixes it if $x = 0$, or moves it to the left if $x < 0$. We can see that if we translate by x and then by y, it is the same as translating by $x + y$. So addition emerges naturally with this context. Basic laws of algebra have a natural meaning here: Translating by x and then by 0 is the same as translating by x, or in symbols

$$x + 0 = x \quad (\ 0 \text{ is the identity})$$

Translating by x and then y is that same translating y and then x, or

$$x + y = y + x \quad \text{(commutative law)}$$

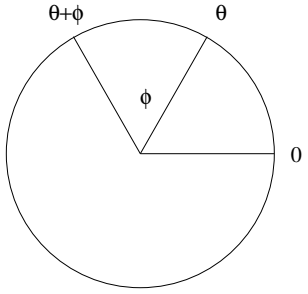
We can always translate back to where we started because

$$\text{Given } x, \text{ we can find } y \text{ with } x + y = 0 \quad \text{(existence of the inverse)}$$

Finally, translating by three numbers x, y, z in succesion is the same as translating by $x + y$ and then z, or x then $y + z$. That is

$$(x + y) + z = x + (y + z) \quad \text{(associative law)}$$

Now we are ready to consider the rotational symmetries of the circle C of finite radius. Let $R_\theta : C \to C$ be the rotation (counterclockwise) through an angle $\theta \in [0, 2\pi) = \{x \in \mathbb{R} \mid 0 \leq x < 2\pi\}$ measured in radians. Note that we can identify C with the set of angles $[0, 2\pi)$ as well. Now we define addition in C as follows: given $\theta, \phi \in C$, let $\theta \oplus \phi$ be given by rotating θ by the additional angle ϕ.



Here are a few simple examples

$$\pi/2 \oplus \pi/2 = \pi$$

$$\pi \oplus \pi = 0$$

In general, we can see that

$$\theta \oplus \phi = \begin{cases} \theta + \phi & \text{if } \theta + \phi < 2\pi \\ \theta + \phi - 2\pi & \text{if } \theta + \phi \geq 2\pi \end{cases}$$

And it will be convenient to adopt this last equation as the official definition.

At first it may seem like a strange operation, but notice that many familiar rules apply:

Lemma 1.1. *If $\theta \in C$, then $\theta \oplus 0 = \theta$.*

Proof. Since $\theta < 2\pi$, $\theta \oplus 0 = \theta + 0 = \theta$ □

Lemma 1.2. *If $\theta, \phi \in C$, then $\theta \oplus \phi = \phi \oplus \theta$.*

Proof. If we compare

$$\phi \oplus \theta = \begin{cases} \phi + \theta & \text{if } \phi + \theta < 2\pi \\ \phi + \theta - 2\pi & \text{if } \phi + \theta \geq 2\pi \end{cases}$$

we see that it is identical to $\theta \oplus \phi$. □

Lemma 1.3. *Given $\theta \in C$, we have $\phi \in C$ such that $\theta \oplus \phi = 0$.*

Proof. We can take $\phi = \ominus\theta = 2\pi - \theta$. □

We omit the proof for now, but the associative law

$$\theta \oplus (\phi \oplus \psi) = (\theta \oplus \phi) \oplus \psi$$

also holds.

So in summary, the set C with the operation $\oplus$ shares the same 4 laws as $\mathbb{R}$ with usual addition: namely the associative and commutative laws, and the existence of identity and inverse. We have a name for such a thing. It is called an *abelian group*, and it will be one of the key concepts in this class. To appreciate the power of this simple set of rules, let us extend a standard result from highschool algebra.

Theorem 1.4. *Suppose that A is any abelian group with operation $+$ and identity 0. For any $a, b \in A$, there is exactly one solution to $x + a = b$.*

Proof. By the axioms, there exists an element that we denote by $-a$ such that $a + (-a) = 0$. Add b to both sides, and use the laws to obtain

$$(b + (-a)) + a = b + (-a + a) = b + 0 = b$$

Therefore $x = b + (-a)$ gives a solution. Suppose that x is any solution to $x + a = b$. Then adding $-a$ to both sides and use the associative law

$$x = x + (a + (-a)) = (x + a) + (-a) = b + (-a)$$

□

We are being a bit pedantic in our notation, since this was the first abstract proof. In the future, we will just write $b - a$ instead of $b + (-a)$.

We want to return to the first example of the triangle, but first we should clarify what kind of mathematical objects we are dealing with. Given a set X,

a permutation of X is a *one to one onto function* $f : X \to X$. Recall that function, or map, mapping or transformation $f : X \to Y$ is a rule for am taking element x of one set X to an element $f(x) \in Y$; it is one to one and onto if every element of Y equals $f(x)$ for exactly one $x \in X$. The symmetries R_+ etc. are just permutations of $\{1, 2, 3\}$. Here are some abstractly given permutations of the set $\{1, 2, 3, 4\}$.

$$f(1) = 2,\ f(2) = 3,\ f(3) = 1,\ f(4) = 4$$

$$g(1) = 1,\ g(2) = 1,\ g(3) = 4,\ g(4) = 3$$

The function h defined by

$$h(1) = h(2) = 1,\ h(3) = h(4) = 2$$

is not a permutation. It may be helpful to visualize these

$$f = \left\{ \begin{array}{ccc} 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 1 \\ 4 & \to & 4 \end{array} \right. = \left\{ \begin{array}{ccc} 2 & \leftarrow & 1 \\ 3 & \leftarrow & 2 \\ 1 & \leftarrow & 3 \\ 4 & \leftarrow & 4 \end{array} \right. ,$$

$$g = \left\{ \begin{array}{ccc} 1 & \to & 2 \\ 2 & \to & 1 \\ 3 & \to & 4 \\ 4 & \to & 3 \end{array} \right. = \left\{ \begin{array}{ccc} 2 & \leftarrow & 1 \\ 1 & \leftarrow & 2 \\ 4 & \leftarrow & 3 \\ 3 & \leftarrow & 4 \end{array} \right.$$

Since the above notations are a bit cumbersome, we often write this in *permutation notation* as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Note these are **not** matrices. There is yet another notation, which a bit more compact. A cycle of a permutation is a sequence of elements $a \to f(a) \to f(f(a)) \ldots \to a$ For f, the cycles are $1 \to 2 \to 3 \to 1$ and $4 \to 4$; for g, $1 \to 2 \to 1$ and $3 \to 4 \to 3$. To specify a permutation it is just enough to list the cycles as in

$$f = (123)(4),\ g = (12)(34)$$

Cycles consisting of just one element are usually omitted, so we would write $f = (123)$. Note that (312) would also represent f.

Given two permutations $f : X \to X$ and $g : X \to X$. We can *multiply* them by *composing* them as functions. In the examples above,

$$f \circ g(1) = f(g(1)) = f(2) = 3, \text{ etc.}$$

We usually omit the $\circ$ symbol. More visually

$$fg = \left\{ \begin{array}{ccccc} 3 & \leftarrow & 2 & \leftarrow & 1 \\ 2 & \leftarrow & 1 & \leftarrow & 2 \\ 4 & \leftarrow & 4 & \leftarrow & 3 \\ 1 & \leftarrow & 3 & \leftarrow & 4 \end{array} \right. = \left\{ \begin{array}{ccc} 3 & \leftarrow & 1 \\ 2 & \leftarrow & 2 \\ 4 & \leftarrow & 3 \\ 1 & \leftarrow & 4 \end{array} \right.$$

Note that we use backword arrows because this is consistent with function composition. Some people (and software) use forward arrows, which is easier to work with, but confusing in other ways.

With a bit of practice, this can this read off directly from the permutation symbols

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

We now return to our triangle example.

$$R_+R_+=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=R_-$$

Let's do two flips, F_{12} followed by F_{13}

$$F_{12}F_{13}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=R_-$$

Doing this the other way gives

$$F_{13}F_{12}=R_+$$

Therefore this multiplication is not commutative.

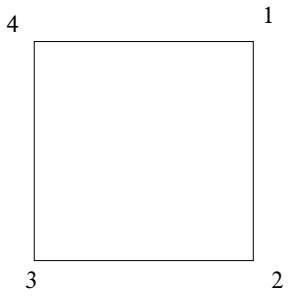
The full multiplication table can be worked out with enough patience as

$\circ$	I	F_{12}	F_{13}	F_{23}	R_+	R_-
I	I	F_{12}	F_{13}	F_{23}	R_+	R_-
F_{12}	F_{12}	I	R_-	R_+	F_{23}	F_{13}
F_{13}	F_{13}	R_+	I	R_-	F_{13}	F_{23}
F_{23}	F_{23}	R_-	R_+	I	F_{12}	F_{13}
R_+	R_+	F_{23}	F_{12}	F_{13}	R_-	I
R_-	R_-	F_{13}	F_{23}	F_{12}	I	R_+

One thing that can be observed from the table is that every element has an inverse, i.e. an element which multiplies with it to give the identity. It is not obvious from the table that the associative law holds, but this is something we will prove later. A *group* is a set with an multiplication, which is associative, has an identity and such that every element has an inverse. We will be clarify the meaning of the axioms later. Suffice it to say that we now have two new examples of groups. One which is abelian and one which isn't.

1.5 Exercises

In the next few exercises, you will study the symmetries of a square with vertices labelled by $1, 2, 3, 4$ as shown



Let

$$I = i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

R be the clockwise rotation

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

and F be the flip

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

1. Show that all the rotations preserving the square are given by $I, R, R^2 = RR$ and R^3. Write these out explicitly in cycle notation.

2. Show that all the flips (including diagonal flips) preserving the square are given by F, FR, FR^2, FR^3. Write these out explicitly in cycle notation.

3. The above 8 rotations and flips is a complete list of all the symmetries of the square. Describe RF in terms of this list. Give an example of a permutation of $\{1, 2, 3, 4\}$ which is not a symmetry of the square.

4. Determine the inverses of the rotations $R, R^2 = RR$ and R^3.

5. Determine the group of symmetries (rotations and flips) of a rectangle which is not a square. Is this abelian?

6. Determine all the symmetries of a regular pentagon. Regular means that all the sides have the same length.

7. (If you forgot what complex numbers are, now is the time to remind yourself.)

   (a) Given $z = a + bi \in \mathbb{C}$, recall that $\bar{z} = a - bi$. Check that $z\bar{z} = a^2 + b^2$, and also that $\bar{z}\bar{w} = \overline{zw}$ for $w = c + di$.

   (b) Let C be the set of complex numbers of the form $a + bi$, where $a^2 + b^2 = 1$. With the help of the previous exercise, prove that if $z \in C$, then $z^{-1} \in C$, and that the product of any two numbers in C is also in C. Conclude that C is a group under multiplication.

(c) Given an angle θ, show that $e^{i\theta} = \cos\theta + i\sin\theta \in C$ and conversely, every element of $z \in C$ is of this form for a unique $\theta \in [0, 2\pi)$. This is another way to turn C into a group which is the *same* as the previous group in an appropriate sense.

Chapter 2

The group of permutations

Recall that a function $f : X \to Y$ is *one to one* if for any pair of distinct elements $x_1, x_2 \in X$, $f(x_1) \neq f(x_2)$. Equivalently, if $f(x_1) = f(x_2)$ then $x_1 = x_2$. f is *onto* if for every $y \in Y$, we can find an $x \in X$ such that $f(x) = y$. An important example of a function is the identity function $id_X : X \to X$ defined by $id_X(x) = x$. This is clearly one to one and onto. If X is understood, we write this as id.

Lemma 2.1. *Suppose that $f : X \to Y$ and $g : Y \to Z$ are functions.*

1. *If f and g are one to one, then so is $g \circ f$.*
2. *If f and g are onto, then so is $g \circ f$.*

Proof. Suppose that f and g are one to one. If $g \circ f(x_1) = g \circ f(x_2)$, then $g(f(x_1)) = g(f(x_2))$. This implies $f(x_1) = f(x_2)$ because g is one to one. Therefore $x_1 = x_2$ because f is one to one. This proves 1.

Suppose that f and g are onto. Given $z \in Z$, we can find $y \in Y$ such that $g(y) = z$ because g is onto. We can also find $x \in X$ such that $f(x) = y$. Therefore $g \circ f(x) = z$. This proves 2. □

Lemma 2.2. *Suppose that $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are functions, then $h \circ (g \circ f) = (h \circ g) \circ f$*

Proof. To be clear two functions are considered to be equal if they produce equal outputs on the same input. Now observe that

$$(h \circ (g \circ f))(x) = h(g(f(x))) = ((h \circ g) \circ f)(x)$$

□

Lemma 2.3. *If $f : X \to Y$ is one to one and onto, there exists a function $f^{-1} : Y \to X$ called the inverse such that $f \circ f^{-1} = id_Y$ and $f^{-1} \circ f = id_X$.*

Proof. For every $y \in Y$, there exists a unique $x \in X$ such that $f(x) = y$. We define $f^{-1}(y) = x$. Then $f^{-1} \circ f(x) = f^{-1}(y) = x$ and $f \circ f^{-1}(y) = f(x) = y$. □

Lemma 2.4. *Given a function $f : X \to Y$, $f \circ id_X = f$ and $id_Y \circ f = f$.*

Proof. The first equation holds because $f \circ id(x) = f(id(x)) = f(x)$. The proof of the second is similar. □

Now come to the key definition.

Definition 2.5. *A group is a set G with an operation $*$ and a special element e satisfying*

1. *The associative law: $(x * y) * z = x * (y * z)$*
2. *e is the identity: $x * e = e * x = x$*
3. *Existence of inverses: given x, there exists y such that $x * y = y * x = e$*

We sometimes say that $(G, *, e)$ is a group we want to specify the operation and identity. Occasionally, we will omit the operation, and simply write xy for $x*y$. We will see in the exercises that each x has exactly one inverse. We denote this by x^{-1}, or sometimes $-x$, depending on the situation.

It is also worth repeating what we said in the first chapter in this context.

Definition 2.6. *An abelian group is a group G for which the commutative law $x * y = y * x$ holds.*

Given a set X, recall that a permutation of X is a one to one onto function $f : X \to X$. Let S_X denote the set of permutations of X. When $X = \{1, 2, \ldots, n\}$, which is the case we will mostly be interested in, we denote this by S_n. Putting the previous lemmas, we get

Theorem 2.7. *S_X becomes a group under composition, with identity given by id.*

S_n is called the *symmetric group on n letters*. Most of you have actually encountered this before, although perhaps not by name, and in particular, you probably already know is that:

Theorem 2.8. *The number of elements of S_n is $n! = 1 \cdot 2 \cdot 3 \cdots n$.*

We will in fact give a proof of this later on. For $n = 3$, we see that S_3 has 6 elements, so it must coincide with the symmetry group of the triangle. For $n = 4$, we have 24 which is much bigger than the symmetries of the square. This a pretty typical. We are often interested not in the whole of S_n, but some interesting piece of it.

Definition 2.9. *Given a group $(G, *, e)$, a subset $S \subset G$ is called a subgroup if $e \in S$, and $x, y \in S$ implies $x * y, x^{-1} \in S$ (one says that S is closed under these operations).*

The definition ensures that if these operations can be restricted to S, we don't leave S.

Proposition 2.10. *A subgroup $S \subset G$ of a group is also a group.*

There is actually nothing to prove. The same laws of G hold for elements of S.

Coming back to permutation notation, we note see that the identity is simply

$$id = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 1 & 2 & 3 & \dots \end{pmatrix}$$

To find the inverse, we simply turn it upside down and then rearrange columns. For example,

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

$$f^{-1} = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

In cycle notation, we simply reverse the cycles

$$f = (243),\ f^{-1} = (342)$$

2.11 Exercises

1. Let X be a nonempty set and let $f : X \to X$ be a function. Prove that f is one to one if and only if there is a function $g : X \to X$ such that $gf = id$; g is called a left inverse. (One direction is easy, and the other will require you to be a bit creative.)

2. Let X be a nonempty set and let $f : X \to X$ be a function. Prove that f is onto if and only if there is a function $g : X \to X$ such that $fg = id$; g is called a right inverse. (People who know some set theory will need to invoke the axiom of choice.)

3. A permutation $f \in S_n$ is a transposition, if it interchanges two numbers, say i and j and fixes everything else, i.e. $f(i) = j, f(j) = i$, $f(x) = x, i \neq x \neq j$, or $f = (ij)$ in cycle notation.

   (a) Check that everything in S_3 is a product of transpositions.

   (b) Check $(12)(34), (123), (1234) \in S_4$ are products of transpositions. Generalizing from these examples, prove that every element of S_4 is a product of transpositions.

4. Given a group $(G, *, e)$, prove that it is has only one identity element. In other words, if $x * e' = e' * x = x$ holds for all x, prove $e' = e$.

5. Given a group $(G, *, e)$,

(a) Prove that every element x as exactly one inverse. We now denote it by x^{-1}.

(b) Prove that $(x * y)^{-1} = y^{-1} * x^{-1}$.

6. Given a group $(G, *, e)$,

   (a) Given $y, z \in G$, prove that there is exactly one $x_1 \in G$ satisfying $x_1 * y = z$ and exactly one $x_2 \in G$ satisfying $y * x_2 = z$.

   (b) Is *always* true that $x_1 = x_2$? If yes, then prove it; if no, then find a *counterexample*, i.e. a group G and elements x_1, x_2, y, z as above with $x_1 \neq x_2$.

7. Let $R = (123)$ and F a transposition in S_3

   (a) Check that $\{I, R, R^2\}$, and $\{I, F\}$, are subgroups of S_3

   (b) Prove that S_3 does not have a subgroup with exactly 4 elements. (If you happen to know Lagrange's theorem, don't use it. Give a direct argument.)

8. Recall that the intersection (respectively union) of two sets $H \cap K$ ($H \cup K$) is the set elements x such that $x \in H$ *and* $x \in K$ (respectively $x \in H$ *or* $x \in K$ – x is allowed to be in both).

   (a) Prove that if H and K are both subgroups of a group G, then $H \cap K$ is a subgroup.

   (b) What about $H \cup K$?