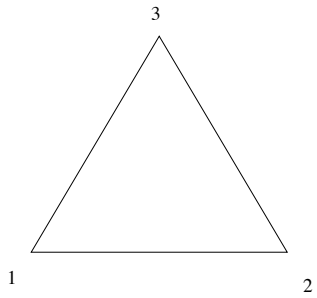
Chapter 2

The symmetric group

Consider the equilateral triangle.



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, call this I. 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

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

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

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

To multiply means to follow one motion by another. For example doing two R_+ rotations takes 1 to 2 and then to 3 etc. So

$$R_+ R_+ = R_+^2 = R_-$$

Let's do two flips, F_{12} followed by F_{13} takes $1 \to 2 \to 2$, $2 \to 1 \to 3$, $3 \to 3 \to 1$, so

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

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

.	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_{13}	F_{23}
F_{13}	F_{13}	R_-	I	R_+	F_{23}	F_{12}
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_+

In exercises, you will study the symmetries of a square with vertices labelled by $1, 2, 3, 4$. But first we need some terminology. Given a set X, say of vertices of triangle, square, or labels for them. A permutation of X is a *one to one onto* function $f : X \to X$. This means to f takes each element of $x \in X$ to another (or perhaps the same) element $f(x) \in X$, and every element of X equals $f(x)$ for exactly one $x \in X$. For examples of permutations of the set $\{1, 2, 3, 4\}$, let

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

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

It may be helpful to visualize this:

$$f = \begin{cases} 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 1 \\ 4 & \to & 4 \end{cases} \quad g = \begin{cases} 1 & \to & 2 \\ 2 & \to & 1 \\ 3 & \to & 4 \\ 4 & \to & 3 \end{cases}$$

Since the above representations 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. Instead of standard functional notation, $f(1) = 2$, it'll be more convenient denote this by

$$1 \xrightarrow{f} 2$$

as above. Think of f some kind of machine which takes an input such as 1, and then spits out the answer 2 We get new permutations by composition, in other words following one by another:

$$1 \xrightarrow{f} 2 \xrightarrow{g} 1$$

so

$$1 \xrightarrow{fg} 1$$

Warning This is opposite of the usual composition rule. So it is easy to get confused.

We can visualize this by splicing the pictures:

$$fg = \begin{cases} 1 & \to & 2 & \to & 1 \\ 2 & \to & 3 & \to & 4 \\ 3 & \to & 1 & \to & 2 \\ 4 & \to & 4 & \to & 3 \end{cases} = \begin{cases} 1 & \to & 1 \\ 2 & \to & 4 \\ 3 & \to & 2 \\ 4 & \to & 3 \end{cases}$$

or in permutation notation,

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

Warning Many authors (including Gallian) multiply permutations in the reverse order to match functional notation.

***

Let S_n denote the set of permutations of $\{1, 2, \ldots, n\}$. It is , called the *symmetric group on n letters*. Most of you have actually encountered this before, although perhaps not by name, in a discrete math, linear algebra, or probability class. In this last case, the elements describe the ways of shuffling a deck of n cards. In linear algebra, you have encountered it in the formula for the determinant which looks something like this

$$\det(a_{ij}) = \sum_{\sigma \in S_n} \pm a_{1\sigma(1)} \ldots a_{n\sigma(n)}$$

We will say more about the sign later on. But note that we almost never use this formula because it's extremely impractical as soon as $n > 3$, because of:

Theorem 2.1. *The number of elements of S_n is $n! = 1 \cdot 2 \cdot 3 \cdots n$.*

We will postpone the proof. In linear algebra class, we learn many alternative methods for computing the determinant which are more efficient. Here is a famous open problem in theoretical computer science: *Find an efficient method for computing the so called permanent of a matrix*

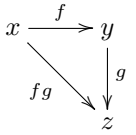
$$\sum_{\sigma \in S_n} a_{1\sigma(1)} \ldots a_{n\sigma(n)}$$

The importance that many other problems in CS would follow from this.

Let us recall some of the special features. This has a special element called the identity which is the function $I(x) = x$, or in permutation notation

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

Given two permutations $f, g \in S_n$, we can form a new permutation $fg \in S_n$ given by composing the functions:



We will often refer to this as multiplication.

Lemma 2.2. *Composition is associative $f(gh) = (fg)h$.*

Proof. Given elements $x, y, z, w \in \{1, \dots, n\}$ such that $x \xrightarrow{f} y$, $y \xrightarrow{g} z$, $z \xrightarrow{h} w$, we have $x \xrightarrow{fg} z$ and therefore $x \xrightarrow{(fg)h} w$. Similarly $y \xrightarrow{gh} w$, so that $x \xrightarrow{f(gh)} w$. Since both $f(gh)$ and $(fg)h$ take x to w, they are equal. □

The identity permutation is the function $i(x) = x$ which does returns the same value it is given. In permutation notation

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

Lemma 2.3. *$if = f$ and $fi = f$*

Proof. We check the first equation

$$if = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 1 & 2 & 3 & \dots \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \dots \\ f(1) & f(2) & f(3) & \dots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \dots \\ f(1) & f(2) & f(3) & \dots \end{pmatrix} = f$$

□

Lemma 2.4. *Given $f \in S_n$, there exists a permutation $g \in S_n$ with $gf = i$ and $fg = i$.*

Proof. Let $X = \{1, 2, 3, \dots, n\}$. SInce f is one to one and onto, given $y \in X$, there exists a unique $x \in X$ with $y = f(x)$. This means that x is determined by y, so we can write $x = g(y)$ for some function g. In our alternate notation, we would write this as $x \xrightarrow{f} y$ and $y \xrightarrow{g} x$. Therefore

$$x \xrightarrow{f} y \xrightarrow{g} x$$

$$y \xrightarrow{g} x \xrightarrow{f} y$$

which means that both fg and gf are the identity. □

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 $x * y = y * x = e$*

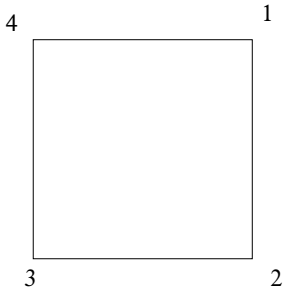
It is also worth repeating what we said in the first chapter in this context.

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

So far we have encountered 3 examples: $\mathbb{R}$ with addition $+$, the circle C with addition $\oplus$ are abelian and S_n is a group, but it is not abelian when $n \geq 3$. We will see many more

2.7 Exercises

Consider a square 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.

2. Show that all the flips (including diagonal flips) are given by F, FR, FR^2, FR^3.

3. The above 8 rotations and flips is a complete list of all the symmetries of the square. Given an example of a permutation in S_4 which is not a symmetry of the square. Describe RF in terms of this list.

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