1. Groups

Suppose that we take an equilateral triangle and look at its symmetry group. There are two obvious sets of symmetries. First one can rotate the triangle through 120°. Suppose that we choose clockwise as the positive direction and denote rotation through 120° as R. It is natural to represent rotation through 240° as R^2, where we think of R^2 as the effect of applying R twice.

If we apply R three times, represented by R^3, we would be back where we started. In other words we ought to include the trivial symmetry I, as a symmetry of the triangle (in just the same way that we think of zero as being a number). Note that the symmetry rotation through 120° anticlockwise, could be represented as R^{-1}. Of course this is the same as rotation through 240° clockwise, so that $R^{-1} = R^2$.

The other obvious sets of symmetries are flips. For example one can draw a vertical line through the top corner and flip about this line. Call this operation $F = F_1$. Note that $F^2 = I$, representing the fact that flipping twice does nothing.

There are two other axes to flip about, corresponding to the fact that there are three corners. Putting all this together we have

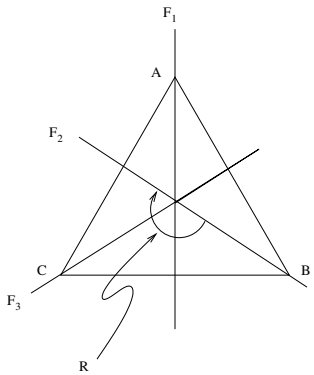

Figure 1. Symmetries of an equilateral triangle

The set of symmetries we have created so far is then equal to

$$\{ I, R, R^2, F_1, F_2, F_3 \}.$$

Is this all? The answer is yes, and it is easy to see this, once one notices the following fact; any symmetry is determined by its action on the vertices of the triangle. In fact a triangle is determined by its vertices, so this is clear. Label the vertices A, B and C, where A starts at the top, B is the bottom right, and C is the bottom left.

Now in total there are at most six different permutations of the letters A, B and C. We have already given six different symmetries, so we must in fact have exhausted the list of symmetries.

Note that given any two symmetries, we can always consider what happens when we apply first one symmetry and then another. However note that the notation RF is ambiguous. Should we apply R first and then F or F first and then R? We will adopt the convention that RF means first apply F and then apply R.

Now RF is a symmetry of the triangle and we have listed all of them. Which one is it? Well the action of RF on the vertices will take

$$\begin{aligned} A &\longrightarrow A \longrightarrow B \\ B &\longrightarrow C \longrightarrow A \\ C &\longrightarrow B \longrightarrow C. \end{aligned}$$

In total then A is sent to B, B is sent to A and C is sent to C. As this symmetry fixes one of the vertices, it must be a flip. In fact it is equal to F_3.

Let us now compute the symmetry FR. Well the action on the vertices is as follows

$$\begin{aligned} A &\longrightarrow B \longrightarrow C \\ B &\longrightarrow C \longrightarrow B \\ C &\longrightarrow A \longrightarrow A. \end{aligned}$$

So in total the action on the vertices is given as A goes to C, B goes to B and C goes to A. Again this symmetry fixes the vertex B and so it is equal to F_2.

Thus $F_3 = RF \neq FR = F_2$.

Let us step back a minute and consider what (algebraic) structure these examples give us. We are given a set (the set of symmetries) and an operation on this set, that is a rule that tells us how to multiply (in a formal sense) any two elements. We have an identity (the symmetry that does nothing). As this symmetry does nothing, composing with this symmetry does nothing (just as multiplying by the number one does nothing).

Finally, given any symmetry there is an inverse symmetry which undoes the action of the symmetry (R represents rotation through 120° clockwise, and R^{-1} represents rotation through 120° anticlockwise, thus undoing the action of R).

Definition 1.1. *A* **group** G *is a set together with two operations (or more simply, functions), one called* **multiplication** $m\colon G \times G \longrightarrow G$ *and the other called the* **inverse** $i\colon G \longrightarrow G$. *These operations obey the following rules*

(1) **Associativity***: For every* g, h *and* $k \in G$,

$$m(m(g,h),k) = m(g,m(h,k)).$$

(2) **Identity***: There is an element* e *in the group such that for every* $g \in G$

$$m(g,e) = g$$

and

$$m(e,g) = g.$$

(3) **Inverse***: For every* $g \in G$,

$$m(g,i(g)) = e = m(i(g),g).$$

It is customary to use different (but equivalent) notation to denote the operations of multiplication and inverse. One possibility is to use the ordinary notation for multiplication

$$m(x,y) = xy.$$

The inverse is then denoted

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

The three rules above will then read as follows

(1)

$$(gh)k = g(hk).$$

(2)

$$ge = g = eg$$

(3)

$$gg^{-1} = eg^{-1}g.$$

Another alternative is to introduce a slight different notation for the multiplication rule, something like $*$. In this case the three rules come out as

(1)

$$(g * h) * k = g * (h * k).$$

(2)

$$g * e = g = e * g$$

(3)

$$g * g^{-1} = e = g^{-1} * g.$$

The key thing to realise is that the multiplication rule need not have any relation to the more usual mutliplication rule of ordinary numbers.

Let us see some examples of groups. Can we make the empty set into a group? How would we define the multiplication? Well the answer is that there is nothing to define, we just get the empty map. Is this empty map associative? The answer is yes, since there is nothing to check. Does there exist an identity? No, since the empty set does not have any elements at all.

Thus there is no group whose underlying set is empty.

Now suppose that we take a set with one element, call it a. The definition of the multiplication rule is obvious. We only need to know how to multiply a with a,

$$m(a,a) = aa = a^2 = a * a = a.$$

Is this multiplication rule associative? Well suppose that g, h and k are three elements of G. Then $g = h = k = a$. We compute the LHS,

$$m(m(a,a),a) = m(a,a) = a.$$

Similarly the RHS is

$$m(a,m(a,a)) = m(a,a) = a.$$

These two are equal and so this multiplication rule is associative. Is their an identity? Well there is only one element of the group, a. We have to check that if we multiply $e = a$ by any other element g of the group then we get back g. The only possible choice for g is a.

$$m(g,e) = m(a,a) = a = g,$$

and

$$m(e,g) = m(a,a) = a = g.$$

So a acts as an identity. Finally does every element have an inverse? Pick an element g of the group G. In fact $g = a$. The only possiblity for an inverse of g is a.

$$m(g,g^{-1}) = m(a,a) = a = e.$$

Similarly

$$g^{-1}g = aa = a = e.$$

So there is a unique rule of multiplication for a set with one element, and with this law of multiplication we get a group.

Consider the set $\{a,b\}$ and define a multiplication rule by

$$\begin{array}{ll} aa = a & ab = b \\ ba = b & bb = a \end{array}$$

Here a plays the role of the identity. a and b are their own inverses. It is not hard to check that associativity holds and that we therefore get a group.

To see some more examples of groups, it is first useful to prove a general result about associativity.

Lemma 1.2. *Let $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$, $h\colon C \longrightarrow D$ be three functions.*

Then

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

Proof. Both the LHS and RHS are functions from $A \longrightarrow D$. To prove that two such functions are equal, it suffices to prove that they give the same value, when applied to any element $a \in A$.

$$\begin{aligned}(h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a)))\end{aligned}$$

Similarly

$$\begin{aligned}((h \circ g) \circ f))(a) &= (h \circ g)(f(a)) \\ &= h(g(f(a))).\end{aligned}$$

□

The set $\{I, R, R^2, F_1, F_2, F_3\}$ is a group, where the multiplication rule is composition of symmetries. Any symmetry, can be interpreted as a function $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$, and composition of symmetries is just composition of functions. Thus this rule of multiplication is associative by (1.2).

I plays the role an identity. Since we can undo any symmetry, every element of the group has an inverse.

Definition 1.3. *The* **dihedral group** *D_n of order n is the group of symmetries of a regular n-gon.*

With this notation, D_3 is the group above, the set of symmetries of an equilateral triangle. The same proof as above shows that D_n is a group.

Definition 1.4. *We say that a group G is* **abelian***, if for every g and h in G,*

$$gh = hg.$$

The groups with one or two elements above are abelian. However D_3 as we have already seen is not abelian. Thus not every group is abelian.

Consider the set of whole numbers $\mathbb{W} = \{1, 2, \dots\}$ under addition. Is this a group?

Lemma 1.5. *Addition and multiplication of complex number is associative.*

Proof. Well-known. □

So addition of whole numbers is certainly associative. Is there an identity? No. So $\mathbb{W}$ is not a group under addition, since there is no identity.

How about if we enlarge this set by adding 0, to get the of natural numbers $\mathbb{N}$? In this case there is an identity, but there are no inverses. For example 1 has no inverse, since if you add a non-negative number to 1 you get something at least one.

On the other hand $(\mathbb{Z}, +)$ is a group under addition, where $\mathbb{Z}$ is the set of integers. Similiarly $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all groups under addition.

How about under multiplication? First how about $\mathbb{Z}$. Multiplication is associative, and there is an identity, one. However not every element has an inverse. For example, 2 does not have an inverse.

What about $\mathbb{Q}$ under multiplication? Associativity is okay. Again one plays the role of the identity and it looks like every element has an inverse. Well not quite, since 0 has no inverse.

Once one removes zero to get $\mathbb{Q}^*$, then we do get a group under multiplication. Similarly $\mathbb{R}^*$ and $\mathbb{C}^*$ are groups under multiplication.

All of these groups are abelian.

We can create some more interesting groups using these examples. Let $M_{m,n}(\mathbb{C})$ denote $m \times n$ matrices, with entries in $\mathbb{C}$. The multiplication rule is addition of matrices (that is add corresponding entries). This operation is certainly associative, as this can be checked entry by entry. The zero matrix (that is the matrix with zeroes everywhere) plays the role of the identity.

Given a matric A, the inverse matrix is $-A$, that is the matrix obtained by changing the sign of every entry. Thus $M_{m,n}(\mathbb{C})$ is a group under addition, which is easily seen to be abelian. We can the replace complex numbers by the reals, rationals or integers.

$\mathrm{GL}_n(\mathbb{C})$ denotes the set of $n \times n$ matrices, with non-zero determinant. Multiplication is simply matrix multiplication. We check that this is a group. First note that a matrix corresponds to a (linear) function $\mathbb{R}^n \longrightarrow \mathbb{R}^n$, and under this identification, matrix multiplication corresponds to composition of functions.

Thus matrix multiplication is associative. The matrix with one's on the main diagonal and zeroes everywhere else is the identity matrix.

For example, if $n = 2$, we get

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The inverse of a matrix is constructed using Gaussian elimination. For a 2×2 matrix

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

it is easy to check that the inverse is given as

$$\frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Note that we can replace the complex numbers by the reals or rationals. Note that D_3 the group of symmetries, can be thought of as set of six matrices. In particular matrix multiplication is not abelian.