3. Definition of a group

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° anti-clockwise, thus undoing the action of R).

Definition 3.1. *A **group** G is a set together with two operations, one called **multiplication** $m\colon G \times G \longrightarrow G$ and the other called **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 $g \in G$,*

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

Note that the operations m and i are just functions. 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)

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

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

(1)

$$(g \star h) \star k = g \star (h \star k).$$

(2)

$$g \star e = g = e \star g$$

(3)

$$g \star g^{-1} = e = g^{-1} \star g.$$

The key thing to realise is that the multiplication rule need not have any relation to the more usual multiplication 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,

$$m(a, a) = aa = a^2 = a \star a = a.$$

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 there 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.