4. Examples of groups

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 4.1. *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 (4.1).

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

Definition 4.2. *The **dihedral group** D_n of order $2n$ 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 4.3. *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 $\mathbb{N} = \{1, 2, \dots\}$ under addition. Is this a group?

Lemma 4.4. *Addition and multiplication of complex number is associative.*

Proof. Well-known. □

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

How about if we enlarge this set by adding 0? 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. 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 matrix 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 replace the 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 $\mathbb{C}^n \longrightarrow \mathbb{C}^n$, 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 (or perhaps better Gauss Jordan 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.