Definition of a Group

A *group* $(G, \circ)$ is a set G together with a binary operation

$$\circ : G \times G \to G$$

written $(a, b) \mapsto a \circ b$, such that the following properties (axioms) hold:

1. (Associativity) For every $a, b, c \in G$ we have $a \circ (b \circ c) = (a \circ b) \circ c$.
2. (Identity) There is some $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$.
3. (Inverses) For every $a \in G$ there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

Given a group $(G, \circ)$ we sometimes omit the notation of the operation $\circ$ and simply write G. However, keep in mind that the group operation is essential information.

In axiom (2), the element $e \in G$ is called an *identity element*. In axiom (3), the element $a^{-1} \in G$ is called an *inverse* of the element a.

Examples

1. The pair $(\mathbb{Z}, +)$, the integers with the operation of addition, is a group:

$$G = \mathbb{Z} = \{\ldots, -3, -2, -1, \quad 0, \quad 1, \quad 2, \quad 3, \ \ldots\}, \qquad \text{“}a \circ b\text{”} = a + b$$

Let us check the 3 axioms of a group. Associativity is the familiar identity $a + (b + c) = (a + b) + c$. An identity “$e$” is given by $0 \in \mathbb{Z}$, as $a + 0 = 0 + a = a$. Finally, given an integer $a \in \mathbb{Z}$, the negative $-a \in \mathbb{Z}$ serves as “a^{-1}” because $a + (-a) = (-a) + a = 0$.

In the same way, the rational numbers with addition $(\mathbb{Q}, +)$, and the real numbers with addition $(\mathbb{R}, +)$, are both examples of groups.

For each of these examples we sometimes just write $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ to mean the above groups, where the operation is addition.

2. Consider $(\mathbb{Q}^\times, \times)$, the *non-zero* rational numbers $\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$ with the operation of *multiplication*. This is a group. Associativity is the familiar identity $a \times (b \times c) = (a \times b) \times c$. An identity element is given by $1 \in \mathbb{Q}^\times$, as $a \times 1 = 1 \times a = a$ for any $a \in \mathbb{Q}^\times$. Finally, an inverse “a^{-1}” of $a \in \mathbb{Q}^\times$ is $1/a \in \mathbb{Q}$. Here we see why the element zero had to have been expelled, as it has no inverse with respect to multiplication. Similarly, the non-zero real numbers with multiplication $(\mathbb{R}^\times, \times)$ is a group.

3. Define $\mathrm{GL}_2(\mathbb{R})$ to be the set of 2×2 matrices with real entries and non-zero determinant:

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{R}, \quad \det(A) = ad - bc \neq 0 \right\}$$

Then $\mathrm{GL}_2(\mathbb{R})$ together with the operation of matrix multiplication is a group. This example is called the *general linear group* of degree 2 over $\mathbb{R}$. An inverse of $A \in \mathrm{GL}_2(\mathbb{R})$ is given by

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

Similarly, we can define $\mathrm{GL}_2(\mathbb{Q})$ by requiring the entries a, b, c, d to be rational.

4. Let $G = \{e\}$ and defined $e \circ e = e$. This is a group, called the *trivial* group.

5. The subset $\{1, -1\} \subset \mathbb{Z}$ with the operation of multiplication is a group.

Some terminology

A group $(G, \circ)$ is *abelian* (or *commutative*) if for all $a, b \in G$ we have $a \circ b = b \circ a$.

The groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^\times, \times)$, $(\mathbb{R}^\times, \times)$, $(\{1, -1\}, \times)$ and the trivial group are all abelian groups.

The general linear group $\mathrm{GL}_2(\mathbb{R})$ is *not* abelian. For example, consider

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Then you can check that $A, B \in \mathrm{GL}_2(\mathbb{R})$ and $AB \neq BA$.

The *order* of a group G is equal to $|G|$, the cardinality (number of elements) of the set G. G has *infinite* order if $|G| = \infty$. If G is a finite set, i.e. $|G| < \infty$, then G is called a *finite group*.

All of the examples given above are groups of infinite order, except for the trivial group (order 1) and $(\{1, -1\}, \times)$ (order 2).

Cayley tables

All of the information of a group $(G, \circ)$ can be encoded in what's called the *Cayley table*. The Cayley table has columns and rows labelled by the elements of G. Given $a, b \in G$, the entry in row a and column b is the element $a \circ b$. For example, if $G = \{a, b, c\}$, it looks like:

	a	b	c
a	$a \circ a$	$a \circ b$	$a \circ c$
b	$b \circ a$	$b \circ b$	$b \circ c$
c	$c \circ a$	$c \circ b$	$c \circ c$

Here is the Cayley table for the finite group $(\{1, -1\}, \times)$ of order 2:

	1	-1
1	1	-1
-1	-1	1

If G is not a finite group, the Cayley table will of course be "infinite", having as many rows and columns as the elements of G.

Whether or not the group is abelian can be read off from the Cayley table: if G is abelian, the Cayley table is symmetric with respect to reflection across the diagonal line that passes through the entries $a \circ a$, $b \circ b$, ...

All of the groups we have seen so far are examples of structures you have encountered in various mathematical settings. Here is an example of an "abstract" group. Let the set G be

$$G = \{e, r, b, g, y, o\}$$

We define the group operation on this set by writing out the Cayley table:

	e	r	b	g	y	o
e	e	r	b	g	y	o
r	r	e	o	y	g	b
b	b	y	e	o	r	g
g	g	o	y	e	b	r
y	y	b	g	r	o	e
o	o	g	r	b	e	y

For example, the table says $r \circ b = o$ and $y \circ r = b$. You can check by brute force that the operation defined by the table satisfies the axioms of a group. The Cayley table is not symmetric with respect to the diagonal line, so this group is not abelian. Thus this group is a non-abelian group of order 6.