Definition of a Group

A **group** G is a **set** together with a **binary operation** that satisfies certain properties. The book calls the **binary operation** a **law of composition.**

Binary operations

Formally speaking, a **binary operation** on G is a function

$$m : G \times G \to G$$

$$m(g_1, g_2) = g_3$$

.

$a - b$

$f(a,b) = a-b$

But we often write binary operations with operators like $+$ or $\circ$.

$x+y$ $\quad f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$

- **plus** : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by **plus**$(x, y) = x + y$.

$x \circ y$

Or sometimes we don't write anything and we just put symbols next to each other, as for multiplication:

- **times** : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by **times**$(x, y) = xy$.

The key thing is that a binary operation on a set G takes two elements of G and gives you back a new one.

Axioms

Definition: If G is a set with a binary operation (which we will write here as if it were multiplication), then G is a group provided that:

xy

- The binary operation is associative, meaning that, for any $x, y, z \in G$, we have $(xy)z = x(yz)$. ☆ xyz
- G has an identity element, meaning that there exists an element $e \in G$ so that $ex = xe = x$ for all $x \in G$.
- Every element of G has an inverse, meaning that, for all $x \in G$, there exists $y \in G$ such that $xy = yx = e$.

☆ $m(m(x,y),z) = m(x, m(y,z)) \leftarrow$

$$xy = yx = e$$

Definition: If, in addition to these axioms, the binary operation also satisfies the condition that, for all $x, y \in G$, $xy = yx$, then G is said to be an **abelian** group.

otherwise nonabelian

The set $\mathbb{Z}$ of integers with addition is a group.

- $a, b, c \in \mathbb{Z}$ $(a+b)+c = a+(b+c)$
- there exists an $e \in \mathbb{Z}$ so that $x+e=e+x=x$ for all $x \in \mathbb{Z}$.
  $e=0$. $0+x=x+0=x$ for all $x \in \mathbb{Z}$.
- If $a \in \mathbb{Z}$, there is $b \in \mathbb{Z}$, so that $a+b=e=0=b+a$.
  $b=-a \in \mathbb{Z}$. $a+(-a)=(-a)+a=0$ for any $a \in \mathbb{Z}$.

So $(\mathbb{Z},+)$ is a group.

- $a+b=b+a$ for all $a,b \in \mathbb{Z}$, $\mathbb{Z}$ is an abelian group.

The set $\mathbb{Q}$ of rational numbers with addition is a group.

- addition is associative.
- $0 \in \mathbb{Q}$
- If $a \in \mathbb{Q}$, so is $-a$.
- $a+b=b+a$ for $a,b \in \mathbb{Q}$

$\mathbb{Q}$ is an abelian group.

The set $\mathbb{R}$ of real numbers with addition is a group.

$\mathbb{R}$ are too.

The integers mod N with addition are a group.

N any integer >0.

- $[a]+([b]+[c]) \overset{?}{=} ([a]+[b])+[c]$

  where $[a], [b], [c]$ are all in $\mathbb{Z}/N\mathbb{Z}$.

  $$[a]+([b]+[c]) = [a]+[(b+c)] = [a+(b+c)]$$
  $$= [(a+b)+c] = [(a+b)]+[c]$$
  $$= ([a]+[b])+[c]$$

- $[0]$ is the identity,

  $[a]+[0] = [a+0] = [a] = [0]+[a]$.

- $[a]+[-a] = [0] = [-a]+[a]$

$N=11$

$[5]+[6] = [11] = [0]$

$[6]=[-5]$ because $6 \equiv -5 \bmod 11$.

$[a]+[b] = [b]+[a] = [a+b]$

$\mathbb{Z}/N$ is an abelian <u>group</u>.
with N elements.

The symmetries of an equilateral triangle are a group.

A symmetry is a function $f: T \to T$ by a rigid motion

$\quad id \qquad\qquad\qquad\qquad \rho_2 \qquad\qquad\qquad\qquad\qquad \rho_1$

identity; Left rotation by 120°; Right rotation by 120°;

3 reflections. μ_1, μ_2, μ_3

Operation is composition

$\rho_2 \rho_1$ means "first ρ_1, then ρ_2"

composition of functions.

•) composition is associative

$a, b, c : T \to T$

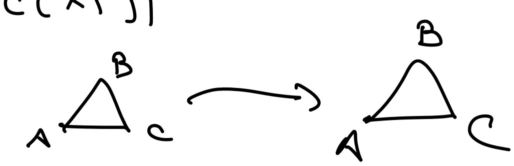
$$(a \circ b) \circ c \stackrel{?}{=} a \circ (b \circ c)$$

if $x \in T$, then $((a \circ b) \circ c)(x)$

$$= (a \circ b)\, c(x) = a(b(c(x)))$$

$$(a \circ (b \circ c))(x) = a(b(c(x)))$$

• identity: $e: T \to T$



If a is any symmetry

$$a \circ e : T \to T = a : T \to T$$

$$e \circ a : T \to T = a : T \to T$$

inverses:

Method 1: symetries are bijective

Inv Fn thm If $f: A \to A$ is bijective then there exists $g: A \to A$ so that $\underline{f \circ g} = \underline{g \circ f} = id_A$.

Method 2: 6 symetries

$id \xleftrightarrow{\text{inverse}} id$

Left rotation $\Longleftrightarrow$ Right rotation

~~reflections~~ ~~$\Longleftrightarrow$~~

$M_1 \longleftrightarrow M_1$

$M_2 \longleftrightarrow M_2$

$M_3 \longleftrightarrow M_3$

$M_2 \circ M_2 = id_A$