# Groups

**Definition.** *Let $(G, *)$ denote a non-empty set $G$ with a binary operation $*$. We say that $G$ is a **group**, if the following hold:*

*(i)* $*$ *is associative,*
*(ii) there exists an identity element $e$ such that $e * g = g * e = g \quad \forall g \in G$,*
*(iii) for each $g \in G$ there exists an inverse $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.*

**Definition.** *If $g_1 * g_2 = g_2 * g_1 \quad \forall g_1, g_2 \in G$, then we say that $*$ is **commutative**, and $G$ is said to be an **abelian group**.*

**Remark.**

*(i) Often people omit writing $*$ and simply juxtapose elements instead.*
*(ii) If a group $G$ has finitely many elements, then it is referred to as a **finite group**. Otherwise it is known as an **infinite group**. For a finite group the number of elements in $G$ is called the **order** of the group, and is denoted by $|G|$.*

**Theorem.**

*(i) The identity $e$ is unique.*
*(ii) Every element $g$ has precisely one inverse $g^{-1}$.*
*(iii) $(g^{-1})^{-1} = g \quad \forall g \in G$.*

**Theorem.** *Suppose $g_1, g_2 \in G$, then*

*(i) $(g_1 g_2)^{-1} = (g_2)^{-1}(g_1)^{-1}$, and*
*(ii) the equations $g_1 x = g_2$ and $y g_2 = g_1$ have unique solutions.*

**Examples.**

(i) $(\mathbb{Z}, +)$

(ii) $(\mathbb{Q}, +)$

(iii) $(\mathbb{R}, +)$

(iv) $(\mathbb{C}, +)$

(v) $(\mathbb{Q}^\times, \times)$ where $\mathbb{Q}^\times$ denotes the non-zero rational numbers.

(vi) $(\mathbb{R}^\times, \times)$ where $\mathbb{R}^\times$ denotes the non-zero real numbers.

(vii) $(\mathbb{C}^\times, \times)$ where $\mathbb{C}^\times$ denotes the non-zero complex numbers.

(viii) $(\mathbb{Z}_n, +)$ where addition is performed modulo $n$.

(ix) $\Big(M_n(\mathbb{R}), +\Big)$ where $M_n(\mathbb{R})$ denotes the set of $(n \times n)$ matrices with real entries.

(x) $\Big(GL(n, \mathbb{R}), \times\Big)$ where $GL(n, \mathbb{R})$ is the set of all real matrices of size $n$ which have a multiplicative inverse. This is known as the **general linear group** over $\mathbb{R}$.

(xi) There also exist general linear groups over other fields - like the complex numbers.

(xii) The set of all $2 \times 2$ real matrices of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ where $a \neq 0$ is a group under multiplication.

(xiii) The set of all functions

$$\Big\{ f_{a,b} : \mathbb{R} \to \mathbb{R} \mid f_{a,b}(x) = ax + b, a \neq 0 \Big\}$$

is a group where the binary operation is given by composition of functions.

Note that when the order of $G$ is small we can explicitly enumerate and construct all the possible groups.

| $\lvert G\rvert$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Number of different groups of order $\lvert G\rvert$ | 1 | 1 | 1 | 2 | 1 |