# Groups

**Definition:** A group $(G, *)$ is a set $G$ and a binary operation $* : G \times G \to G$ that satisfies the following properties:

a.) For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$. *Associativity*

b.) There exists $e \in G$ where for all $a \in G$ we have $a * e = a$. *Identity*

c.) For all $a \in G$, there exists $a^{-1} \in G$ where $a * a^{-1} = e$. *Inverses*

d.) For all $a, b \in G$, we have $a * b \in G$. *Closure*

**Definition:** Let $(G, *_G)$ and $(H, *_H)$ be groups, then $(G \times H, *)$ is a group where $*$ is defined as

$$(g, h) * (g', h') = (g *_G g', h *_H h')$$

where $(g', h'), (g', h') \in G \times H$.

**Proposition:** Let $(G, *)$ be a group. Then the following are true:

a.) The identity $e \in G$ is unique.

b.) For all $a \in G$, $a^{-1}$ is unique.

c.) For all $a \in G$, $(a^{-1})^{-1} = a$.

d.) For all $a, b \in G$, we have $(ab)^{-1} = b^{-1}a^{-1}$.

*Proof of (a):* Suppose $e, f \in G$ are both identities in $G$, then for $a \in G$ we have

$$ae = a = af \implies a^{-1}ae = a^{-1}af \implies e = f,$$

thus the identity is unique. ■

*Proof of (b):* Suppose $b, b' \in G$ are both inverses of $a \in G$, then

$$ab = e = ab' \implies a^{-1}ab = a^{-1}ab' \implies b = b',$$

thus inverses are unique. ■

**Definition:** Suppose $G$ is a group and let $x \in G$, then the **order** of $x$ (written $|x|$), is the smallest positive integer $n$ where $x^n = e$, where $x^n$ denotes

$$\underbrace{x * x * \cdots * x}_{n \text{ times}}.$$

If no such $n$ exists, we say $x$ has infinite order and write $|x| = \infty$.

# Dihedral Groups and Symmetries of Geometric Objects

**Definition:** For $n \in \mathbb{Z}_{\geq 3}$, we define $D_{2n}$ as the **dihedral group** of order $2n$, i.e. the symmetries of an $n$-gon. These symmetries are described by certain permutations of $\{1, 2, \ldots, n\}$. The group $D_{2n}$ is generated by $r$, a rotation by $2\pi/n$, and $s$, a reflection across the vertical axis.

We can present $D_{2n}$ using the elements $r$ and $s$:

$$D_{2n} = \left\langle r, s : rs = sr^{-1} \right\rangle,$$

where $r^{-1} = r^{n-1}$. This is in terms of "generators and relations".