Groups Rings and Fields

Author: Thobias K. Høivik
Date: Spring Semester 2026

Table of Contents

Groups

Definition: Group

A group is a set S together with a binary operation $\circ : S \times S \to S$ so that the following properties hold:

1. Identity: There exists an element $e \in S$, called the identity, such that $e \circ s = s \circ e = s$, $\forall s \in S$.
2. Inverses: For any $s \in S$ there exists some element $p \in S$ such that $s \circ p = p \circ s = e$.
3. Associativity: For all $a, b, c \in S$, $(a \circ b) \circ c = a \circ (b \circ c)$.

A group is then the tupple $(S, \circ)$.

Where it will not lead to confusion we may use the following conventions:

- For some group $(G, \circ)$ we may write just write G to refer to the group.
- Write ab instead of $a \circ b$ for the binary operation $\circ$.
- Use s^{-1} to denote the inverse of some element s in the group.

Familiar Examples

1. The integers $\mathbb{Z}$ with regular addition $+$ forms a group.
2. The positive real numbers $\mathbb{R}^+$ with multiplication $\cdot$ forms a group.
3. The natural numbers $\mathbb{N}$ (with $0 \in \mathbb{N}$) with addition $+$ does not form a group since, for example, 1 does not have an inverse. If we assume $0 \notin \mathbb{N}$ then we would be missing an identity element, also.

Definition: Abelian Group

A group G with some binary operation $+$ is called abelian if for any $a, b \in G$, $a + b = b + a$, i.e. the operation is commutative.

Notice that examples 1 and 2 from above are abelian groups.