Groups, Rings and Fields

Thobias Høivik

Spring 2026

Contents

1 Groups

Definition 1.1 (Group). *A group is a set S together with a binary operation $\circ$ such that the following properties hold:*

1. *Identity: There exists an element $e \in S$, satisfying*

$$e \circ a = a \circ e = a$$

   for every $a \in S$.

2. *Inverses: For every $a \in S$ there exists $b \in S$ such that*

$$a \circ b = b \circ a = e, \text{ the identity element}$$

   We usually denote this element as a^{-1} or $-a$, depending on context.

3. *Associativity: For any $a, b, c \in S$, we require*

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

A group is then the tupple $(S, \circ)$. We will often just write the set to refer to the group, e.g. refering to the group $(\mathbb{Z}, +)$ as just $\mathbb{Z}$.

1.1 Basic Examples

Example 1.1 (Integers under addition). *The set of integers $\mathbb{Z}$ with the operation $+$ forms a group:*

- *Identity: 0 since $0 + n = n + 0 = n$ for all $n \in \mathbb{Z}$.*
- *Inverses: For $n \in \mathbb{Z}$, the inverse is $-n$.*
- *Associativity: Addition is associative.*

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

Example 1.2 (Non-example: Natural numbers under addition). *The set $\mathbb{N}$ under $+$ is* not *a group since there is no inverse for $n > 0$.*

1.2 Basic Properties

Theorem 1.1 (Uniqueness of identity). *The identity element in a group is unique.*

Proof. Suppose e and e' are both identities. Then

$$e = e \circ e' = e',$$

so the identity is unique. □

Theorem 1.2 (Uniqueness of inverses). *Each element in a group has a unique inverse.*

Proof. Suppose b and c are inverses of a. Then

$$b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c.$$

□

1.3 Example Problem

Problem 1.1. *Determine whether the set*

$$G = \{1, -1, i, -i\} \subset \mathbb{C}$$

with multiplication is a group.

Solution. We check the group axioms:

1. **Closure:** Multiplying any two elements of G yields another element in G. True.
2. **Identity:** The element 1 acts as identity. True.
3. **Inverses:** Each element has an inverse in G: $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$, $(-i)^{-1} = i$. True.
4. **Associativity:** Multiplication of complex numbers is associative. True.

Hence $(G, \cdot)$ is a group, in fact it is an abelian group which we shall describe below in definition 1.2. □

1.4 Abelian Groups

Definition 1.2 (Abelian Group). *A group $(G, \circ)$ is* abelian *(or commutative) if*

$$a \circ b = b \circ a \quad \forall a, b \in G.$$

Example 1.3. *The group $(\mathbb{Z}, +)$ is abelian because $m + n = n + m$.*