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* $m + n = n + m$.

2 Important Groups

First let's define some often used notation.

For $g \in G$, define:

- $g^n = gg \dots g \, (n > 0)$
- $g^0 = e$
- $g^{-n} = (g^{-1})^n$

and recognize the following identities (which are provable by induction):
$$g^m g^n = g^{m+n}, \quad (g^m)^n = g^{mn}$$

Definition 2.1 (Roots of Unity).
$$U_n = \{e^{2\pi i k/n} : 0 \le k < n\}$$
are called the n-th roots of unity.

Definition 2.2. An subset $\{g_1, \dots, g_k\} \subseteq G$ is a generating set if every $g \in G$ can be expressed as

$$g_1^{n_1} \cdots g_k^{n_k}$$

If a singleton g' alone generates a group then it is called a generator of G and G is said to be cyclic.

The n-th roots of unity are finite, with exactly n elements. They are cyclic, with generator $e^{2i\pi/n}$.

Definition 2.3 (Symmetric Group). The symmetric group S_n is the set of all permutations of n elements under composition. In other words it is the set of all $\sigma : [n] \to [n]$ with composition as its operation.

The symmetric group is non-abelian for $n \ge 3$. The identity corresponds to the identity permutation (doing nothing) and inverses are undoing a permutation. We have the following notation for permutations in the symmetric Group (assume $n = 3$ for this example):

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

corresponds to $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$.

Another way to write the same permutation is:

$$(1\,2\,3)$$

3 Subgroups

> **Definition 3.1** (Subgroup). *Let G be a group under $\star$. A subgroup $H \leq G$ is a subset $H \subseteq G$ that is itself a group under $\star$.*

Having to mechanically check if $H \subseteq G$ satisfies all the required axioms can be a bit tedious so next we introduce a powerful theorem which let's us easily determine whether some subset is a subgroup or not.

> **Theorem 3.1** (Subgroup Test). *A nonempty subset $H \subseteq G$ is a subgroup if and only if*
> $$\forall x, y \in H, \ xy^{-1} \in H.$$

Proof Idea. If H is a subgroup the required conditions follows.

Conversely:

- Nonempty so some $h \in H$.

- $hh^{-1} = e \in H$.

- Closure under xy^{-1} will give inverses and closure.

$\square$

We get some nice corollaries from this, as well as a nice and tidy way to prove whether or not a subset is a subgroup.

> **Corollary 3.1.** *The intersection of any collection of subgroups is a subgroup.*
> *Given any subset $S \subseteq G$, there is a smallest subgroup containing it.*

> **Definition 3.2** (Cyclic Subgroups). *Let G be a group.*
> *For any $g \in G$, define:*
> $$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$
> $\langle g \rangle$ *is called the cyclic subgroup generated by g.*

It is very straightforward to show that the cyclic subgroup generated by some $g \in G$ is indeed a subgroup with the use of theorem 3.1.

On page 6 we say that a group is cyclic if it has a signle element which generates it, but now we can simply say that a group G is cyclic if $G = \langle g \rangle$ for some $g \in G$.

> **Theorem 3.2.** *Suppose a group G is cyclic, i.e. $G = \langle g \rangle$ for some $g \in G$.*
> *Then it is isomorphic to one of the following:*
>
> - $(\mathbb{Z}, +)$*, or*
>
> - $(\mathbb{Z}/n\mathbb{Z}, +)$ *for some $n \geq 1$.*

3.1 Structure of Cyclic Subgroups

> **Definition 3.3** (Order). *The order of an element $g \in G$ is*
> $$\text{ord}(g) = |\langle g \rangle|$$

Furthermore, if $\text{ord}(g) = n < \infty$, then $g^n = e$ and n is minimal, otherwise we say g has infinite order.

If $\text{ord}(g) = n$, then:
$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$$

Moreover:

- $g^k = e \Leftrightarrow n \mid k$
- $\langle g^k \rangle = \langle g \rangle \Leftrightarrow \gcd(k, n) = 1$

> **Theorem 3.3.** *Every subgroup of a cyclic group is cyclic.*
> *More precisely:*
>
> - *Subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$.*
>
> - *Subgroups of $\mathbb{Z}/n\mathbb{Z}$ correspond to the divisors of n.*

With all of this machinery we can approach group theory with geometric and algebraic intuition. Cyclic groups are like repeated motion, finite cyclic groups corresponding to rotations by rational angles and infinite ones corresponding to translations.

4 Cosets and Lagrange's Theorem

> **Definition 4.1** (Left and Right Cosets). *Let $H \leq G$, and let $g \in G$.*
> *The left- and right cosets are:*
>
> $$gH = \{gh : h \in H\} \quad Hg = \{hg : h \in H\}$$
>
> *respectively.*

A key intuition is that a coset is like a copy of H shifted by g. We may also recognize that the cosets are the same size as H by identifying $h \mapsto gh$ to be a bijection and so forth.

The next natural question is when are two cosets equal? Like with showing when a subset is a subgroup we have a little trick for this problem.

> **Theorem 4.1.** *Let G be a group.*
> *For $g_1, g_2 \in G$, the following are equivalent:*
>
> $$g_1 H = g_2 H$$
> $$\Updownarrow$$
> $$g_2^{-1} g_1 \in H$$
> $$\Updownarrow$$
> $$g_1 \in g_2 H$$

> **Theorem 4.2.** *The set of all left cosets of $H \leq G$ forms a partition of G.*
> *That is,*
>
> - *Every element of G is in exactly on coset.*
>
> - *Two cosets are either the same or disjoint.*

> **Definition 4.2.** *Let G be a group with $H \leq G$.*
> *The index of H in G, written $[G : H]$, is the number of left cosets of H.*

If G is finite we get $|G| = [G : H] \cdot |H|$.

> **Theorem 4.3** (Lagrange's Theorem). *Let G be a group with $H \leq G$. Then:*
> $$|H| \mid |G|$$

Proof. Let G be a group with $H \leq G$.

Recall that by theorem 4.2 we have that the set of left cosets of H, $g_1 H, g_2 H, \dots, g_k H$ (this set is finite since G is finite) are pairwise disjoint, satisfying

$$G = \bigcup_{i=1}^{k} g_i H$$

meaning

$$|G| = \sum_{i=1}^{k} |g_i H|$$

Recall also that $|H| = |g_i H|, \forall i \in [k]$. Thus

$$|G| = \sum_{i=1}^{k} |H| = k|H|$$

In other words $|G|$ is $|H|$ times some integer k, therefore $|H|$ divides $|G|$. □

Theorem 4.3 has the following immediate consequences:

- The order of any element divides $|G|$.

- $g^{|G|} = e$ for every $g \in G$.

Beware that it does not follow from Lagrange's Theorem that there exists a subgroup with the order of a divisor of $|G|$ for every divisor of G. The alternating group of order 12, A_4, has no subgroup of order 6 for example.

> **Proposition 4.1.** *A group of order p where p is prime, is cyclic.*

Proof Sketch. Let G be a group with $|G| = p$ (prime).

Let $g \in G \setminus \{1\}$. Consider it's generated subgroup $\langle g \rangle$. By Lagrange's Theorem the order of this subgroup divides p so $|\langle g \rangle|$ is 1 or p, but it can't be 1 as $g \neq 1$ so it's order is p, i.e. g generates the entirety of G. □