# Introduction to Abstract Algebra

Lecture notes for Math 113

## Contents

# 1 Course description and some notations

The goal of this course is to generalize and study algebraic objects and structures. More specifically, we will mostly study *sets* (see section 2.1) with some operations on them. The main examples of those come from various number sets.

**Example 1.0.1.** Positive integer (natural) numbers

$$\mathbb{Z}_{>0} = \{1, 2, 3, 4, \ldots\}$$

admit two operations: addition ($+$) and multiplication ($\times$). Note that these operations have no inverse operations in general (i.e. no subtraction and division).

If we want to have a well-defined subtraction, we need to formally adjoin negative numbers and zero. So we get the following

**Example 1.0.2.** The set of integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

with operation of addition, which is now invertible, and a non-invertible operation of multiplication.

Inverting the multiplication on $\mathbb{Z}$, we get

**Example 1.0.3.** The set of rational numbers $\mathbb{Q}$ is defined as the quotient of the set

$$\{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{Z}_{>0}\}$$

by the *equivalence relation* (see section 2.2)

$$(m_1, n_1) \sim (m_2, n_2), \text{ if } m_1 n_2 = m_2 n_1.$$

It admits both addition (with the inverse operation of subtraction) and multiplication (with the inverse operation of division).

Other examples include

**Example 1.0.4.** The set of real numbers $\mathbb{R}$, defined as the set of infinite decimal expansions

$$\{a_0.a_1a_2a_3\ldots \mid a_0 \in \mathbb{Z}, a_i \in \{0, 1, \ldots 9\} \text{ for } i = 1, 2, 3, \ldots\}$$

subject to the equivalence relation

$$a_0.a_1a_2\ldots a_m 99999\ldots = a_0.a_1a_2\ldots(a_m + 1)00000\ldots,$$

on which one can define invertible addition and multiplication.

As well as

**Example 1.0.5.** The set of complex numbers

$$\mathbb{C} = \{a + b\sqrt{-1} |\ a, b \in \mathbb{R}\}$$

with coordinate-wise addition and subtraction:

$$(a_1 + b_1\sqrt{-1}) + (a_2 + b_2\sqrt{-1}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-1},$$

$$(a_1 + b_1\sqrt{-1}) - (a_2 + b_2\sqrt{-1}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{-1}$$

and multiplication given by opening the brackets and using the relation $(\sqrt{-1})^2 = -1$: ‘

$$(a_1 + b_1\sqrt{-1}) \cdot (a_2 + b_2\sqrt{-1}) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{-1}.$$

**Remark 1.0.6.** It is common to denote $\sqrt{-1} \in \mathbb{C}$ by $i$ (which stands for imaginary).

**Exercise 1.0.7.** Let $z_1 = a_1 + b_1\sqrt{-1}, z_2 = a_2 + b_2\sqrt{-1} \in \mathbb{C}$ and suppose $z_2 \neq 0$. Define $\overline{z_2} = a_2 - b_2\sqrt{-1}$ and

$$z_1/z_2 = \frac{1}{a_2^2 + b_2^2} \cdot z_1 \cdot \overline{z_2} = \frac{a_1a_2 + b_1b_2}{a_2^2 + b_2^2} + \frac{b_1a_2 - a_1b_2}{a_2^2 + b_2^2}\sqrt{-1}.$$

Prove that this operation defines division on $\mathbb{C}$, that is $(z_1 \cdot z_2)/z_2 = z_1$.

We get the series of inclusions:

$$\mathbb{Z}_{>0} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

We will start this course by developing the theory of sets with a single operation (called *monoids*), like $\mathbb{Z}_{>0}$ with addition or $\mathbb{Z}$ with multiplication. We will focus especially on those sets for which this operation is invertible (called *groups*), like $\mathbb{Z}$ with addition or $\mathbb{C} - \{0\}$ with multiplication. See Sections 3, 4, 5, 6.

The second half of the course will be dedicated to the study of *rings* (sets with addition, subtraction and multiplication, like $\mathbb{Z}$) and *fields* (sets with all four operations like $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$). See Sections 8, **??**, 9 .

# 2 Preliminaries

We will heavily use the language of set theory in this class. Below is a short reminder of some of the definitions and notations.

## 2.1 Basic set theory

**Definition 2.1.1.** A set is an (unordered) collection of elements.

**Example 2.1.2.** A set of positive integers, a set of people in this class, a set of triangles on the plane, and so on.

### Notations

1. Logical operators and quantifiers:
   - $P \Rightarrow Q$ means “statement $Q$ follows from statement $P$”;
   - $P \iff Q$ means “statement $Q$ is true if and only if statement $P$ is true”;
   - $\exists$ means “there exists”;

- $\forall$ means " for all".
- We will use the word "**and**" (sometimes replaced with a comma or an ampersand) for logical conjunction and the word "**or**" for logical disjunction. Note that "or" is always meant to be non-exclusive.

2. Notation for sets:

   - $S = \{$ elements of $S\}$, e.g. $S = \{1, 2, 5\}$, $S = \{\bullet, \star, \square\}$, or $S = \{1, 2, 3, 4, \ldots\}$;
   - The empty set is the set containing no elements, denoted by $\emptyset$;
   - $s \in S$ means $s$ is an element of $S$, and $s \notin S$ means $s$ is not an element of $S$;
   - $S$ is called **finite** if it contains finitely many elements;
   - $|S|$ or $\#S$ denotes the number of elements in a finite set $S$, also called the **order** of $S$.
   - We can define a set by some property

     $$S = \{ \text{ notation for elements in } S \mid \text{ property they satisfy}\},$$

     e.g. $2\mathbb{Z} = \{x \in \mathbb{Z} \mid x \text{ is divisible by } 2\}$ or $S = \{x \mid x \in A, x \notin B\}$.
   - The set of elements contained *both* in $S$ and in $T$ is called their **intersection**, denoted $S \cap T$. We have

     $$S \cap T = \{s \mid s \in S \text{ and } s \in T\}.$$

   - The set of elements contained in *either* $S$ or $T$ is called their **union**, denoted $S \cup T$. We have

     $$S \cup T = \{s \mid s \in S \text{ or } s \in T\}.$$

   - The sets $S$ and $T$ are called **disjoint** if they have no elements in common, i.e. $S \cap T = \emptyset$. If $S$ and $T$ are disjoint, we will sometimes use another notation for their union:

     $$S \sqcup T,$$

     called the **disjoint union**.
   - The **cartesian product** (or simply the product) of sets $S$ and $T$ is the set

     $$S \times T = \{(s, t) \mid s \in S, t \in T\}$$

     of (ordered) pairs of elements of $S$ and $T$.
   - We write $T \subset S$ if all elements of $T$ are also elements of $S$, we say "$T$ is contained in $S$" or "$T$ is a subset of $S$". Note that if $T \subset S$ and $S \subset T$ then $T = S$.
   - If $T \subset S$, we denote by $S - T$ or $S \backslash T$ the **complement** of $T$ in $S$, that is

     $$S - T = \{s \in S \mid s \notin T\}.$$

   - We write $T \not\subset S$ to mean that $T$ is not contained in $S$, in other words (using our previous notations):

     $$\exists\, t \in T : \ t \notin S.$$

**Remark 2.1.3.** Note that the statement $T \not\subset S$ is the **negation** of the statement $T \subset S$ and vice versa. Here is a general recipe for how to form a negation of a given statement. Suppose you are given a statement that involves some quantifiers:

$$\forall\, t \in T : \ t \in S.$$

To construct the negation of this statement you should change all quantifiers for the opposite ones and change the property for its negative:

$$\exists\, t \in T : \ t \notin S.$$

If your statement involved some "and" or (non-exclusive) "or" then you should swap "and" for "or" and "or" for "and" in its negation. For example, the negation of

$$\forall\ x \in \mathbb{R}, \forall\ n \in \mathbb{Z}_{\geq 0}, \exists\ y \in \mathbb{R} :\ x = y^n \text{ or } x = -y^n$$

is

$$\exists\ x \in \mathbb{R}, \exists\ n \in \mathbb{Z}_{\geq 0}, \forall\ y \in \mathbb{R} :\ x \neq y^n \text{ and } x \neq -y^n.$$

**Functions (maps)**

**Definition 2.1.4.** A **map** (also called a **function**) from set $A$ to set $B$ is a *rule*, that assigns to *each* element of $A$ a *unique* element of $B$.

**Notation:** If $f$ is a function from $A$ to $B$ we write $f : A \to B$. We denote by $f(a)$ the unique element of $B$, that was assigned to $a$ via $f$ (called the image of $a$ under $f$ or the value of $f$ at $a$).

- Sometimes we define a function $f : A \to B$ by specifying its values at each element of $A$. In this case we write $f : a \mapsto b$ (meaning $f(a) = b$). For example,

  $$f : n \mapsto 2n$$

  defines a function $f : \mathbb{Z} \to \mathbb{Z}$.

- We say that $f : A \to B$ is **well-defined** if for any $a_1, a_2 \in A$

  $$a_1 = a_2 \Rightarrow f(a_1) = f(a_2).$$

  **Example 2.1.5.** Suppose we have two maps $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$. We want to define $f : A_1 \cup A_2 \to B$ by setting

  $$f(a) = \begin{cases} f_1(a), \text{ if } a \in A_1, \\ f_2(a), \text{ if } a \in A_2. \end{cases}$$

  Then one can check that $f$ is well-defined if and only if $f_1(a) = f_2(a)$ for any $a \in A_1 \cap A_2$.

- Let $A \subset B$ and let $g : B \to C$ then the **restriction** of $g$ to $A$ is a map from $A$ to $C$, that sends $a$ to $g(a)$. It is denoted by $g|_A$.

- For a map $f : A \to B$ we define the set

  $$f(A) = \{f(a) \mid a \in A\} \subset B$$

  called the **image** of $f$ (also denoted $\operatorname{Im} f$).

- Let $f : A \to B$ and $C \subset B$. The **preimage** of $C$ under $f$ is the set

  $$f^{-1}(C) = \{a \in A |\ f(a) \in C\} \subset A.$$

  Note that $f^{-1}(C)$ is just a notation, it doesn't mean that there exists the inverse function $f^{-1}$.

- The identity map on $A$ is the map

  $$Id_A : a \mapsto a, \quad \forall\ a \in A.$$

- Let $f : A \to B,\ g : B \to C$ be two functions. Their **composition** is the map $g \circ f : A \to C$, given by

  $$g \circ f : a \mapsto g(f(a)).$$

- A map $f : A \to B$ is called **injective** if for any $a_1, a_2 \in A$

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

- A map $f : A \to B$ is called **surjective** if

$$\forall\ b \in B, \exists\ a \in A :\ f(a) = b.$$

- A map $f : A \to B$ is called **bijective** (or one-to-one) if it is both injective and surjective.

**Definition 2.1.6.** Let $f : A \to B,\ g : B \to A$ be two maps. Then $g$ is called

1. a **left inverse** of $f$, if $g \circ f = Id_A$;
2. a **right inverse** of $f$, if $f \circ g = Id_B$;
3. the (two-sided) **inverse** of $f$ if it is both a left and a right inverse of $f$. In this case it is denoted by $f^{-1}$.

**Remark 2.1.7.** A map $f : A \to B$ can possibly admit multiple left (or right) inverses. However, if the two-sided inverse of $f$ exists, then it is unique.

**Proposition 2.1.8.** *Let $A, B$ be two nonempty sets and let $f : A \to B$ be a function. Then*

1. *$f$ admits a left inverse if and only if $f$ is injective;*
2. *$f$ admits a right inverse if and only if $f$ is surjective;*
3. *$f$ admits a two-sided inverse if and only if $f$ is bijective.*

*Proof.* We will prove only part 1 of the proposition. The proof of part 2 is left as an exercise, and part 3 follows directly from parts 1 and 2.

Suppose $f$ is injective. Let $C = B - f(A)$ be the complement of the image of $f$. Let us fix some element $a_0 \in A$.

We define $g : B \to A$ by setting

$$g(b) = \begin{cases} a_0, \text{ if } b \in C, \\ a, \text{ if } b = f(a) \in f(A). \end{cases}$$

We need to check that $g$ is a well-defined function, because if $b = f(a_1) = f(a_2)$ then the value of $g$ at $b$ is ambiguous and could be set to be either $a_1$ or $a_2$. However, since $f$ is injective, $f(a_1) = f(a_2)$ implies $a_1 = a_2$, which means that there is actually no ambiguity. Note also that $f(A)$ and $C$ are disjoint subsets of $B$. So, combining the previous observation with Example 2.1.5, we deduce that $g$ is a well-defined function $B \to A$.

Now $g \circ f(a) = g(f(a)) = a$, so $g \circ f = Id_A$.

Let us prove the converse now. Suppose that there exist a left inverse $g : B \to A$. Let $a_1, a_2 \in A$ and suppose $f(a_1) = f(a_2)$. Then since $g \circ f = Id_A$,

$$a_1 = g(f(a_1)) = g(f(a_2)) = a_2,$$

which proves that $f$ is injective. ■

## 2.2 Equivalence relations

**Definition 2.2.1.** Let $A$ be a non-empty set. A subset $R \subset A \times A$ is called a **binary relation** on $A$.

**Notation:** If $(a, b) \in R$ then elements $a$ and $b$ of $A$ are said to be in relation $R$, we write $a\ R\ b$.

**Example 2.2.2.** Define a binary relation $<$ on $\mathbb{Z}$, such that $(a, b) \in <$ if $b - a \in Z_{>0}$. Then $(a, b) \in < \iff a < b$.

**Definition 2.2.3.** A binary relation $\sim$ on $A$ is called an **equivalence relation** if it is

(a) **reflexive**, i.e. $a \sim a$ for all $a \in A$;

(b) **symmetric**, i.e. if $a \sim b$ then $b \sim a$;

(c) **transitive**, i.e. if $a \sim b$ and $b \sim c$ then $a \sim c$.

**Example 2.2.4.**

1. The relation $<$ from Example 2.2.2 is transitive, but not reflexive or symmetric.

2. Let us fix some $n \in \mathbb{Z}_{>0}$. For $a, b \in \mathbb{Z}$ let $a \sim b$ if $(a-b)$ is divisible by $n$ (notation: $n \mid (a-b)$). Then $\sim$ is an equivalence relation on $\mathbb{Z}$.

   *Proof.* (a) $a \sim a$ for any $a \in \mathbb{Z}$ because $n \mid 0$;
   (b) if $a \sim b$ the $n$ divides $(a - b)$, hence it divides $(b - a)$, so $b \sim a$;
   (c) if $n$ divides both $x$ and $y$ then $n$ divides $x + y$, therefore if $a \sim b, b \sim c$ then $n$ divides $(a - b) + (b - c) = a - c$, and thus $a \sim c$.

■

3. Let $A = \mathbb{Z} \times \mathbb{Z}_{>0} = \{(m, n) \mid m \in Z, n \in \mathbb{Z}_{>0}\}$. Define the relation $\sim$ on $A$ by putting

$$(m_1, n_2) \sim (m_2, n_2), \text{ if } m_1 n_2 = m_2 n_1.$$

   Then $\sim$ is an equivalence relation.

   *Proof.* (a) $(m, n) \sim (m, n)$, since $mn = mn$;
   (b) if $(m_1, n_1) \sim (m_2, n_2)$ then clearly $(m_2, n_2) \sim (m_1, n_1)$;
   (c) if $(m_1, n_1) \sim (m_2, n_2)$ and $(m_2, n_2) \sim (m_3, n_3)$ then

$$m_1 n_2 = m_2 n_1,\ m_2 n_3 = m_3 n_2,$$

   and thus

$$m_1 n_2 n_3 = m_2 n_1 n_3 = m_3 n_1 n_2,$$

   from which we deduce that $m_1 n_3 = m_3 n_1$ as $n_2 \neq 0$.

■

**Definition 2.2.5.** Let $\sim$ be an equivalence relation on $A$ and let $a \in A$. The **equivalence class** of $a$ is the subset $[a] = \{b \in A \mid a \sim b\} \subset A$. All elements in $[a]$ are said to be *equivalent* to $a$.

**Definition 2.2.6.** A **partition** of a set $A$ is a collection of subsets $\{A_i\}_{i \in I}$, such that

$$A = \bigcup_{i \in I} A_i = \{a \mid \exists\ i \in I :\ a \in A_i\}, \text{ and}$$

$$A_i \cap A_j = \emptyset, \text{ if } i \neq j.$$

**Proposition 2.2.7.** *1. Let $A$ be a set with an equivalence relation $\sim$ on it. The set of equivalence classes of elements of $A$ forms a partition of $A$.*

*2. Conversely, let $\{A_i\}_{i\in I}$ be a partition of $A$ then the relation $a \sim b$ if $\exists\ i \in I :\ a, b \in A_i$ is an equivalence relation on $A$. In this case $\{A_i\}_{i\in I}$ is precisely the set of equivalence classes for $\sim$.*

*Proof.* 1. Let $I$ be some indexing set of **distinct** equivalence classes in $A$. That is, we pick some elements $a_i \in A, i \in I$, such that $[a_i] \neq [a_j]$ if $i \neq j$, and for any $a \in A$ there exists $i \in I$, such that $[a] = [a_i]$. We need to prove that $\{[a_i]\}_{i\in I}$ is a partition of $A$. First, by construction it is clear that

$$A = \bigcup_{a\in A} \{a\} \subset \bigcup_{a\in A} [a] = \bigcup_{i\in I} [a_i],$$

(since $a \in [a]$ by the reflexive property).

So it is only left to prove that $[a_i] \cap [a_j] = \emptyset$ if $i \neq j$. Let $b \in [a_i] \cap [a_j]$ then $a_i \sim b$ and $a_j \sim b$. Using the symmetric and transitive properties, we deduce that $a_i \sim a_j$. For any $b \in [a_j]$ we get $a_i \sim a_j, a_j \sim b \Rightarrow a_i \sim b$, so $b \in [a_i]$ and $[a_j] \subset [a_i]$. similarly, one can show that $[a_i] \subset [a_j]$ and thus $[a_i] = [a_j]$ and $i = j$.

2. Exercise.

■

**Definition 2.2.8.** Let $A$ be a set equipped with an equivalence relation $\sim$. Define $A/\sim$ to be the set of equivalence classes in $A$. We call this set the **quotient** of $A$ under the equivalence relation $\sim$.

There is a natural *surjective* map $q : A \to A/\sim$, that sends $a$ to $[a]$ called the **quotient map**.

**Example 2.2.9.** 1. Let us equip $\mathbb{Z}$ with the equivalence relation $\sim$ from Example 2.2.4.2 for $n = 2$. Then $\mathbb{Z}/\sim = \{[0], [1]\}$, and $q : \mathbb{Z} \to \mathbb{Z}/\sim$ is given by

$$q(m) = \begin{cases} [0], \text{ if } m \text{ is divisible by 2,} \\ [1], \text{ otherwise .} \end{cases}$$

**Remark 2.2.10.** Since $[0] = [2]$ we could also say that $\mathbb{Z}/\sim = \{[1], [2]\}$.

2. Let $A = \mathbb{Z} \times \mathbb{Z}_{>0}$ be the set equipped with the equivalence relation $\sim$ from Example 2.2.4.3. Then $A/\sim$ is the set of rational numbers. We denote the equivalence class $[(m, n)]$ by $\frac{m}{n}$.

**Definition 2.2.11.** Let $C \subset A$ be the equivalence class in $A$ under some equivalence relation $\sim$. Then an element $b \in C$ is called a **representative** of the class $C$.

## 2.3 Properties of the integers

Let us recall some of the properties of the integers without proofs. We will prove generalization of some of these properties when we cover ring theory.

- $\mathbb{Z}_{>0}$ is *well-ordered*, meaning that any nonempty subset of $\mathbb{Z}_{>0}$ has the minimal element.
- *Mathematical induction:* if for a collection of statements $\{P(n)\}_{n\in\mathbb{Z}_{>0}}$ we know that
  1. $P(1)$ is true, and (*Base Case*)
  2. $P(n) \Rightarrow P(n+1)$ for any $n \in \mathbb{Z}_{>0}$, (*Induction Step*)

  then $P(n)$ is true for all $n \in \mathbb{Z}_{>0}$.
- We say that $b$ divides $a$ if there exists an element $c \in \mathbb{Z}$, such that $a = bc$. In this case we write $b \mid a$ ( and if $b$ doesnt divide $a$, we write $b \nmid a$ ).

- An integer $p > 1$ is called **prime** if $a \mid p$ implies $a = 1$ or $a = p$ for any $a \in Z_{>0}$.
- *The Fundamental Theorem of Arithmetic*: Any positive integer $n$ can be factored uniquely into the product of primes. That is, there exist *distinct* primes $p_1 < p_2 < ... < p_s$ and positive integers $a_1, \ldots, a_s$, such that
$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}.$$
This factorization is unique in the sense that if $q_1 < q_2 < \ldots < q_t$ are distinct primes and $b_1, \ldots, b_t$ are positive integers, such that
$$n = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_t^{b_t},$$
then $s = t$ and $p_i = q_i, a_i = b_i$ for all $i = 1, \ldots, s$.
- If $a, b \in \mathbb{Z} - \{0\}$ then there is a unique positive integer $d$ called the **greatest common divisor** of $a$ and $b$ (denoted $\gcd(a, b)$), satisfying
  1. $d \mid a$ and $d \mid b$ (i.e. $d$ is a *common divisor* for $a$ and $b$),
  2. if $c \mid a$ and $c \mid b$ then $c \mid d$ ($d$ is the *greatest* such divisor).

  If $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdot \ldots p_n^{\beta_n}$, where $p_1, \ldots, p_n$ are distinct primes, then
$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}.$$
  **Definition 2.3.1.** If $\gcd(a, b) = 1$ then integers $a$ and $b$ are called **coprime**.
- If $a, b \in \mathbb{Z} - \{0\}$ then there exists a unique positive integer $l$ called the **least common multiple** of $a$ and $b$ (denoted $\mathrm{lcm}(a, b)$), satisfying
  1. $a \mid l$ and $b \mid l$ (i.e. $l$ is a *common multiple* of $a$ and $b$),
  2. if $a \mid m$ and $b \mid m$ then $l \mid m$ (i.e. $l$ is the *least* such multiple).

  If $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdot \ldots p_n^{\beta_n}$, where $p_1, \ldots, p_n$ are distinct primes, then
$$\mathrm{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}.$$
- *The Division Algorithm:* If $a, b \in \mathbb{Z} - \{0\}$ then there exist unique $q, r \in \mathbb{Z}$, such that
$$a = bq + r \text{ and } 0 \leq r < |b|,$$
where $q$ is called the **quotient** and $r$ is called the **remainder**.

## 2.4 Euclidean algorithm

. The *Euclidean Algorithm* is an important procedure which produces the greatest common divisor of two integers $a$ and $b$ by iterating the Division Algorithm.

Consider two nonzero integers $a$ and $b$. We obtain a sequence of quotients and remainders

$$\begin{aligned} a &= bq_0 + r_0, \\ b &= r_0 q_1 + r_1, \\ r_0 &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\ldots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1}, \end{aligned}$$

where $r_n$ is the last nonzero remainder. Such $r_n$ exists since $|b| > r_0 > r_1 > \ldots > r_n$ is a decreasing sequence of strictly positive integers, so it cannot continue indefinitely.

**Proposition 2.4.1.** *The remainder $r_n$ is the* $\gcd(a, b)$.

*Proof.* It is enough to prove that $\gcd(a, b) = \gcd(b, r_0)$ and then apply this iteratively to obtain $r_n = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \ldots = \gcd(b, r_0) = \gcd(a, b)$.

So, let $d = \gcd(a, b)$ then $d$ divides both $a$ and $b$, and therefore it divides $r_0 = a - bq_0$. Suppose $c$ is some common divisor of $b$ and $r_0$ then it also divides $a = bq_0 + r_0$. Thus, by the property of $\gcd(a, b)$ we get that $c \mid d$, proving that $d$ is the g.c.d. of $b$ and $r_0$. ■

**Example 2.4.2.** Let us apply the Euclidean Algorithm to $a = 12345, b = 6789$. We get

$$12345 = 6789 + 5556,$$

$$6789 = 5556 + 1233,$$

$$5556 = 1233 \cdot 4 + 624,$$

$$1233 = 624 + 609,$$

$$624 = 609 + 15,$$

$$609 = 15 \cdot 40 + 9,$$

$$15 = 9 + 6,$$

$$9 = 6 + 3,$$

$$6 = 3 \cdot 2.$$

Thus, $\gcd(12345, 6789) = 3$.

**Corollary 2.4.3.** *Let $a, b \in \mathbb{Z} - \{0\}$ then there exist integers $u, v$ such that*

$$\gcd(a, b) = a \cdot u + b \cdot v.$$

*Proof.* Tracing back the Euclidean Algorithm, we construct $u$ and $v$ by induction. Since $r_n = r_{n-2} + r_{n-1} \cdot (-q_n)$, we put $u_0 = 1, v_0 = -q_n$. Then suppose $r_n = r_{k-1} \cdot u_{n-k-1} + r_k \cdot v_{n-k-1}$. Since $r_k = r_{k-2} + r_{k-1} \cdot (-q_k)$, putting

$$v_{n-k} = u_{n-k-1} - q_k \cdot v_{n-k-1},$$

$$u_{n-k} = v_{n-k-1},$$

we get that $r_n = r_{k-2} \cdot u_{n-k} + r_{k-1} \cdot v_{n-k}$.

Now we put $u = u_n, v = v_n$ to get

$$r_n = a \cdot u + b \cdot v.$$

■

**Example 2.4.4.** Let us use Example 2.4.2 to express 3 in terms of 12345 and 6789.

$$3 = 9 - 6,$$

$$3 = 9 - (15 - 9) = 9 \cdot 2 - 15,$$

$$3 = (609 - 15 \cdot 40) \cdot 2 - 15 = 609 \cdot 2 - 15 \cdot 81,$$

$$3 = 609 \cdot 2 - (624 - 609) \cdot 81 = 609 \cdot 83 - 624 \cdot 81,$$

$$3 = (1233 - 624) \cdot 83 - 624 \cdot 81 = 1233 \cdot 83 - 624 \cdot 164,$$

$$3 = 1233 \cdot 83 - (5556 - 1233 \cdot 4) \cdot 164 = 1233 \cdot 739 - 5556 \cdot 164,$$

$$3 = (6789 - 5556) \cdot 739 - 5556 \cdot 164 = 6789 \cdot 739 - 5556 \cdot 903,$$

$$3 = 6789 \cdot 739 - (12345 - 6789) \cdot 903 = 6789 \cdot 1642 - 12345 \cdot 903.$$

We get $u = -903, v = 1642$.

## 2.5 The integers modulo n

.

Let $n$ be a fixed positive integer. Define a relation on $\mathbb{Z}$ by

$$a \sim b \text{ if and only if } n \mid (a-b).$$

We proved in Example 2.2.4.2 that this is an equivalence relation. Let us adopt one more notation for this equivalence relation. We will write

$$a \equiv b \mod n$$

if $a \sim b$.

**Definition 2.5.1.** Define $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\sim$ (in the sense of Definition 2.2.8) to be the set of equivalence classes of integers **modulo n**.

Let $m \in \mathbb{Z}$. The equivalence class $[m]$ is called the *congruence class* or *residue class* of $m$ mod $n$. We will, thereafter, use the notation $m \mod n$ for $[m]$ sometimes.

**Remark 2.5.2.** Let $m \in \mathbb{Z}$ then the equivalence class $[m]$ consists of all integers that have the same remainder when divided by $n$.

Following the remark above, we deduce that there are precisely $n$ distinct equivalence classes. We can pick class representatives between 0 and $n-1$ (all possible remainders modulo $n$). Thus,

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

The natural quotient map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sends an integer $m$ to $[r]$, where $r$ is its remainder mod $n$. Applying map $q$ to an integer $m$ is called *reducing $m$ modulo $n$*.

We can define addition and multiplication on elements of $\mathbb{Z}/n\mathbb{Z}$ as follows: let $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ we define

1. $[a] + [b]$ as $[a+b]$, and
2. $[a] \cdot [b]$ as $[a \cdot b]$.

Namely, we choose some class representatives, add (or multiply) them as integers, and then reduce the result modulo $n$.

**Example 2.5.3.** Let $n = 12$ then $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [11]\}$.

Let now $[a] = [5], [b] = [8]$. We have

$$[5] + [8] = [13] = [1],$$

$$[5] \cdot [8] = [40] = [4].$$

**Proposition 2.5.4.** *The operations of addition and multiplication defined above are both well defined. That is, the result does not depend on the choice of class representatives.*

Before we prove this let us consider an

**Example 2.5.5.** Let $n = 12, [a] = [5], [b] = [8]$. Note that $[a]$ could also be expressed as $[29]$ and $[b]$ is also equal to $[-4]$. Let us compute their sum and product:

$$[29] + [-4] = [25] = [1],$$

$$[29] \cdot [-4] = [-116] = [120 - 116] = [4].$$

Note that we obtained the same answer as before.

*Proof.* Let $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ and suppose $a, a' \in [a]$ and $b, b' \in [b]$. We want to show that

$$[a+b] = [a'+b'] \text{ and } [a \cdot b] = [a' \cdot b']. \quad (\star)$$

Let $a' = a + nk$ and $b' = b + nl$ then

$$(a'+b') - (a+b) = n(k+l)$$

and

$$a'b' - ab = (a+nk)(b+nl) - ab = n(kb + al + nkl).$$

Both are divisible by $n$, so we deduce the desired result $(\star)$. ∎

**Remark 2.5.6.** The class $[0] \in \mathbb{Z}/n\mathbb{Z}$ behaves like 0 in $\mathbb{Z}$:

$$[a] + [0] = [a], \text{ for all } [a] \in \mathbb{Z}/n\mathbb{Z},$$

and the class $[1]$ behaves like 1:

$$[a] \cdot [1] = [a], \text{ for all } [a] \in \mathbb{Z}/n\mathbb{Z}.$$

**Example 2.5.7.** The arithmetic of remainders allows to answer some interesting questions. For instance, can we compute the last two digits of $2^{10000}$ without computing the number itself?

Let us note that that the last two digits of a number are given by its remainder modulo 100. Now we can make some observations of the behavior of powers of 2 modulo 100. For example,

$$[2^{12}] = [4096] = [-4].$$

So,

$$[2^{10000}] = [2^{833 \cdot 12}] \cdot [2^4] = [(-4)^{833}] \cdot [2^4] = -[2^{1670}].$$

Now,

$$-[2^{1670}] = -[2^{139 \cdot 12}] \cdot [2^2] = -[(-4)^{139}] \cdot [2^2] = [2^{280}],$$

proceeding further in the same way, we get

$$[2^{280}] = [2^{23 \cdot 12}] \cdot [2^4] = -[2^{50}] =$$

$$= -[2^{4 \cdot 12}] \cdot [2^2] = -[2^{10}] = [-24] = [76].$$

Thus 76 are the last two digits of $2^{10000}$.

A very important result about the arithmetic of remainders is

**Theorem 2.5.8** (Fermat's Little Theorem)**.** *Let $p$ be a prime number and let $a$ be any integer then*

$$a^p \equiv a \mod p.$$

Note that it is enough to prove this for $0 \leq a < p$. We will do this by induction starting with the obvious case $a = 0$. To prove the induction step we will need the following

**Lemma 2.5.9.** *For any $k \in \mathbb{Z}$ and any prime $p$*

$$(k+1)^p \equiv k^p + 1 \mod p.$$

*Proof of Lemma 2.5.9.* We have

$$(k+1)^p = \sum_{i=0}^{p} \binom{p}{i} k^i,$$

so it is enough to prove that $\binom{p}{i}$ is divisible by $p$ for any $1 \leq i \leq p-1$. By definition

$$\binom{p}{i} = \frac{p!}{i!(p-i)!},$$

so since for $1 \leq i \leq p-1$ the denominator is not divisible by $p$, we deduce that

$$\binom{p}{i} \equiv 0 \mod p,\ i = 1, 2, \ldots, p-1.$$

■

*Proof of Theorem 2.5.8.* Suppose we know that $a^p \equiv a \mod p$ for $a = k$. Consider now $a = k+1$:

$$(k+1)^p \equiv k^p + 1 \equiv k + 1 \mod p.$$

■

We proved that, similarly to $\mathbb{Z}$, the set $\mathbb{Z}/n\mathbb{Z}$ has well defined addition and multiplication. The question we would like to answer now is which numbers become invertible modulo $n$ (with respect to multiplication).

Define

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \exists [u] \in \mathbb{Z}/n\mathbb{Z} :\ [a] \cdot [u] = [1]\}.$$

**Proposition 2.5.10.** *An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if* $\gcd(a, n) = 1$.

*Proof.* Suppose $\gcd(a, n) = 1$ then by Corollary 2.4.3 there exist $u, v \in \mathbb{Z}$ with

$$1 = a \cdot u + n \cdot v.$$

It follows that modulo $n$

$$[1] = [a \cdot u] = [a] \cdot [u],$$

so $[a]$ is invertible.

Conversely, if $[a]$ is invertible then there exists $u \in \mathbb{Z}$, such that

$$[1] = [a] \cdot [u] = [a \cdot u],$$

thus,

$$1 = a \cdot u + n \cdot v$$

for some $v \in \mathbb{Z}$. Then if $d$ is the g.c.d. of $a$ and $n$, it must also divide 1. Hence, $d = 1$. ■

**Remark 2.5.11.** If $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^\times$ then $[a] \cdot [b] = [a \cdot b] \in (\mathbb{Z}/n\mathbb{Z})^\times$. If $[u]$ and $[v]$ are the inverses of $[a]$ and $[b]$ respectively, then $[v \cdot u]$ is the inverse of $[a \cdot b]$, since

$$[a \cdot b] \cdot [v \cdot u] = [a \cdot b \cdot v \cdot u] = [a] \cdot ([b] \cdot [v]) \cdot [u] = [a] \cdot [1] \cdot [u] = [a] \cdot [u] = [1].$$

**The Euler $\varphi$-function.**

Define a function $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ by putting $\varphi(n)$ to be the number of positive integers *smaller* than $n$ and *coprime* with $n$.

**Definition 2.5.12.** Function $\varphi$ above is called Euler (totient) $\varphi$-function.

**Example 2.5.13.** Let $n = 15$: numbers smaller than 15 and coprime with 15 are

$$1, 2, 4, 7, 8, 11, 13, 14,$$

so $\varphi(15) = 8$.

**Proposition 2.5.14.** *The number of elements in* $(\mathbb{Z}/n\mathbb{Z})^\times$ *is* $\varphi(n)$.

*Proof.* This follows directly from Proposition 2.5.10. ■

We will prove later the following property of the $\varphi$-function:

**Proposition 2.5.15.** *If* $m$ *and* $n$ *are coprime integers then* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

**Remark 2.5.16.** It is not true in general if $m$ and $n$ have common divisors.

Now, because of the Fundamental Theorem of Arithmetic and Proposition 2.5.15, it is enough to compute $\varphi$ for powers of prime numbers.

**Lemma 2.5.17.** *Let* $p$ *be a prime number and* $k \in \mathbb{Z}_{>0}$ *then* $\varphi(p^k) = p^k - p^{k-1}$.

*Proof.* The integers not coprime with $p^k$ are precisely those divisible by $p$. There are $p^{k-1}$ multiples of $p$ between 1 and $p^k$. Thus there are $p^k - p^{k-1}$ integers between 1 and $p^k$ that are coprime with $p^k$. ■

**Corollary 2.5.18.** *Let* $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, *where* $p_1, \ldots, p_k$ *are distinct primes. Then*

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{a_i}) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i - 1}).$$

**Example 2.5.19.** Let $n = 8100$ then $n = 2^2 \cdot 5^2 \cdot 3^4$, so

$$\varphi(8100) = \varphi(2^2) \cdot \varphi(5^2) \cdot \varphi(3^4) = (4-2)(25-5)(81-27) = 2 \cdot 20 \cdot 54 = 2160.$$

# 3 Groups

## 3.1 Axioms and examples

**Definition 3.1.1.** 1. A **binary operation** on a set $G$ is a function $\star : G \times G \to G$. We will write $a \star b$ for $\star(a, b)$.

2. A binary operation $\star$ on a set $G$ is called **associative** if

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

for all $a, b, c \in G$.

3. If $\star$ is a binary operation on a set $G$ we say elements $a$ and $b$ of $G$ **commute** if $a \star b = b \star a$. We say $(G, \star)$ is **commutative** if $a \star b = b \star a$ for all $a, b \in G$.

**Example 3.1.2.** 1. $+$ (usual addition) is a commutative, associative binary operation on $\mathbb{Z}_{>0}$ (or on $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively);

2. $\times$ (usual multiplication) is a commutative, associative binary operation on $\mathbb{Z}_{>0}$ (or on $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}$, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively);

3. $-$ (usual subtraction) is a non-commutative, non-associative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$.

   Note that $-$ is not a binary operation on $\mathbb{Z}_{>0}$, since $-$ does not map $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ into $\mathbb{Z}_{>0}$ (for instance $-(3, 5) = -2 \notin \mathbb{Z}_{>0}$).

4. The operations min and max are both associative, commutative binary operations on $\mathbb{Z}_{>0}$ (or on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ respectively).

**Definition 3.1.3.** 1. A **group** is a pair $(G, \star)$, where $G$ is a set and $\star$ is a binary operation on $G$, such that

   (a) (Associativity): $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$, i.e. $\star$ is *associative*;

   (b) (Identity): there exists an element $e \in G$, called an *identity* of $G$, such that for all $a \in G$ we have $a \star e = e \star a = a$;

   (c) (Inverses): for each $a \in G$ there is an element $a^{-1} \in G$ called an *inverse* of $a$, such that $a \star a^{-1} = a^{-1} \star a = e$.

2. A group $(G, \star)$ is called **abelian** (or **commutative**) if $a \star b = b \star a$ for all $a, b \in G$.

3. If a pair $(G, \star)$ satisfies only the first two axioms of part 1 (i.e. it has no inverses), it is called a **monoid**. If it only satisfies axiom (a) then it is called a **semigroup** (i.e. no inverses and no identity).

Let us immediately become less formal in our notations.

- *Abuse of notation:* We will say that $G$ is a group under $\star$ instead of saying that $(G, \star)$ is a group (or sometimes we will just say that $G$ is a group assuming that some operation is fixed and/or is clear from the context).

- *Multiplicative notation:* In most cases we will assume that the binary operation is denoted multiplicatively by $\cdot$ (a dot) and sometimes we will drop it all together, similarly to how one can write $xy$ instead of $x \cdot y$ for multiplication.

  In this notation the first axiom can be written as $a(bc) = (ab)c$ and the commutativity property can be formulated as $ab = ba$.

  Note that the order in which the symbols are written is important as not all groups are commutative!

**Example 3.1.4.** 1. The set $\{1\}$ with the operation $1 \cdot 1 = 1$ is called the **trivial group**.

2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are abelian groups under $+$ (addition) with $e = 0$ and $a^{-1} = -a$.

3. $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}$ are abelian groups under $\times$ (multiplication) with $e = 1$ and $a^{-1} = \frac{1}{a}$.
   Note that $\mathbb{Q}$ is not a group under multiplication as 0 is not invertible.

4. $\mathbb{Z} - \{0\}$ is not a group under multiplication, since 2 has no inverse. However, it is a (commutative) monoid.

5. $\mathbb{Z}/n\mathbb{Z}$ is a commutative group under addition. Note that it is not a group under multiplication, since $[0]$ is not invertible. So when the operation on $\mathbb{Z}/n\mathbb{Z}$ is not specified, it is automatically presumed to be addition.

6. $(\mathbb{Z}/n\mathbb{Z})^\times$ is a commutative group under multiplication. Note that $(\mathbb{Z}/n\mathbb{Z})^\times$ is not *closed under* addition, therefore addition is not even a binary operation on $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus, if the operation on $(\mathbb{Z}/n\mathbb{Z})^\times$ is not specified, it is always presumed to be multiplication.

7. If $(A, \circ)$ and $(B, \star)$ be are groups, we can form a new group $A \times B$, called the **direct product**, whose elements are those in the Cartesian product

$$A \times B = \{(a, b) \mid a \in A, b \in B\},$$

   with the operation defined componentwise:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \circ a_2, b_1 \star b_2).$$

**Proposition 3.1.5.** *If $G$ is a group under operation $\cdot$ then*

1. *the identity of $G$ is unique;*
2. *for each $a \in G$ its inverse $a^{-1}$ is uniquely determined;*
3. *$(a^{-1})^{-1} = a$;*
4. *$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$;*
5. *for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ is independent of how the expression is bracketed.*

*Proof.* 1. Suppose $e$ and $f$ are both identities of $G$. Then, by axiom (b) of Definition 3.1.3, $e = e \cdot f = f$ (for the first equality take $a = f$, for the second $a = e$).

2. Let $e$ denote the identity of $G$ and suppose elements $b, c \in G$ are both inverse to $a$. By axiom (c), $a \cdot b = e = c \cdot a$. Thus

$$\begin{aligned} c &= c \cdot e && \text{(axiom (b))} \\ &= c \cdot (a \cdot b) = (c \cdot a) \cdot b && \text{(axiom (a))} \\ &= e \cdot b = b. && \text{(axiom (b))} \end{aligned}$$

3. We need to show that $a$ is the inverse of $a^{-1}$. By part 2, since the inverse is uniquely determined, we just need to check that $a$ satisfies conditions of axiom (c). Indeed,

$$a^{-1} \cdot a = a \cdot a^{-1} = e.$$

4. Again, we just need to check that the element $b^{-1} \cdot a^{-1}$ satisfies the required conditions. We have

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = ((a \cdot b) \cdot b^{-1}) \cdot a^{-1} = (a \cdot (b \cdot b^{-1})) \cdot a^{-1} =$$
$$= (a \cdot e) \cdot a^{-1} = a \cdot a^{-1} = e,$$

and similarly

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot (a \cdot b)) = b^{-1} \cdot ((a^{-1} \cdot a) \cdot b) =$$
$$= b^{-1} \cdot (e \cdot b) = b^{-1} \cdot b = e.$$

5. Exercise on induction on $n$.

■

**Remark 3.1.6.** Proposition 3.1.5 implies, in particular, that we can use the definite article when talking about **the** identity in $G$ or **the** inverse of a particular element, as they are uniquely determined.

*Multiplicative notation:*

- When using the multiplicative notation for a group $G$, we will often denote the identity element by 1.
- Furthermore, for $x \in G$ and $k \in \mathbb{Z}_{>0}$ we will denote by $x^k$ the product $\underbrace{x \cdot x \cdot \ldots \cdot x}_{k \text{ times}}$ and by $x^{-k}$ the product $\underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{k \text{ times}}$; and $x^0$ is always assumed to be equal to the identity.

**Exercise 3.1.7.** Let $G$ be a group, $x \in G$ and $a, b \in \mathbb{Z}_{>0}$. Prove that $x^{a+b} = x^a \cdot x^b$, and in particular $(x^a)^{-1} = x^{-a}$.

*Additive notation:*

- When using the additive notation for a group $G$ (which we will do only for some examples of abelian groups, where $+$ is the traditional notation for the group operation, e.g. for $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$ and so on), we will often denote the identity element by 0.
- Furthermore, for $x \in G$ and $k \in \mathbb{Z}_{>0}$ we will denote by $k \cdot x$ the sum $\underbrace{x + x + \ldots + x}_{k \text{ times}}$ and by $(-k) \cdot x$ the product $\underbrace{(-x) + (-x) + \ldots + (-x)}_{k \text{ times}}$; and $0 \cdot x$ is always assumed to be equal to the identity 0.

**Proposition 3.1.8.** *Let $G$ be a group (written multiplicatively) and $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions. In particular, if*

$$au = av$$

*or if*

$$ua = va$$

*then $u = v$.*

*Proof.* Existence: put $x = a^{-1} \cdot b$ and $y = b \cdot a^{-1}$.

Uniqueness: if $b = au = av$ then $a^{-1} \cdot b = a^{-1} \cdot a \cdot u = a^{-1} \cdot a \cdot v$. Thus $1 \cdot u = 1 \cdot v$, which implies $u = v$. ■

**Definition 3.1.9.** Let $G$ be a group and $x \in G$. The **order** of $x$, denoted $|x|$, is the minimal *positive* integer $k$ for which $x^k = 1$. If no such integer exists we will say that $x$ has infinite order ($|x| = \infty$).

**Example 3.1.10.**

1. For any group $G$ the identity is the unique element of $G$ of order 1.
2. If $G$ is finite then all elements of $G$ have finite order: if $x \in G$ then the set $\{x^n \mid n \in \mathbb{Z}\} \subset G$ is finite. Thus $x^k = x^m$ for some $k < m$ in $\mathbb{Z}$, and therefore $x^{m-k} = 1$.
3. All nonzero (i.e. non-identity) elements in *additive* groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have infinite order.
4. In the multiplicative groups $\mathbb{R} - \{0\}, \mathbb{Q} - \{0\}$ the element $-1$ is of order 2 and all other non-identity elements have infinite order.
5. Elements of order $n$ in the multiplicative group $\mathbb{C} - \{0\}$ are precisely the primitive $n$'th roots of unity: $e^{\frac{2\pi k}{n} \cdot i} = \cos(\frac{2\pi k}{n}) + \sin(\frac{2\pi k}{n}) \cdot i$ for $1 \leq k < n$ coprime with $n$ and $i = \sqrt{-1}$.
6. In the additive group $\mathbb{Z}/9\mathbb{Z}$ the element $[1]$ has order 9, as $\underbrace{[1] + \ldots + [1]}_{k \text{ times}} = [k]$, and the element $[3] = [1] + [1] + [1]$ has order 3 (recall that $[0]$ is the identity element here).
7. In the multiplicative group $(\mathbb{Z}/7\mathbb{Z})^\times$ the element $[2]$ has order 3 as $[2]^3 = [8] = [1]$ and $[2]^2 = [4] \neq [1]$, and the element $[3]$ has order 6 since

$$[3]^2 = [2],$$

$$[3]^3 = [-1].$$

## 3.2 Symmetric group

**Definition 3.2.1.** Let $X$ be a set. Define $S_X$ to be the set of all bijections $X \to X$. The elements of $S_X$ are called **permutations** of $X$.

In the special case when $X = \{1, 2, \ldots, n\}$ we denote this set by $S_n$.

Let $\sigma, \tau \in S_X$ be two bijections then their composition $\sigma \circ \tau : X \to X$ is also a bijection.

**Proposition 3.2.2.** *The set $S_X$ is a group under the operation of composition of functions.*

*Proof.* We need to check the three axioms of Definition 3.1.3.

(a) Function composition is associative by definition:

$$((\sigma \circ \tau) \circ \rho)(x) = (\sigma \circ \tau)(\rho(x)) = \sigma(\tau(\rho(x))) = (\sigma \circ (\tau \circ \rho))(x)$$

for any $\sigma, \tau, \rho \in S_X, x \in X$.

(b) The identity map $Id_X$ is the identity under composition:

$$Id_X \circ \sigma = \sigma \circ Id_X = \sigma$$

for any $\sigma \in S_X$.

(c) Any bijection $\sigma \in S_X$ admits the unique two-sided inverse $\sigma^{-1} \in S_X$:

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id_X.$$

■

- We call $S_X$ the **symmetric group** on $X$.
- The group $S_n$ is called the *symmetric group of degree $n$*.

We will casually use the multiplicative notation for $S_X$.

**Remark 3.2.3.** Note that the composition of two functions has to be read *from right to left*. That is, if $\sigma, \tau$ are elements of $S_X$ then their product in the group $\sigma \cdot \tau$ is the permutation that is obtained by first applying $\tau$ and then applying $\sigma$.

We will mostly work with groups $S_n$, $n \in \mathbb{Z}_{>0}$ from now on. They play a very important role in the theory of finite groups.

**Exercise 3.2.4.** The order of $S_n$ is $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

- *The two-line notation:* to codify a permutation $\sigma \in S_n$ let us use the following notation

$$\begin{bmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n-1) & \sigma(n) \end{bmatrix}.$$

  For example, $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ denotes a permutation in $S_3$ that sends 1 to 3, 2 to 1 and 3 to 2.

- To compose two permutations one should then trace the path of each element. For example let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}, \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}.$$

  Recall that the product $\sigma \cdot \tau$ should be read from right to left, so, we first apply $\tau$ and then $\sigma$. We trace the path of 1: it is first sent to 2 by $\tau$ and then 2 is being sent to 2 by $\sigma$. We write $1 \to 2 \to 2$. We do the same with the remaining numbers: $2 \to 4 \to 3, 3 \to 3 \to 1, 4 \to 1 \to 4$. Thus

$$\sigma \cdot \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

- To compute the inverse of a given permutation one should just read it from bottom to top. For example, let
$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{bmatrix}.$$
We flip it upside down and rearrange to obtain its inverse:
$$\sigma^{-1} = \begin{bmatrix} 3 & 1 & 5 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{bmatrix}.$$

## 3.3 Cycle decomposition

.

A **cycle** of length $k$ is a string $(a_1\ a_2\ \dots\ a_k)$ of integers in $\{1, \dots, n\}$, which represents a permutation in $S_n$ that *cyclically* permutes those integers. That is, it sends $a_1 \to a_2, a_2 \to a_3, \dots,$ $a_{k-1} \to a_k$, and finally, it sends $a_k$ back to $a_1$ (leaving all other elements intact).

**Remark 3.3.1.**
1. Note that the strings $(a_1\ a_2\ \dots\ a_{k-1}\ a_k)$ and $(a_2\ a_3\ \dots\ a_k\ a_1)$ denote the same permutation.
2. The order of a cycle $(a_1\ a_2\ \dots\ a_k)$ is $k$.
3. The inverse of a cycle $\sigma = (a_1\ a_2\ \dots\ a_k)$ is the cycle obtained from it by reversing the order of the elements:
$$\sigma^{-1} = (a_k\ a_{k-1}\ \dots\ a_1).$$
4. A cycle of length 2 has a special name: it is called a **transposition**.

**Example 3.3.2.** We have
$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$
and
$$(1\ 3\ 2) = (3\ 2\ 1) = (2\ 1\ 3) = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$
in $S_3$.

The cycles $(a_1\ a_2\ \dots\ a_k)$ and $(b_1\ b_2\ \dots\ b_l)$ are called **disjoint** if they have no numbers in common, i.e. $\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset$.

**Remark 3.3.3.** Disjoint cycles commute since they permute different numbers (so it doesn't matter in which order we apply them). If $(a_1\ a_2\ \dots\ a_k)$ and $(b_1\ b_2\ \dots\ b_l)$ are disjoint then
$$(a_1\ a_2\ \dots\ a_k)(b_1\ b_2\ \dots\ b_l) = (b_1\ b_2\ \dots\ b_l)(a_1\ a_2\ \dots\ a_k).$$
Products of disjoint cycles do not depend on the order in which we multiply them.

**Proposition 3.3.4.** *Every permutation $\sigma$ in $S_n$ can be expressed uniquely as the product of (pairwise) disjoint cycles. That is, there exists a partition of the set $\{1, 2, \dots, n\}$ into $l$ subsets*
$$\{1, \dots, n\} = \{a_1, \dots, a_{k_1}\} \sqcup \{a_{k_1+1}, \dots, a_{k_2}\} \sqcup \dots \sqcup \{a_{k_{l-1}+1}, \dots, a_n\},$$
*such that*
$$\sigma = (a_1\ \dots\ a_{k_1}) \cdot (a_{k_1+1}\ \dots\ a_{k_2}) \cdot \dots \cdot (a_{k_{l-1}+1}\ \dots\ a_n).$$
*Moreover, this decomposition is unique up to rearranging the cycles and up to cyclic shifts of numbers within each cycle (which as we know do not change the underlying permutation).*

The proof of Proposition 3.3.4 is algorithmic and is best understood by looking at an example. Consider a permutation in $S_{10}$:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 2 & 1 & 10 & 9 & 8 & 3 & 5 & 6 & 4 \end{bmatrix}.$$

**Cycle Decomposition Algorithm**

| | **Method** | **Example** |
|---|---|---|
| *Step 1* | To start a new cycle pick the smallest element of $\{1, \ldots, n\}$ that has not yet appeared in a previous cycle (if such number doesn't exist, exit the algorithm). Call it $a$ (for the very first step put $a = 1$); begin the new cycle: $(a$ | $(1$ |
| *Step 2* | Look at $\sigma(a)$, call this element $b$. If $b = a$, close the cycle without writing $b$ down; this completes the cycle, go back to Step 1.<br><br>If $b \neq a$ write $b$ next to $a$: $(a\ b$ | $b = \sigma(1) = 7, b \neq 1$, so write: $(1\ 7$ |
| *Step 3* | Look at $\sigma(b)$ and call it $c$. If $c = a$, close the cycle without writing $c$ down and go back to Step 1.<br><br>If $c \neq a$, write $c$ next to $b$ in this cycle: $(a\ b\ c$ Then put $b = c$ and repeat this step. | $c = \sigma(7) = 3 \neq 1$, so write $(1\ 7\ 3$<br><br>Put $b = 3$ and repeat the step: $c = \sigma(3) = 1 = a$, so close the cycle: $(1\ 7\ 3)$ |

In our example, we continue applying the algorithm until all numbers in $\{1, \ldots, 10\}$ are arranged in cycles. The smallest number we did not use yet is 2. We get

$$(1\ 7\ 3)(2\ ,$$

and then since $\sigma(2) = 2$, we immediately close the cycle and start again, now with number 4:

$$(1\ 7\ 3)(2)(4\ .$$

The final result is:

$$\sigma = (1\ 7\ 3)(2)(4\ 10)(5\ 9\ 6\ 8).$$

**Remark 3.3.5.** 1. The order of a permutation $\sigma$ is the lowest common multiple of lengths of cycles in the cycle decomposition of $\sigma$ (because each of the cycles involved should "complete a full circle").

In the example that we considered above, for

$$\sigma = (1\ 7\ 3)(2)(4\ 10)(5\ 9\ 6\ 8)$$

we have

$$|\sigma| = \mathrm{lcm}(3, 1, 2, 4) = 12.$$

2. The inverse of $\sigma$ can be obtained by taking the product of inverses of all cycles in the cycle decomposition of $\sigma$ (this is a corollary of Remark 3.3.3 and Proposition 3.1.5.4).

   In our example:

$$\sigma^{-1} = (3\ 7\ 1)(2)(10\ 4)(8\ 6\ 9\ 5) = (1\ 3\ 7)(2)(4\ 10)(5\ 8\ 6\ 9).$$

**Definition 3.3.6.** 1. Let $n$ be a positive integer. A **partition** $\lambda$ of $n$ is a tuple $(\lambda_1, \lambda_2, \ldots \lambda_l)$ of positive integers with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_l$ and

$$n = \lambda_1 + \lambda_2 + \ldots + \lambda_l.$$

   Another notation for $\lambda$ is $\lambda_1 + \lambda_2 + \ldots + \lambda_l$.

   For example, partitions of 4 are

$$(4),\ (3,1),\ (2,2),\ (2,1,1),\ (1,1,1,1),$$

   or we can write them as

$$4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1$$

   to avoid confusion with permutations. In this notation the partition $1+3$ is the same as $3+1$.

2. Let $\sigma \in S_n$ be the product of $l$ disjoint cycles of lengths $k_1, k_2, \ldots, k_l$ respectively, so that every number in $\{1, \ldots, n\}$ is involved in one of the cycles. Then the partition $k_1+k_2+\ldots+k_l$ of $n$ is called the **cycle type** of $\sigma$.

Sometimes, it is useful to add one final step to the cycle decomposition algorithm to obtain a shorter notation:

**Cycle Decomposition Algorithm (cont.)**

| | | |
|---|---|---|
| *Final step* | Remove all cycles of length 1. | |

In this notation permutations (1 3)(2 4) and (1 2 3 4) can be regarded as elements of $S_n$ for any $n \geq 4$. For example in $S_6$ their "full" cycle decompositions would be (1 3)(2 4)(5)(6) and (1 2 3 4)(5)(6) respectively. Moreover, the multiplication rules for these elements do not depend on the embedding into $S_n$ and are the same as in $S_4$.

**Corollary 3.3.7.** *The symmetric group $S_n$ is non-abelian for all $n \geq 3$.*

*Proof.* The transpositions (1 2) and (2 3) can be regarded as elements of $S_n$ for any $n \geq 3$. We note that these permutations do not commute:

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

$$(2\ 3)(1\ 2) = (1\ 3\ 2).$$

■

**Example 3.3.8.** The 6 elements of $S_3$ have the following cycle decomposition:

**The Group $S_3$**

| Permutation | Full cycle decomposition | Short cycle notation | Cycle type |
|---|---|---|---|
| $\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix}$ | (1)(2)(3) | $e$ | $1+1+1$ |
| $\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}$ | (1 2)(3) | (1 2) | $2+1$ |
| $\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$ | (1 3)(2) | (1 3) | |
| $\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}$ | (1)(2 3) | (2 3) | |
| $\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}$ | (1 2 3) | (1 2 3) | 3 |
| $\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$ | (1 3 2) | (1 3 2) | |

## 3.4 Dihedral groups

An important class of examples of groups is the class of groups whose element are symmetries of geometric objects. The simplest subclass of such objects are regular planar figures.

**Definition 3.4.1.** For each $n \geq 3$ let $D_{2n}$ be the set of symmetries of the regular $n$-gon, where symmetry is a motion of the plane, that preserves distances between points and fixes the $n$-gon as a set.

It is easy to check that any such symmetry must map the vertices of the $n$-gon to vertices and edges to edges. Moreover, since a symmetry preserves distances, it must preserve the connectivity between the vertices, i.e. if two vertices were connected by an edge, they stay connected, and if they were disconnected they stay disconnected. So every symmetry preserves the relative order of vertices either fixing the clock-wise orientation of the numbering or reversing it.

Let us number the vertices of the $n$-gon in the clockwise direction by numbers $\{1, \dots, n\}$. Then each symmetry $s$ can be described by the corresponding permutation $\sigma$, where $\sigma(i) = j$ if $s$ maps vertex $i$ to vertex $j$. For example, if $s$ is the clockwise rotation by $\frac{2\pi}{n}$ radians then $\sigma = (1\ 2\ 3\ \dots\ n)$ is the cycle of length $n$.

We make $D_{2n}$ into a group by defining $st$ for symmetries $s$ and $t$ to be their composition: we first apply $t$ and then apply $s$. If $\sigma$ and $\tau$ are permutations corresponding to $s$ and $t$ respectively then the permutation corresponding to $st$ is $\sigma \circ \tau$.

This binary operation is associative since function composition is associative. The identity element is the identity symmetry, and the inverses are the inverse functions (as symmetries are bijective).

**Definition 3.4.2.** We call $D_{2n}$ the **dihedral group** of order $2n$.

**Proposition 3.4.3.** *The order of $D_{2n}$ is indeed $2n$.*

*Proof.* Let $s \in D_{2n}$ and let $\sigma \in S_n$ be the corresponding permutation.

We claim that a symmetry $s$ is uniquely determined by where it sends vertices 1 and 2. Indeed, suppose $\sigma(1) = i$ (note that there are $n$ options for the value of $i$) then $\sigma(2)$ must be the number of a vertex connected to vertex $i$ by an edge. So, $\sigma(2) = i \pm 1$ (where we put $0 = n, n+1 = 1$), hence there are two options for it.

Note that if $\sigma(2) = i + 1$ then this means that $s$ preserves the orientation, and in this case we deduce that $\sigma(3) = i + 2, \sigma(4) = i + 3$, and so on (where these equations are considered modulo $n$).

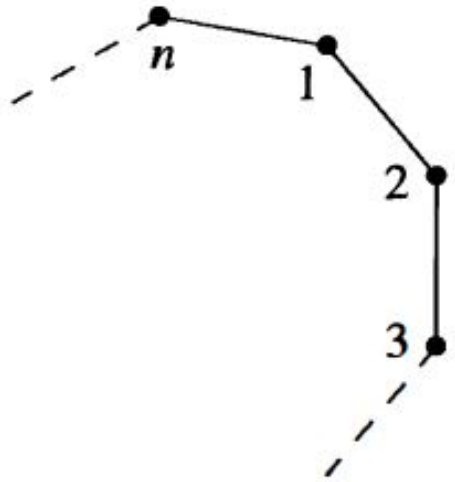



Figure 1: Labeling of vertices

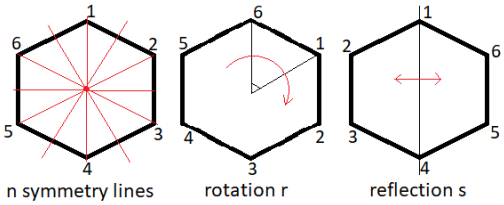



Figure 2: Symmetries $r$ and $s$

In the case when $\sigma(2) = i - 1$, the symmetry $s$ changes the orientation, and we deduce that $\sigma(3) = i - 2, \sigma(4) = i - 3$, and so on.

Hence, the values of $\sigma$ on $\{3, 4, \ldots, n\}$ are determined by its values on $\{1, 2\}$.

Moreover, we have showed that there are at most $2n$ elements in $D_{2n}$. Let us show next that every possibility above can be actually realized by some symmetry.

Let us first apply the rotation by $\frac{2\pi i}{n}$ radians. It sends 1 to $i$ and 2 to $i + 1$. If we follow by a reflection about the line passing through vertex $i$, then 2 will be sent to $i - 1$. ■

**Remark 3.4.4.** Using the proof above let us list all the elements in $D_{2n}$. Let $r$ denote the clockwise rotation by $\frac{2\pi}{n}$ radians and let $s$ denote the reflection about the line passing through vertex 1. Let $\rho$ and $\sigma$ be the permutations corresponding to $r$ and $s$ respectively.

Note that the clockwise rotation by $\frac{2\pi i}{n}$ radians can be expressed as $r^i$ and that $r^{n-i} = r^{-i}$ (i.e. the counter-clockwise rotation by $\frac{2\pi i}{n}$ radians is the same as the clockwise rotation by $\frac{2\pi(n-i)}{n}$ radians). Moreover, we claim that reflection about the line passing through $i$ can be expressed as $r^i \cdot s \cdot r^{-i}$. Indeed, it is enough to check that it preserves vertex $i$ and sends $i + 1$ to $i - 1$:

$$\rho^i \circ \sigma \circ \rho^{-i}(i) = \rho^i \circ \sigma(1) = \rho^i(1) = i,$$

$$\rho^i \circ \sigma \circ \rho^{-i}(i + 1) = \rho^i \circ \sigma(2) = \rho^i(n) = i - 1.$$

Thus we have $n$ orientation preserving symmetries (i.e. rotations):

$$e = r^0,\ r,\ r^2,\ \ldots,\ r^{n-1},$$

and we have $n$ orientation-altering symmetries (i.e. a rotation by $\frac{2\pi i}{n}$ radians followed by a reflection about the line passing through vertex $i$). By the above discussion, those can be expressed as $(r^i \cdot s \cdot r^{-i}) \cdot r^i = r^i \cdot s$. So the full list is:

$$D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

We have seen that every element of $D_{2n}$ can be expressed in terms of rotation $r$ and reflection $s$. Now we would like to know how to multiply and invert such expressions. For example, we have established that

1.
$$(r^i)^{-1} = r^{n-i}, \text{ for all } i \in \{0, \ldots, n-1\}.$$

Moreover, it is easy to see that

2.
$$s^{-1} = s,$$

as $s$ is a reflection.

Now the question is: what kind of symmetry $sr^i$ or $r^k s \cdot r^i s$ are? We know that it must either be of the form $r^a s$ or just $r^b$. We claim that

3.
$$sr^i = r^{-i}s, \text{ for all } i \in \{0, \ldots, n-1\}.$$

To show this it is enough to prove that $sr = r^{-1}s$ and then proceed by induction. Recall again that to check the equality of two symmetries, we can just make sure that they send vertices $n$ and 1 to the same vertices. We claim that both $sr$ and $r^{-1}s$ just swap these two vertices:

$$\sigma \circ \rho(n) = \sigma(1) = 1, \text{ and } \rho^{-1} \circ \sigma(n) = \rho^{-1}(2) = 1;$$
$$\sigma \circ \rho(1) = \sigma(2) = n, \text{ and } \rho^{-1} \circ \sigma(1) = \rho^{-1}(1) = n.$$

We can phrase the equations 1,2 and 3 above in a more compact way as follows:

1'. $r^n = e$,

2'. $s^2 = e$,

3'. $sr = r^{-1}s$.

The equations above are called **relations**, whereas the elements $s$ and $r$ are called **generators** of $D_{2n}$. Note that knowing these relations we know how multiply any two elements in $D_{2n}$. For instance,

$$r^a s \cdot r^b s = r^a (r^{-b} s) s = r^{a-b},$$

and

$$r^a s \cdot r^b = r^a (r^{-b} s) = r^{a-b} s.$$

## 3.5 Group presentations

We can follow the example of Dihedral groups and introduce the notion of generators and relations for any abstract group.

**Definition 3.5.1.** A subset $S$ of $G$ is called a set of **generators** of $G$ if any element of $G$ can be written as a finite product (including the empty product to express the identity element) of elements of $S$ and their inverses. That is, for any $g \in G$ one can find $s_1, \ldots, s_k \in S$ (not necessarily distinct) and $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$, so that

$$g = s_1^{\varepsilon_1} \cdot s_2^{\varepsilon_2} \cdot \ldots \cdot s_k^{\varepsilon_k}.$$

In case $S$ is a set of generators of $G$ we write $G = \langle S \rangle$, and we say "$S$ **generates** $G$" or "$G$ **is generated by** $S$".

**Remark 3.5.2.** The way to express $g$ in terms of elements of $S$ doen't have to be unique.

**Example 3.5.3.**

1. The set $\{1\}$ generates the additive group $\mathbb{Z}$ as any $n \in \mathbb{Z}$ can be expressed as
$$\underbrace{1+1+\ldots+1}_{n \text{ times}},$$
if it is non-negative, or as
$$\underbrace{(-1)+(-1)+\ldots+(-1)}_{n \text{ times}},$$
if it is negative.
2. Similarly, $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$.
3. We have established that $D_{2n} = \langle r, s \rangle$.

**Proposition 3.5.4.** *The symmetric group $S_n$ is generated by the set of all transpositions $\{(i\ j)\}_{1 \le i < j \le n}$.*

*Proof.* We need to show that any permutation can be expressed as a product of transpositions. Note that since every permutation is a product of cycles, it is enough to show that any cycle $(a_1\ a_2\ \ldots\ a_k)$ can be written as a product of transpositions. It is easy to verify that

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k),$$

since

$$(a_1\ a_2)(a_2\ a_3)\ldots(a_{k-1}\ a_k)[a_i] = (a_1\ a_2)\ldots(a_{i-1}\ a_i)(a_i\ a_{i+1})[a_i] = (a_1\ a_2)\ldots(a_{i-1}\ a_i)[a_{i+1}] = a_{i+1}.$$

■

**Exercise 3.5.5.** It can be shown that $S_n$ can in fact be generated by a smaller set: the set of elementary transpositions $\{s_i\}_{1 \le i \le n-1}$, where $s_i = (i\ i+1)$.

Any equations satisfied by the generators of a group $G$ are called **relations.**

Thus $r^n = 1, s^2 = 1$ and $rs = sr^{-1}$ are relations in $D_{2n}$. Moreover, these relations satisfy the property that any other relation can be deduced from these three.

Let now $S$ be a set of generators of $G$ and $R_1, \ldots, R_k$ be relations (i.e. equations involving products of elements of $S$, their inverses, and 1). We say that

$$G = \langle S \mid R_1, \ldots, R_k \rangle$$

is a **presentation** of $G$ if any other relation that elements of $S$ satisfy in $G$ can be deduced from the relations above.

**Example 3.5.6.**

1. We have proved that
$$D_{2n} = \langle r, s |\ r^n = 1,\ s^2 = 1,\ rs = sr^{-1} \rangle.$$
2. The following presentation is not obvious, but we will leave it without a proof:
$$S_n = \langle s_1,\ \ldots,\ s_{n-1} \mid s_i^2 = e, s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, s_i s_j = s_j s_i,\ \text{for } |i-j| \ge 2 \rangle,$$
where $s_i = (i\ i+1)$.
3. $\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1 \rangle$ is a presentation of $\mathbb{Z}/n\mathbb{Z}$ in the multiplicative notation (with $x = [1]$).

**Definition 3.5.7.** A group $G$ is called free on the set of generators $S$ if $G = \langle S \rangle$ and there are no nontrivial relations that elements of $S$ satisfy.

A more rigorous definition of a free group and an explicit construction for it exist, but they are out of scope of this class.

**Example 3.5.8.** The additive group $\mathbb{Z}$ is a free group generated by $\{1\}$, i.e. $\mathbb{Z} = \langle 1 \rangle$ is actually a presentation of $\mathbb{Z}$.

In general group presentations are very useful for computation, however, they are not easy to deal with. First of all, it might be difficult to prove that the set of relations that we picked is really enough and that all other possible relations can be deduced from them. Second, given a group presentation, it is often difficult to understand if two elements, written as products of generators and their inverses, are actually equal.

**Exercise 3.5.9.** One can show that in the group

$$G = \langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \rangle$$

every element is equal to the identity, i.e. $G = \{1\}$. In particular, one can deduce from the relations above that $u = v = 1$.

## 3.6 Group homomorphisms

In general a notion of a homomorphism between two algebraic objects means a map that respects the algebraic structure. For groups it yields the following

**Definition 3.6.1.** 1. Let $(G, \star)$ and $(H, \circ)$ be two groups. A **group homomorphism** from $G$ to $H$ is a function

$$\phi : G \to H$$

on the underlying sets, such that

$$\phi(a \star b) = \phi(a) \circ \phi(b)$$

for any $a, b \in G$.

2. A group homomorphism $\phi : G \to H$ is called an **isomorphism** if it is bijective. If there exists an isomorphism between $G$ and $H$ we say that $G$ and $H$ are **isomorphic**, we write: $G \cong H$.

   **Remark 3.6.2.** If $\phi : G \to H$ is an isomorphism then the inverse map $\phi^{-1} : H \to G$ is also a group homomorphism, as

$$\phi^{-1}(\phi(a) \cdot \phi(b)) = \phi^{-1}(\phi(a \cdot b)) = a \cdot b.$$

3. A homomorphism from $G$ to itself is called an **endomorphism**.

4. A bijective endomorphism (i.e. an isomorphism from $G$ to itself) is called an **automorphism** of $G$.

**Example 3.6.3.** 1. For any group $G$ the identity map $id_G : G \to G$ is an automorphism of $G$.

2. For any two groups $G, H$ there exist a homomorphism $t : G \to H$ called the **trivial homomorphism** given by

$$t(g) = 1 \quad \forall\, g \in G.$$

3. The exponential map $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ defined by $\exp(x) = e^x$ is a group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \times)$.

4. The quotient map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a surjective homomorphism of additive groups.

5. Any bijection $f : X \to Y$ induces an isomorphism $\phi : S_X \to S_Y$ of symmetric groups given by

$$\phi(\sigma) = f \circ \sigma \circ f^{-1}.$$

6. The inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ induce injective homomorphisms of additive groups.

   Similarly, the inclusions $\mathbb{Q}_{>0} \subset \mathbb{Q} - \{0\} \subset \mathbb{R} - \{0\} \subset \mathbb{C} - \{0\}$ give injective homomorphisms of multiplicative groups.

7. The map $\phi : D_{2n} \to S_n$ that sends a symmetry $t$ to the corresponding permutation of vertices $\tau$ is an injective group homomorphism.

   Note that different choices of numbering of the vertices give different group homomorphisms $D_{2n} \to S_n$. A more conceptual way of saying this is to say that there is an injective group homomorphism $D_{2n} \to S_V$, where $V$ is the set of vertices.

**Remark 3.6.4.** If $\phi : G \to H, \psi : H \to K$ are group homomorphisms then their composition $\psi \circ \phi : G \to K$ is also a group homomorphism, since

$$\psi(\phi(a \cdot b)) = \psi(\phi(a) \cdot \phi(b)) = \psi(\phi(a)) \cdot \psi(\phi(b)).$$

**Exercise 3.6.5.** Let $\phi : G \to H$ be a group homomorphism then

1. $\phi(1) = 1$, and
2. $\phi(g)^{-1} = \phi(g^{-1})$ for any $g \in G$.

**Proposition 3.6.6.** *Let $\phi : G \to H$ be an isomorphism of groups. Then*

1. *$|G| = |H|$,*
2. *$G$ is abelian if and only if $H$ is abelian,*
3. *$|x| = |\phi(x)|$ for any $x \in G$.*

*Proof.* 1. This is true for bijective maps.

2. It is enough to prove this in one direction and then apply this to the isomorphism $\phi^{-1} : H \to G$. So, suppose $H$ is abelian and let $a, b \in G$ then $a \cdot b = \phi^{-1}(\phi(a) \cdot \phi(b)) = \phi^{-1}(\phi(b) \cdot \phi(a)) = b \cdot a$. Which proves that $G$ is abelian as well.

3. Let $|x| = n \in \mathbb{Z}_{>0}$. Note that $\phi(x^k) = \phi(x)^k$ for any $k \in \mathbb{Z}$. Therefore, $\phi(x)^n = \phi(x^n) = \phi(1) = 1$ (by Exercise 3.6.5.1). Moreover, if $\phi(x)^k = 1$ then $\phi(x^k) = 1$, however, the only element that maps to 1 in $H$ is $1 \in G$ (as $\phi$ is one-to-one). So we deduce that $x^k = 1$ and thus $k \geq n$.

■

**Example 3.6.7.** 1. The groups $\mathbb{Z}/6\mathbb{Z}$ and $S_3$ have the same number of elements, however they are not isomorphic, as the first one is abelian, and the second one is not.

2. The groups $D_6$ and $S_3$ are isomorphic with isomorphism given by the natural map $D_6 \to S_3$ sending a symmetry $t$ to the corresponding permutation $\tau$ (this map is an injective map of finite sets of the same order).

**Lemma 3.6.8.** *If $S$ is a set of generators of $G$ and $\phi : G \to H$ is a group homomorphism then $\phi$ is uniquely determined by its restriction to $S$.*

*Proof.* By definition, any $g \in G$ can be expressed as a product $s_1^{\varepsilon_1} \cdot \ldots \cdot s_k^{\varepsilon_k}$ for $s_1, \ldots, s_k \in S$ and $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$. Therefore, we recover $\phi(g)$ as $\phi(s_1)^{\varepsilon_1} \cdot \ldots \cdot \phi(s_k)^{\varepsilon_k}$ (as $\phi$ is a group homomorphism). ■

**Remark 3.6.9.** Let $G = \langle S \mid R_1, \ldots, R_k \rangle$ be a presentation of group $G$ and let $H$ be any other group.

If $\phi : G \to H$ is a homomorphism then the set of elements $\{\phi(s)\}_{s \in S}$ must satisfy the relations $\phi(R_1), \ldots, \phi(R_k)$.

Moreover, any map of sets $\overline{\phi} : S \to H$, such that the relations $\overline{\phi}(R_1), \ldots, \overline{\phi}(R_k)$ are satisfied in $H$ can be extended to a (unique) group homomorphism $\phi : G \to H$.

**Example 3.6.10.** Recall that $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$. Suppose $G$ is a group containing elements $a, b$, such that

$$a^n = b^2 = 1, \text{ and } ab = ba^{-1} \quad (\star).$$

Then there exist a unique group homomorphism $\phi : D_{2n} \to G$ such that $\phi(r) = a$ and $\phi(s) = b$.

For example, let $k$ be a divisor of $n$ and let $D_{2k} = \langle a, b \mid a^k = b^2 = 1,\ ab = ba^{-1} \rangle$ (that is let $a$ denote the clockwise rotation by $\frac{2\pi}{k}$ and $b$ denote a reflection fixing one of the vertices). Note that since $k \mid n$ the elements $a$ and $b$ satisfy the relations $(\star)$. We get a surjective group homomorphism

$$\phi : D_{2n} \to D_{2k},$$

$$r \mapsto a,$$

$$s \mapsto b.$$

**Definition 3.6.11.** The kernel of a group homomorphism $\phi : G \to H$ is the subset

$$\mathrm{Ker}(\phi) = \{x \in G |\ \phi(x) = 1\} \subset G,$$

**Example 3.6.12.**

1. Let $t : G \to H$ be the trivial homomorphism, then $\mathrm{Ker}(t) = G$.
2. Let $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the quotient map, then $\mathrm{Ker}(\pi) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.
3. Let $n = k \cdot d$ and let $\phi : D_{2n} \to D_{2k}$ be the map from Example 3.6.10, then
$$\mathrm{Ker}(\phi) = \{1, r^k, r^{2k}, \ldots, r^{(d-1)k}\}.$$
4. Let $\phi : D_{2n} \to S_n$ be the standard map, then $\mathrm{Ker}(\phi) = \{1\}$.

**Proposition 3.6.13.** *A group homomorphism $\phi : G \to H$ is injective if and only if* $\mathrm{Ker}(\phi) = \{1\}$.

*Proof.* By Exercise 3.6.5, $1 \in \mathrm{Ker}(\phi)$ for any homomorphism $\phi$. If $\phi$ is injective then the only element that maps to 1 is 1, so $\mathrm{Ker}(\phi = \{1\}$.

Conversely, suppose $\mathrm{Ker}(\phi) = \{1\}$. Suppose $a, b \in G$ are such that $\phi(a) = \phi(b)$ then $\phi(ab^{-1}) = \phi(a) \cdot \phi(b)^{-1} = 1$, so $ab^{-1} \in \mathrm{Ker}(\phi)$. Therefore, $ab^{-1} = 1 \Rightarrow a = b$. ∎

# 4 Subgroups

## 4.1 Definitions and examples

When dealing with some class of algebraic objects, we will use the word *subobject* to indicate a subset that inherits the algebraic structure from a bigger object. In case of group we get the following

**Definition 4.1.1.** A **subgroup** of a group $G$ is a *nonempty* subset $H \subset G$ that is closed under products and inverses, i.e.

- $x, y \in H \Rightarrow xy \in H$,
- $x \in H \Rightarrow x^{-1} \in H$.

**Notation:** We will write $H \leq G$ to indicate that $H$ is a subgroup of $G$.

**Remark 4.1.2.** If $H$ is a subgroup of $G$ then $H$ itself is a group with respect to the same operation (i.e. the binary operation on $G$ restricts to the binary operation on $H$). Note that the identity element of $G$ belongs to $H$, since $H$ is nonempty and contains some element $x \in H$, and thus $x^{-1} \in H$ and

$$1 = x \cdot x^{-1} \in H.$$

The element 1 is the identity element of group $H$.

**Remark 4.1.3.** The relation "is a subgroup of" is transitive, i.e. if $K \leq H$ and $H \leq G$ then $K \leq G$.

**Example 4.1.4.**

1. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$;
2. $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$;
3. $(\mathbb{Q} - \{0\}, \times)$ is a subgroup of $(\mathbb{R} - \{0\}, \times)$;
4. Any group $G$ has two subgroups $H = G$ and $H = \{1\}$; the latter is called the *trivial subgroup* of $G$.
5. $n\mathbb{Z} = \{a \in \mathbb{Z} |\ a \text{ is divisible by } n\}$ is a subgroup of $\mathbb{Z}$ (w.r.t. addition).
6. The set $H = \{1, r, r^2, \ldots, r^{n-1}\}$ of all rotations is a subgroup of $D_{2n} = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$.
7. The set $\{-1, 1\}$ is a subgroup in $(\mathbb{R} - \{0\}, \times)$.
8. If $X \subset Y$ then $S_X$ is naturally a subgroup of $S_Y$. We think of permutations $X \to X$ as permutations $Y \to Y$ fixing elements of $Y - X$. E.g. $S_2 = \{e, (`1\ 2)\} \leq S_k$ for any $k \geq 2$.
9. Here are some examples of subsets that are **not** subgroups:
   (a) $\mathbb{Q} - \{0\}$ under multiplication is not a subgroup of $\mathbb{R}$ under addition, even though both are groups and $\mathbb{Q} - \{0\}$ is naturally a subset of $\mathbb{R}$. This is because the operation of multiplication on $\mathbb{Q} - \{0\}$ is not the restriction of the operation of addition on $\mathbb{R}$.
   (b) Similarly, $(\mathbb{Z}/n\mathbb{Z})^\times$ is not a subgroup of $\mathbb{Z}/n\mathbb{Z}$.
   (c) $\mathbb{Z}_{\geq 0}$ is not a subgroup of $\mathbb{Z}$ as it is not closed under inverses.
   (d) $D_6$ is not a subgroup of $D_8$ since the former is not a subset of the latter.
   (e) The set $A = \{-1, 0, 1\}$ is not a subgroup of $\mathbb{Z}$ since it is not closed under addition (e.g. $1 + 1 = 2 \notin A$).

**Proposition 4.1.5** (The Subgroup Criterion)**.** *A subset $H$ of a group $G$ is a subgroup if and only if*

1. *$H \neq \emptyset$, and*
2. *for any $x, y \in H,\ xy^{-1} \in H$.*

*Proof.* Suppose $H$ is a subgroup, then $H$ is nonempty and for any $x, y \in H$ we have $y^{-1} \in H$ and therefore $xy^{-1} \in H$.

Conversely, if $H$ satisfies conditions 1 and 2 then there exists some $a \in H$, and thus $1 = a \cdot a^{-1} \in H$. For any $y \in H$ we must have $1 \cdot y^{-1} = y^{-1} \in H$, so $H$ is closed under inverses. Moreover, for any $x, y \in H,\ y^{-1} \in H$ and $x \cdot (y^{-1})^{-1} = xy \in H$, and thus $H$ is closed under multiplication. ∎

**Lemma 4.1.6.** *If $H_i \leq G$ for all $i \in I$ then $\bigcap_{i \in I} H_i \leq G$.*

*Proof.* Since $1 \in H_i$ for all $i \in I$, we have $1 \in \bigcap_{i \in I} H_i$, so the intersection is nonempty. Moreover, for any $x, y \in \bigcap_{i \in I} H_i,\ xy^{-1} \in H_i$ for all $i \in I$, since each $H_i$ is a subgroup, so $xy^{-1} \in \bigcap_{i \in I} H_i$, and thus $\bigcap_{i \in I} H_i$ is a subgroup by the subgroup criterion. ∎

**Remark 4.1.7.** In general the union of two subgroups is not a subgroup.

**Exercise 4.1.8.** Let $\phi : G \to H$ be a group homomorphism then $\mathrm{Ker}(\phi) \leq G$ and $\mathrm{Im}(\phi) \leq H$.

**Definition 4.1.9.** Let $A$ be a subset of a group $G$. Define

$$\langle A \rangle = \bigcap_{H \leq G, A \subset H} H \leq G$$

to be the intersection of all subgroups of $G$ containing $A$. Then $\langle A \rangle$ is the smallest subgroup of $G$ containing $A$. We say that $\langle A \rangle$ is the subgroup generated by $A$.

**Proposition 4.1.10.** *$\langle A\rangle$ is the set of all finite products (including the empty product, i.e. the identity of $G$) $a_1^{\varepsilon_1}\cdot\ldots a_k^{\varepsilon_k}$, where $a_i\in A$ and $\varepsilon_i\in\{-1,1\}$.*

*Proof.* If $H\leq G$ and $A\subset H$ then $H$ must contain all products of elements of $A$ and their inverses, i.e. $\{a_1^{\varepsilon_1}\cdot\ldots a_k^{\varepsilon_k}|\ a_i\in A,\varepsilon_1\in\{-1,1\}\}\subset H$. Thus, this set is contained in the intersection of such subgroups:

$$\{a_1^{\varepsilon_1}\cdot\ldots a_k^{\varepsilon_k}|\ a_i\in A,\varepsilon_1\in\{-1,1\}\}\subset\langle A\rangle.$$

On the other hand, the set $\{a_1^{\varepsilon_1}\cdot\ldots a_k^{\varepsilon_k}|\ a_i\in A,\varepsilon_1\in\{-1,1\}\}$ is a subgroup of $G$ containing $A$, because "

- $1\in\{a_1^{\varepsilon_1}\cdot\ldots a_k^{\varepsilon_k}|\ a_i\in A,\varepsilon_1\in\{-1,1\}\}$ is the empty product;
- it is closed under inverses: $(a_1^{\varepsilon_1}\cdot\ldots a_k^{\varepsilon_k})^{-1}=a_k^{-\varepsilon_k}\cdot\ldots\cdot a_1^{-\varepsilon_1}$;
- it is closed under products (obviously).

■

**Example 4.1.11.** 1. $n\mathbb{Z}=\langle n\rangle\leq\mathbb{Z}$;

2. $H=\{1,r,r^2,\ldots,r^{n-1}\}=\langle r\rangle\leq D_{2n}$;

3. $\mathbb{Z}=\langle 1\rangle\leq\mathbb{Q}$.

**Remark 4.1.12.** If $H\leq G$ then $H$ is a group equipped with an injective group homomorphism $i:H\to G,\ i(h)=h$.

Conversely, if $G,H$ are two groups and $i:H\to G$ is an injective group homomorphism then $H$ is isomorphic to the subgroup $i(H)$ of $G$.

## 4.2 Centralizers, normalizers, and the center

Let $A$ be a nonempty subset of a group $G$.

**Definition 4.2.1.** The **centralizer** of $A$ in $G$ (denoted $C_G(A)$) is the set of elements in $G$ that commute with elements of $A$, i.e.

$$C_G(A)=\{g\in G\mid\forall a\in A:\ ga=ag\}.$$

One can equivalently define $C_G(A)$ as the set of all $g\in G$ for which $gag^{-1}=a$ for any $a\in A$.

**Proposition 4.2.2.** *The centralizer of $A$ in $G$ is a subgroup of $G$.*

*Proof.* First, we note that $1\in C_G(A)$.

Second, if $x,y\in C_G(A)$ and $a\in A$ then

$$ya=ay\iff a=y^{-1}ay\iff ay^{-1}=y^{-1}a,$$

so $y\in C_G(A)$, and

$$(xy)a=x(ya)=x(ay)=(xa)y=(ax)y=a(xy),$$

so $xy\in C_G(A)$. ■

**Definition 4.2.3.** If $A=G$ the centralizer $C_G(G)$ is called the **center** of $G$ and denoted $Z(G)$ (i.e. $Z(G)$ is the set elements of $G$ that commute with all other elements of $G$).

**Corollary 4.2.4** (of Proposition 4.2.2)**.** *The center $Z(G)$ is a subgroup of $G$.*

**Remark 4.2.5.** The center $Z(G)$ is a subset of $C_G(A)$ for any $A\subset G$.

**Proposition 4.2.6.** *If $S$ is a set of generators of $G$ and $x\in G$ commutes with all elements of $S$ then $x\in Z(G)$.*

*Proof.* For any $s \in S$

$$xs = sx \iff x = sxs^{-1} \iff s^{-1}x = xs^{-1},$$

so $x$ commutes with $s^{-1}$ and therefore

$$x(s_1^{\varepsilon_1} \cdot \ldots \cdot s_k^{\varepsilon_k}) = s_1^{\varepsilon_1} \cdot x \cdot s_2^{\varepsilon_2} \cdot \ldots \cdot s_k^{\varepsilon_k} = \ldots = s_1^{\varepsilon_1} \cdot \ldots \cdot s_{k-1}^{\varepsilon_{k-1}} \cdot x \cdot s_k^{\varepsilon_k} = (s_1^{\varepsilon_1} \cdot \ldots \cdot s_k^{\varepsilon_k})x$$

for any $s_i \in S$ and any $\varepsilon_i \in \{-1, 1\}$. ■

**Definition 4.2.7.** Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. The **normalizer** of $A$ in $G$ is the set

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

Equivalently, $N_G(A)$ is the set of all $g \in G$ for which

$$gA = Ag,$$

where $gA = \{ga \mid a \in A\}$ and $Ag = \{ag \mid a \in A\}$.

**Remark 4.2.8.** We have $C_G(A) \subset N_G(A)$. However, the opposite inclusion doesn't hold in general. For $g \in N_G(A)$ and $a \in A$ the element $gag^{-1}$ lies in $A$, however it doesn't have to be equal to $a$.

**Proposition 4.2.9.** *The normalizer $N_G(A)$ is a subgroup of $G$.*

*Proof.* First, $1 \in N_G(A)$ since $C_G(A) \subset N_G(A)$.

Second, let $x, y \in N_G(A)$. Note that if $A = B$ as subsets of $G$ then for any $g \in G$

$$gA = gB \text{ and } Ag = Bg.$$

We deduce that

$$Ay^{-1} = y^{-1}(yAy^{-1}) = y^{-1}A,$$

so $y^{-1} \in N_G(A)$. Moreover,

$$(xy)A(xy)^{-1} = (xy)A(y^{-1}x^{-1}) = x(yAy^{-1})x^{-1} = xAx^{-1} = A,$$

so $xy \in N_G(A)$. ■

**Example 4.2.10.**

1. If $G$ is abelian, all elements of $G$ commute with each other, so $Z(G) = G$.
2. Let $G = D_{2n}$ and let $A = \{1, r, r^2, \ldots, r^{n-1}\}$. We show that $C_G(A) = A$.

   Note that no reflections commute with $r$:

   $$(r^k s)r = r^{k-1}s \neq r(r^k s).$$

   However, all rotations commute with each other. So we deduce that $C_G(A) = A$.
3. Let $G$ and $A$ be as in the previous example. We will show that $N_G(A) = G$.

   Since $C_G(A) \subset N_G(A)$, it is enough to show that any reflection belongs to the normalizer. We have

   $$r^k s\{1, r, r^2 \ldots, r^{n-1}\}sr^{-k} = r^k\{1, r^{-1}, r^{-2}, \ldots, r^{1-n}\}r^{-k} = \{1, r^{n-1}, r^{n-2}, \ldots, r\} = A.$$
4. Let $G = D_{2n}$. If $n = 2k$ is even then $Z(G) = \{1, r^k\}$. If $n$ is odd then $Z(G) = \{1\}$.

   *Proof.* Suppose $n = 2k$. First, note that $r^k \cdot r = r \cdot r^k$ and $r^k \cdot s = s \cdot r^{-k} = s \cdot r^k$, so $r^k \in Z(G)$. Second, by part 2 above, no reflection commutes with $r$ and if $l \neq 0, n/2$

   $$r^l s = sr^{n-l} \neq sr^l,$$

   so $r^l \notin Z(G)$. We conclude that $Z(G) = \{1, r^k\}$.

   Now suppose $n$ is odd. All the reasoning above still applies to $D_{2n}$, and thus no reflection commutes with $r$ and no rotation $r^l$ commutes with $s$ unless $l = 0$ (since $l \neq n/2$). Thus, the center $Z(G)$ contains only the identity element. ■

## 4.3 Cyclic groups

**Definition 4.3.1.** 1. A group $G$ is called **cyclic** if it is generated by a single element, i.e. there exists $x \in G$ such that $G = \langle x \rangle$.

2. We say that a subgroup $H$ of $G$ is cyclic if it is generated by a single element of $G$.

**Example 4.3.2.** 1. $\mathbb{Z} = \langle 1 \rangle$ is a cyclic group;

2. $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$ is a cyclic group;

3. The subgroup $n\mathbb{Z} \leq \mathbb{Z}$ is a cyclic subgroup generated by $n$;

4. The set $\{1, r, r^2, \ldots, r^{n-1}\}$ is a cyclic subgroup of $D_{2n}$ generated by $r$;

5. The set $\{e, (1\ 2)\}$ is a cyclic subgroup of $S_4$ generated by $(1\ 2)$.

Suppose $G = \langle x \rangle$ is a cyclic group. Then in the multiplicative notation:

$$G = \{x^n \mid n \in \mathbb{Z}\},$$

i.e. all elements of $G$ are integer powers of the generator $x$.

In the additive notation $G = \{nx \mid n \in \mathbb{Z}\}$, where

$$nx = \underbrace{x + \ldots + x}_{n \text{ times}}$$

for $n \in \mathbb{Z}_{\geq 0}$ and $(-n)x = -nx$.

**Remark 4.3.3.** If $G$ is cyclic then the generator doesn't have to be unique: if $G = \langle x \rangle$ then $G = \langle x^{-1} \rangle$. For instance, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

**Proposition 4.3.4.** *Let $G = \langle x \rangle$ then $|G| = |x|$. More specifically,*

1. *if $|G| = n < \infty$, then $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are all distinct elements of $G$, and*

2. *if $|G| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for any $a \neq b$ in $\mathbb{Z}$.*

*Proof.* Suppose $|G| < \infty$ then $|x|$ must be finite. If $|x| = m$ them $x^m = 1$ and elements $1, x, \ldots, x^{m-1}$ are all distinct (because if $x^a = x^b$ for $0 \leq a < b < m$ then $x^{b-a} = 1$ for $b - a < m$). We conclude that if $|x| = m < \infty$ then

$$G = \{1, x, \ldots, x^{m-1}\}, \text{ and } |G| = m.$$

Now suppose $|G| = \infty$ then $|x| = \infty$ (because if $|x| = m < \infty$ then $|G| = m < \infty$). We deduce that $x^n \neq 1$ for all $n \neq 0$ and that $x^a \neq x^b$ for $a \neq b$ (because otherwise $x^{b-a} = 1$). ■

**Corollary 4.3.5.** *A finite group $G$ is cyclic if and only if there exists $x \in X$, such that $|x| = |G|$.*

**Proposition 4.3.6.** *Let $x \in G$ be an element of some group $G$ and let $m, n \in \mathbb{Z}$. Suppose $x^m = x^n = 1$ then $x^d = 1$, where $d = \gcd(m, n)$. In particular, $x^m = 1$ if and only if $|x|$ divides $m$.*

*Proof.* Recall that by Corollary 2.4.3, there exist integers $u, v$ so that

$$d = n \cdot u + m \cdot v.$$

We have

$$x^d = (x^n)^u \cdot (x^m)^v = 1.$$

Thus if $x^m = 1$ and $|x| = n$ then $x^d = 1$ for $d = \gcd(m, n) \leq n$, and therefore $d = n$.

■

**Theorem 4.3.7.** *Any two cyclic groups of the same order are isomorphic.*

*Proof.* 1. Suppose $G = \langle x \rangle$ and $H = \langle y \rangle$ are two cyclic groups of order $n$. By Proposition 4.3.4, $|x| = |y| = n$. Define

$$\phi : G \to H,$$
$$x^k \mapsto y^k.$$

Let us prove that $\phi$ is well-defined. Suppose $x^r = x^s$ then $x^{r-s} = 1$, so by Proposition 4.3.6, $n \mid (r-s)$, hence $y^{r-s} = 1$ and $y^r = y^s$, which means that $\phi(x^r) = \phi(x^s)$ and thus $\phi$ is well-defined.

Note also that $\phi$ is a group homomorphism by construction, as $y^{r+s} = \phi(x^r \cdot x^s) = \phi(x^r) \cdot \phi(x^s) = y^r \cdot y^s$.

Since $H = \{y^k \mid k \in \mathbb{Z}\}$ and $y^k$ is the image of $x^k$, the map $\phi$ is a surjection of finite sets of the same order, and therefore is a bijection.

2. Now suppose that $G = \langle x \rangle$ has infinite order. Define

$$\phi : \mathbb{Z} \to G,$$
$$k \mapsto x^k.$$

The map $\phi$ is a surjective group homomorphism since $\phi(k+l) = \phi(k) \cdot \phi(l)$ and $G = \{x^k \mid k \in \mathbb{Z}\}$. Moreover, if $\phi(a) = \phi(b)$ then $x^a = x^b$. By Proposition 4.3.4, elements $x^a$ and $x^b$ are equal only if $a = b$. Thus $\phi$ is also injective. ■

**Corollary 4.3.8.** *Any cyclic group of order $n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and any cyclic group of infinite order is isomorphic to $\mathbb{Z}$ (in particular, all cyclic groups are abelian).*

**Example 4.3.9.** Let us try to understand when the product $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is cyclic. Recall that the order of the element $([a], [b])$ is the lowest common multiple of of $|[a]|$ and $|[b]|$. Note that $|[a]| \leq n$ for any $a$ (otherwise the subgroup $\langle [a] \rangle$ would be larger than the whole group), and similarly $|[b]| \leq m$. This means that $|([a], [b])| \leq n \cdot m$ and $([a], [b]) = n \cdot m$ if and only if $|[a]| = n, |[b]| = m$, and $\gcd(n, m) = 1$. Thus, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is cyclic if and only if $\gcd(n, m) = 1$ (in that case $([1], [1])$ generates it).

Moreover, we get that the map $a \cdot [1] = [a] \mapsto a \cdot ([1], [1]) = ([a], [a])$ establishes an isomorphism between $\mathbb{Z}/nm\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (when $\gcd(n, m) = 1$). This gives us (a weak version of) the **Chinese Remainder Theorem**: Let $\gcd(n_i, n_j) = 1$ for $i \neq j, i, j \in \{1, \ldots, k\}$, and $n = n_1 \cdot \ldots \cdot n_k$, then

$$\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$$
$$a \mod n \mapsto (a \mod n_1, \ldots, a \mod n_k)$$

is an isomorphism of groups.

As noted earlier, a given cyclic group may have more than one generator. The next two propositions determine precisely which powers of $x$ generate the group $\langle x \rangle$.

**Proposition 4.3.10.** *Let $G$ be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.*

1. *If $|x| = \infty$ then $|x^a| = \infty$.*
2. *If $|x| = n < \infty$ then $|x^a| = \frac{n}{\gcd(n,a)}$.*

*Proof.* 1. By way of contradiction assume $(x^a)^m = 1$ then $x^{am} = 1$, which implies that $|x| < \infty$.

2. Let $\gcd(a, n) = d, a = dk, n = dl$ then $\gcd(k, l) = 1$ and

$$(x^a)^{\frac{n}{d}} = x^{dkl} = (x^n)^k = 1.$$

Thus, $|x^a|$ divides $l = \frac{n}{d}$. Let $b = |x^a|$ then $x^{ab} = 1$, and so by Proposition 4.3.6, $n$ divides $ab$. Therefore, $l$ divides $kb$ and since $l$ and $k$ are coprime we must have $l \mid b$. We deduce that $l = b$.

■

**Proposition 4.3.11.** *Let $G = \langle x \rangle$.*

1. *Assume $|x| = \infty$ then $G = \langle x^a \rangle$ if and only if $a = \pm 1$.*
2. *Assume $|x| = n < \infty$ then $G = \langle x^a \rangle$ if and only if* $\gcd(a, n) = 1$.

*Proof.* 1. Exercise.

2. By Proposition 4.3.9.2, $|x^a| = |G| = |x|$ if and only if $\gcd(a, n) = 1$.

■

**Example 4.3.12.** Proposition 4.3.11 tells us that $[a]$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$, i.e. if $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$.

The final theorem in this section gives the complete subgroup structure of a cyclic group.

**Theorem 4.3.13.** *Let $G = \langle x \rangle$ be a cyclic group.*

1. *Every subgroup $H$ of $G$ is cyclic. More precisely, if $H \leq G$ then either $H = \{1\}$ or $H = \langle x^d \rangle$, where $d$ is the smallest positive integer for which $x^d \in H$.*
2. *If $|G| = \infty$, then $\langle x^a \rangle = \langle x^b \rangle$ if and only if $a = \pm b$. So that the subgroups of $G$ correspond bijectively with nonegative integers.*
3. *If $|G| = n < \infty$, then for every positive integer $a$ dividing $n$ there is a unique subgroup $H$ of $G$ of order $a$, namely, $H = \langle x^d \rangle$, where $d = \frac{n}{a}$.*

   *Furthermore, for every integer $m$, $\langle x^m \rangle = \langle x^{\gcd(m,n)} \rangle$, so that the subgroups of $G$ correspond bijectively with the positive divisors of $n$.*

*Proof.* 1. Let $H \leq G$ and assume $H \neq \{1\}$ (otherwise $H = \langle 1 \rangle$ and we are done). Thus, there exists $a \in Z - \{0\}$ for which $x^a \in H$, since $H$ is a subgroup, $x^{-a} \in H$, so we might assume that there exists a *positive* integer $a$ such that $x^a \in H$. Let $d = \min\{a \in \mathbb{Z}_{>0} |\ x^a \in H\}$ (such $d$ exist since this set is nonempty and $\mathbb{Z}_{>0}$ is well-ordered). Note that $\langle x^d \rangle = \{x^m \mid m \text{ is divisible by } d\}$. Take any $x^a \in H$ and take $u, v \in \mathbb{Z}$ such that $\gcd(a, d) = ua + vd$. Then

$$x^{\gcd(a,d)} = (x^a)^u \cdot (x^d)^v \in H.$$

Since $\gcd(a, d) \leq d$ we deduce that $\gcd(a, d) = d$ and thus $d$ divides $a$. So,

$$H \leq \{x^m \mid m \text{ is divisible by } d\} = \langle x^d \rangle.$$

On the other hand, $x^d \in H$ and thus $\langle x^d \rangle \leq H$. So, $H = \langle x^d \rangle$.

2. The subgroup $\langle x^a \rangle$ is trivial if and only if $a = 0$, so let us assume that $a, b \neq 0$. If $\langle x^a \rangle = \langle x^b \rangle$ then

$$\{m \in \mathbb{Z} \mid m \text{ is divisible by } a\} = \{m \in \mathbb{Z} \mid m \text{ is divisible by } b\}.$$

WLOG suppose $|a| \leq |b|$ then $a \in \{m \in \mathbb{Z} \mid m \text{ is divisible by } b\}$ only if $|a| = |b|$, i.e. $a = \pm b$.

3. Note first that if $d = \frac{n}{a}$ then by Proposition 4.3.9, the order of $\langle x^d \rangle$ is $\frac{n}{\gcd(n,d)} = \frac{n}{d} = a$. By part 1, every subgroup $H \leq G$ is cyclic. So, let $H$ be any subgroup of order $a$ then $H = \langle x^b \rangle$, where $b$ is the smallest positive integer for which $x^b \in H$. We know that $\gcd(n, b)$ must then equal to $d$. Let $u, v \in \mathbb{Z}$ be such that $d = nu + bv$ then $x^d = (x^n)^u \cdot (x^b)^v = (x^b)^v \in \langle x^b \rangle$. Since $d = \gcd(n, b) \leq b$ we deduce that $d = b$.

■

**Example 4.3.14.** Let us list all subgroups of $\mathbb{Z}/12\mathbb{Z}$:

1. $\langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle = \mathbb{Z}/12\mathbb{Z}$ has order 12;

2. $\langle[2]\rangle = \langle[10]\rangle$ has order 6;

3. $\langle[3]\rangle = \langle[9]\rangle$ has order 4;

4. $\langle[4]\rangle = \langle[8]\rangle$ has order 3;

5. $\langle[6]\rangle$ has order 2;

6. $\langle[0]\rangle$ has order 1.

# 5 Group actions

## 5.1 Actions and permutation representation

**Definition 5.1.1.** A (left) **group action** of a group $G$ on a set $A$ is a map $\rho : G \times A \to A$ satisfying the following properties:

1. $\rho(g_1 \cdot g_2, a) = \rho(g_1, \rho(g_2, a))$ for any $g_1, g_2 \in G, a \in A$,

2. $\rho(1, a) = a$ for all $a \in A$.

*Multiplicative notation:* We will often use the multiplicative notation for the action map $\rho : G \times A \to A$. Namely, we will denote this map by $\cdot$ and write $g \cdot a$ or even $ga$ for $\rho(g, a)$. One should think about a left group action of $G$ on $A$ as a rule, which tells us how to multiply elements of $A$ by elements of $G$ on the left (without knowing how to multiply two elements of $A$).

**Remark 5.1.2.** Note that axioms 1 and 2 in Definition 5.1.1 imply that we can use the multiplicative notation for the group operation on $G$ and for the action of $G$ on $A$ simultaneously. The two operations are compatible with each other: so, the first property becomes some variation of the associativity property and the second is a variation of the identity axiom:

1. $(g_1 \cdot g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$,

2. $1 \cdot a = a$.

Let us fix a group action of $G$ on $A$ and an element $g \in G$. Define a map $\sigma_g : A \to A, a \mapsto g \cdot a$.

**Proposition 5.1.3.** *The map $\sigma_g : A \to A$ is a permutation of $A$ and the map $\phi : G \to S_A$ given by $\phi(g) = \sigma_g$ is a group homomorphism.*

*Proof.* By axiom 1, $\sigma_{g^{-1}} \circ \sigma_g(a) = g^{-1} \cdot (g \cdot a) = (g^{-1} \cdot g) \cdot a = 1 \cdot a$, which by axiom 2 is equal to $a$. Similarly, $\sigma_g \circ \sigma_{g^{-1}}(a) = g \cdot g^{-1} \cdot a = 1 \cdot a = a$. So, $\sigma_{g^{-1}} = \sigma_g^{-1}$, meaning that $\sigma_g$ is invertible, i.e. bijective.

Now, $\phi(g_1 \cdot g_2)(a) = \sigma_{g_1 \cdot g_2}(a) = (g_1 \cdot g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a)) = \sigma_{g_1} \circ \sigma_{g_2}(a) = \phi(g_1) \circ \phi(g_2)(a)$, meaning that $\phi$ is a homomorphism. ∎

**Definition 5.1.4.** We call the homomorphism $\phi : G \to S_A$ the **permutation representation** associated with the given action.

**Remark 5.1.5.** Each element $g \in G$ is said to act on $A$ through the corresponding permutation $\sigma_g$.

Note that one can reverse the process above: given a group homomorphism $\phi : G \to S_A, g \mapsto \sigma_g$ one can define a group action $\rho : G \times A \to A$ as follows:

$$g \cdot a = \rho(g, a) = \sigma_g(a) = \phi(g)(a).$$

We get then that

$$(g_1 \cdot g_2) \cdot a = \sigma_{g_1 \cdot g_2}(a) = \sigma_{g_1}(\sigma_{g_2}(a)) = g_1 \cdot (g_2 \cdot a)$$

and

$$1 \cdot a = \sigma_1(a) = Id_A(a) = a.$$

We get a one-to-one correspondence:

$$\{\text{(Left) group actions of } G \text{ on } A\} \leftrightarrow \{\text{Group homomorphisms } G \to S_A\}.$$

Now let us now finally look at some examples.

**Example 5.1.6.**

1. Let $g \cdot a = a$ for all $g \in G, a \in A$: it is called the *trivial action* of $G$ on $A$. The associated permutation representation is the trivial homomorphism $t : G \to S_A$.
2. For any nonempty set $A$, the symmetric group $S_A$ acts naturally on $A$ via
$$\sigma \cdot a = \sigma(a), \ \forall \sigma \in S_A, \ \forall a \in A.$$
3. Let $V$ be the sets of vertices of a regular $n$-gon. Then $D_{2n}$ acts naturally on $V$ by permuting vertices. We have seen the permutation representation $D_{2n} \to S_V$ in Example 3.6.3.7. When we label the vertices by numbers $1, 2, \ldots, n$, we get the usual injective map $D_{2n} \to S_n$.
4. Let us label the vertices of an $n$-gon in the clockwise direction by numbers $1, 2, \ldots, n$. Suppose $n = 2k$ is even and let $A$ be the set of all unordered pairs of opposite vertices: $A = \{\{1, k+1\}, \{2, k+2\}, \ldots, \{k-1, 2k-1\}, \{k, 2k\}\}$. Then $D_{2n}$ also acts on this set $A$ since every symmetry of an $n$-gon sends a pair of opposite vertices to a set of opposite vertices.
5. $\mathbb{Z}$ acts on the real line $\mathbb{R}$ by translations:
$$n \cdot t = t + n.$$
6. The circle $S^1$ is the group of unit elements in $\mathbb{C}$
$$S^1 = \{z \in \mathbb{C} \mid z \cdot \overline{z} = 1\} = \{\exp(i\phi) \mid \phi \in [0, 2\pi)\},$$
One can identify elements of $S^1$ with real numbers in $[0, 2\pi)$, so that $\phi \in [0, 2\pi)$ corresponds to the complex number $\exp(i\phi) = \cos(\phi) + i\sin(\phi)$.
The group $S^1$ acts on the real plane $\mathbb{R}^2$ by rotations around $(0, 0)$, with element $\phi \in [0, 2\pi)$ acting via the rotation by $\phi$ radians:
$$\phi \cdot (x, y) = (\cos(\phi)x - \sin(\phi)y, \sin(\phi)x + \cos(\phi)y).$$

## 5.2 Orbits, stabilizers

**Definition 5.2.1.** Let $\phi : G \times A \to A$ be a group action of $G$ on $A$, and let $\phi : G \to S_A$ be the corresponding permutation representation.

1. An element $g \in G$ is said to **act trivially** on $A$ if $g \cdot a = a$ for all $a \in A$. Note that $g$ acts trivially on $A$ if and only if $\sigma_g = Id_A$, i.e. $\phi(g) = e \in S_A$.
2. The **kernel** of the action is the set $\{g \in G \mid g \cdot a = a \ \forall a \in A\}$ of all elements of $G$ that act *trivially* on $A$. Note that it is precisely the kernel $\mathrm{Ker}(\phi)$ of the permutation representation.
3. The action is called **faithful** if $\mathrm{Ker}(\phi) = 1$.
4. For each $a \in A$ the **stabilizer** of $a$ in $G$ is the set of group elements that fix the element $a$:
$$G_a = \{g \in G \mid g \cdot a = a\} \subset G.$$

**Remark 5.2.2.** The kernel of an action is the intersection of all stabilizers:

$$\mathrm{Ker}(\phi) = \bigcap_{a \in A} G_a.$$

**Proposition 5.2.3.** *Let $G$ act on a set $A$, then for any $a \in A$ the stabilizer $G_a$ is a subgroup of $G$.*

*Proof.* By axiom 2 of group actions, the identity 1 fixes every element $a$, so $1 \in G_a$. Now if $x, y \in G_a$ then $(xy^{-1}) \cdot a = x \cdot (y^{-1} \cdot a) = \sigma_x(\sigma_y^{-1}(a)) = \sigma_x(a) = a$ (here we used the observation that if $\sigma \in S_A$ fixes $a$ then $\sigma^{-1}(a) = a$). So by the subgroup criterion, $G_a \leq G$. ■

**Example 5.2.4.**

1. If $G$ acts trivially on $A$ then for any $a \in A$ the stabilizer $G_a$ is the whole group $G$. Note that the action is trivial if and only if $\mathrm{Ker}(\phi) = G$.
2. The natural action of $G = S_n$ on $\{1, 2, \ldots, n\}$ is faithful and for each $i \in \{1, \ldots, n\}$, the stabilizer $G_i$ is a subgroup isomorphic to $S_{n-1}$.
3. The action of $G = D_{2n}$ on the set of vertices $V$, which we label clockwise by $\{1, \ldots, n\}$, is faithful. The stabilizer $G_i$ of the vertex labeled by $i \in \{1, \ldots, n\}$ is
$$G_i = \{1, r^{2i-2}s\}.$$
4. If $n = 2k$ is even, the action of $D_{2n}$ on the set of unordered pairs of opposite vertices $A$ is not faithful with
$$\mathrm{Ker}(\phi) = \{1, r^k\}.$$
5. The action of $\mathbb{Z}$ on $\mathbb{R}$ by translations is faithful, and for any $t \in R$ the stabilizer of $t$ is trivial (contains only the identity element 0).
6. The action of $S^1$ on $\mathbb{R}^2$ by rotations is faithful. The stabilizer of any nonzero point in $\mathbb{R}^2$ is trivial, whereas the stabilizer of $(0, 0)$ is the whole group $S^1$.

Let $G$ act on a set $A$. Define a binary relation $\sim$ on $A$ by

$$a \sim b, \text{ if and only if } a = g \cdot b \text{ for some } g \in G.$$

**Proposition 5.2.5.** *The binary relation $\sim$ above is an equivalence relation.*

*Proof.* Let us prove that $\sim$ satisfies the three properties of equivalence relations:

1. $a \sim a$ because $a = 1 \cdot a$;
2. if $a \sim b$ with $a = g \cdot b$ then $g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = 1 \cdot b = b$, so $b \sim a$;
3. if $a \sim b, b \sim c$ with $a = g \cdot b, b = h \cdot c$ then $a = g \cdot (h \cdot c) = (g \cdot h) \cdot c$, so $a \sim c$.

■

**Definition 5.2.6.**

1. For each $a \in A$ the **orbit** of $a$ is the set
$$G \cdot a = \{g \cdot a \mid g \in G\} \subset A.$$
Note that $G \cdot a$ is the equivalence class of $a$ with respect to the relation $\sim$.
2. The action is called **transitive** if there is only one orbit, i.e. given $a, b \in A$ there exists $g \in G$ such that $a = g \cdot b$ (i.e. all elements of $A$ are equivalent to each other w.r.t. $\sim$).

   Equivalently, the action of $G$ on $A$ is transitive if for some $a \in A$ :
$$G \cdot a = A.$$

**Corollary 5.2.7.** *A group $G$ acting on a set $A$ partitions $A$ into disjoint equivalence classes under the action of $G$ (called orbits of $G$).*

**Example 5.2.8.**

1. If $G$ acts trivially on $A$ then $G \cdot a = a$ for every $a \in A$.
2. The action of $S_n$ on $A = \{1, 2, \ldots, n\}$ is transitive, so the orbit of every element $i \in A$ is $A$.
3. A more interesting example is the following: take any permutation $\sigma \in S_n$ and consider the subgroup $H = \langle \sigma \rangle \leq S_n$. Then $H$ acts faithfully on the set $A = \{1, 2, \ldots, n\}$. Suppose $\sigma = (a_1 \ \ldots a_{k_1})(a_{k+1} \ \ldots \ a_{k_2}) \ldots (a_{k_{l-1}} \ \ldots \ a_n)$ is the full cycle decomposition of $\sigma$. Then the sets $\{a_1, \ldots, a_{k_1}\}, \{a_{k_1+1}, \ldots, a_{k_2}\}, \ldots, \{a_{k_{l-1}}, \ldots, a_n\}$ are precisely orbits in $A$ under the action of $H$.
4. The action of $D_{2n}$ on the set of vertices $V$ is transitive.
5. If $n = 2k$, the action of $D_{2n}$ on the set $A$ of unordered pairs of opposite vertices is also transitive.
6. The orbit of a real number $t \in \mathbb{R}$ under the action of $\mathbb{Z}$ by translations is the set $\mathbb{Z} \cdot t = \{r \in R \mid r - t \in \mathbb{Z}\}$. There are infinitely many orbits in $\mathbb{R}$ under this action.
7. Let $S^1$ act on $\mathbb{R}^2$ by rotations. The orbit of $(0, 0)$ is $S^1 \cdot (0, 0) = \{(0, 0)\}$, and for any nonzero point $p = (x, y) \in \mathbb{R}^2$ the orbit $S^1 \cdot p$ is the circle of radius $d$ with the center in $(0, 0)$, where $d$ is the distance between $p$ and zero: $d = \sqrt{x^2 + y^2}$. Note that the plane is the disjoint union of circles of all possible non-negative radii.

**Exercise 5.2.9.** Let $a, b \in A$ be in the same orbit under the action of $G$ on $A$ with $a = g \cdot b$ then their stabilizers are connected via the following relation:

$$G_a = gG_bg^{-1}.$$

**Definition 5.2.10.** Let a group $G$ act on a set $A$, and let $\sim$ be the equivalence relation on $A$ induced by this action (i.e. $a \sim b$ if $a = g \cdot b$ for some $g \in G$). The quotient $A/\sim$ is denoted $G\backslash A$ and is called the quotient of $A$ by the action of $G$. Namely, $G\backslash A$ is the set of all orbits in $A$ under the action of $G$.

Recall that $G\backslash A$ is equipped with the natural surjective map $q : A \to G\backslash A$.

**Remark 5.2.11.** We write $G\backslash A$ instead of $A/G$ to stress that $G$ acts on the left on $A$. When the distinction between left and right actions of $G$ becomes unimportant to us, we will use the more convenient notation $A/G$ for the quotient.

**Example 5.2.12.**

1. The quotient $G\backslash A$ of a set $A$ under the trivial action of some group $G$ is $A$.
2. If $G$ acts transitively on $A$ then the quotient $G\backslash A$ is a single element set.
3. The quotient $\mathbb{Z}\backslash\mathbb{R}$ of $\mathbb{R}$ under the action of $\mathbb{Z}$ by translations can be identified with the segment $[0, 1)$, since the orbit of each $x \in \mathbb{R}$ contains a unique representative in this range, namely the fractional part of $x$: $\{x\} = x - \lfloor x \rfloor$ (the quotient map thus sends $x$ to $\{x\}$). More precisely, we can identify $\mathbb{Z}\backslash\mathbb{R}$ with $S^1$ via sending $\mathbb{Z} \cdot t$ to $e^{2\pi i \cdot t}$ (note that this is well-defined as $e^{2\pi i \cdot n} = 1$ for any $n \in \mathbb{Z}$.
4. Recall that the quotient $S^1\backslash\mathbb{R}^2$ of the real plane $\mathbb{R}^2$ by the action of $S^1$ by rotations is the set of all circles on the plane with the center at $(0, 0)$ (including the degenerate case of the circle of radius zero, i.e. the point $(0, 0)$). It can be identified with the non-negative half-line $\mathbb{R}_{\geq 0}$ via assigning to each circle its radius. The quotient map then sends a point $p \in \mathbb{R}^2$ to the distance between $p$ and $(0, 0)$.

## 5.3 Groups acting on themselves by left multiplication

One important example of a left group action for any group $G$ is the action of $G$ on itself by left multiplication. That is, we can take $\rho : G \times G \to G$ to be the group operation map. Then axioms 1 and 2 of group actions become the associativity and the identity axioms for groups, which implies that this is a well-defined group action.

- The action $G \times G \to G, (g, h) \mapsto g \cdot h$ is faithful, moreover, all stabilizers $G_x$ are trivial: if $g \cdot x = x$ then $g = x \cdot x^{-1} = 1$.
- This action is also transitive, since

$$G \cdot 1 = \{g \cdot 1 \mid g \in G\} = G,$$

  so the orbit of 1 is $G$, and hence the orbit of every other element is $G$.

**Theorem 5.3.1** (Cayley's Theorem)**.** *Any finite group $G$ is isomorphic to a subgroup of $S_n$ for some $n \in \mathbb{Z}_{>0}$.*

*Proof.* Let $|G| = n$. Consider the action of $G$ on itself by left multiplication and the associated permutation representation $\phi : G \to S_G$. Since this action is faithful, $\phi$ is injective, thus the composition of $\phi$ with some isomorphism $\tau : S_G \to S_n$ gives an isomorphism between $G$ and a subgroup $\tau \circ \phi(G)$ of $S_n$. ∎

To make this action more interesting let us look at some subgroup $H \leq G$. Then $H$ also acts on $G$ by left multiplication. Since we obtain this action by restricting the action of $G$ on itself to $H$, it is still faithful with trivial stabilizers.

**Example 5.3.2.**

1. $\mathbb{Z} \leq \mathbb{R}$, $\mathbb{Z}$ acts on $\mathbb{R}$ by translations.
2. $S^1 = \{z \in \mathbb{C} \mid z \cdot \overline{z} = 1\} \leq \mathbb{C} - \{0\}$, $S^1$ acts on $\mathbb{C} - \{0\}$ by multiplication. If we identify $\mathbb{C} - \{0\}$ with punctured real plane $\mathbb{R}^2 - \{(0, 0)\}$, this action coincides with the action of $S^1$ on $\mathbb{R}^2 - \{(0, 0)\}$ by rotations.

**Definition 5.3.3.** For any $x \in G$ the orbit $H \cdot x$ is called the **right coset** of $x$ with respect to $H$ (because $x$ is on the right in the expression $H \cdot x$, although $H$ acts by *left* multiplication, which might be a little confusing).

The set of right cosets with respect to $H$ is, by definition, the quotient $H\backslash G$. Since they are equivalence classes of elements in $G$, right cosets $\{H \cdot x\}_{x \in G}$ partition $G$:

$$G = \bigsqcup_{\mathcal{O} \in H\backslash G} \mathcal{O}. \tag{5.3.3.1}$$

For any $\mathcal{O} \in H\backslash G$ an element $x \in \mathcal{O}$ is called a **coset representative** of the coset $\mathcal{O}$.

**Example 5.3.4.** For the case of $n\mathbb{Z}$ acting on $\mathbb{Z}$ we get that the orbits (right cosets) are precisely the equivalence classes for the relation $x \sim y$ if $n \mid (x - y)$. So we get the identification $n\mathbb{Z}\backslash\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ (this identification will be further explained when we study right actions, but it follows from the fact that $\mathbb{Z}$ is abelian, and so there is no difference between left and right multiplication).

Note that if $H$ is finite then the number of elements in $H \cdot x$ is equal to the number of elements in $H$ (there is a bijection between these two sets given by right multiplication by $x$: $h \mapsto h \cdot x$, the inverse of this bijection is multiplication by $x^{-1}$).

**Theorem 5.3.5** (Lagrange's Theorem)**.** *Let $G$ be a finite group and let $H$ be a subgroup of $G$ then $|H|$ divides $|G|$. Moreover,*

$$|G| = |H| \cdot |H\backslash G|.$$

*Proof.* Follows from (5.3.3.1) and the fact that $|\mathcal{O}| = |H|$ for any $\mathcal{O} \in H\backslash G$. ∎

**Definition 5.3.6.** Let $G$ be a finite group and $H \leq G$ the number of left cosets $|H\backslash G|$ is called the **index** of $H$ in $G$, denoted $[G:H]$. We get that $[G:H] = \frac{|G|}{|H|}$.

**Corollary 5.3.7.** *As a direct consequence of Lagrange's theorem we get that the order of any element in a finite group divides the order of the group (because it is equal to the order of the subgroup generated by this element).*

## 5.4 Groups acting on themselves by conjugation

Let us define another action of $G$ on itself, called the action by conjugation. Define the action map via:

$$G \times G \to G$$
$$(g, x) \mapsto g \star x = gxg^{-1}.$$

Then $1 \star x = x$ and $(gh) \star x = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g \star (hxh^{-1}) = g \star (h \star x)$. So, this is a well-defined left group action of $G$.

Note that each map $\sigma_g \in S_G, \sigma_g(x) = gxg^{-1}$ is not just a bijection on $G$, but actually a group automorphism:

$$\sigma_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \sigma_g(x)\sigma_g(y).$$

We say that the corresponding permutation representation *factors through* the group of automorphism of $G$:

$$\phi : G \to \mathrm{Aut}(G) \leq S_G$$
$$g \mapsto \sigma_g.$$

Automorphisms $\sigma_g, g \in G$ (given by the conjugation by elements of $G$) are called *inner automorphisms* of $G$.

**Definition 5.4.1.** The orbit of $x \in G$ with respect to the conjugation action is called the **conjugacy class** of $x$:

$$Cl(x) = \{gxg^{-1} \mid g \in G\}.$$

**Remark 5.4.2.**

1. The stabilizer $G_x$ of $x$ with respect to the conjugation action is the centralizer $C_G(x)$.
2. If $g \in Z(G)$ then $Cl(g) = \{g\}$.
3. If $G$ is abelian, the conjugation action is trivial, and $Cl(x) = \{x\}$ for all $x \in G$.

## 5.5 Conjugacy classes in the symmetric group

As $S_n$ is our main example of a finite non-abelian group, let us study the conjugation action on $S_n$.

**Proposition 5.5.1.** *Let $\sigma \in S_n$ and let $\tau = (a_1\ a_2\ \ldots\ a_k)$ be a cycle of length $k$ in $S_n$ then*

$$\sigma\tau\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)),$$

*i.e. $\sigma\tau\sigma^{-1}$ is also a cycle of length $k$, where we replace each $a_i$ with $\sigma(a_i)$.*

*Proof.* Suppose $b \neq \sigma(a_i)$ for any $i = 1, 2, \ldots, k$ then $\sigma^{-1}(b) \neq a_i$, and thus $\tau(\sigma^{-1}(b)) = \sigma^{-1}(b)$. So, $\sigma\tau\sigma^{-1}(b) = b$.

Now if $b = \sigma(a_i)$ then $\sigma\tau\sigma^{-1}(b) = \sigma\tau(a_i) = \sigma(a_{i+1})$, where we consider $i+1$ modulo $k$. ∎

**Corollary 5.5.2.** *Let $\sigma \in S_n$, and let $\tau = C_1 \cdot C_2 \cdot \ldots \cdot C_l$ be the product of disjoint cycles, then*

$$\sigma\tau\sigma^{-1} = \sigma C_1\sigma^{-1} \circ \sigma C_2\sigma^{-1} \circ \ldots \circ \sigma C_l\sigma^{-1}.$$

*So if $\tau = (a_1\ \ldots\ a_{k_1})(a_{k_1+1}\ \ldots\ a_{k_2})\ldots(a_{k_{l-1}+1}\ \ldots\ a_{k_l})$ then*

$$\tau = (\sigma(a_1)\ \ldots\ \sigma(a_{k_1}))(\sigma(a_{k_1+1})\ \ldots\ \sigma(a_{k_2}))\ldots(\sigma(a_{k_{l-1}+1})\ \ldots\ \sigma(a_{k_l})).$$

**Remark 5.5.3.** Basically, to conjugate a product of cycles by some permutation $\sigma$ replace all numbers in the cycles with their image under $\sigma$.

**Remark 5.5.4.** Conjugation by $\sigma \in S_n$ is an isomorphism $S_n \to S_n$ induced from the bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ (see Example 3.6.3.5).

**Example 5.5.5.** Let $\tau = (1\ 6\ 7\ 8)(2\ 5\ 3)(9\ 10)$ and let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 10 & 2 & 1 & 6 & 3 & 8 & 5 & 9 \end{bmatrix}$ then

$$\sigma\tau\sigma^{-1} = (7\ 6\ 3\ 8)(4\ 1\ 10)(5\ 9).$$

**Proposition 5.5.6.** *Let $\tau = C_1C_2 \ldots C_l \in S_n$, where $C_j, j = 1, \ldots, l$ are disjoint cycles of corresponding lengths $k_j, j = 1, \ldots, l$ with $\sum k_j = n$. Then the conjugacy class of $\tau$ consists of all permutations of (the same) cyclic type $k_1 + k_2 + \ldots + k_j$.*

*Proof.* We will show that if $\tau$ has cyclic type $k_1 + k_2 + \ldots + k_l$ $(= n)$ then there exists $\sigma \in S_n$ such that

$$\sigma\tau\sigma^{-1} = (1\ 2\ \ldots\ k_1)((k_1+1)\ \ldots\ (k_1+k_2)) \ldots ((k_1 + \ldots + k_{l-1} + 1)\ \ldots\ n) = \rho.$$

This will imply that $Cl(\tau) = Cl(\rho)$ and that any $\tau$ of cyclic type $k_1 + \ldots + k_l$ lies in $Cl(\rho)$.

Now to prove this statement, suppose

$$\tau = (a_1\ \ldots\ a_{k_1})(a_{k_1+1}\ \ldots\ a_{k_1+k_2}) \ldots (a_{k_1+\ldots+k_{l-1}+1}\ \ldots\ a_{k_l}).$$

Consider $\sigma^{-1}$ which sends $i$ to $a_i$ (i.e. $\sigma$ sending $a_i$ to $i$) then by Corollary 5.5.2,

$$\sigma\tau\sigma^{-1} = \rho.$$

■

**Example 5.5.7.** Let $\tau = (1\ 4)(2)(3\ 6\ 5) \in S_6$ and let $\sigma = (1)(2\ 3\ 4)(5\ 6)$ then

$$\sigma\tau\sigma^{-1} = (1\ 2)(3)(4\ 5\ 6).$$

The conjugacy class of $\tau$ consists of all permutations in $S_6$ of cyclic type 3+2+1, e.g. $(1\ 4\ 6)(2\ 5)(3) \in Cl(\tau)$.

**Corollary 5.5.8.** *The center $Z(S_n)$ is trivial.*

## 5.6 Right group actions and orbit-stabilizer theorem

Let $A$ be a set and let $G$ be a group. We can try to imitate Definition 5.1.1 replacing left multiplication right multiplication. Namely, we would like to define $a \cdot g$ for $a \in A$ and $g \in G$ with the property that $a \cdot (g_1 \cdot g_2) = (a \cdot g_1) \cdot g_2$. We obtain the following

**Definition 5.6.1.** A **right** *group action* of $G$ on $A$ is a map $\rho : G \times A \to A$, satisfying the following properties:

1. $\rho(g_2, \rho(g_1, a)) = \rho(g_1g_2, a)$, for all $g_1, g_2 \in G, a \in A$,
2. $\rho(1, a) = a$ for all $a \in A$.

Let us denote $\rho(g, a)$ by $a \cdot g$ then we can rewrite these properties as follows:

1. $(a \cdot g_1) \cdot g_2 = a \cdot (g_1g_2)$ for all $g_1, g_2 \in G, a \in A$, and
2. $a \cdot 1 = a$ for all $a \in A$.

**Remark 5.6.2.** Note that the difference between left (Definition 5.1.1) and right (Definition 5.6.1) group actions is more than just in the notation for $\rho(g,a)$. Let us look at what property 1 would look like if we were to denote $\rho(g,a)$ by $g \cdot a$ like for left group actions:

$$\rho(g_2, \rho(g_1, a)) = g_2 \cdot (g_1 \cdot a) = (g_1 g_2) \cdot a = \rho(g_1 g_2, a).$$

**Example 5.6.3.** Right multiplication gives rise to a right action of $G$ on itself.

Recall that to each left group action of $G$ on $A$ we assigned the permutation representation, which happened to be a group homomorphism $G \to S_A$. To understand what happens in the case of right group actions we need the following

**Definition 5.6.4.** A map $\phi : G \to H$ is called an **antihomomorphism** if

$$\phi(a \cdot b) = \phi(b) \cdot \phi(a)$$

for all $a, b \in G$.

**Example 5.6.5.** 1. The main example of an antihomomorphism is the map $G \to G, g \mapsto g^{-1}$.

2. If $G$ is abelian then antihomomorphisms are the same as homomorphisms.

**Proposition 5.6.6.** *The map $g \mapsto \sigma_g$, where $\sigma_g(a) = \rho(g,a) = a \cdot g$ is an antihomomorphism $\phi$ from $G$ to $S_A$ (with $\phi(g) = \sigma_g$).*

*Proof.* Let $g, h \in G$ and $a \in A$ then $\phi(gh)[a] = \sigma_{gh}[a] = a \cdot (gh) = (a \cdot g) \cdot h = \sigma_h[a \cdot g] = \sigma_h \circ \sigma_g[a] = \phi(h) \circ \phi(g)[a]$. ■

There is a way one can turn any left action into a right action and vice versa:

**Proposition 5.6.7.** *Suppose $\rho : (g,a) \mapsto g \cdot a$ is a left action of $G$ on $A$ then $\rho' : (g,a) \mapsto g^{-1} \cdot a$ defines a right action of $G$ on $A$. Similarly, if $\rho : (g,a) \mapsto a \cdot g$ is a right action of $G$ on $A$ then $\rho' : (g,a) \mapsto a \cdot g^{-1}$ defines a left action of $G$ on $A$.*

*Proof.* We will only prove the first part, the second one being similar.

Let $g, h \in G, a \in A$ then $\rho'(gh, a) = (gh)^{-1} \cdot a = h^{-1} \cdot g^{-1} \cdot a = \rho'(h, g^{-1} \cdot a) = \rho'(h, \rho'(g, a))$.

■

As a corollary we get that the relation $a \sim b$ if $\exists g \in G : \ a = b \cdot g$ is an equivalence relation (because if we turn it into a left group action, this becomes an equivalence relation from Definition 5.2.10). We denote the corresponding quotient $A/\sim$ by $A/G$.

Note that if we turn a left group action of $G$ on $A$ into a right action as in Proposition 5.6.7 then the orbits will remain the same, so we actually have the equality of quotients $G\backslash A = A/G$ for these two actions. We will therefore use the more convenient notation $A/G$ for the quotient with respect to a left group action in all cases, except when we need to distinguish between the left and right multiplication of $G$ on itself.

Let $H \leq G$ then the right multiplication $(h, g) \mapsto g \cdot h$ defines a right action of $H$ on $G$.

**Definition 5.6.8.** For $x \in G$ the orbit $x \cdot H$ is called the **left coset** of $x$ with respect to $H$.

The quotient $G/H$ is the set of left cosets with respect to $H$. Note that if $G$ is commutative, there is no difference between left and right multiplication, so $G/H = H\backslash G$. Hence we can use the preferred notation $\mathbb{Z}/n\mathbb{Z}$ without any ambiguity.

We can state Lagrange's theorem for right multiplication: since $G = \bigsqcup_{\mathcal{O} \in G/H} \mathcal{O}$, we have

$$|G| = |H| \cdot |G/H|.$$

In particular, we get that the number of left cosets with respect to $H$ is equal to the number of right cosets (even for non-abelian groups): $|G/H| = |H\backslash G|$.

Let us now look more closely at the quotient $G/H$. Note that the left multiplication action of $G$ on itself gives rise to a transitive left action of $G$ on $G/H$:

$$\rho : G \times G/H \to G/H$$

$$(g, xH) \mapsto g \cdot xH = (gx)H.$$

For any point $[x] = xH \in G/H$ the stabilizer $G_{[x]}$ is equal to $xHx^{-1}$.

This action is important since every other set with transitive left action of $G$ "looks similar" to $G/H$ in the following sense:

**Theorem 5.6.9** (Orbit-Stabilizer Theorem)**.** *Suppose $G$ acts transitively on $A$ (i.e. for any $a \in A$ the orbit $G \cdot a$ is equal to $A$). Then for any $a \in A$ the map*

$$f : G/G_a \to A$$

$$g \cdot G_a \mapsto g \cdot a$$

*is well-defined and bijective.*

*Proof.* Suppose $g \cdot G_a = h \cdot G_a$ then $g = h \cdot x$, where $x \in G_a$, so

$$f(g \cdot G_a) = g \cdot a = g \cdot (x \cdot a) = (g \cdot x) \cdot a = f(h \cdot G_a),$$

which proves that $f$ is well-defined.

Furthermore, it is surjective since $G \cdot a = A$ and if $f(g \cdot G_a) = f(h \cdot G_a)$ then $g \cdot a = h \cdot a$, so $h^{-1}g \cdot a = a$, therefore $h^{-1}g \in G_a$ and $g = h(h^{-1}g) = hx$, where $x \in G_a$, so $g \cdot G_a = h \cdot G_a$, which proves that $f$ is injective. ∎

**Corollary 5.6.10.** *Suppose $G$ is a finite group acting on a set $A$ then for any $a \in A$*

$$|G| = |G \cdot a| \cdot |G_a|.$$

**Example 5.6.11.**

1. Let $A = G/H$ and $a = 1 \cdot H$ then $G_a = H, G \cdot a = G/H$ and we get the Lagrange's theorem:
$$|G| = |G/H| \cdot |H|.$$

2. For the action of $G$ on itself by conjugation we get for any $x \in G$
$$|G| = |Cl(x)| \cdot |C_G(x)|.$$

3. Consider $G = S^1$ acting on $A = \mathbb{R}^2$ by rotations. Let $a = (x, y) \in A$ with $r = |a| = \sqrt{x^2 + y^2}$ then if $r \neq 0$ the stabilizer $G_a$ is trivial and we have a bijection between $S^1$ and the orbit of $a$. As we established earlier, $G \cdot a = \{p \in \mathbb{R}^2 \mid |p| = r\}$ and the bijection between $S^1$ and $G \cdot a$ is given by the homothety at zero with ratio $= r$. If $r = 0$ then the action of $G$ on $a$ is trivial, so the stabilizer $G_a = G$ and the bijection in question is the identification between two singleton sets $G/G \to \{(0, 0)\}$.

4. Consider the subgroup $H = S_k \times S_{n-k}$ of $G = S_n$ (namely the set of permutations of $\{1, \ldots, n\}$ that preserve the subset $\{1, \ldots, k\}$). Recall that $G$ acts transitively on the set of $k$-element subsets of $\{1, \ldots, n\}$. Then $H$ is the stabilizer of $\{1, \ldots, k\}$, and its orbit is the whole set of $k$-element subsets, then the orbit-stabilizer tells us the following:
$$|S_n| = |S_k| \cdot |S_{n-k}| \cdot |\{k - \text{element subsets of } \{1, \ldots, n\}\}|,$$
i.e.
$$n! = k! \cdot (n - k)! \cdot \binom{n}{k}.$$

5. Following example 2 here: let $\sigma = C_1 \cdot \ldots \cdot C_k \in S_n$ be the product of disjoint cycles with the length of $C_i$ equal to $l_i$ and $n = \sum_{i=1}^{k} l_i$. Recall that $Cl(\sigma)$ consists of all permutations of the same cyclic type. Suppose $\{l_1, \ldots, l_k\} = \{1^{a_1}, 2^{a_2}, \ldots, n^{a_n}\}$ as a multiset, i.e. there are $a_i$ occurrences of number $i$ among $l_1, \ldots, l_k$ for each $i = 1, \ldots, n$ (for example if $n = 10$ and $l_1 =$

$1, l_2 = 3, l_3 = 2, l_4 = 1, l_5 = 3$ then $\{l_1, \ldots, l_5\} = \{1^2, 2^1, 3^2, 4^0, 5^0, \ldots, 10^0\} = \{1^2, 2^1, 3^2\}$). Let us count the number of elements in $Cl(\sigma)$. Recall that for any $1 \leq l \leq n$ the number of cycles of length $l$ in $S_n$ is equal to $\frac{n!}{(n-l)!\cdot l}$. Now if we want to count how many products of $a$ disjoint cycles of (the same) length $l$ there are in $S_n$ we get

$$\frac{n!}{(n-l)!\cdot l} \cdot \frac{(n-l)!}{(n-2l)!\cdot l} \cdot \ldots \cdot \frac{(n-(a-1)l)!}{(n-al)!\cdot l} \cdot \frac{1}{a!} = \frac{n!}{(n-al)!\cdot l^a} \cdot \frac{1}{a!},$$

where we divide by $a!$ to account for permutations of cycles of the same length (e.g. $(1\ 3)(2\ 4) = (2\ 4)(1\ 3)$). Now if $\sum l_i = n$ and $\{l_1, \ldots, l_k\} = \{1^{a_1}, 2^{a_2}, \ldots, n^{a_n}\}$ (i.e. $\sum_{i=1}^{n} i \cdot a_i = n$) we get that there are precisely

$$\frac{n!}{(n-a_1)!\cdot 1^{a_1}} \cdot \frac{1}{a_1!} \cdot \frac{(n-a_1)!}{(n-a_1-2a_2)!\cdot 2^{a_2}} \cdot \frac{1}{(a_2!} \cdot \ldots \cdot \frac{(n-a_1-2a_2-\ldots-(n-1)a_{n-1})!}{(n-\sum_{i=1}^{n} ia_i)!\cdot n^{a_n}} \cdot \frac{1}{a_n!} =$$

$$\frac{n!}{0!} \cdot \frac{1}{1^{a_1}\cdot 2^{a_2}\cdot \ldots \cdot n^{a_n}} \cdot \frac{1}{a_1!\cdot a_2! \cdot \ldots a_n!} = \frac{n!}{\prod_{i=1}^{n}(i^{a_i}\cdot a_i!)}$$

elements of cyclic type $l_1 + \ldots + l_k = \sum_{i=1}^{n} a_i \cdot i$ in $S_n$. As a result of this computation and the orbit-stabilizer theorem we get that there are

$$\prod_{i=1}^{n}(i^{a_i}\cdot a_i!)$$

elements in $S_n$ that commute with $\sigma$.

For example, take $\sigma = (1\ 3\ 5)(2)(4\ 6)(7\ 8)(9)$ in $S_9$ then cyclic type of $\sigma$ is $1+1+2+2+3$, so $a_1 = 2, a_2 = 2, a_3 = 1, a_i = 0$ for $i > 3$. We get

$$|Cl(\sigma)| = \frac{9!}{(1^2\cdot 2!)\cdot(2^2\cdot 2!)\cdot(3^1\cdot 1!)} = \frac{9!}{48},$$

and thus

$$|C_{S_9}(\sigma)| = 48.$$

**Remark 5.6.12.** Note that Corollary 5.6.10 only gives an expression for the number of elements in a single orbit, it knows nothing about the total number of orbits in $A$.

# 6 Quotient groups

## 6.1 Quotients by subgroup actions

Let us look at the quotient $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$ by the multiplication (in this case addition?) action of the subgroup $n\mathbb{Z}$ (note that the left and right multiplication are the same in the commutative case, so we do not distinguish between left and right cosets). We proved that this quotient inherited the group operation (addition) from $\mathbb{Z}$ in a way that made the quotient map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ into a group homomorphism.

Let us try to answer a similar question about any abstract group $G$ and a subgroup $H \leq G$.

**Question:** When does the quotient $G/H$ inherit the group structure from $G$? That is, if we denote by $[x]$ the coset $xH$ for any $x \in G$, we would like to define the multiplication on $G/H$ by putting

$$[x]\cdot[y] = [x\cdot y],$$

and the question now is when this operation is well-defined and makes $G/H$ into a group.

**Remark 6.1.1.** Note that we can also ask this question for the left quotient $H\backslash G$, however it turns out that the answer that we get in this case will be the same.

**Definition 6.1.2.** A subgroup $H$ of $G$ is called **normal** in $G$ if $gHg^{-1} = H$ for every $g \in G$. We write $H \trianglelefteq G$ to indicate that $H$ is a normal subgroup of $G$.

**Remark 6.1.3.**
1. A subgroup $H$ is normal if and only if $gH = Hg$ for all $g \in G$, that is, left cosets with respect to $H$ coincide with right cosets, so we get $H\backslash G = G/H$.
2. We have $H \trianglelefteq G$ if and only if $N_G(H) = G$.
3. The relation "is a normal subgroup in" is **not transitive**. That is, if $K \trianglelefteq H$ and $H \trianglelefteq G$, then this doesn't imply that $K$ is a normal subgroup of $G$.

**Example 6.1.4.**
1. The subgroups $\{1\}$ and $G$ are always normal in $G$.
2. Let $G$ be abelian then any subgroup $H \leq G$ is normal in $G$, because $gH = Hg$ for all $g \in G$.
3. Similarly, if $H \leq Z(G)$ then $H \trianglelefteq G$ for the same reason, in particular $Z(G) \trianglelefteq G$.
4. Let $H = \langle r \rangle \leq D_{2n}$. Recall that $N_{D_{2n}}(H) = D_{2n}$, thus $H$ is a normal subgroup of $D_{2n}$.
5. To see that relation $\trianglelefteq$ is not necessarily transitive consider $K = \langle s \rangle \leq H = \langle s, r^2 \rangle \leq G = D_8$. Note that $r^2 \in Z(G)$, so $H$ is abelian, and hence $K \trianglelefteq H$. Moreover, it is easy to check that $N_G(H) = G$ as $r(s)r^{-1} = r^2 s, s(r^2)s^{-1} = r^{-2} = r^2, r(sr^2)r^{-1} = s, s(sr^2)s^{-1} = sr^2$.

   Note however that $K$ is not normal in $G$ since $rsr^{-1} = r^2 s \notin K$.
6. Another example of a non-normal subgroup is $\langle (1\ 2) \rangle \leq S_n$ for $n \geq 3$, since

$$(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3) \notin \langle (1\ 2) \rangle.$$

**Proposition 6.1.5.** *The operation $\cdot : G/H \times G/H \to G/H$ given by*

$$[x] \cdot [y] = [x \cdot y]$$

*(where $x, y \in G, [x] = xH, [y] = yH$) is well-defined (i.e. does not depend on the choice of coset representatives for $xH$ and $yH$) if and only if $H$ is a normal subgroup of $G$.*

*Proof.* Let us pick some other representatives $x' \in [x], y' \in [y]$, where $x' = xh, y' = yk$ with $h, k \in H$ then

$$[x' \cdot y'] = x'y'H = (xhyk)H = (xhy)H.$$

We want $(xy)H = (xhy)H$ for any $h \in H$ and any $x, y \in G$. Note that it is equivalent to asking that $yH = hyH$ for any $h \in H, y \in G$. This condition holds if and only if $Hy = yH$ (because we want $yh' = hy$ for some $h' \in H$ and any $h \in H$) for all $y \in G$. That is, this operation is well-defined if and only if $yH = Hy$ for all $y \in G$, i.e. $H \trianglelefteq G$.

■

Thus we get that $G/H$ is a group when $H \trianglelefteq G$ (the three axioms follow from the axioms for the multiplication on $G$), and in this case it is called the **quotient group** of $G$ with respect to $H$. The quotient map

$$q : G \to G/H$$

is then a group homomorphism (by construction, as $q(x \cdot y) = [x \cdot y] = [x] \cdot [y] = q(x) \cdot q[y]$).

**Remark 6.1.6.** Let $G = \langle S \rangle$ and let $H \trianglelefteq G$ then the set $q(S)$ generates the group $G/H$, because any $a \in G/H$ is equal to $q(x)$ for some $x \in G$ and if $x = s_1^{\varepsilon_1} \cdot \ldots \cdot s_k^{\varepsilon_k}$ for $s_i \in S$ then $q(x) = q(s_1)^{\varepsilon_1} \cdot \ldots \cdot q(s_k)^{\varepsilon_k}$. As a consequence we get that any quotient of a cyclic group is also cyclic.

**Proposition 6.1.7.** *Let $H \trianglelefteq G$ and let $q : G \to G/H$ be the quotient map. For any group $K$ the following map between sets of group homomorphisms:*

$$f : \mathrm{Hom}(G/H, K) \to \{\psi \in \mathrm{Hom}(G, K) \mid \psi(h) = 1\ \forall h \in H\}.$$

$$\phi \mapsto \phi \circ q.$$

*is a bijection. That is, maps out of $G/H$ are maps out of $G$, that are trivial on $H$.*

*Proof.* First of all if $\phi \in \mathrm{Hom}(G/H, K)$ and $\psi = \phi \circ q$ then for any $h \in H$ we have $q(h) = 1 \in G/H$, so $\psi(h) = 1 \in K$. So the map $f$ is well-defined.

Now suppose $f(\phi_1) = f(\phi_2)$ for some $\phi_1, \phi_2 : G/H \to K$. Then for any $g \in G$ we have

$$\phi_1(q(g)) = \phi_2(q(g)) \iff \phi_1([g]) = \phi_2([g]),$$

which implies that $\phi_1 = \phi_2$.

The non-trivial part of this proposition is proving that $f$ is surjective. Consider a map $\psi : G \to K$, such that $\psi(h) = 1$ for every $h \in H$. Define $\psi : G/H \to K$ as follows:

$$\phi([g]) = \psi(g) \text{ for any } g \in G.$$

We need to show that this map is well defined, i.e. doesn't depend on the choice of coset representatives. Suppose $[g'] = [g]$, i.e. $g' = gh$ for some $h \in H$, then

$$\phi([g']) = \phi([gh]) = \psi(gh) = \psi(g)\psi(h) = \psi(g) = \phi([g])$$

which proves that $\phi$ is well defined. Moreover, $\phi$ is a group homomorphism by construction:

$$\phi([g_1] \cdot [g_2]) = \phi([g_1 \cdot g_2]) = \psi(g_1 \cdot g_2) = \psi(g_1) \cdot \psi(g_2) = \phi([g_1]) \cdot \phi([g_2]).$$

We get that $f(\phi)(g) = \phi(q(g)) = \phi([g]) = \psi(g)$ for any $g \in G$, thus the map $f$ is surjective. ∎

**Example 6.1.8.**

1. The quotient $G/\{1\}$ is naturally identified with $G$. And the quotient $G/G$ is the trivial group.

2. As discussed before $\mathbb{Z}/n\mathbb{Z}$ turned out to be a well-defined additive group, since $\mathbb{Z}$ is abelian, and so $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Note that since all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for $n \geq 0$ the groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}, n = 1, 2, \ldots$ are the only possible quotient groups of $\mathbb{Z}$.

3. The group $G = \mathbb{Z}/n\mathbb{Z}$ is cyclic, and thus has a unique subgroup $H_d$ of order $d$ for every $d \mid n$, for a fixed $d$ this subgroup is cyclic and thus it is isomorphic to $\mathbb{Z}/d\mathbb{Z}$. We get that

$$G/H_d = (\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/d\mathbb{Z}) \simeq \mathbb{Z}/k\mathbb{Z},$$

   where $k = n/d$, since it is a cyclic group of order $k$.

4. Let $H = \langle r \rangle \leq D_{2n}$ then $H \simeq \mathbb{Z}/n\mathbb{Z}$ is a subgroup of index 2, and the quotient $D_{2n}/H$ is a group with two elements, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

5. We claim that $\mathbb{R}/\mathbb{Z}$ is isomorphic to $S^1$. Define

$$\phi : \mathbb{R}/\mathbb{Z} \to S^1$$

$$[t] \mapsto e^{2\pi i \cdot t}.$$

   This is a well-defined group homomorphism since the map $\psi : \mathbb{R} \to S^1$ sending $t$ to $e^{2\pi i \cdot t}$ is trivial on $\mathbb{Z}$. Moreover, this map is injective as $e^{2\pi i \cdot t} = 1$ if and only if $t \in \mathbb{Z}$, and it is obviously surjective.

6. The quotient $\mathbb{C} - \{0\}/S^1$ is isomorphic to $\mathbb{R}_{>0}$ via the polar decomposition of complex numbers: for any $z \in \mathbb{C} - \{0\}$ there exists a unique $r = |z| \in \mathbb{R}_{>0}$ and a unique point $e^{i\phi}$ on $S^1$ such that $z = r \cdot e^{i\phi}$. This decomposition actually gives an isomorphism between $\mathbb{C} - \{0\}$ and the direct product $S^1 \times \mathbb{R}_{>0}$. The quotient map is then the projection onto $\mathbb{R}_{>0}$.

**Remark 6.1.9.** As promised, if $H \trianglelefteq G$ then $H\backslash G = G/H$, so we can stick to our preferred notation with no remorse or hesitations.

## 6.2 Isomorphism theorem

Let $H \trianglelefteq G$ and let $q : G \to G/H$ be the quotient map. Then

$$\mathrm{Ker}(q) = H.$$

Moreover, we can state the following

**Proposition 6.2.1.** *A subgroup $H$ of $G$ is normal if and only if it is the kernel of some group homomorphism $G \to K$ (for some group $K$).*

*Proof.* If $H \trianglelefteq G$ then $H = \mathrm{Ker}(q)$, for $q : G \to G/H$ the quotient map.

Now, if $\psi : G \to K$ is a group homomorphism then for any $x \in \mathrm{Ker}(\psi)$ and any $g \in G$ we have

$$\psi(gxg^{-1}) = \psi(g)\psi(x)\psi(g^{-1}) = \psi(g)\psi(g)^{-1} = 1.$$

Thus, $gxg^{-1} \in \mathrm{Ker}(\psi)$, and so $N_G(\mathrm{Ker}(\psi)) = G$. ■

Recall that any subgroup $H$ of $G$ comes naturally equipped with an injective group homomorphism $i : H \to G$ (the embedding of $H$ into $G$). Moreover, if $\phi : H \to G$ is an injective group homomorphism then $H$ is isomorphic to the subgroup $\phi(H)$ of $G$.

The counterpart of these statements for quotient groups is the following: note that any quotient group $G/H$ comes naturally equipped with a surjective group homomorphism $q : G \to G/H$. Moreover, we have the following

**Proposition 6.2.2.** *Let $\psi : G \to K$ be a surjective group homomorphism then $K \simeq G/H$, where $H = \mathrm{Ker}(\psi)$.*

*Proof.* Let $H = \mathrm{Ker}(\psi)$ then $\psi(h) = 1$ for any $h \in H$. By Proposition 6.1.7, there is a unique homomorphism $\phi : G/H \to K$ with $\psi = \phi \circ q$. Let us prove that $\phi$ is bijective.

First note that $\phi(G/H) = \psi(G) = K$, so $\phi$ is surjective.

Moreover, if $\phi([g_1]) = \phi([g_2])$ then $\psi(g_1) = \psi(g_2)$, thus $g_1 g_2^{-1} \in \mathrm{Ker}(\psi) = H$, so $g_1^{-1} g_2 = h$ for some $h \in H$ and hence $g_2 = g_1 h$, so $[g_1] = [g_2]$.

■

As the corollary of this proposition we get

**Theorem 6.2.3** (The First Isomorphism Theorem)**.** *Let $\phi : G \to K$ be a group homomorphism. Then* $\mathrm{Ker}(\phi) \trianglelefteq G$ *and*

$$G/\mathrm{Ker}(\phi) \simeq \phi(G).$$

*Proof.* Apply Proposition 6.2.2 to the surjective homomorphism $G \to \phi(G)$. ■

**Remark 6.2.4.** So we established that one can think about quotient groups of $G$ as groups coming with a surjective homomorphism out of $G$.

Taking quotients is also a way to make a group smaller. If $G$ is a finite group then if we start taking quotients of quotients of $G$ we will eventually end up with the trivial group. We can "reduce" $G$ to smaller groups until we encounter something "irreducible".

**Definition 6.2.5.** A group $G$ is called **simple** if the only normal subgroups of $G$ are $\{1\}$ and $G$. Simple groups are groups that admit no nontrivial quotients.

**Example 6.2.6.** The group $\mathbb{Z}/n\mathbb{Z}$ is simple if and only if $n$ is prime (recall that subgroups of $\mathbb{Z}/n\mathbb{Z}$ correspond to divisors of $n$).

Simple groups are essentially "building blocks" for all other groups (look up Jordan-Hölder Theorem and composition series). By the discussion above every group has a nontrivial simple quotient: $q : G \to G/H = S$, the kernel of the quotient map $q$ is a subgroup $H \leq G$ of smaller size than $G$.

If we were going to try to classify all finite groups we could start by classifying finite simple groups (which was successfully done already, you can look it up!) and then try to classify ways to glue $G$ out of two smaller group: $G/H$ and $H$. The latter part of this endeavour has proven to be quite difficult. However, we will discuss later some specific ways to glue a new group out of two smaller ones (see Section 7.1.7).

**Definition 6.2.7.** We say that $G$ is an extension between $K$ and $H$ if there exists a surjective homomorphism $\pi : G \to K$ and an isomorphism between $H$ and $\mathrm{Ker}(\pi)$.

**Example 6.2.8.**

1. Let $A, B$ be two groups and let $G = A \times B$ then $A \times \{1\} \simeq A$ is a normal subgroup of $G$ and $G/A \simeq B$. Direct product is one example of an extension between $B$ and $A$. It is called the **trivial extension** between $B$ and $A$. (Note that $A \times B$ is also an extension between $A$ and $B$.)

2. Let $n = m \cdot k$ then $G = \mathbb{Z}/n\mathbb{Z}$ has a unique subgroup $H$ isomorphic to $\mathbb{Z}/m\mathbb{Z}$, and the quotient $G/H$ is isomorphic to $\mathbb{Z}/k\mathbb{Z}$. Thus $\mathbb{Z}/n\mathbb{Z}$ is an extension between $\mathbb{Z}/k\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$.

3. Let $n = m \cdot k$ as before. Note that $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ if and only of $\gcd(m, k) = 1$. So when $m$ and $k$ are not coprime there exists a **nontrivial** extension between $\mathbb{Z}/k\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$.

4. Let $H = \langle r \rangle \leq D_{2n}$. Recall that $H \simeq \mathbb{Z}/n\mathbb{Z}$ is a normal subgroup of index 2 in $D_{2n}$, and $D_{2n}/H \simeq \mathbb{Z}/2\mathbb{Z}$, so $D_{2n}$ is a nontrivial extension between $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ (it is nontrivial because it is not abelian).

5. Let $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ then $\mathbb{Z}/n\mathbb{Z}$ is "built out of" $a_1$ copies of $\mathbb{Z}/p_1\mathbb{Z}$, $a_2$ copies of $\mathbb{Z}/p_2\mathbb{Z}, \ldots,$ $a_k$ copies of $\mathbb{Z}/p_k\mathbb{Z}$. In the sense that

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z},$$

and for any prime $p$: $\mathbb{Z}/p^a\mathbb{Z}$ is an extension between $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^{a-1}\mathbb{Z}$, thus $\mathbb{Z}/p^a\mathbb{Z}$ is "glued out of" $a$ copies of $\mathbb{Z}/p\mathbb{Z}$.

## 6.3 Sign map for the symmetric group

In this section we will construct new examples of simple groups, called **alternating groups**, and describe the symmetric group $S_n$ as an extension between two simple groups when $n \geq 5$.

**Definition 6.3.1.** For any $\sigma \in S_n$ an **inversion** of $\sigma$ is a pair $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ with

$$i < j \text{ and } \sigma(i) > \sigma(j).$$

We denote by $Inv(\sigma)$ the set of all inversions of $\sigma$ and by $inv(\sigma)$ the number of elements in this set.

**Example 6.3.2.** Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 7 & 6 & 5 & 3 \end{bmatrix}$ then

$$Inv(\sigma) = \{(1,2), (1,3), (1,7), (2,3), (4,5), (4,6), (4,7), (5,6), (5,7), (6,7)\}.$$

So, $inv(\sigma) = 10$.

**Quick way to compute:**

1. Look at the second line of the two-line presentation of $\sigma : \sigma(1), \sigma(2), \ldots, \sigma(n)$. Start with $\sigma(i)$ and look at all the numbers to the right of it marking those smaller than $\sigma(i)$. Add a pair $(i, j)$ to the list of inversions of $\sigma$ for every position $j$ to the right of $i$ with $\sigma(j) > \sigma(i)$.

In our example, $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 7 & 6 & 5 & 3 \end{bmatrix}$ we start with $\sigma(1)$:

$$\underline{4}\ \textcircled{2}\ \textcircled{1}\ 7\ 6\ 5\ \textcircled{3},$$

so we add $(1,2),(1,3),(1,7)$. We proceed with $\sigma(2)$ :

$$4\ \underline{2}\ \textcircled{1}\ 7\ 6\ 5\ 3,$$

we add $(2,3)$. There are no such numbers for $\sigma(3)$ as $\sigma(3) = 1$, we skip it. We proceed with $\sigma(4)$ :

$$4\ 2\ 1\ \underline{7}\ \textcircled{6}\ \textcircled{5}\ \textcircled{3},$$

we add $(4,5),(4,6),(4,7)$. We proceed with $\sigma(5)$ :

$$4\ 2\ 1\ 7\ \underline{6}\ \textcircled{5}\ \textcircled{3},$$

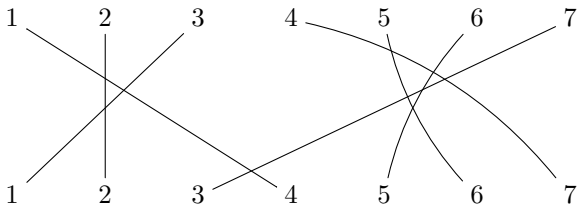
we add $(5,6),(5,7)$. Lastly we do this for $\sigma(6)$ :

$$4\ 2\ 1\ 7\ 6\ \underline{5}\ \textcircled{3},$$

we add $(6,7)$.

2. If one is just interested in the number $inv(\sigma)$, one can do the following computation instead. Draw a diagram for $\sigma$: place points $1, 2, \ldots, n$ in two rows and connect $i$ in the top row with $\sigma(i)$ in the bottom row.

   For example for $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 7 & 6 & 5 & 3 \end{bmatrix}$ we get:




   Now the number of intersections between lines is precisely $inv(\sigma)$ (make sure to avoid triple intersections).

**Definition 6.3.3.** Define a map

$$sgn : S_n \to \{-1, 1\}$$

via

$$sgn(\sigma) = (-1)^{inv(\sigma)}.$$

This map is called the **sign map** and $sgn(\sigma)$ is called the **sign** of $\sigma$.

A permutation $\sigma$ is called **even** if $sgn(\sigma) = 1$, and it is called **odd** if $sgn(\sigma) = -1$.

**Example 6.3.4.** 1. Let $e$ be the identity in $S_n$ then $inv(e) = 0$ and thus $e$ is even.

2. Let $\sigma = (i\ i+1)$ be a transposition of two consecutive elements then $Inv(\sigma) = \{(i, i+1)\}$ and thus $\sigma$ is odd.

**Proposition 6.3.5.** *The map $sgn : S_n \to \{-1, 1\}$ is a group homomorphism (where $\{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ is a multiplicative version of the cyclic group of order 2).*

To prove this proposition we need the following

**Lemma 6.3.6.** *Let $s_i = (i\ i+1)$ and $\sigma \in S_n$ then*

$$|inv(\sigma \circ s_i) - inv(\sigma)| = 1.$$

*Proof of Lemma.* Suppose $\sigma(i) < \sigma(i+1)$ then $(i, i+1) \notin Inv(\sigma)$, however

$$\sigma \circ s_i(i) = \sigma(i+1) > \sigma(i) = \sigma \circ s_i(i+1),$$

so $(i, i+1) \in Inv(\sigma \circ s_i)$.

If $\sigma(i) > \sigma(i+1)$ then $(i, i+1) \in Inv(\sigma)$ and

$$\sigma \circ s_i(i) = \sigma(i+1) < \sigma(i) = \sigma \circ s_i(i+1),$$

so $(i, i+1) \notin Inv(\sigma \circ s_i)$.

Moreover, if $(a, b) \neq (i, i+1)$ then $(a, b) \in Inv(\sigma)$ if and only if $(s_i(a), s_i(b)) \in Inv(\sigma \circ s_i)$ (note that $s_i(a) < s_i(b)$ when $a < b$ and $(a, b) \neq (i, i+1)$, also $(s_i(a), s_i(b)) \neq (i, i+1)$). □

Now we are ready to prove the proposition:

*Proof.* By Lemma 6.3.6 we get that

$$sgn(\sigma \circ s_i) = -sgn(\sigma)$$

for any $\sigma \in S_n$. Recall that the transpositions $s_1, \ldots, s_{n-1}$ generate $S_n$, thus for any two permutations $\sigma, \tau$ we can choose a decomposition

$$\sigma = s_{i_1} \circ \ldots \circ s_{i_k},$$

$$\tau = s_{j_1} \circ \ldots s_{j_l},$$

with $i_a, j_b \in \{1, \ldots, n-1\}$. We get that $sgn(\sigma) = (-1)^k, sgn(\tau) = (-1)^l$, and

$$sgn(\sigma \circ \tau) = sgn(s_{i_1} \circ \ldots \circ s_{i_k} \circ s_{j_1} \circ \ldots s_{j_l}) = (-1)^{k+l} = sgn(\sigma) \cdot sgn(\tau).$$

■

**Corollary 6.3.7.** *1. Let $\sigma \in S_n$ then $sgn(\sigma) = sgn(\sigma^{-1})$.*

*2. Let $\sigma = (i\ j)$ be any transposition then $sgn(\sigma) = -1$.*

*3. Let $\sigma = (a_1\ \ldots\ a_m)$ be a cycle of length $m$ then $sgn(\sigma) = (-1)^{m-1}$.*

*4. Let $\sigma = C_1 \cdot \ldots \cdot C_k$ be a product of $k$ cycles of lengths $m_1, \ldots, m_k$ then*

$$sgn(\sigma) = (-1)^{\sum_{i=1}^{k}(m_k - 1)}.$$

*Proof.* 1. We have $sgn(\sigma^{-1}) = sgn(\sigma)^{-1} = sgn(\sigma)$.

2. Let $\tau$ be a permutation that sends 1 to $i$ and 2 to $j$ and fixes every other element. Then

$$\tau \circ (1\ 2) \circ \tau^{-1} = (i\ j).$$

We have

$$sgn(\tau \circ (1\ 2) \circ \tau^{-1}) = sgn(\tau) \cdot sgn((1\ 2)) \cdot sgn(\tau)^{-1} = -1 = sgn((i\ j)).$$

3. We have

$$\sigma = (a_1\ a_2)(a_2\ a_3) \ldots (a_{m-1}\ a_m),$$

so

$$sgn(\sigma) = (-1)^{m-1}.$$

4. This is a direct corollary of Proposition 6.3.5 and part 3.

■

**Example 6.3.8.** Let $\sigma = (1\ 3)(2\ 5\ 7)(4)(6\ 8)$ then $sgn(\sigma) = (-1) \cdot 1 \cdot 1 \cdot (-1) = 1$.

**Definition 6.3.9.** Define the **alternating group** $A_n$ to be the set of all even permutations in $S_n$.

We get that $A_n \trianglelefteq S_n$ since $A_n = \mathrm{Ker}(sgn)$. Moreover, we get that $S_n$ is an extension between $\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ and $A_n$ (i.e. $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$).

We get that $A_n$ has index 2 in $S_n$, thus $|A_n| = \frac{n!}{2}$.

We will leave the next theorem without a proof:

**Theorem 6.3.10.** *When $n \geq 5$, $A_n$ is a simple group and a unique normal subgroup of $S_n$.*

# 7 Direct and semidirect products of groups

## 7.1 Recognizing direct products

*In the context of extension between groups, let us try to understand for a given group $G$ whether $G$ can be decomposed as a direct product of two smaller groups.*

**Proposition 7.1.1.** *Let $G_1, \ldots, G_k$ be groups and let $G = G_1 \times \ldots \times G_k$ be their direct product. Then*

1. *For each $i = 1, \ldots, k$ the set*

$$1 \times \ldots \times 1 \times G_i \times 1 \times \ldots \times 1 = \{(1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\}$$

*is a subgroup of $G$ isomorphic to $G_i$. If we identify $G_i$ with this subgroup then $G_i \trianglelefteq G$ and*

$$G/G_i \simeq G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_k.$$

*We have $G_i \cap G_j = 1$ if $i \neq j$.*

2. *For each $i = 1, \ldots, k$ define the map*

$$\pi_i : G \to G_i$$

$$(g_1, \ldots, g_k) \mapsto g_i.$$

*Then $\pi_i$ is a surjective group homomorphism with*

$$\mathrm{Ker}(\pi_i) = G_1 \times \ldots \times G_{i-1} \times 1 \times G_i \times \ldots \times G_k \simeq$$

$$\simeq G_1 \times \ldots \times G_{i-1} \times G_i \times \ldots \times G_k$$

3. *Under the identification of part 1, if $x \in G_i \leq G$ and $y \in G_j \leq G$ then $xy = yx$ when $i \neq j$.*

*Proof.* All parts easily follow from homework exercises. ■

*We deduce that if $G$ is a direct product of two groups then $G$ must have two normal subgroups $H, K \trianglelefteq G$ with $H \cap K = \{1\}$, such that elements of $H$ commute with elements of $K$ (think $G = H \times K$). Moreover, for each $g \in G$ we have $g = hk$ for unique elements $h \in H, k \in K$.*

*Given two subgroups $H, K$ of $G$ define*

$$HK = \{hk \mid h \in H, k \in K\}.$$

**Proposition 7.1.2.** *$HK$ is a subgroup of $G$ if $H \leq N_G(K)$ or $K \leq N_G(H)$.*

*Proof.* We want $HK$ to be closed under taking inverses and products. Suppose $H \leq N_G(K)$ then for any $k \in K$ and $h \in H$ there exists $k_0 \in K$ such that $hkh^{-1} = k_0$. Thus

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k_0^{-1} \in HK.$$

Now if $h_2^{-1}k_1h_2 = k_3 \in K$ then

$$(h_1k_1) \cdot (h_2k_2) = (h_1h_2)(k_3k_2) \in HK.$$

The proof for the case $K \leq N_G(H)$ is similar. ■

**Example 7.1.3.** If $H = \langle(1\ 2)\rangle$ and $K = \langle(2\ 3)\rangle$ in $S_3$ then

$$HK = \{e, (1\ 2), (2\ 3), (1\ 2\ 3)\},$$

so it is easy to see that $HK$ is not closed under inverses as $(1\ 2\ 3)^{-1} = (1\ 3\ 2) \notin HK$.

**Proposition 7.1.4.** *Let $H, K \leq G$ and suppose $H \cap K = \{1\}$. Then every element $g \in HK$ has a **unique** decomposition $g = hk$ for $h \in H, k \in K$.*

*Proof.* Suppose $hk = h_0k_0$ then $kk_0^{-1} = h^{-1}h_0$, so $kk_0 \in H \cap K$ so $kk_0^{-1} = h^{-1}h_0 = 1$, which implies $k = k_0, h = h_0$. ■

**Proposition 7.1.5.** *Suppose $H, K \trianglelefteq G$ with $H \cap K = \{1\}$ then $hk = kh$ for every $h \in H, k \in K$.*

*Proof.* Let $h \in H, k \in K$ consider the element $x = hkh^{-1}k^{-1}$. We want to prove $x = 1$. Note that since $N \trianglelefteq G$, we have $kh^{-1}k^{-1} \in H$, and thus $x \in H$. Similarly, since $K \trianglelefteq G$, $hkh^{-1} \in K$, and thus $x \in K$. We deduce that $x \in H \cap K = \{1\}$. ■

**Remark 7.1.6.** Note that under conditions $H, K \trianglelefteq G$, we automatically get that $HK \leq G$.

**Theorem 7.1.7.** *Let $H, K \trianglelefteq G$ with $H \cap K = \{1\}$ and $HK = G$ then $G \simeq H \times K$ (we call $G$ an internal direct product of $H$ and $K$.*

*Proof.* Define a map

$$\phi : H \times K \to G,$$
$$(h, k) \mapsto hk.$$

Let us prove that it is a bijective group homomorphism.

First note that $\phi$ is surjective as $G = HK$. Moreover, if $\phi(h, k) = \phi(h_0, k_0)$ then $hk = h_0k_0$, which by Proposition 7.1.4 implies that $h = h_0, k = k_0$, and thus $\phi$ is injective.

Now $\phi(hh_0, kk_0) = (hh_0)(kk_0) = (hk)(h_0k_0) = \phi(h, k)\phi(h_0, k_0)$, since $h_0k = kh_0$ by Proposition 7.1.5. ■

**Example 7.1.8.** Let $G = \mathbb{Z}/21\mathbb{Z}$ and let $H = \langle[3]\rangle, K = \langle[7]\rangle$. Since $G$ is abelian, we get $H, K \trianglelefteq G$. Moreover, $H \cap K = \{[0]\}$, thus $HK$ (or better to say $H + K$ as the group operation is addition) is a subgroup that has $|H| \cdot |K| = 7 \cdot 3 = 21$ elements (by Proposition 7.1.4). We get that $G = H + K$, and thus $G \simeq H \times K$. Note that since $H \simeq \mathbb{Z}/7\mathbb{Z}, K \simeq \mathbb{Z}/3\mathbb{Z}$, we get the already familiar decomposition $\mathbb{Z}/21\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

## 7.2 Semidirect products

In this section we will describe a construction of a an extension between $K$ and $H$ that generalizes the direct product construction.

Let $G$ be a group and let $H, K \leq G$. Note that we don't need both $H$ and $K$ to be normal in order for $HK$ to be a subgroup in $G$. So let us relax this condition a little bit and try to formulate a generalization of Theorem 7.1.7 under the assumption that

1. $H \trianglelefteq G$,

2. $G = HK$,

3. $H \cap K = \{1\}$.

Note that Proposition 7.1.4 still holds, so the map $\phi : H \times K \to G, (h,k) \mapsto hk$ is still bijective. So we can think about elements of $G$ as pairs $(h,k), h \in H, k \in K$. Given elements $h_1k_1, h_2k_2$ let us try to understand how to write their product as an element of $HK$. Note that since $H \trianglelefteq$,

$$k_1h_2k_1^{-1} \in H$$

, and thus

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})(k_1k_2) = h_3k_3,$$

where $h_3 = h_1(k_1h_2k_1^{-1}), k_3 = k_1k_2$.

**Proposition 7.2.1.** *Let $H, K \leq G$ satisfy the conditions above (i.e. $H \trianglelefteq G, G = HK, H \cap K = \{1\}$) then*

$$G/H \simeq K,$$

*so $G$ is an extension between $K$ and $H$.*

*Proof.* Define the map $\pi : G \to K$ by putting

$$\pi(hk) = k.$$

Then $\pi$ is surjective and

$$\pi(h_1k_1 \cdot h_2k_2) = \pi(h_3k_3) = k_3 = k_1k_2 = \pi(h_1k_1) \cdot \pi(h_2k_2),$$

so $\pi$ is a group homomorphism. Clearly, $\mathrm{Ker}(\pi) = \{h \cdot 1 \mid h \in H\} = H$, so by the isomorphism theorem we get that $K \simeq G/H$. ∎

**Definition 7.2.2.** If $H, k \leq G$ with $H \trianglelefteq G, G = HK, H \cap K = \{1\}$ we call $G$ an *internal semidirect product* of $H$ and $K$.

**Remark 7.2.3.** Note that if $K$ is also a normal subgroup of $G$ (for example when $G$ is abelian) then the semidirect product of $H$ and $K$ is the same as their direct product.

So, given groups $H$ and $K$, how do we construct a group $G$ for which $H$ and $K$ are subgroups satisfying the conditions of Definition 7.2.2? We know that as a set $G = H \times K$ (every element of $G$ can be written uniquely as a product $hk, h \in H, k \in K$). Let us define a new group operation on this set. Recall that in the product of $h_1k_1$ and $h_2k_2$ appears the element $k_1h_2k_1^{-1} \in H$. As $H$ was a normal subgroup, the conjugation action of $K$ on $G$ could be restricted to $H$ and we had $k \star h = khk^{-1}$ so

$$(h_1k_1) \cdot (h_2k_2) = (h_1 \cdot (k_1 \star h_2))(k_1 \cdot k_2)$$

This shows that multiplication in $G = HK$ depends only on multiplication in $H$, multiplication in $K$ and the action of $K$ on $H$ by group automorphisms, so $G$ can be defined intrinsically in terms of $H$ and $K$.

**Definition 7.2.4.** Let $H$ and $K$ be two groups and let $K$ act on $H$ by group homomorphisms, i.e. let us fix a homomorphism of groups $\phi : K \to \mathrm{Aut}(H)$ with $\phi(k)(h) = k \star h$. Define the **semidirect product** of $H$ and $K$ as a group $H \rtimes_\phi K$ with the underlying set $H \times K$ and the operation

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot (k_1 \star h_2), k_1 \cdot k_2).$$

Let us prove that $H \rtimes_\phi K$ with the operation defined above satisfies group axioms:

1. We have
$$(h_1,k_1)\cdot((h_2,k_2)\cdot(h_3,k_3)) = (h_1,k_1)\cdot(h_2\cdot(k_2\star h_3),k_2\cdot k_3) =$$
$$= (h_1\cdot(k_1\star(h_2\cdot(k_2\star h_3))),k_1\cdot k_2\cdot k_3) = (h_1\cdot(k_1\star h_2)\cdot((k_1k_2)\star h_3),k_1k_2k_3) =$$
$$= (h_1\cdot(k_1\star h_2),k_1k_2)\cdot(h_3,k_3) = ((h_1,k_1)\cdot(h_2,k_2))\cdot(h_3,k_3).$$
Note that we used here that $K$ acts on $H$ by group automorphisms, i.e. that $k\star(h\cdot h') = (k\star h)\cdot(k\star h')$.

2. We claim that $(1,1)$ is the identity of $H\rtimes K$ since
$$(h,k)\cdot(1,1) = (h\cdot(k\star 1),k) = (h,k) = (1\cdot(1\star h),k)(1,1)\cdot(h,k).$$
We use here that $\phi(1)$ is an automorphism of $H$, and thus $\phi(1) = id_H$, so $\phi(1)(h) = 1\star h = h$.

3. Suppose
$$(h_1,k_1)\cdot(h_2,k_2) = (h_1\cdot(k_1\star h_2),k_1\cdot k_2) = (1,1)$$
then $k_2 = k_1^{-1}$ and we want
$$k_1\star h_2 = h_1^{-1},$$
so
$$h_2 = k_1^{-1}\star h_1^{-1}.$$
Let us check that $(k_1^{-1}\star h_1^{-1},k_1^{-1})$ is the inverse of $(h_1,k_1)$:
$$(h_1,k_1)\cdot(k_1^{-1}\star h_1^{-1},k_1^{-1}) = (h_1\cdot(k_1\star k_1^{--1}\star h_1^{-1},k_1k_1^{-1}) = (1,1),$$
and
$$(k_1^{-1}\star h_1^{-1},k_1^{-1})\cdot(h_1,k_1) = ((k_1^{-1}\star h_1^{-1})\cdot(k_1^{-1}\star h_1),k_1^{-1}k_1) = (k_1^{-1}\star(h_1^{-1}\cdot h_1),1) = (1,1).$$
Again we use the fact that $k\star(h\cdot h') = (k\star h)\cdot(k\star h')$ and that $k\star 1 = \phi(k)(1) = 1$.

**Theorem 7.2.5.** *Let $H,K$ be two groups, let $\phi: K\to \mathrm{Aut}(H)$ be a group homomorphism, and let $G = H\rtimes_\phi K$ then the set*
$$H\times 1 = \{(h,1)\mid h\in H\}\subset G$$
*is a subgroup of $G$ isomorphic to $H$, and the set*
$$1\times K = \{(1,k)\mid k\in K\}\subset G$$
*is a subgroup of $G$ isomorphic to $K$. Under the identification $H = H\times 1$ and $K = 1\times K$ we get that $H\trianglelefteq G, G = HK, H\cap K = \{(1,1)\}$. Thus $G$ is the internal semidirect product of subgroups $H$ and $K$.*

*Proof.* 1. Let us prove that $H\times 1$ is a subgroup isomorphic to $H$:
First, note that $(1,1)\in H\times 1$. Next, let $(h_1,1),(h_2,1)\in H$ then
$$(h_1,1)^{-1} = (1\star h_1^{-1},1) = (h_1^{-1},1)\in H\times 1$$
and
$$(h_1,1)\cdot(h_2,1) = (h_1\cdot(1\star h_2),1) = (h_1h_2,1)\in H\times 1, \quad (*)$$
so $H\times 1$ is a subgroup.
Moreover, equation $(*)$ implies that the map $H\times 1\to H, (h,1)\mapsto h$ is a group isomorphism.

2. Let us prove that $1 \times K$ is a subgroup isomorphic to $K$:

   We have $(1,1)$ and for $(1,k_1),(1,k_2) \in 1 \times K$ we get

   $$(1,k_1)^{-1} = (k_1^{-1} \star 1, k_1^{-1}) = (\phi(k_1^{-1})(1), k_1^{-1}) = (1, k_1^{-1}) \in 1 \times K,$$

   and

   $$(1,k_1) \cdot (1,k_2) = (k_1 \star 1, k_1 k_2) = (1, k_1 k_2) \in 1 \times K, \quad (**)$$

   so $1 \times K$ is a subgroup.

   Moreover, equation $(**)$ implies that the map $1 \times K \to K, (1,k) \to k$ is a group isomorphism.

3. Let us prove that $H \trianglelefteq G$, $G = H \cap K$, and that $H \cap K = ((1,1))$ (the last part is obvious). First note that

   $$(h,k) = (h,1)(1,k),$$

   so $G = HK$.

   Define the map

   $$\pi : G \to K$$
   $$(h,k) \to k.$$

   Since $\pi((h_1,k_1)(h_2,k_2)) = \pi(h_1 \cdot (k_1 \star h_2), k_1 k_2) = k_1 k_2 = \pi(h_1,k_1)\pi(h_2,k_2)$, we get that $\pi$ is a surjective group homomorphism, and $\mathrm{Ker}(\pi) = \{(h,1) \mid h \in H\} = H$. Therefore, $H \trianglelefteq G$.

■

**Remark 7.2.6.** Note that this means that $H \rtimes_\phi K$ is an extension between $K$ and $H$. Extensions of this form are called **split**.

**Exercise 7.2.7.** Let $G = H \rtimes_\phi K$ and let $h \in H, k \in K$ then

$$(1,k) \cdot (h,1) \cdot (1,k)^{-1} = (k \star h, 1).$$

**Example 7.2.8.**

1. Let $\phi : K \to \mathrm{Aut}(H)$ be the trivial homomorphism then

   $$H \rtimes_\phi K = H \times K.$$

2. By construction, elements of $H$ commute with elements of $K$ inside $H \rtimes_\phi K$ if and only if $\phi$ is trivial.

3. Let $H = \langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ and $K = \langle s \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ be subgroups of $G = D_{2n}$ then $H \trianglelefteq G, G = HK, H \cap K = \{1\}$, so $G$ is the semidirect product of $H$ and $K$.

   Conversely, define the action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/n\mathbb{Z}$ by automorphism as follows:

   $$[1] \star [k] = [-k].$$

   Then with respect to this action we get $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_{2n}$.

4. $\mathbb{Z}/12\mathbb{Z}$ is **not** a split extension between $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$. By part 2, we get that the only commutative split extension between $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ is their direct product, and we know that $\mathbb{Z}/12\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Proposition 7.2.9.** *Let $G$ be an extension between $K$ and $H$ and let $\pi : G \to K$ be the surjective quotient map with $\mathrm{Ker}(\pi) \simeq H$. Then $G \simeq H \rtimes_\phi K$ for some $\phi : K \to \mathrm{Aut}(K)$ if and only if there exists a group homomorphism $\sigma : K \to G$ with $\pi \circ \sigma = id_K$.*

*Proof.* Exercise. ■

**Example 7.2.10.**

1. $S_n$ is isomorphic to the semidirect product $A_n \rtimes \mathbb{Z}/2\mathbb{Z}$. The map $s : \{\pm 1\} \to S_n, -1 \mapsto (1\ 2)$ is a homomorphism, satisfying $sgn \circ s = id$.

2. Let $n = 2k$ with $k$ odd, recall that $Z(D_{2n}) = \{1, r^k\} \simeq \mathbb{Z}/2\mathbb{Z}$ then $D_{2n}/Z(D_{2n})$ is isomorphic to $D_{2k}$ (the quotient map is the surjective map $\pi : D_{2n} \to D_{2k}$ that sends $r$ to $r$ and $s$ to $s$, see Example 3.6.10). Consider the map

$$\sigma : D_{2k} \to D_{2n}$$
$$r \mapsto r^{k+1},$$
$$s \mapsto s.$$

Since $k$ is odd, we have $|r^{k+1}| = \frac{n}{\gcd(n,k+1)} = \frac{2k}{2} = k$, and so $\sigma$ is a well-defined group homomorphism. Moreover, $\pi \circ \sigma$ is the identity map on $D_{2k}$. We get that $D_{2n} \simeq \mathbb{Z}/2\mathbb{Z} \rtimes D_{2k}$. Note however that $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = \{1\}$, so $D_{2n} \simeq \mathbb{Z}/2\mathbb{Z} \times D_{2k}$.

## 7.3 Classification of finitely generated abelian groups

To finish our discussion of group theory let us state without proof an important classification result for abelian groups. We will deuce this result later when we build enough theory of modules over rings, see Section **??**.

**Definition 7.3.1.** 1. A group $G$ is called **finitely generated** if there exists a finite subset $S \subset G$ that generates $G$ (i.e. $G = \langle S \rangle$).

2. For each $r \in \mathbb{Z}_{\geq 0}$ let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ be the direct product of $r$ copies of $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$ is the trivial group. The group $\mathbb{Z}^r$ is called the *free abelian group of rank $r$*.

**Theorem 7.3.2.** *1. Let $G$ be a finitely generated abelian group. Then*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z},$$

*where $r \geq 0, n_j \geq 2$ for $j = 1, \ldots, k$, and*

$$n_{i+1} \mid n_i \text{ for } 1 \leq i \leq k-1.$$

*The integer $r$ is called the free rank of $G$ and $n_i$'s are called invariant factors of $G$.*

*2. The expression in part 1 is unique: if*

$$G \simeq \mathbb{Z}^s \times \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_l\mathbb{Z}$$

*for $s \geq 0, m_i \geq 2$ and $m_i \mid m_{i+1}$ then*

$$s = r, k = l, \text{ and } m_i = n_i \text{ for all } i = 1, \ldots, k.$$

*Sketch of proof.* If $G$ is a finitely generated abelian group with generators $s_1, \ldots, s_m$ then we obtain a surjective group homomorphism

$$\pi : \mathbb{Z}^m \to G,$$

which sends $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 in the $i$'th place) to $s_i$. Let $N = \mathrm{Ker}(\pi) \leq \mathbb{Z}^m$. We would like to choose a new "basis" $f_1, \ldots, f_m$ in $\mathbb{Z}^m$, so that $N$ is generated by $n_1 f_1, \ldots, n_k f_k$ with $k \leq m$ for some $r \geq 0$. If we can do this, we get that $G \simeq \mathbb{Z}^m/N \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$. Note that some of $n_i$'s could be equal to 1, in this case we just discard all trivial quotients $\mathbb{Z}/\mathbb{Z}$ and leave only those $n_i$'s that are greater or equal than 2.

**Corollary 7.3.3.** *If $G$ is a finite abelian group of order $n$ then*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z},$$

*where $n_j \geq 2$ for $j = 1, \ldots, k$,*

$$n_{i+1} \mid n_i \text{ for } 1 \leq i \leq k-1,$$

*and $n = n_1 \cdot \ldots \cdot n_k$.*

**Remark 7.3.4.** Suppose $n = n_1 \cdot \ldots \cdot n_k$ with $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. Let $n = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}$ be the prime decomposition for $n$ then we get that

$$n_i = p_1^{b_{i1}} \cdot \ldots \cdot p_m^{b_{im}} \text{ for } 1 \leq i \leq k,$$

with $b_{1j} \geq b_{2j} \geq \ldots \geq b_{kj} \geq 0$ and $b_{1j} + b_{2j} + \ldots + b_{kj} = a_j$. Since $n_j \geq 2$, we must have $b_{ij} > 0$ for some $i = 1, \ldots, m$ (for each $j = 1, \ldots, k$).

Note that this implies that $b_{1j} \geq 1$ for every $j = 1, \ldots, m$, so $n_1$ must have the same prime divisors as $n$.

Moreover, we can continue this inductively: we have $\frac{n}{n_1} = n_2 \cdot \ldots \cdot n_k$, so $n_2$ must have the same prime divisors as $\frac{n}{n_1}$. Similarly, $n_3$ must have the same prime divisors as $\frac{n}{n_1 n_2}$, and so on.

**Example 7.3.5.**

1. Suppose $n = p_1 \cdot \ldots \cdot p_m$, where $p_i \neq p_j$ for $i \neq j$ (e.g. $n = 210$) then $\mathbb{Z}/n\mathbb{Z}$ is the unique (up to isomorphism) abelian group of order $n$ (by the remark above we must have $n_1 = n$).

2. Let us classify all abelian groups of order 180. We have $180 = 2^2 \cdot 3^2 \cdot 5$. We have four options for the value of $n_1$:

   $$n_1 = 180 = 2^2 \cdot 3^2 \cdot 5,\ 90 = 2 \cdot 3^2 \cdot 5,\ 60 = 2^2 \cdot 3 \cdot 5, \text{ or } 30 = 2 \cdot 3 \cdot 5.$$

   We can then figure out possible values for $n_2$ in each of the last three cases. In our situation in all these cases $\frac{n}{n_1}$ is the product of distinct primes, so we obtain $n_2 = \frac{n}{n_1}$. The final answer is the following classification:

| **Invariant factors** | **Abelian groups** |
|---|---|
| $2^2 \cdot 3^2 \cdot 5$ | $\mathbb{Z}/180\mathbb{Z}$ |
| $2 \cdot 3^2 \cdot 5,\ 2$ | $\mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ |
| $2^2 \cdot 3 \cdot 5,\ 3$ | $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ |
| $2 \cdot 3 \cdot 5,\ 2 \cdot 3$ | $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ |

**Exercise 7.3.6.**

1. Prove that the number of isomorphism classes of abelian groups of order $p^n$, where $p$ is prime, is equal to $\pi(n)$, the number of partitions of $n$.

2. Deduce that the the number of isomorphism classes of abelian groups of order $n = p_1^{a_1} \cdot \ldots p_m^{a_m}$ is $\pi(a_1) \cdot \ldots \pi(a_m)$.

**Example 7.3.7.** Let us illustrate the preceding exercise with an example. Let $n = p^5$ then we get the following classification of abelian groups of order $n$:

| **Partitions of 5** | **Invariant factors** | **Abelian groups** |
|---|---|---|
| $5$ | $p^5$ | $\mathbb{Z}/p^5\mathbb{Z}$ |
| $4+1$ | $p^4,\ p$ | $\mathbb{Z}/p^4\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ |
| $3+2$ | $p^3,\ p^2$ | $\mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ |
| $3+1+1$ | $p^3,\ p,\ p$ | $\mathbb{Z}/p^3\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^2$ |
| $2+2+1$ | $p^2,\ p^2,\ p$ | $(\mathbb{Z}/p^2)^2 \times \mathbb{Z}/p\mathbb{Z}$ |
| $2+1+1+1$ | $p^2,\ p,\ p,\ p$ | $\mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^3$ |
| $1+1+1+1+1$ | $p,\ p,\ p,\ p,\ p$ | $(\mathbb{Z}/p\mathbb{Z})^5$ |

Let us also approach classification of finite abelian groups by applying prime decomposition and the Chinese Remainder Theorem to Corollary 7.3.3. Recall that if $n = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}$ then

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{a_m}\mathbb{Z}.$$

Now let $n = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m} = n_1 \cdot \ldots \cdot n_k$ with $n_{i+1} \mid n_i$ for $1 \leq i \leq k-1$. Using the notations of Remark 7.3.4, we get

$$\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \simeq$$

$$\simeq (\mathbb{Z}/p_1^{b_{11}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{b_{1m}}\mathbb{Z}) \times (\mathbb{Z}/p_1^{b_{21}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{b_{2m}}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_1^{b_{km}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{b_{km}}\mathbb{Z}) \simeq$$

$$\simeq (\mathbb{Z}/p_1^{b_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{b_{21}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_1^{b_{k1}}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_m^{b_{1m}}\mathbb{Z} \times \mathbb{Z}/p_m^{b_{2m}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{b_{km}}\mathbb{Z}),$$

where $b_{1j} \geq b_{2j} \geq \ldots \geq b_{kj} \geq 0$ and $b_{1j} + b_{2j} + \ldots + b_{kj} = a_j$.

We deduce that each abelian group of order $n = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}$ is isomorphic to

$$(\mathbb{Z}/p_1^{b_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{b_{21}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_1^{b_{k1}}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_m^{b_{1m}}\mathbb{Z} \times \mathbb{Z}/p_m^{b_{2m}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{b_{km}}\mathbb{Z})$$

for a unique choice of partitions $b_{1j} + b_{2j} + \ldots + b_{kj}$ of $a_j$ for each $j = 1, \ldots, m$ (note that some of the $b_{ij}$ are equal to zero, in this case we just disregard them).

To summarize our discussion above:

**Translation between partitions and invariant factors.** Let $n_1, \ldots, n_k$ be invariant factors for group $G$ of order $n = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}$ then

$$n_i = p_1^{b_{i1}} \cdot \ldots p_m^{b_{im}} \text{ for } 1 \leq i \leq k,$$

with $b_{1j} \geq b_{2j} \geq \ldots \geq b_{kj} \geq 0$ and $b_{1j} + b_{2j} + \ldots + b_{kj} = a_j$. We assign to $G$ partitions $b_{1j} + b_{2j} + \ldots + b_{kj}$ of each $a_j,\ j = 1 \ldots, m$.

Conversely, given partitions $b_{1j} + b_{2j} + \ldots + b_{k_j j}$ of $a_j$ for each $j = 1, \ldots, m$, define $k = \max(k_1, \ldots, k_m)$ and put $b_{ij} = 0$ for $k_j < i \leq k$. Define

$$n_i = p_1^{b_{i1}} \cdot \ldots \cdot p_m^{b_{im}} \text{ for } 1 \leq i \leq k.$$

Then $n_{i+1} \mid n_i$ since $b_{i+1\ j} \leq b_{ij}$ for all $j$, and $n_i \geq 2$ for all $i = 1, \ldots, k$. Moreover, $n_1 \cdot \ldots \cdot n_k = n$.

**Example 7.3.8.** Let $n_1 = 2^3 \cdot 3^2 \cdot 5, n_2 = 2^2 \cdot 3 \cdot 5, n_3 = 2 \cdot 3, n_4 = 3$ then $n = n_1 \cdot \ldots \cdot n_4 = 2^6 \cdot 3^5 \cdot 5^2$, and the corresponding partitions of $6, 5$, and $2$ are

$$3 + 2 + 1,\ 2 + 1 + 1 + 1,\ 1 + 1.$$

In this case

$$G \simeq \mathbb{Z}/360\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq$$

$$\simeq (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}).$$

For the converse transformation, let $n = 3^7 \cdot 7^3 \cdot 11^4$ and let us fix some partitions of $7, 3$, and $4$, for example

$$3 + 2 + 1 + 1,\ 1 + 1 + 1,\ 2 + 1 + 1.$$

Then the corresponding invariant factors are

$$n_1 = 3^3 \cdot 7 \cdot 11^2,\ n_2 = 3^2 \cdot 7 \cdot 11,\ n_3 = 3 \cdot 7 \cdot 11,\ n_4 = 3.$$

In this case

$$G \simeq (\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}) \simeq$$

$$\simeq \mathbb{Z}/(3^3 \cdot 7 \cdot 11^2)\mathbb{Z} \times \mathbb{Z}/(3^3 \cdot 7 \cdot 11)\mathbb{Z} \times \mathbb{Z}/(3 \cdot 7 \cdot 11)\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

# 8 Rings

## 8.1 Basic definitions and examples

**Definition 8.1.1.** 1. A **ring** $R$ is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

(a) $(R, +)$ is an abelian group (we use the additive notation, so the additive identity in $R$ is denoted by 0, and the additive inverse of $a$ is denoted by $-a$);

(b) $\times$ is associative :

$$(a \times b) \times c = a \times (b \times c) \text{ for all } a, b, c \in R;$$

(c) the distributive laws hold in $R$: for all $a, b, c \in R$

$$(a + b) \times c = (a \times c) + (b \times c) \text{ and } a \times (b + c) = (a \times b) + (a \times c);$$

(d) $R$ has multiplicative identity: there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a.$$

2. The ring $R$ is **commutative** if multiplication is commutative.

3. Sometimes people omit axiom (d) in the definition of a ring. The resulting object $R$ is called a **non-unitary ring** or a ring without identity. In contrast, people refer to rings satisfying axiom (d) as unitary rings or rings with identity. We will mostly consider unitary rings in this class, so I will call them simply rings.

*Notation:* As usual, we will adopt the shorter multiplicative notation and write $a \cdot b$ or $ab$ instead of $a \times b$.

**Remark 8.1.2.** The condition that $R$ is a group under addition is fairly natural, which cannot by said, at first glance, about the condition that $(R, +)$ is abelian. To see where this comes from consider the product

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = 1a + 1b + 1a + 1b = a + b + a + b,$$

and

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = 1a + 1a + 1b + 1b = a + a + b + b.$$

Since $R$ is a group under addition, $a + b + a + b = a + a + b + b$ implies $b + a = a + b$. Therefore, the commutativity of addition *is forced* by the remaining axioms.

**Definition 8.1.3.** A ring $R$ is called a **division ring** if $1 \neq 0$ in $R$ and $R - \{0\}$ is a group under multiplication, that is, for every nonzero element $a \in R$ admits a multiplicative inverse, i.e. there exists $b \in R$ with $a \cdot b = b \cdot a = 1$. A commutative division ring is called a **field**.

**Example 8.1.4.**

1. The *zero ring* $R = \{0\}$. Note that by our definition the zero ring is not a field.

2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R},$ and $\mathbb{C}$ are commutative rings. Among them $\mathbb{Q}, \mathbb{R},$ and $\mathbb{C}$ are fields.

3. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring for each $n > 1$. It is a field if and only if $n$ is prime.

4. (The *real Quaternions*) Define $\mathbb{H}$ to be the collection of elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ (similarly to complex numbers being defined as $\mathbb{R}$-linear combinations $a + bi$). As an additive group $\mathbb{H}$ is isomorphic to $\mathbb{R}^4$ with coordinate-wise addition. That is, we put

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k.$$

Multiplication is $\mathbb{R}$-linear and defined by opening the brackets in

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = aa' + ab'i + ac'j + ad'k + ba'i +$$

$$+bb'i^2 + bc'ij + bd'ik + ca'j + cb'ji + cc'j^2 + cd'jk + da'k + db'ki + dc'kj + dd'k^2,$$

and then using the relations

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j,$$

so

$$(a+bi+cj+dk)(a'+b'i+c'j+d'k) = (aa'-bb'-cc'-dd')+$$
$$+(ab'+ba'+cd'-dc')i+(ac'+ca'-bd'+db')j+(ad'+da'+bc'-cb')k.$$

For example, $(1+i+k)(3-2i-j) = 3-2i-j+3i-2i^2-ij+3k-2ki-kj = 5+2i-3j+2k$. Since $ij \neq ji$, $\mathbb{H}$ is not a commutative ring.

5. A lot of important examples of rings are rings of functions: for example, $\mathrm{Fun}(\mathbb{R},\mathbb{R})$, the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, is a ring under addition and multiplication of functions, i.e. $(f\cdot g)(x) = f(x)\cdot g(x)$, and $(f+g)(x) = f(x)+g(x)$. The constant functions $0 : x \mapsto 0 \in \mathbb{R}$ and $1 : x \mapsto 1 \in \mathbb{R}$ are the additive and multiplicative identities correspondingly.

**Exercise 8.1.5.** Prove that $\mathbb{H}$ is a division ring.

**Proposition 8.1.6.** *Let $R$ be a ring. Then*

1. *$0\cdot a = a\cdot 0 = 0$ for any $a \in R$;*
2. *$(-a)b = a(-b) = -ab$ for any $a, b \in R$;*
3. *$(-a)(-b) = ab$ for any $a, b \in R$;*
4. *the identity $1$ is unique and $-a = (-1)a = a(-1)$.*

*Proof.* 1. Using the distributive law we get

$$0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a,$$

thus since $R$ is a group under addition, we get $0 = 0\cdot a$ (the case $a\cdot 0$ is similar).

2. We have $(-a)b + ab = ((-a)+a)b = 0\cdot b = 0$, so $(-a)b$ is the additive inverse of $ab$ (the case of $a(-b)$ is similar.

3. By part 2, $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

4. If $1$ and $1'$ are multiplicative identities then

$$1 = 1\cdot 1' = 1'.$$

We have $(-1)a + a = (-1)a + 1\cdot a = ((-1)+1)a = 0\cdot a = 0$ (similarly, $a(-1) = -1$).

■

**Definition 8.1.7.** Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a **zero divisor** if there exists a nonzero element $b \in R$ with $ab = 0$ or $ba = 0$.
2. An element $u \in R$ is called a **unit** if there is some $v \in R$ such that $uv = vu = 1$. The set of units in $R$ is denoted $R^\times$. It is easy to check that $R^\times$ is a group under multiplication.

A field $F$ then is a commutative ring, in which every nonzero element is a unit, i.e. $F^\times = F - \{0\}$.

Observe that a zero divisor can never be a unit since if $ab = 0$ and $va = 1$, we get that $b = 1b = vab = v0 = 0$. This shows in particular that fields contain no zero divisors.

**Example 8.1.8.** 1. $\mathbb{Z}$ has no zero divisors and $\mathbb{Z}^\times = \{\pm 1\}$.

2. Since $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, we get that $\mathbb{Q}^\times = \mathbb{Q} - \{0\}, \mathbb{R}^\times = \mathbb{R} - \{0\}, \mathbb{C}^\times = \mathbb{C} - \{0\}$.

3. All nonzero elements in $\mathbb{Z}/n\mathbb{Z}$ are either zero divisors or units. Recall that $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \mid \gcd(a,n) = 1\}$. If $\gcd(a,n) = d = \frac{n}{k}$ then $[a]\cdot[k] = [0]$.

4. Let $f \in \text{Fun}(\mathbb{R}, \mathbb{R})$ then $f$ is a unit if and only if $f(x) \neq 0$ for all $x \in \mathbb{R}$ (with inverse $\frac{1}{f}$). If $f(x) = 0$ for some $x \in \mathbb{R}$ then $f \cdot g = 0$ for $g : \mathbb{R} \to \mathbb{R}$ defined as follows:

$$g(y) = 0, \text{ if } y \neq x,$$

$$g(x) = 1.$$

So in $\text{Fun}(\mathbb{R}, \mathbb{R})$ similarly all nonzero elements are either units or zero divisors.

**Definition 8.1.9.** A nonzero commutative ring with no zero divisors is called an **integral domain**.

Although $R - \{0\}$ is not necessarily a group for an integral domain $R$, it still enjoys the cancellation property:

**Proposition 8.1.10.** *Let $R$ be an integral domain, $a, b, c \in R$ and $ab = ac$ then either $a = 0$ or $b = c$.*

*Proof.* We get $a(b-c) = 0$, since $R$ is an integral domain, this means that at least one of the terms in the product is zero. ■

**Corollary 8.1.11.** *Any finite integral domain $R$ is a field.*

*Proof.* For each $a \in R - \{0\}$ multiplication by $a$ gives an injective map $R \to R, x \mapsto ax$. Since $R$ is finite, it must be bijective. Therefore, there exists $x$ that maps to 1, i.e. $ax = 1$. ■

**Definition 8.1.12.** A subring of a ring $R$ is an additive subgroup $S \leq R$ satisfying the following properties:

1. $1 \in S$,
2. for all $a, b \in S$ we have $ab \in S$ (i.e. it is closed under multiplication).

Operations of addition and multiplication on $R$ when restricted to $S$ give $S$ the structure of a ring.

**Example 8.1.13.**

1. The relation "is a subring of" is clearly transitive.
2. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ is a subring of $\mathbb{R}$, and $\mathbb{R}$ is a subring of $\mathbb{C}$.
3. The set $C(\mathbb{R}, \mathbb{R})$ of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring in $\text{Fun}(\mathbb{R}, \mathbb{R})$.
4. If $R$ is a subring of a field $F$ then $R$ is an integral domain. As we will see, the converse of this statement is also true.
5. The set $\mathbb{H}_{\mathbb{Z}} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ of integral Quaternions is a subring in $\mathbb{H}$. Unlike $\mathbb{H}$, it is not a division ring.

## 8.2 Constructing new rings from existing rings

In this section we will expand our collection of examples by constructing "larger" rings from given rings.

### Polynomial rings

Fix a commutative ring $R$. A *formal sum*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a **polynomial** in $x$ with coefficients in $R$. If $a_n \neq 0$, the polynomial is said to have **degree** $n$, $a_n x^n$ is called the **leading term**, and $a_n$ is called the **leading coefficient**. The polynomial is called **monic** if $a_n = 1$.

**Remark 8.2.1.** The zero polynomial 0 is said to have degree $-\infty$. It is not an integer, but it can be treated as one by putting $-\infty < n$ for any $n \in \mathbb{Z}$ and $-\infty + n = -\infty$ for any $n \in \mathbb{Z}$.

**Definition 8.2.2.** The **ring of polynomials** in the variable $x$ **with coefficients in** $R$ is the set $R[x]$ of all polynomials in $x$ with coefficients in $R$, with the component-wise addition:

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_n x^n + \ldots + b_1 x + b_0) = (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + (a_0 + b_0),$$

and the multiplication defined by putting $ax^i \cdot bx^j = abx^{i+j}$ and using the distributive law to extend this to all polynomials (expanding out and collecting the terms):

$$(a_0 + a_1 x + a_2 x^2 + \ldots) \cdot (b_0 + b_1 x + b_2 x^2 + \ldots) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

(the coefficient of $x^k$ is $\sum_{i=0}^{k} a_i b_{k-i}$).

It is easy to verify that $R[x]$ is a commutative ring. The ring $R$ can be identified with the subring of **constant polynomials** in $R[x]$.

**Remark 8.2.3.** One does not need to assume that $R$ is commutative in order to define $R[x]$. Note however that $R[x]$ is commutative if and only if $R$ is.

We assume $R$ is commutative since this is the situation we will mostly be interested in.

**Example 8.2.4.**

1. The rings $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ are the "usual" polynomials with integer, rational, real, and complex coefficients respectively.

2. One can also consider the polynomial ring $\mathbb{Z}/n\mathbb{Z}[x]$ with coefficients in $\mathbb{Z}/n\mathbb{Z}$. The calculations in this ring are performed *modulo* $n$. For instance, $\mathbb{Z}/3\mathbb{Z}[x]$ consists of polynomials with coefficients $0, 1$, and 2. Let $p(x) = x^2 + 2x + 1$ and $q(x) = x^3 + 2x + 2$ then

$$p(x) + q(x) = x^3 + x^2 + x \in \mathbb{Z}/3\mathbb{Z}[x], \text{ and}$$

$$p(x)q(x) = x^5 + 2x^4 + 2.$$

The ring of coefficient makes a substantial difference in the behavior of polynomials. For instance, $x^2 + 1$ is not a square of any polynomial in $\mathbb{Z}[x]$, however in $\mathbb{Z}/2\mathbb{Z}[x]$ we have

$$x^2 + 1 = (x + 1)^2.$$

**Proposition 8.2.5.** *Let $R$ be an integral domain and let $p(x), q(x)$ be elements of $R[x]$. Then*

1. *degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$;*
2. *the units of $R[x]$ are the constant polynomials in $R^\times$;*
3. *$R[x]$ is an integral domain.*

*Proof.*

1. Suppose $p(x) = a_n x^n + \ldots + a_1 x + a_0$ and $q(x) = b^m x^m + \ldots + b_1 x + b_0$ with $a_n, b_m \neq 0$ (so that degree $p(x) = n$ and degree $q(x) = m$). Then

$$p(x)q(x) = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} + \ldots + (a_1 b_0 + a_0 b_1)x + a_0 b_0,$$

and since $R$ is an integral domain, $a_n b_m \neq 0$, so $a_n b_m x^{n+m}$ is the leading term in $p(x)q(x)$, thus degree $p(x)q(x) = m + n$.

2. If $p(x)q(x) = 1$, by part 1, we get that both $p(x)$ and $q(x)$ should be of degree zero.

3. If $p(x)q(x) = 0$ then the leading term $a_n b_m x^{n+m}$ should be zero, so either $p(x)$ or $q(x)$ is equal to zero.

■

**Remark 8.2.6.** If $R$ has zero divisors then so does $R[x]$. Moreover, if $ab = 0$ in $R$ then $ax^i \cdot bx^j = 0$, so the degree rule no longer holds.

If $S$ is a subring of $R$ then $S[x]$ is a subring of $R[x]$, e.g. $\mathbb{Z}[x]$ is a subring of $\mathbb{R}[x]$.

**Example 8.2.7.** We could continue the process and define a ring of polynomials with coefficients in a ring of polynomials: $R[x_1][x_2]$. We will denote this ring by $R[x_1, x_2]$ and call it a polynomial ring in two variables. One could define the polynomial ring $R[x_1, \ldots, x_n]$ in $n$ variables inductively by adjoining variables one by one.

### Matrix rings

Fix an arbitrary ring $R$ and a positive integer $n$. Let $M_n(R)$ be the set of all $n \times n$ matrices with entries from $R$. The element $(a_{ij})$ of $M_n(R)$ is an $n \times n$ square array of elements of $R$, whose entry in the $i$'th row and $j$'th column is $a_{ij} \in R$. The addition on $M_n(R)$ is component-wise: the $i, j$ entry of the matrix $(a_{ij}) + (b_{ij})$ is $a_{ij} + b_{ij}$. The multiplication is the standard matrix multiplication: the $i, j$ entry of the matrix $(a_{ij}) \cdot (b_{ij})$ is $\sum_{k=1}^{n} a_{ik} b_{kj}$.

It is straightforward calculation to check that $M_n(R)$ is a ring. The multiplicative identity is given by the identity matrix $(\delta_{ij})$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$. As an additive abelian group $M_n(R)$ is the product of $n^2$ copies of $R$.

**Remark 8.2.8.** Note that if $R$ is any nonzero ring then $M_n(R)$ is **not commutative** for any $n \geq 2$.

Define $E_{ij}$ to be the matrix whose only nonzero entry is its $i, j$ entry, which is equal to 1. Then $E_{12} \cdot E_{21} = E_{11}$ and $E_{21} \cdot E_{12} = E_{22}$.

Observe further that $M_n(R)$ always has zero divisors if $n \geq 2$, as $E_{11} \cdot E_{22} = 0$.

**Definition 8.2.9.** The group of units in $M_n(R)$ is the set of all invertible matrices with entries in $R$. It is called the **general linear group** of degree $n$ over $R$ and denoted $GL_n(R)$

An element $(a_{ij})$ of $M_n(R)$ is called a scalar matrix if it is a diagonal matrix, whose diagonal entries are all equal, i.e. $(a_{ij})$ satisfies $a_{ij} = 0$ if $i \neq j$ and $a_{ii} = a_{jj}$ for all $i, j \leq n$. Scalar matrices form a subring, that can be naturally identified with $R$. If $R$ is commutative, scalar matrices commute with all other matrices.

If $S$ is a subring of $R$ then $M_n(S)$ is a subring of $M_n(R)$. Another example of a subring of $M_n(R)$ is the set of all upper-triangular matrices $\{(a_{ij}) \mid a_{pq} = 0 \text{ if } p > q\}$.

**Example 8.2.10.** What happens if we iterate this process and consider $M_n(M_k(R))$? It turns out that we just get matrices of larger size with $M_n(M_k(R)) = M_{nk}(R)$.

### Group rings

Let $G = \{g_1, \ldots, g_n\}$ be a finite group with the identity element $g_1$, and let $R$ be a commutative ring. Define the **group ring** $RG$ of $G$ with coefficients in $R$ to be the set of all formal sums

$$a_1 g_1 + \ldots + a_n g_n,$$

with $a_i \in R$. We shall write $a_1 g_1$ simply as $a_1$. Similarly we shall write the element $1g$ for $g \in G$ simply as $g$.

Addition is defined component-wise:

$$(a_1 g_1 + \ldots + a_n g_n) + (b_1 g_1 + \ldots + b_n g_n) = (a_1 + b_1) g_1 + \ldots + (a_n + b_n) g_n,$$

i.e. as an additive group $RG$ is isomorphic to $R^n$.

Multiplication is defined by putting $(ag) \cdot (bh) = ab(gh)$ and then extending this to all elements of $RG$ by using the distributive law (expanding out and collecting the terms):

$$(\sum_{g \in G} a_g g) \cdot (\sum_{g \in G} b_g g) = \sum_{g \in G} (\sum_{h \in G} a_h b_{h^{-1}g})(h \cdot h^{-1} g) = \sum_{g \in G} (\sum_{h \in G} a_h b_{h^{-1}g}) g.$$

It is straightforward to check that these operations make $RG$ into a ring. The multiplicative identity is $1 = 1g_1 + 0g_2 + \ldots + 0g_n$. The associativity of multiplication follows from the associativity of the group operation in $G$. The ring $RG$ is commutative if and only if $G$ is a commutative group.

**Example 8.2.11.** Let $G = D_6 = \{1, r, r^2, s, rs, r^2s\}$ and $R = \mathbb{Z}$. Consider $\alpha = 1 + r + 2s + r^2s$, $\beta = r - r^2 - s - 2rs$. We have

$$\alpha + \beta = 1 + 2r - r^2 + s - 2rs + r^2s,$$

$$\alpha \cdot \beta = (r - r^2 - s - 2rs) + (r^2 - r^3 - rs - 2r^2s) +$$
$$+(2sr - 2sr^2 - 2s^2 - 4srs) + (r^2sr - r^2sr^2 - r^2s^2 - 2r^2srs) =$$
$$= (r - r^2 - s - 2rs) + (r^2 - 1 - rs - 2r^2s) + (2r^2s - 2rs - 2 - 4r^2) + (rs - s - r^2 - 2r) =$$
$$= -3 - r - 5r^2 - 2s - 4rs.$$

The ring $R$ can be identified with the subring $Rg_1$ of constant formal sums in $RG$. The group $G$ can also be identified with the subset $\{1g \mid g \in G\}$ of $RG$, and as these elements are invertible in $RG$ we can say that $G$ is a subgroup of $(RG)^\times$.

**Remark 8.2.12.** If $|G| > 1$ then $RG$ always has zero divisors. For example, if $g \in G$ is an element of order $m$ then

$$0 = 1 - g^m = (1 - g)(1 + g + g^2 + \ldots + g^{m-1}),$$

so $(1 - g)$ is a zero divisor in $RG$ (for any $g \in G$ actually, since $G$ is a finite group, and so all elements have finite order).

If $S$ is a subring of $R$ then $SG$ is a subring of $RG$. Furthermore, if $H$ is a subgroup of $G$ then $RH$ is a subring of $RG$.

### Rings of functions and direct products

**Definition 8.2.13.** Let $R$ be a ring and let $X$ be some nonempty set. The **ring of functions** from $X$ to $R$ is the set $\mathrm{Fun}(X, R)$ of all set-theoretic functions from $X$ to $R$ with addition and multiplication defined via

$$(f + g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$

The ring $\mathrm{Fun}(X, R)$ is commutative if and only if $R$ is. The ring $R$ can be identified with the subring of constant functions in $\mathrm{Fun}(X, R)$. The multiplicative identity in $\mathrm{Fun}(X, R)$ is the constant function $1 : x \mapsto 1 \in R$.

If $S$ is a subring of $R$ then $\mathrm{Fun}(X, S)$ is a subring of $\mathrm{Fun}(X, R)$.

**Remark 8.2.14.** If $|X| > 1$ then $\mathrm{Fun}(X, R)$ always has zero divisors. For example, let $x_1, x_2$ be two distinct elements of $X$. Define $f_i : X \to R,\ i = 1, 2$, by setting $f_i(x_i) = 1$ and $f_i(x) = 0$ for all $x \neq x_i$, then $f_1 \cdot f_2 = 0$.

**Definition 8.2.15.** Let $R_1, \ldots, R_k$ be rings. The direct product ring $R_1 \times \ldots \times R_k$ is the ring, whose underlying additive group is the direct product $R_1 \times \ldots \times R_k$, and the multiplication is defined component-wise:

$$(r_1, \ldots, r_k) \cdot (s_1, \ldots, s_k) = (r_1 s_1, \ldots, r_k s_k).$$

The ring $R_1 \times \ldots \times R_k$ is commutative if and only if each $R_i$ is commutative. The multiplicative identity in $R_1 \times \ldots \times R_k$ is $(1, 1, \ldots, 1)$.

**Remark 8.2.16.** If $R_i$'s are nonzero rings, the subgroups

$$0 \times \ldots \times 0 \times R_i \times 0 \times \ldots \times 0$$

are not subrings, as they do not contain the identity.

**Remark 8.2.17.** If $k > 1$ the ring $R_1 \times \ldots \times R_k$ always has zero divisors. For example

$$(r_1, 0, \ldots, 0) \cdot (0, \ldots, 0, r_k) = (0, \ldots, 0).$$

**Definition 8.2.18.** Define the ring $R^k$ to be the direct product of $k$ copies of $R$.

The ring $R$ can be identified with the *diagonal subring* $\{(r, \ldots, r) \mid r \in R\}$ in $R^k$. If $S$ is a subring of $R$ then $S^k$ is the subring of $R^k$.

## 8.3 Ring homomorphisms and quotient rings

**Definition 8.3.1.** Let $R$ and $S$ be rings.

1. A **ring homomorphism** is a map $\phi : R \to S$ satisfying
   (a) $\phi(a + b) = \phi(a) + \phi(b)$ for any $a, b \in R$,
   (b) $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in R$,
   (c) $\phi(1_R) = 1_S$, where $1_R$ and $1_S$ are multiplicative identities in $R$ and $S$ respectively.

   In other words, $\phi$ is a homomorphism of additive groups, that respects the multiplication and preserves the identity.
2. The **kernel** of $\phi$ is the set of all elements in $R$ that map to zero in $S$, that is $\operatorname{Ker}\phi$ is the kernel of $\phi$ as a homomorphism of additive groups.
3. A bijective ring homomorphism is called an **isomorphism**.

**Example 8.3.2.**
1. Note that condition (c) in Definition 8.3.1.1 does not follow from condition (b). Unlike the case of group homomorphisms, we do not allow *trivial* homomorphisms between rings: $R \to S, r \mapsto 0$ for all $r \in R$ is not a ring homomorphism. The only **trivial homomorphism** is the map $R \to 0$ to the zero ring.
2. The quotient map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a surjective homomorphism of rings.
3. The embeddings $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Q} \to \mathbb{R}$, and $\mathbb{R} \to \mathbb{C}$ are injective ring homomorphisms.
4. Let $R$ be a commutative ring and let $r$ be any element of $R$ then the map

   $$ev_r : R[x] \to R$$

   $$f(x) \mapsto f(r),$$

   i.e. $ev_r$ sends $a_n x^n + \ldots + a_1 x + a_0$ to $a_n r^n + \ldots + a_1 r + a_0$ in $R$, is a surjective ring homomorphism.
5. If $S$ is a subring of $R$ then the embedding $S \to R, s \mapsto s \in R$ is an injective ring homomorphism. It applies in particular to the following maps:
   (a) the map $R \to R[x]$, sending elements of $R$ to constant polynomials in $R[x]$,
   (b) the map $R \to M_n(R)$, sending elements of $R$ to scalar matrices in $M_n(R)$,
   (c) the map $R \to RG$ sending element $r$ of $R$ to $rg_1$, where $g_1$ is the identity in $G$,
   (d) the map $R \to \operatorname{Fun}(X, R)$ sending $r \in R$ to the constant function $r : x \mapsto r$ for all $x \in X$,
   (e) the map $R \to R^k$ sending $r \in R$ to the $k$-tuple $(r, r, \ldots, r) \in R^k$.

**Exercise 8.3.3.** Let $X$ be a finite set of order $k > 0$. Prove that the ring $\operatorname{Fun}(X, R)$ is isomorphic to $R^k$.

**Exercise 8.3.4.** Let $G$ be a finite group and let $R$ be a commutative ring. Consider the set $\mathrm{Fun}(G,R)$ with the standard addition of functions: $(f_1+f_2)(x)=f_1(x)+f_2(x)$. Define the operation of **convolution** on $\mathrm{Fun}(G,R)$ as follows:

$$(f_1\star f_2)(x)=\sum_{y\in G} f_1(xy^{-1})f_2(y).$$

1. Prove that $\mathrm{Fun}(G,R)$ is a ring under these two operations.
2. Define the map $\phi: RG\to \mathrm{Fun}(G,R)$, that sends $x\in G$ to the function $f_x$ defined via

   $$f_x(x)=1,\ f_x(y)=0 \text{ if } y\neq x,$$

   and sends the sum $\sum_{x\in G} a_x x\in RG$ to $\sum_{x\in G} a_x\cdot f_x\in \mathrm{Fun}(G,R)$. Prove that $\phi$ is an isomorphism of rings when $\mathrm{Fun}(G,R)$ is endowed with multiplication given by convolution. (Hint: prove that $f_x\star f_y=f_{xy}$ and then use $R$-linearity.)

**Example 8.3.5.** The constructions of rings in Section 8.2 are **functorial**. That is, any ring homomorphism $\phi: R\to S$ induces

1. a ring homomorphism $\phi': R[x]\to S[x]$;
2. a ring homomorphism $\phi': M_n(R)\to M_n(S)$;
3. a ring homomorphism $\phi': RG\to SG$ for any group $G$;
4. a ring homomorphism $\phi': \mathrm{Fun}(X,R)\to \mathrm{Fun}(X,S)$ for any nonempty set $X$.

Moreover, the homomorphism $\phi'$ is injective (resp. surjective) if and only if $\phi$ is injective (resp. surjective).

Recall that for any group homomorphism $\phi: G\to H$ the kernel of $\phi$ was a *normal* subgroup of $G$, whereas the image of $\phi$ was a subgroup of $H$ (note the asymmetry). The next proposition is a version of this statement for rings:

**Proposition 8.3.6.** *Let $\phi: R\to S$ be a ring homomorphism.*

1. *The image of $\phi$ is a subring of $S$.*
2. *The kernel of $\phi$ is an additive subgroup of $R$ with the additional property that for any $x\in\mathrm{Ker}\,\phi$ and any $r\in R$*

   $$rx\in\mathrm{Ker}\,\phi \text{ and } xr\in\mathrm{Ker}\,\phi.$$

   *The kernel of $\phi$ contains $1$ only when $S=0$.*

*Proof.* 1. Exercise.

2. $\mathrm{Ker}\,\phi$ is automatically an additive subgroup of $R$. Now consider $x\in\mathrm{Ker}\,\phi$ and $r\in R$ then

   $$\phi(rx)=\phi(r)\phi(x)=\phi(r)0=0=0\phi(r)=\phi(x)\phi(r)=\phi(xr).$$

   Thus $rx, xr\in\mathrm{Ker}\,\phi$.

■

If $\phi: R\to S$ is a ring homomorphism with kernel $I\subset R$ then the fibers of $\phi$ are cosets $r+I$ (since $\phi$ is a group homomorphism). By the isomorphism theorem, we get the isomorphism of additive groups $\sigma: \mathrm{Im}(\phi)\to R/I$ that sends $\phi(r)$ to $r+I$. Note that the fact that $\phi$ is a ring homomorphism means that we obtain a ring structure on $R/I$ with $(r+I)+(s+I)=(r+s)+I$ and

$$(r+I)\cdot(s+I)=rs+I,$$

(that is, on the left hand side of the bijection $\sigma$ this corresponds to saying that $\phi(r)\cdot\phi(s)=\phi(rs)$).

Let us then start with an arbitrary subgroup $I \leq R$ and ask ourselves when is $R/I$ becomes a ring under the operations

$$(r+I)+(s+I)=(r+s)+I, \text{ and}$$
$$(r+I)\cdot(s+I)=rs+I.$$

**Definition 8.3.7.** Let $I$ be an additive subgroup of a ring $R$.

1. $I$ is called a **left ideal** of $R$ if $ri \in I$ for any $i \in I$ and $r \in R$.
2. $I$ is called a **right ideal** of $R$ if $ir \in I$ for any $i \in I$ and any $r \in R$.
3. $I$ is called a **two-sided ideal** of $R$ if it is both a left and a right ideal.

**Remark 8.3.8.** If $R$ is commutative then all left ideals are simultaneously right and two-sided ideals. In this case they a referred to simply as **ideals** of $R$.

Note also that the second part of Proposition 8.3.6 proves that the kernel of any ring homomorphism is a two-sided ideal.

**Proposition 8.3.9.** *Let $R$ be a ring and let $I$ be an additive subgroup of $R$. Then $R/I$ is a ring with respect to the operations*

$$(r+I)+(s+I)=(r+s)+I, \text{ and}$$
$$(r+I)\cdot(s+I)=rs+I,$$

*if and only if $I$ is a two-sided ideal of $R$.*

*Proof.* The addition is well-defined and makes $R/I$ an abelian additive group since $I$ is a normal subgroup of $R$. We only need to check that multiplication is well-defined, i.e. doesn't depend on the choice of coset representatives. So, let $r' = r + i \in r + I$ and $s' = s + j \in s + I$ then

$$r's' = (r+i)(s+j) = r + is + rj + ij.$$

We want $r + is + rj + ij \in rs + I$ for every $r, s \in R$ and every $i, j \in I$. Note that if $I$ is a two-sided ideal, this property holds as $is, rj,$ and $ij \in I$.

To prove the converse, first, put $r = 0, j = 0$. This conditions now tells us that for each $s \in R$ and each $i \in I$ we must have $is \in I$, meaning that $I$ is a right ideal. Now, put $s = 0, i = 0$ to get that $rj \in I$, meaning that $I$ is a left ideal. We deduce that $I$ must be a two-sided ideal. ∎

**Corollary 8.3.10.** *If $I$ is a two sided ideal of $R$ then $R/I$ is a ring, and the quotients map*

$$\pi : R \to R/I,$$
$$r \mapsto r + I$$

*is a surjective ring homomorphism. The multiplicative identity in $R/I$ is the coset $1 + I$.*

**Theorem 8.3.11** (The isomorphism theorem for rings)**.** *Let $\phi : R \to S$ be a ring homomorphism with $I = \operatorname{Ker}\phi$. Then the map $r + I \mapsto \phi(r)$ gives a ring isomorphism*

$$R/I \simeq \phi(R).$$

*Proof.* By isomorphism theorem for groups, this map is well defined and is an isomorphism of additive groups (in particular it is bijective). Moreover, $(r+I)(s+I) = rs+I \mapsto \phi(rs) = \phi(r)\phi(s)$ and $1 + I \mapsto \phi(1) = 1$. ∎

**Notation:** We will often use the bar notation for reduction mod $I$: $\overline{r} = r + I$. With this notation operations in the quotient ring $R/I$ look as follows:

$$\overline{r} + \overline{s} = \overline{r+s},$$
$$\overline{r} \cdot \overline{s} = \overline{rs}.$$

**Example 8.3.12.** 1. For any ring $R$ subsets $\{0\}$ and $R$ are two sided ideals. An ideal $I$ of $R$ is called **proper** if $I \neq R$.

2. Subgroup $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. So, $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring of $\mathbb{Z}$. Note that since all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, we get that those are the only ideals that $\mathbb{Z}$ has. Hence $\{0\}, \mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ are the only possible quotient rings of $\mathbb{Z}$.

3. The kernel of the surjective ring homomorphism $ev_r : R[x] \to R$ is the ideal $I_r$ of all polynomials $p(x) \in R[x]$ with $p(r) = 0$. We get that $R[x]/I_r \simeq R$. The ideal $I_0$ consists of all polynomials with zero constant term.

4. We can compose ring homomorphisms. For instance, given a ring homomorphism $\phi : R \to S$, we obtain a homomorphism
$$\phi \circ ev_r : R[x] \to S.$$
Let $R = \mathbb{Z}$ and let $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the quotient map. Then
$$\mathrm{Ker}(\phi \circ \mathrm{ev}_0) = \{a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \mid a_0 \in n\mathbb{Z}\}.$$

5. Let $S$ be a ring and let
$$I = \{x^2 p(x) \mid p(x) \in S[x]\}.$$
Then $I$ is an ideal of $R = S[x]$. Let us describe the quotient ring $R/I$. Note that for any polynomial $a(x) \in S[x]$ we have
$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = (a_0 + a_1 x) + x^2(a_2 + \ldots a_n x^{n-2}).$$
So, $\overline{a(x)} = \overline{a_0 + a_1 x}$ in $R/I$. Moreover,
$$\overline{a_0 + a_1 x} = \overline{b_0 + b_1 x}$$
in $R/I$ if and only if $a_0 = b_0$ and $a_1 = b_1$. The addition and multiplication are performed on coset representatives as follows:
$$(\overline{a_0 + a_1 x}) + (\overline{b_0 + b_1 x}) = \overline{(a_0 + b_0) + (a_1 + b_1)x}, \text{ and}$$
$$(\overline{a_0 + a_1 x}) \cdot (\overline{b_0 + b_1 x}) = \overline{a_0 b_0 + (a_0 b_1 + a_1 b_0)x + a_1 b_1 x^2} = \overline{a_0 b_0 + (a_0 b_1 + a_1 b_0)x}.$$

6. Let $\phi : R \to S$ be a homomorphism of commutative rings with $I = \mathrm{Ker}\,\phi$. Then the subset $M_n(I) \subset M_n(R)$ is a two-sided ideal, moreover, it is the kernel of the induced homomorphism $\phi' : M_n(R) \to M_n(S)$. We get that
$$M_n(R)/M_n(I) \simeq M_n(R/I) \simeq M_n(\phi(R)).$$
For instance $M_n(2\mathbb{Z})$ is the set of all integral matrices with even entries. It is a two-sided ideal in $M_n(\mathbb{Z})$, and the quotient $M_n(\mathbb{Z})/M_n(2\mathbb{Z})$ is isomorphic to the ring of matrices with entries in $\mathbb{Z}/2\mathbb{Z}$.

7. Let $R$ be a commutative ring and let $G$ be a group. Define the **augmentation map**
$$\varepsilon : RG \to R$$
$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g.$$
This map is a surjective ring homomorphism. Its kernel is called the **augmentation ideal** of $RG$, it consists of all sums $\sum_{g \in G} a_g g$, for which the sum of coefficients $\sum_{g \in G} a_g$ is equal to zero. For instance, all differences $g - h$ for $g, h \in G$ lie in the augmentation ideal.

8. To obtain examples of one-sided ideals, consider the ring of matrices $M_n(R)$ for some nonzero commutative ring $R$ and $n \geq 2$. Let $L_j$ be the set of matrices with arbitrary entries in the $j$'th column and zero entries everywhere else:

$$L_j = \{a_1E_{1j} + a_2E_{2j} + \ldots + a_nE_{nj} \mid a_1, \ldots, a_n \in R\}$$

Then $L_j$ is a left ideal, but not a right ideal. For instance if $i \neq j$ then $E_{jj} \in L_j$, however $E_{jj} \cdot E_{ji} = E_{ji} \notin L_j$. Note also that $E_{ab} \cdot E_{ij} \in L_j$ for every $a, b, i \in \{1, \ldots, n\}$.

**Definition 8.3.13.** Let $I$ and $J$ be two-sided ideals of $R$.

1. Define the sum of $I$ and $J$ by

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

2. Define the product of $I$ and $J$, denoted by $IJ$, to be the set of all finite sums of the form $ab$, where $a \in I, b \in J$. That is,

$$IJ = \{a_1b_1 + \ldots + a_kb_k \mid k \in \mathbb{Z}_{\geq 0}, a_i \in I, b_i \in J, \ \forall i = 1, \ldots, k\}.$$

3. For any $n \geq 1$ define inductively the $n$'th power of $I$, denoted by $I^n$, by putting $I^1 = I$ and $I^n = I \cdot I^{n-1}$.

**Proposition 8.3.14.** *Let $R$ be a ring and let $I, J$ be two-sided ideals of $R$. Then*

1. *$I + J, IJ$ and $I \cap J$ are two sided ideals of $R$.*
2. *$I + J$ is the smallest (by inclusion) ideal containing both $I$ and $J$.*
3. *$IJ$ is contained in $I \cap J$.*

*Proof.* Exercise ■

**Example 8.3.15.**

1. Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ in $\mathbb{Z}$. Then

$$I + J = \gcd(n, m)\mathbb{Z},$$
$$IJ = nm\mathbb{Z},$$
$$I \cap J = \operatorname{lcm}(n, m)\mathbb{Z}.$$

2. Let $I$ be the kernel of the map $\phi \circ ev_0 : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ (here $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the quotient map), i.e. $I$ consists of all polynomials with even constant term. Then $x, 2 \in I$, so both $x^2$ and 4 are elements of $I^2$, as is their sum $x^2 + 4$. Note however that $x^2 + 4$ cannot be written as a single product $p(x)q(x)$ of two elements of $I$.

## 8.4 Properties of ideals

**Proposition 8.4.1.** *Let $R$ be a ring and let $\{I_\alpha, \alpha \in A\}$ be a collection of (left, right, or two-sided) ideals of $R$. Then their intersection $\bigcap_{\alpha \in A} I_\alpha$ is also a (resp. left, right, or two-sided) ideal of $R$.*

*Proof.* By Lemma 4.1.6, $\bigcap_{\alpha \in A} I_\alpha$ is an additive subgroup of $R$. Moreover, for each $x \in \bigcap_{\alpha \in A} I_\alpha$ and $r, s \in R$ we have $x \in I_\alpha$, so $rx$ (or $xs$, or $rxs$ resp.) is in $I_\alpha$ for each $\alpha \in A$, hence $rx, xs$, or $rxs$ is in $\bigcap_{\alpha \in A} I_\alpha$. ■

**Definition 8.4.2.** Let $A$ be a subset of a ring $R$.

1. Let $(A)$ denote the smallest ideal of $R$ containing $A$, called the **ideal generated by** $A$. We get that

$$(A) = \bigcap_{\substack{I \text{ an ideal,} \\ A \subset I}} I.$$

2. Let $RA$ denote the set of all finite sums of elements of the form $ra, r \in R, a \in A$, i.e.

$$RA = \{r_1a_1 + r_2a_2 + \ldots + r_ka_k \mid k \geq 0, r_i \in R, a_i \in A \text{ for } i = 1, \ldots, k\}.$$

Similarly, let

$$AR = \{a_1r_1 + a_2r_2 + \ldots + a_krk \mid k \geq 0, r_i \in R, a_i \in A \text{ for } i = 1, \ldots, k\}$$

and

$$RAR = \{r_1a_1r'_1 + r_2a_2r'_2 + \ldots + r_ka_kr'_k \mid k \geq 0, r_i, r'_i \in R, a_i \in A \text{ for } i = 1, \ldots, k\}.$$

3. An ideal $(a)$ generated by a single element $a \in R$ is called a **principal ideal**.

4. An ideal $(a_1, a_2, \ldots, a_n)$ generated by a finite set $A = \{a_1, \ldots, a_n\} \subset R$ is called a **finitely generated ideal**.

**Proposition 8.4.3.** *Let $A \subset R$. Then*

1. *$RA$ is the left ideal generated by $A$.*
2. *$AR$ is the right ideal generated by $A$.*
3. *$RAR$ is the two-sided ideal generated by $A$.*

*Proof.* Let us prove part 3 only, parts 1 and 2 being analogous.

First, it is easy to show that $RAR$ is a two-sided ideal of $R$, containing $A$, so $(A) \subset RAR$. On the other hand, any two-sided ideal containing $A$ should also contain elements of the form $rar'$ with $r, r' \in R, a \in A$, as well as their finite sums. Thus, $RAR \subset (A)$. ■

If $R$ is a commutative ring then $RA = AR = RAR = (A)$. Principal ideals in commutative rings are particularly simple:

$$(a) = \{ra \mid r \in R\},$$

so the ideal $(a)$ consists of all elements **divisible** by $a$.

**Remark 8.4.4.** This no longer works for two-sided principal ideals in non-commutative rings. The set $\{rar' \mid r, r' \in R\}$ is not equal to $(a)$ since we also need to include finite sums of elements: e.g. we cannot apply the distributive laws to the sum $ra + ar'$.

**Example 8.4.5.**

1. The trivial ideal 0 and the ideal $R$ are both principal: $0 = (0),\ R = (1)$.

2. We have $n\mathbb{Z} = \mathbb{Z}n = (n) = (-n)$ for all integers $n$. As noted before, all ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, thus all ideals of $\mathbb{Z}$ are principal.

   Moreover, we have $(n, m) = (\gcd(n, m)) \subset \mathbb{Z}$. So $n$ and $m$ are relatively prime if and only if $(n, m) = (1) = \mathbb{Z}$.

3. Let $I$ be the ideal of $\mathbb{Z}[x]$ consisting of polynomials with even constant term (recall that $I$ is the kernel of the homomorphism $\phi \circ ev_0 : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z},\ p(x) \mapsto p(0) \mod 2$, see Example 8.3.15.2). Note that $2, x \in I$, and moreover for any $p(x) = a_0 + a_1x + \ldots + a_nx^n \in I$ we have $a_0 = 2b$, and thus

$$p(x) = 2 \cdot b + x \cdot (a_1 + a_2x + \ldots + a_nx^{n-1}) \in (2, x).$$

   We get that $I = (2, x)$.

   Let us prove that $I$ is not principal, i.e. cannot be generated by a single element.

   Suppose $I = (p(x))$, then $2 = p(x)q(x)$ and $x = p(x)r(x)$. The former equation implies that $\deg\ p(x) = 0$ and that $p(x) = p_0 = \pm 1, \pm 2$. If $r_mx^m$ is the leading term of $r(x)$ then $x = p_0r_mx^m$, thus $m = 1$ and $p_0r_1 = 1$, so $p_0 \neq \pm 2$. Note also that $p_0$ cannot be equal to $\pm 1$, since $(\pm 1) = \mathbb{Z}[x] \neq I$.

4. The symbol $(A)$ is ambiguous if the ring is not specified. For example $(2)$ in $\mathbb{Q}[x]$ is the entire ring, and $(2) \neq \mathbb{Z}[x]$ as an ideal of $\mathbb{Z}[x]$ (we just showed that $x \notin (2)$).

5. We will prove later that every ideal of $F[x]$, for any field $F$, is principal.

6. Consider the set $I$ of all functions $f \in \mathrm{Fun}(\mathbb{R}, \mathbb{R})$ with the property that $f(0) = 0$. It is easy to see that this is an ideal. Moreover, let $g$ be the function whose value at 0 is 0, and $g(x) = 1$ for each $x \neq 1$. Then $g \in I$ and for any $f \in I$ we have $f = fg$, so $I = (g)$ is a principal ideal.

   Note however that if we consider such an ideal in the ring $C(\mathbb{R}, \mathbb{R})$ of all continuous functions then it no longer will be principal, nor will it be finitely generated.

7. If $G$ is a finite group then the augmentation ideal $I$ in $RG$ is generated by the set $\{1-g \mid g \in G\}$. Moreover, if $G$ is cyclic with generator $x$ then $I$ is principal with $I = (1 - x)$.

**Proposition 8.4.6.** *Suppose $R$ is commutative and let $A = (a_1, \ldots, a_k), B = (b_1, \ldots, b_l)$ be two ideals in $R$. Then*

1. *$A + B = (a_1, \ldots, a_k, b_1, \ldots, b_l)$;*
2. *$A \cdot B = (\{a_i b_j \mid i \leq k, j \leq l\})$.*

*Proof.* 1. We have

$$A = \{r_1 a_1 + \ldots + r_k a_k \mid r_i \in R\},$$
$$B = \{s_1 b_1 + \ldots + s_l b_l \mid s_j \in R\},$$

so

$$A + B = \{r_1 a_1 + \ldots + r_k a_k + s_1 b_1 + \ldots + s_l b_l \mid r_i, s_j \in R\} = (a_1, \ldots, a_k, b_1, \ldots, b_l).$$

2. A product of two elements $a = r_1 a_1 + \ldots + r_k a_k \in A$ and $b = s_1 b_1 + \ldots + s_l b_l \in B$ can be expressed in terms of products of generators:

$$ab = \sum_{i \leq k, j \leq l} (r_i s_j)(a_i b_j).$$

   Thus,

$$A \cdot B = \{ \sum_{i \leq k, j \leq l} r_{ij} \cdot a_i b_j \mid r_{ij} \in R\} = (\{a_i b_j \mid i \leq k, j \leq l\}).$$

■

**Corollary 8.4.7.** *The product of two principal ideals is principal.*

**Proposition 8.4.8.** *Let $I$ be an ideal of $R$. Then*

1. *$I = R$ if and only if $I$ contains a unit.*
2. *Assume $R$ is commutative. Then $R$ is a field if and only if the only ideals of $R$ are $0$ and $R$.*

*Proof.* 1. If $I = R$ then $1 \in I$. Conversely, if $uv = vu = 1$ and $u \in R$ then for any $r \in R$ we have $rvu = uvr = r \in I$.

2. First, suppose $R$ is a field and $I$ is a nonzero ideal of $R$, then $I$ contains some nonzero element, which must be then a unit, so $I = R$.

   Second, assume any nonzero ideal of $R$ is everything, consider some nonzero $a \in R$. Then $(a) = R$, so there exists $b \in R$ such that $ab = 1$.

■

**Corollary 8.4.9.** *Let $F$ be a field then any nonzero ring homomorphism from $F$ to another ring is injective.*

*Proof.* The kernel of this homomorphism is an ideal, so it must be zero. ■

**Definition 8.4.10.** 1. An ideal $I \subset R$ is called **proper** if $I \neq R$. In particular, only nonzero rings can have proper ideals.

2. An ideal $\mathfrak{m} \subset R$ is called **maximal** if $\mathfrak{m}$ is proper, and the proper only ideal containing $\mathfrak{m}$ is $\mathfrak{m}$.

If we order all proper ideals of $R$ by inclusion then maximal ideals are precisely the maximal elements of this partially ordered set. Not all partially ordered sets have maximal elements (take for example $\mathbb{Z}$), however the case of rings and ideals is "nice" and we can state the following

**Theorem 8.4.11.** *Let $R$ be a nonzero ring. Then any proper ideal $I \subset R$ is contained in a maximal ideal.*

To prove this theorem we need to use the theory of partially ordered sets and Zorn's lemma.

**Definition 8.4.12.** 1. A **partially ordered set** (poset) is a set $P$ equipped with a binary relation $\leq$, that is *reflexive* (i.e. $x \leq x$ for all $x \in X$), *antisymmetric* (i.e. if $x \leq y$ and $y \leq x$ then $x = y$), and *transitive* (i.e. if $x \leq y, y \leq z$ then $x \leq z$).

2. A poset $P$ is called **totally ordered** if any two elements of $P$ are *comparable*, i.e. for all $x, y \in P$ either $x \leq y$ or $y \leq x$.

3. Any subset $S$ of a poset $P$ is a poset with respect to the same binary relation $\leq$ restricted to $S$. A totally ordered subset $S \subset P$ is called a **chain**.

4. An element $m$ of a poset $P$ is called **maximal** if there is no element greater than $m$, i.e. $m \leq x$ implies $x = m$.

5. Given a subset $S$ of a poset $P$, an element $u \in P$ is called an **upper bound** of $S$ if it is greater than or equal to every element of $S$, that is $s \leq u$ for all $s \in S$.

The following is an important result of set theory, which is equivalent to the *axiom of choice*, so it can be assumed as one of the axioms of set theory, so we will not give a proof for it.

**Lemma 8.4.13** (Zorn's Lemma)**.** *Suppose $P$ is a nonempty poset with the property that every chain in $P$ has an upper bound in $P$. Then $P$ contains at least one maximal element.*

Let us apply Zorn's lemma to our situation.

*Proof of Theorem 8.4.11.* We will give a proof for left ideals. The proof for right and two-sided ideals is analogous.

Let $I$ be a proper ideal of $R$. Consider the set $\mathcal{P}$ of all proper ideals in $R$ containing $I$. Then $\mathcal{P}$ is nonempty ($I \in \mathcal{P}$) and partially ordered by inclusion. Let $\mathcal{C} \subset \mathcal{P}$ be any chain. Define

$$U = \bigcup_{J \in \mathcal{C}} J.$$

Clearly, $J \subset U$ for any $J \in \mathcal{C}$ and $I \subset U$. To prove that $U$ is an upper bound for $\mathcal{C}$ we just need to show that $U$ is an ideal. Let $r \in R$ and $u \in U$ then there exists $J \in \mathcal{C}$ such that $u \in J$, so $ru \in J$ and thus $ru \in U$. Now we need to prove that $U$ is an additive subgroup. Since $I \subset U$, it is clearly nonempty. Now let $u, v \in U$ then there exist $J, J' \in \mathcal{C}$ such that $u \in J, v \in J'$. WLOG suppose $J' \subset J$ (either this or $J \subset J'$ is true since $\mathcal{C}$ is a chain). Then $u, v \in J$, so $u - v \in J$, and therefore $u - v \in U$.

We showed that $\mathcal{P}$ satisfies the conditions of Zorn's lemma, therefore it has a maximal element $\mathfrak{m}$, which is a proper ideal containing $I$. If $\mathfrak{m} \subset J$ for some proper ideal $J$ then $I \subset J$, so $J \in \mathcal{P}$, and therefore $J = \mathfrak{m}$, hence $\mathfrak{m}$ is a maximal ideal containing $I$. □

For commutative rings the next result characterizes maximal ideals by the structure of their quotient rings.

**Proposition 8.4.14.** *Assume $R$ is commutative. An ideal $\mathfrak{m} \subset R$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

*Proof.* Suppose $\mathfrak{m}$ is maximal and let $\overline{x}$ be a nonzero element of $R/\mathfrak{m}$. Consider an element $x \in R$ for which $x + \mathfrak{m} = \overline{x}$. Since $\overline{x} \neq 0$, element $x$ is not in $\mathfrak{m}$. Thus the ideal $(x) + \mathfrak{m}$ is larger than $\mathfrak{m}$ and contains $\mathfrak{m}$. We must have $(x) + \mathfrak{m} = R$ since $\mathfrak{m}$ is maximal. Thus, $1 = rx + m$ for some $r \in R$ and $m \in \mathfrak{m}$. So, we get that $\overline{1} = \overline{r} \cdot \overline{x}$ in the quotient ring $R/\mathfrak{m}$, and thus $\overline{x}$ is invertible with inverse $\overline{r} = r + \mathfrak{m}$.

Conversely, suppose $R/\mathfrak{m}$ is a field and let $I$ be an ideal containing $\mathfrak{m}$. Suppose there exists $x \in I$ with $x \notin \mathfrak{m}$. Consider $\overline{x} = x + \mathfrak{m} \in R/\mathfrak{m}$. By assumption, $\overline{x}$ is nonzero, so it has an inverse $\overline{r} = r + \mathfrak{m}$ (for some $r \in R$). The equation $\overline{r} \cdot \overline{x} = \overline{1}$ in $R/\mathfrak{m}$ implies that in $R$ we have that $1 = rx + m$ for some $m \in \mathfrak{m}$. This means that $1 \in I$, so $I = R$. ■

**Example 8.4.15.**

1. An ideal $n\mathbb{Z}$ is maximal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field, that is $n$ is prime. Note also that we have $n\mathbb{Z} \subset m\mathbb{Z}$ if and only if $m$ divides $n$.
2. The ideal $(2, x)$ in $\mathbb{Z}[x]$ is maximal because the quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
3. The ideal $(x)$ in $\mathbb{Z}[x]$ is not maximal because the quotient is isomorphic to $\mathbb{Z}$, which is not a field. We also see that $(x) \subset (2, x)$.
4. Let $R = \mathrm{Fun}(\mathbb{R}, \mathbb{R})$, $a \in \mathbb{R}$, and let $M_a = \{f \in R \mid f(a) = 0\}$. Then $R/M_a \simeq \mathbb{R}$, so $M_a$ is a maximal ideal.
5. If $F$ is a field then the augmentation ideal $I$ in $FG$ is maximal, as $FG/I \simeq F$.

**Definition 8.4.16.** Assume $R$ is commutative. A proper ideal $\mathfrak{p}$ in $R$ is called **prime** if whenever the product $ab$ of two elements $a, b \in R$ is an element of $\mathfrak{p}$ then at least of one of $a, b$ is an element of $\mathfrak{p}$.

**Proposition 8.4.17.** *An ideal $p\mathbb{Z}$ of $\mathbb{Z}$ is prime if and only if either $p$ is a prime number or $p = 0$.*

*Proof.* This proposition is equivalent to the following statement about prime numbers:

A positive integer $p$ is prime if and only if whenever $p$ divides the product $ab$ of two numbers $a, b \in \mathbb{Z}$ then $p$ divides at least one of $a, b$.

The proof of this statement is an exercise. ■

**Proposition 8.4.18.** *Assume $R$ is commutative. An ideal $\mathfrak{p}$ of $R$ is prime if and only if the quotient ring $R/\mathfrak{p}$ is an integral domain.*

*Proof.* Suppose $\mathfrak{p}$ is prime and suppose $\overline{a} \cdot \overline{b} = 0$ for some $\overline{a} = a + \mathfrak{p}, \overline{b} = b + \mathfrak{p}$ in $R/\mathfrak{p}$ (for some $a, b \in R$). Then $ab \in \mathfrak{p}$ in $R$, so either $a$ or $b$ is in $\mathfrak{p}$. Hence either $\overline{a}$ or $\overline{b}$ is zero. Thus $R/\mathfrak{p}$ has no zero divisors.

Conversely, suppose $ab \in \mathfrak{p}$ for some $a, b \in R$ and suppose $R/\mathfrak{p}$ is an integral domain. We have $\overline{a} \cdot \overline{b} = 0$ in $R/\mathfrak{p}$, so either $\overline{a}$ or $\overline{b}$ is zero, meaning that either $a$ or $b$ is in $\mathfrak{p}$. ■

**Corollary 8.4.19.** *Assume $R$ is commutative.*

1. *The zero ideal $(0)$ in $R$ is prime if and only if $R$ is an integral domain.*
2. *Every maximal ideal in $R$ is prime.*

**Example 8.4.20.**

1. Ideals $(p) = p\mathbb{Z}$ generated by prime numbers are both maximal and prime in $\mathbb{Z}$. The zero ideal $(0) \subset \mathbb{Z}$ is prime, but not maximal.
2. The ideal $(x)$ in $\mathbb{Z}[x]$ is prime, but it is not maximal. Similarly, the zero ideal $(0)$ in $\mathbb{Z}[x]$ is prime, since $\mathbb{Z}[x]$ is an integral domain, but not maximal.

## 8.5 The Chinese Remainder Theorem

Throughout this section all rings are assumed to be nonzero and commutative.

**Definition 8.5.1.** Two ideals $A, B$ of $R$ are called **comaximal** if $A + B = R$.

**Theorem 8.5.2** (Chinese Remainder Theorem)**.** *Let $A_1, \ldots, A_k$ be ideals in $R$. The map*

$$\phi : R \to R/A_1 \times R/A_2 \times \ldots R/A_k,$$

$$r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

*is a ring homomorphism with kernel $A_1 \cap A_2 \cap \ldots \cap A_k$. If for each $i \neq j \in \{1, \ldots, k\}$ the ideals $A_i$ and $A_j$ are comaximal, then this map is surjective and $A_1 \cap \ldots \cap A_k = A_1 \cdot \ldots \cdot A_k$, so*

$$R/(A_1 \cdot \ldots \cdot A_k) = R/(A_1 \cap \ldots \cap A_k) \simeq R/A_1 \times \ldots \times R/A_k.$$

*Proof.* First note that $\phi$ is a ring homomorphism since it is just the natural projection $R \to R/A_i$ for each component. Now, $r \in \operatorname{Ker} \phi$ if and only if $r \mod A_i = 0$ for each $i \leq k$, meaning that $r \in A_i$ for each $i \leq k$. Hence $\operatorname{Ker} \phi = A_1 \cap \ldots \cap A_k$.

Let us first prove the second half of the statement for $k = 2$. Let $A = A_1, B = A_2$ be two ideals of $R$ with $A + B$. Let us prove that $A \cap B = A \cdot B$. Recall that we always have the inclusion $A \cdot B \subset A \cap B$. Now since $A + B = R$ there exist $a \in A$ and $b \in B$ such that $a + b = 1$. Consider some element $x \in A \cap B$. Since $x \in A, b \in B$, we have $xb \in A \cdot B$, and since $x \in B, a \in A$, we have $xa = ax \in A \cdot B$. Therefore, $x = x(a + b) = xa + xb \in A \cdot B$. So $A \cap B = A \cdot B$.

Now let us prove that $\phi$ is surjective. Consider any element $(x + A, y + B)$ in $R/A \times R/B$ and put $z = xb + ya$. Then

$$\phi(z) = (z + A, z + B) = (xb + A, ya + B) = (xb + xa + A, ya + yb + B) = (x + A, y + B).$$

Now let us proceed by induction on $k$. Suppose the statement is true for every collection of $k - 1$ pairwise comaximal ideals of $R$. Let $A_1, \ldots, A_k$ be ideals of $R$ with $A_i + A_j = R$ for $i \neq j$. Put $A = A_1, B = A_2 \cdot \ldots \cdot A_k$. The statement follows immediately from the case $k = 2$ and the inductive assumption once we know that $A$ and $B$ are comaximal.

By hypothesis, for each $i \in \{2, \ldots, k\}$ there exist elements $x_i \in A_1$ and $y_i \in A_i$ with $1 = x_i + y_i$. Since $x_i + y_i \equiv y_i \mod A_1$, it follows that

$$1 = (x_2 + y_2) \cdot \ldots \cdot (x_k + y_k) \equiv y_2 \cdot \ldots \cdot y_k \mod A_1$$

is an element in $A_1 + A_2 \cdot \ldots \cdot A_k = A + B$. So $A + B = R$. ∎

Note that for $R = \mathbb{Z}$ we obtain the classical Chinese Remainder Theorem. As $n\mathbb{Z} + m\mathbb{Z} = \gcd(n, m)\mathbb{Z}$, we get that two ideals $n\mathbb{Z}$ and $m\mathbb{Z}$ are comaximal if and only if $n$ and $m$ are coprime. Thus, if $\gcd(n, m) = 1$ we get an isomorphism of rings

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Note that this result is slightly stronger than the one we had before as we get an isomorphism of rings, not just additive groups. We can now deduce an important corollary:

**Corollary 8.5.3.** *Suppose* $\gcd(n, m) = 1$ *then we get an isomorphism of groups*

$$(\mathbb{Z}/nm\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

*In particular, for coprime numbers $n, m \in \mathbb{Z}_{>0}$ we have $\varphi(nm) = \varphi(n)\varphi(m)$, where $\varphi$ is the Euler $\varphi$-function.*

We have finally proved Proposition 2.5.15.

**Example 8.5.4.** In $R = \mathbb{C}[x]$ we have

$$(x-1) + (x+3) = R,$$

since $1 = \frac{1}{2}((x-1) + (x+3))$, so

$$\mathbb{C}[x]/(x^2 + 2x - 3) \simeq \mathbb{C}[x]/(x-1) \times \mathbb{C}[x]/(x+3).$$

We will prove that for an integral domain $R$ the ideal $(x-a)$ is precisely the kernel of the evaluation homomorphism $ev_a : R[x] \to R$. Thus $R[x]/(x-a) \simeq R$. We then deduce that

$$\mathbb{C}[x]/(x^2 + 2x - 3) \simeq \mathbb{C} \times \mathbb{C}.$$

## 8.6 Fields of fractions

We will now imitate the construction of rational numbers as fractions of integers to prove the following

**Proposition 8.6.1.** *Let $R$ be an integral domain. Then there exists a field $F(R)$, which admits an injective homomorphism $\iota$ from $R$ (so that $R$ can be identified with a subring of $F(R)$). Moreover, any injective homomorphism $\phi$ from $R$ to some field $F$ can be extended to a homomorphism $\phi' : F(R) \to F$ (so that $F(R)$ is in a sense the minimal field containing $R$).*

*Proof.* Define a binary relation $\sim$ on the set $R \times R_{\neq 0} = \{(a,b) \mid b \neq 0\}$ as follows:

$$(a,b) \sim (c,d) \iff ad = bc.$$

Let us prove that $\sim$ is an equivalence relation.

1. $(a,b) \sim (a,b)$;
2. $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$;
3. if $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ then $ad = bc$ and $cf = de$, so

$$adf = bcf = bde.$$

Using the cancellation property of integral domains and the fact that $d \neq 0$, we deduce that

$$af = be,$$

so $(a,b) \sim (e,f)$.

Now let us denote the equivalence class of $(a,b)$ by $\frac{a}{b}$. Define

$$F(R) = R \times R_{\neq 0}/_{\sim} \;=\; \left\{ \frac{a}{b} \mid a, b \in R,\ b \neq 0 \right\}.$$

Define addition and multiplication on $F(R)$ as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Let us check that these operations are well-defined. Suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, i.e. $ab' = a'b, cd' = c'd$. We need to check that

$$(ad + bc, bd) \sim (a'd' + b'c', b'd'), \text{ and } (ac, bd) \sim (a'c', b'd').$$

We have

$$(ad+bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')bd, \text{ and}$$

$$ac \cdot b'd' = a'c' \cdot bd.$$

It is straightforward to check that these operations make $F(R)$ into a field with

$$1 = \frac{1}{1},$$

$$0 = \frac{0}{1},$$

$$-\frac{a}{b} = \frac{-a}{b},$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Define $\iota : R \to F(R)$ via

$$\iota(r) = \frac{r}{1}.$$

Then

$$\operatorname{Ker} \iota = \{r \in R \mid (r,1) \sim (0,1)\} = \{0\}.$$

Now if $\phi : R \to F$ is an injective ring homomorphism and $F$ is a field, define

$$\phi' : F(R) \to F$$

via

$$\frac{a}{b} \mapsto \phi(a) \cdot \phi(b)^{-1}.$$

Note that this map is well-defined since $b \neq 0$, so $\phi(b)$ is invertible (as $\phi$ is injective). Moreover,

$$\phi'(\frac{a}{b} + \frac{c}{d}) = \phi'(\frac{ad+bc}{bd}) = \phi(ad+bc) \cdot \phi(bd)^{-1} =$$

$$= \phi(a)\phi(d) \cdot \phi(b)^{-1}\phi(d)^{-1} + \phi(b)\phi(c) \cdot \phi(b)^{-1}\phi(d)^{-1} = \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} = \phi'(\frac{a}{b}) + \phi'(\frac{c}{d});$$

$$\phi'(\frac{a}{b} \cdot \frac{c}{d}) = \phi(a)\phi(c)\phi(b)^{-1}\phi(d)^{-1} = \phi'(\frac{a}{b}) \cdot \phi'(\frac{c}{d}),$$

$$\phi'(1) = \phi(1) = 1.$$

■

**Definition 8.6.2.** $F(R)$ is called the **field of fractions** of $R$.

**Example 8.6.3.**

1. If $R = \mathbb{Z}$ then $F(R) = \mathbb{Q}$.
2. If $R = S[x]$, where $S$ is an integral domain, then

$$F(R) = S(x)$$

is the field of rational functions.

## 8.7 Euclidean domains and polynomial division

**Definition 8.7.1.** Any function $N : R \to \mathbb{Z}_{\geq 0}$ with $N(0) = 0$ is called a **norm** on the integral domain $R$.

This notion of a norm is fairly weak and it is possible for the same integral domain $R$ to possess several different norms.

**Definition 8.7.2.** The integral domain $R$ is said to be a **Euclidean domain** if there is a norm $N$ (called the Euclidean norm) on $R$ such that for any two elements $a$ and $b$ of $R$ with $b \neq 0$ there exist elements $q$ and $r$ in $R$ with

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b).$$

The element $q$ is called the **quotient** and the element $r$ the **remainder** of the division.

The importance of the existence of a division algorithm on an integral domain $R$ is that it allows a Euclidean algorithm for two nonzero elements $a$ and $b$ of $R$: by successive "divisions" we can write

$$\begin{aligned} a &= q_0 b + r_0, \\ b &= q_1 r_0 + r_1, \\ r_0 &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n, \end{aligned}$$

where $r_n$, is the last nonzero remainder. Such an $r_n$, exists since $N(b) > N(r_0) > N(r_1) > \ldots > N(r_n)$ is a decreasing sequence of nonnegative integers if the remainders are nonzero, and such a sequence cannot continue indefinitely. Note also that there is no guarantee that these elements are unique.

**Example 8.7.3.**

1. Fields are trivial examples of Euclidean domains where any norm will satisfy the defining condition (e.g., $N(a) = 0$ for all $a$). This is because for every $a, b$ with $b \neq 0$ we have $a = qb + 0$, where $q = ab^{-1}$.
2. The integers $\mathbb{Z}$ are a Euclidean Domain with norm given by $N(a) = |a|$, the usual absolute value. Note however, that our definition allows for several possibilities for the quotient and the remainder. For example,
$$5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$$
are the two ways of applying the division algorithm in $\mathbb{Z}$ to $a = 5$ and $b = 2$. The quotient and remainder are unique if we require the remainder to be nonnegative.
3. If $F$ is a field, then the polynomial ring $F[x]$ is a Euclidean domain with norm given by $N(p(x)) =$ the degree of $p(x)$. We will prove later that $R[x]$ is a Euclidean domain if and only if $R$ is a field.

**Proposition 8.7.4.** *Let $R$ be a Euclidean domain with Euclidean norm $N$. Then all ideals in $R$ are principal.*

*Proof.* Let $I \subset R$ be a nonzero ideal. Define

$$m = \min\{N(x) \mid x \in I, x \neq 0\},$$

and let $a \in I$ be an element with $N(a) = m$. Let us prove that $I = (a)$.

Clearly, $(a) \subset I$. Now for any $x \in I$ we can perform the division algorithm:

$$x = aq + r, \ N(r) < m \text{ or } r = 0.$$

Note that $r = x - aq \in I$, so $N(r) \geq m$ or $r = 0$. Thus, $x = aq \in (a)$. ∎

**Example 8.7.5.** Recall that $(2, x) \subset \mathbb{Z}[x]$ is not a principal ideal. We deduce that $\mathbb{Z}[x]$ is not a Euclidean domain.

**Definition 8.7.6.** Let $R$ be an integral domain and let $a, b \in R_{\neq 0}$.

1. An element $d \in R$ is called a divisor of $a$ (write $d \mid a$) if $a = dr$ for some $r \in R$, i.e. $a \in (d)$.
2. An element $d$ is called a **greatest common divisor** of $a$ and $b$ if
   (a) $d \mid a$ and $d \mid b$;
   (b) if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

   That is, $a, b \in (d)$ and if $a, b \in (d')$ then $(d') \subset (d)$. So $(d)$ is the "minimal" principal ideal containing $a, b$.

**Proposition 8.7.7.** *If the ideal $(a, b)$ in $R$ is principal with generator $d$ then $d$ is a greatest common divisor of $a$ and $b$.*

*Proof.* First, suppose $(a, b) = (d)$, Then $a, b \in (d)$. Moreover, if $a, b \in d'$ then $(d) = (a, b) \subset (d')$. ■

**Corollary 8.7.8.** *If $R$ is a Euclidean domain then $d$ is a greatest common divisor of $a$ and $b$ if and only if $(a, b) = (d)$.*

*Proof.* We proved one direction. Now suppose $d$ is a greatest common divisor of $a$ and $b$, so $(a, b) \subset (d)$. By Proposition 8.7.4, $(a, b) = (d')$ for some $d'$. Thus, $(a, b) \subset (d')$ and therefore $(d) \subset (d')$ and $(d') \subset (d)$. Hence $(a, b) = (d)$. ■

**Corollary 8.7.9.** *If $R$ is a Euclidean domain, $a, b \in R$ and $d$ is a greatest common divisor of $a$ and $b$ then there exist elements $u, v \in R$ such that*

$$d = ua + vb.$$

**Exercise 8.7.10.** Suppose $R$ is an integral domain and suppose $(d) = (d')$ for some $d, d' \in R$. Prove that there exists a unit $u \in R^\times$, such that $d = ud'$.

**Theorem 8.7.11.** *Let $R$ be a Euclidean domain and let $a, b$ be two nonzero elements of $R$. Let $r_n$ be the last nonzero remainder in the Euclidean algorithm for $a$ and $b$. Then $r_n$ is a greatest common divisor of $a$ and $b$.*

*Proof.* Note that $r_0 = a - q_0 b \in (a, b)$ and $r_{i+1} = r_{i-1} - q_{i+1} r_i \in (r_{i-1}, r_i)$. By induction, we have $r_n \in (a, b)$.

Conversely, $r_{n-1} = q_{n+1} r_n \in (r_n)$, $r_{n-2} = q_n r_{n-1} + r_n = (q_n q_{n+1} + 1) r_n \in (r_n)$ , and $r_{n-i-1} = q_{n-i+1} r_{n-i} + r_{n-i+1} \in (r_{n-i}, r_{n-i+1})$, so by induction we have $a, b \in (r_n)$, and thus $(a, b) = (r_n)$. ■

### Polynomial long division

Let $F$ be a field and let $a(x) = a_n x^n + \ldots + a_1 x + a_0$ and $b(x) = b_m x^m + \ldots + b_1 x + b_0$ be two elements of $F[x]$ with $b_m \neq 0$ and $n \geq m$. Let us define the polynomial $q(x)$ as follows:

$$q(x) = c_0 x^{n-m} + c_1 x^{n-m-1} + \ldots + c_{n-m-1} x + c_{n-m},$$

where $c_i$'s are defined recursively by solving the linear equations:

$$c_0 b_m = a_n,$$

$$c_1 b_m + c_0 b_{m-1} = a_{n-1},$$

$$c_2 b_m + c_1 b_{m-1} + c_2 b_{m-2} = a_{n-2},$$

$$\dots$$

$$c_{n-m}b_m + c_{n-m-1}b_{m-1} + \dots = a_m.$$

These equations ensure that

$$q(x)b(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_{m+1}x^{m+1} + a_m x^m + \text{ lower order terms.}$$

Therefore we can put $r(x) = a(x) - q(x)b(x)$ as degree $r(x) < m$.

**Remark 8.7.12.** The equation above can be solved, since $b_m$ is invertible in $F$.

Also note that the resulting $q(x)$ and $r(x)$ are *unique*.

**Example 8.7.13.** Let us perform long division for $a(x) = x^6 + x^5 - 3x^4 + 2, b(x) = 2x^2 + 1$:

$$q(x) = c_0x^4 + c_1x^3 + c_2x^2 + c_3x + c_4,$$

$$c_0 = \frac{1}{2};$$
$$2c_1 = 1,$$

so

$$c_1 = \frac{1}{2}.$$

Then

$$2c_2 + c_0 = -3 \Rightarrow$$

$$c_2 = \frac{-7}{4}.$$

Similarly,

$$2c_3 + c_1 = 0 \Rightarrow$$

$$c_3 = \frac{-1}{4},$$

and

$$2c_4 + c_2 = 0 \Rightarrow$$

$$c_4 = \frac{7}{8}.$$

We have

$$q(x)b(x) = (\frac{1}{2}x^4 + \frac{1}{2}x^3 - \frac{7}{4}x^2 - \frac{1}{4}x + \frac{7}{8})(2x^2 + 1) =$$
$$= x^6 + x^5 - 3x^4 - \frac{1}{4}x + \frac{7}{8} =$$
$$= a(x) - r(x) = (x^6 + x^5 - 3x^4 + 2) - (\frac{1}{4}x + \frac{9}{8}).$$

We have $q(x) = \frac{1}{2}x^4 + \frac{1}{2}x^3 - \frac{7}{4}x^2 - \frac{1}{4}x + \frac{7}{8}$, $r(x) = \frac{1}{4}x + \frac{9}{8}$.

We essentially proved the following

**Proposition 8.7.14.** *If $F$ is a field then $F[x]$ is a Euclidean domain with Euclidean norm $N(p(x)) =$ degree $p(x)$ (here we put $N(0) = 0$).*

**Corollary 8.7.15.** *If $F$ is a field, all ideals in $F[x]$ are principal.*

We can now describe all quotient rings of $F[x]$. Let $I \subset F[x]$ be an ideal, then $I = (b(x))$ since it must be principal. Similarly to the case of $\mathbb{Z}/n\mathbb{Z}$, we can now choose remainders as canonical coset representatives for elements of $R[x]/I$. Namely, if $a(x) = b(x)q(x) + r(x)$, then $\overline{a(x)} = \overline{r(x)}$ in $R/I$. Moreover, $\overline{a_1(x)} = \overline{a_2(x)}$ in $R/I$ if and only if $a_1(x)$ and $a_2(x)$ have the same remainder when divided by $b(x)$. Thus

$$R/I = \{\overline{r(x)} \mid r(x) \in F[x], \deg\ r(x) < \deg\ b(x)\}$$

with multiplication given by

$$\overline{p(x)} \cdot \overline{q(x)} = \overline{r(x)},$$

where $r(x)$ is the remainder of $p(x)q(x)$ modulo $b(x)$.

**Example 8.7.16.** Let $I = (x^2 + 2) \subset \mathbb{R}[x]$. Then

$$\mathbb{R}[x]/I = \{\overline{ax + b} \mid a, b \in \mathbb{R}\},$$

and

$$\overline{(ax + b)} \cdot \overline{(cx + d)} = \overline{(ad + bc)x + (bd - 2ac)},$$

because

$$\overline{x} \cdot \overline{x} = \overline{-2}.$$

**Theorem 8.7.17.** *Let $F$ be a field and let $a \in F$ then*

$$\operatorname{Ker} ev_a = (x - a),$$

*where $ev_a : F[x] \to F$ is the evaluation map at $a$ :*

$$ev_a(p(x)) = p(a).$$

*Proof.* Note that if $p(x) = (x - a)q(x)$ then $p(x) \in \operatorname{Ker} ev_a$.

Now suppose $p(x) \in \operatorname{Ker} ev_a$. Let us perform long division for $p(x)$ and $(x - a)$. We have

$$p(x) = (x - a)q(x) + r,$$

where degree $r = 0$, so $r \in F$. Now

$$0 = p(a) = (a - a)q(a) + r = r,$$

so $p(x) = (x - a)q(x)$. ■

**Corollary 8.7.18.** *Let $R$ be an integral domain and let $a \in R$. Then $\operatorname{Ker} ev_a = (x - a)$, where $ev_a : R[x] \to R$ is the evaluation homomorphism at $a$.*

*Proof.* Let $F = F(R)$. For any $p(x) \in \operatorname{Ker} ev_a$, consider $p(x)$ as an element of $F[x]$. Then we know that $p(x) = (x - a)q(x)$ for some $q(x) \in F[x]$.

Let us prove that $q(x) \in R[x]$. Suppose $q(x) = c_n x^n + \ldots + c_1 x + c_0$, where $c_i \in F$. Then

$$(x-a)q(x) = c_n x^{n+1} + (c_{n-1} - ac_n)x^n + (c_{n-2} - ac_{n-1})x^{n-1} + \ldots + (c_0 - ac_1)x - ac_0 = p(x) \in R[x]$$

Thus $c_n \in R$, and we proceed by induction: if $c_{n-k} \in R$ and $c_{n-k-1} - ac_{n-k} \in R$ then $c_{n-k-1} \in R$. ■

**Corollary 8.7.19.** *Suppose $R$ is an integral domain then any polynomial $p(x) \in R[x]$ of degree $n$ has at most $n$ roots in $R$.*

*Proof.* Suppose $a_1, \ldots, a_k \in R$ are distinct roots of $p(x)$, i.e. $ev_{a_i}(p(x)) = 0$ for $i = 1, \ldots, k$. By Corollary 8.7.18 we get that $p(x) = (x - a_1)p_1(x)$, and $p(a_2) = (a_2 - a_1)p_1(a_2) = 0$. Thus, $p_1(x) = (x - a_2)p_2(x)$. We deduce by induction that $p(x) = (x - a_1)(x - a_2)\ldots(x - a_k)p_k(x)$. Hence, $n = k+$ deg $p_k(x)$, so $k \leq n$.

■

**Remark 8.7.20.** Note that we used the fact that $R$ is an integral domain when we assume that $(a_2 - a_1)$ is not a zero divisor. Note that when $R$ has zero divisors, the statement no longer holds: for example the degree one polynomial $\overline{6}x$ in $\mathbb{Z}/12\mathbb{Z}[x]$ has six roots.

The following theorem is a very important property of complex number, which however can only be proved using analytic methods. So we will state it without a proof.

**Theorem 8.7.21** (The Fundamental Theorem of Algebra)**.** *Any nonconstant polynomial in* $\mathbb{C}[x]$ *has a root. That is, if* $\deg\ p(x) > 0$ *then there exists* $a \in \mathbb{C}$ *such that* $ev_a(p(x)) = p(a) = 0$.

**Corollary 8.7.22.** *Any nonconstant polynomial in* $\mathbb{C}[x]$ *is a product of linear terms: for any* $p(x) \in \mathbb{C}[x]$ *with* $\deg\ p(x) = n > 0$ *there exist constants* $a_1, \ldots, a_n \in \mathbb{C}$*, such that*

$$p(x) = (x - a_1)(x - a_2)\ldots(x - a_n).$$

*Proof.* By the Fundamental Theorem of Algebra and Corollary 8.7.18, there exists $a_1 \in \mathbb{C}$ and a polynomial $p_1(x) \in \mathbb{C}[x]$ of degree $n-1$, such that $p(x) = (x - a_1)p_1(x)$. By induction, $p_1(x) = (x - a_2)\ldots(x - a_n)$ for some $a_2, \ldots, a_n \in \mathbb{C}$. ■

**Example 8.7.23.** Suppose a polynomial $p(x) \in \mathbb{C}[x]$ of degree $n$ has $n$ distinct roots $a_1, \ldots, a_n \in \mathbb{C}$ then

$$\mathbb{C}[x]/(p(x)) \simeq \mathbb{C}^n.$$

*Proof:* Note that if $a_i \neq a_j$ then the ideals $(x - a_i)$ and $(x - a_j)$ are comaximal in $\mathbb{C}[x]$. So, by the Chinese Remainder Theorem,

$$\mathbb{C}[x]/p(x) \simeq \mathbb{C}[x]/(x - a_1) \times \ldots \times \mathbb{C}[x]/(x - a_n).$$

On the other hand $\mathbb{C}[x]/(x - a_i) = \mathbb{C}[x]/\operatorname{Ker} ev_{a_i} \simeq \mathbb{C}$.

## 8.8 Principal ideal domains and unique factorization domains

**Definition 8.8.1.** A **Principal Ideal Domain** (P.I.D.) is an integral domain in which every ideal is principal.

We proved in Proposition 8.7.4 that every Euclidean domain is a principal ideal domain.

**Remark 8.8.2.** The converse is not true: not every PID is a Euclidean domain. It can be shown that the ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}] = \mathbb{Z}[x]/(x^2 - x + 5)$ is not a Euclidean domain, however it is a PID. There are some techniques to prove statements like these, but they are out of scope of this class. You can look up the proof in the textbook.

**Proposition 8.8.3.** *Every nonzero prime ideal in a PID* $R$ *is maximal.*

*Proof.* Suppose $(p) \subset R$ is a prime ideal and suppose $(p) \subset (m)$. Then $p = mx$ for some $x \in R$, so $mx \in (p)$. Since $(p)$ is prime, either $x \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(p) = (m)$.

Suppose $x \in (p)$. Then $x = py$ for some $y \in R$. So $mpy = p$, and thus $my = 1$, so $1 \in (m)$ and $(m) = R$. ■

**Proposition 8.8.4.** *The ring* $R[x]$ *is a PID if and only if* $R$ *is a field.*

*Proof.* We proved that $R[x]$ is an integral domain if and only if $R$ is an integral domain. Now if $R$ is an integral domain, then the ideal $(x) = \operatorname{Ker} ev_0$ is prime (because $R[x]/(x) \simeq R$). So if $R[x]$ is a PID, by the previous proposition, $(x)$ is a maximal ideal. Therefore, $R \simeq R[x]/(x)$ is a field.

Conversely, if $R$ is a field, then $R[x]$ is a Euclidean domain, and hence a PID. ■

**Definition 8.8.5.** Let $R$ be an integral domain.

1. An element $r$ of $R$ is called **irreducible** if whenever $r = ab$ then either $a$ or $b$ is a unit in $R$. Otherwise it is said to be **reducible.**

2. A nonzero element $p \in R$ is called **prime** if the ideal $(p)$ is prime.

**Proposition 8.8.6.** *In an integral domain $R$ a prime element $p$ is always irreducible.*

*Proof.* Suppose $p = ab$ then either $a \in (p)$ or $b \in (p)$. WLOG suppose $a = px$ for some $x \in R$. Then $p = pxb$, so $1 = xb$, and therefore $b$ is a unit. ■

**Remark 8.8.7.** The converse is not necessarily true. Consider the ring $R = \mathbb{Z}[x]/(x^2 + 5)$. Then $\overline{3} \in R$ is not prime, since

$$\overline{3}^2 = \overline{(2 + x)} \cdot \overline{(2 - x)},$$

however it can be shown that neither $\overline{2 + x}$ nor $\overline{2 - x}$ are divisible by $\overline{3}$. Moreover, one can show that $\overline{3}$ is irreducible in $R$.

If $R$ is a Principal Ideal Domain however, the notions of prime and irreducible elements are the same. In particular these notions coincide in $\mathbb{Z}$ and in $F[x]$ (where $F$ is a field).

**Proposition 8.8.8.** *In a PID an element is prime if and only if it is irreducible.*

*Proof.* Suppose $R$ is a PID and $p \in R$ is irreducible. We want to show that $(p)$ is a maximal ideal (and hence it is prime).

Suppose $(p)$ is contained in some other ideal (which must be principal since $R$ is a PID). Then $(p) \subset (m)$ implies that $p = mr$ for some $r \in R$. Since $p$ is irreducible, either $m \in R^\times$, which implies $(m) = R$, or $r \in R^\times$, which implies $(p) = (m)$. ■

**Definition 8.8.9.** A ring $R$ is called a **Unique Factorization Domain** (UFD) if every nonzero element $r \in R$, which is not a unit, can be written as a finite product of irreducibles:

$$r = p_1 \cdot \ldots \cdot p_k,$$

where $p_1, \ldots, p_k$ are non-necessarily distinct irreducible elements. Moreover, such decomposition is unique up to multiplication by units and permutations of factors, i.e. if

$$r = q_1 \cdot \ldots \cdot q_l$$

for some irreducibles $q_1, \ldots, q_l$ then $k = l$ and there exists a permutation $\sigma \in S_k$, so that

$$(p_i) = (q_{\sigma(i)}).$$

**Remark 8.8.10.** Recall that the condition $(p) = (q)$ essentially means that $p$ and $q$ differ by multiplication by a unit, i.e. there exists $u \in R^\times$, such that $p = uq$.

**Proposition 8.8.11.** *In a Unique Factorization domain $R$ a nonzero element is prime if and only if it is irreducible.*

*Proof.* Note that because of Proposition 8.8.6 we just need to show the "if direction".

Suppose $p \in R$ is irreducible and suppose $ab \in (p)$, so that $ab = pr$ for some $x \in R$. Consider the decomposition of $a$, $b$, and $x$ into the product of irreducibles:

$$a = q_1 \cdot \ldots \cdot q_m,$$

$$b = r_1 \cdot \ldots \cdot r_l,$$

$$x = y_1 \cdot \ldots \cdot y_k.$$

Then

$$q_1 \cdot \ldots \cdot q_m \cdot r_1 \cdot \ldots \cdot r_l = p \cdot y_1 \cdot \ldots \cdot y_k.$$

Since $p$ is irreducible, the uniqueness of factorization implies that either $(p) = (q_i)$ for some $i = 1, \ldots, m$, or $(p) = (r_j)$ for some $j = 1, \ldots, l$.

WLOG suppose $(p) = (q_i)$. Then $q_i \in (p)$ and, consequently, $a \in (p)$. Thus, $(p)$ is a prime ideal. ■

We will leave the following statement without a proof:

**Proposition 8.8.12.** *Every Principal Ideal Domain is a Unique Factorization Domain.*

Consider instead an exercise:

**Exercise 8.8.13.** Prove that the polynomial ring $F[x]$, where $F$ is a field, is a UFD.

1. Prove first the existence of factorization into irreducibles for a polynomial $f(x) \in F[x]$ using induction on degree $f(x)$.
2. Then to show uniqueness, suppose
$$p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l.$$
Use induction on $k$.
   (a) (Base case). Suppose $p_1 = q_1 \cdot \ldots \cdot q_l$. Use the fact that $p_1$ is irreducible.
   (b) (Step). Assume that we know that if $p_1 \cdot \ldots \cdot p_{k-1} = q_1 \cdot \ldots \cdot q_l$ then $l = k-1$ and there exists a permutation $\sigma$ in $S_{k-1}$, such that $(p_i) = (q_{\sigma(i)})$.
   Now suppose $p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$. Deduce that $q_1 \cdot \ldots \cdot q_l \in (p_k)$. Use the fact that the ideal $(p_k)$ is prime to show that there exists $i$ with $q_i \in (p_k)$.
   (c) Use irreducibility of $q_i$ to show that $q_i = u \cdot p_k$ with $u \in F^\times$. Note that $u \cdot q_{i+1}$ is also irreducible to reduce to the case for $k-1$:
$$p_1 \cdot \ldots \cdot p_{k-1} = q_1 \cdot \ldots \cdot q_{i-1} \cdot (u \cdot q_{i+1}) \cdot \ldots \cdot q_l.$$

So, we have the following examples of UFDs:

**Example 8.8.14.** 1. $\mathbb{Z}$ is a UFD, with factorization in question being the prime factorization. This is known as the Fundamental Theorem of Arithmetic.

2. $F[x]$ is a UFD when $F$ is a field.

It turns out, however, that the list of examples of UFDs is much larger. For instance, it can be proved that

**Proposition 8.8.15.** *$R$ is a UFD if and only if $R[x]$ is a UFD.*

As a corollary we get that

**Example 8.8.16.** 1. The ring $F[x_1, \ldots, x_k]$ is a UFD for any $k \geq 1$.

2. The ring $\mathbb{Z}[x_1, \ldots, x_k]$ is a UFD for any $k \geq 1$.

**Proposition 8.8.17.** *Let $s$ and $t$ be two nonzero elements in a UFD $R$ and suppose*
$$s = u \cdot p_1^{a_1} \cdot \ldots \cdot p_k^{a_k},$$
$$t = v \cdot p_1^{b_1} \cdot \ldots \cdot p_k^{b_k},$$
*where $u, v \in R^\times$, $p_1, \ldots, p_k$ are distinct irreducibles (that is $(p_i) \neq (p_j)$ when $i \neq j$), and $a_1, \ldots, a_k, b_1, \ldots, b_k$ are nonnegative integers (possibly zero). Then the element*
$$d = p_1^{\min(a_1, b_1)} \cdot \ldots \cdot p_k^{\min(a_k, b_k)}$$
*is a greatest common divisor of $s$ and $t$.*

*Proof.* Clearly, $d$ is a divisor of both $s$ and $t$. Now suppose $c$ is some other common divisor of $s$ and $t$ with $s = c \cdot x$ and $t = c \cdot y$.

Since the decomposition into the product of irreducibles is unique, it follows that the irreducible factors of $c$ must form a subset of irreducible factors of $s$ and of $t$, that is
$$c = w \cdot p_1^{m_1} \cdot \ldots \cdot p_k^{m_k},$$
where $w \in R^\times$ and $m_i \leq a_i, b_i$. This implies that $m_i \leq \min(a_i, b_i)$, and therefore $d$ is a divisor of $c$. ■

**Corollary 8.8.18.** *Let $F$ be a field. Two ideals $(f(x))$ and $(g(x))$ in $F[x]$ are comaximal if and only if $f(x)$ and $g(x)$ have no irreducible factors in common.*

**Example 8.8.19.** Suppose $f(x) = p_1(x)^{a_1} \cdot \ldots \cdot p_k(x)^{a_k}$, where $p_1(x), \ldots, p_k(x)$ are distinct irreducible polynomials in $F[x]$ (where $F$ is a field). Then

$$F[x]/(f(x)) \simeq F[x]/(p_1(x)^{a_1}) \times \ldots \times F[x]/(p_k(x)^{a_k}).$$

### Summary:

$$\{\text{Euclidean domains}\} \subset \{\text{PIDs}\} \subset \{\text{UFDs}\}.$$

# 9 Field extensions

## 9.1 Basic definitions

**Definition 9.1.1.** The **characteristic** of a field $F$ is the smallest positive integer $p$ such that

$$\underbrace{1 + 1 + \ldots + 1}_{p \text{ times}} = 0 \text{ in } F.$$

If no such integer exists, the characteristic is defined to be zero.

**Proposition 9.1.2.** *The characteristic of a field is either zero or prime.*

**Example 9.1.3.**
1. Fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero.
2. The field $\mathbb{Z}/p\mathbb{Z}$, usually denoted $\mathbb{F}_p$ in this context, has characteristic $p$.
3. Every field of characteristic zero is infinite, and every finite field has positive characteristic.
4. Some infinite fields have positive characteristic. For example, the field $\mathbb{F}_p(x)$ of rational functions in one variable over $\mathbb{F}_p$ has characteristic $p$.

**Definition 9.1.4.** The **prime subfield** of a field $F$ is the subfield of $F$ generated by 1 (i.e. the minimal subfield containing 1). When $F$ has characteristic zero, the prime subfield of $F$ is isomorphic to $\mathbb{Q}$, and if $F$ has characteristic $p$, this subfield is isomorphic to $\mathbb{F}_p$.

**Example 9.1.5.**
1. The prime subfield of $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ is $\mathbb{Q}$.
2. The prime subfield of $\mathbb{F}_p(x)$ is $\mathbb{F}_p$.

**Definition 9.1.6.** If $K$ is a field containing the subfield $F$, then $K$ is said to be an **extension** of $F$, denoted $K/F$ (reads "$K$ over $F$", not to be confused with quotients).

$F$ is called the **base field** of the extension.

In particular, every field is the extension over its prime subfield.

If $K/F$ is a field extension, then multiplication and addition in $K$ (specifically, multiplication by elements of $F$) makes $K$ into a vector space over $F$.

**Definition 9.1.7.** The **degree** of a field extension $K/F$, denoted $[K : F]$ (not to be confused with the index of a subgroup) is the dimension $\dim_F K$ of $K$ as a vector space over $F$.

The extension $K/F$ is said to be **finite** if $[K : F] < \infty$, and is said to be **infinite** otherwise.

**Example 9.1.8.**
1. The extensions $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, and $\mathbb{F}_p(x)/\mathbb{F}_p$ are infinite.
2. The extension $\mathbb{C}/\mathbb{R}$ is finite, and $[\mathbb{C} : \mathbb{R}] = 2$.

**Remark 9.1.9.** One can think of field extensions (up to isomorphisms) as nonzero homomorphisms of fields. That is, if $K/F$ is a field extension then the embedding $F \to K$ is a nonzero homomorphism of fields. Moreover, if $F \to K$ is a nonzero field homomorphism, then it is injective (because its kernel is a proper ideal of $F$, so it must be zero, since $F$ is a field) then $F$ is isomorphic to a subfield of $K$.

An important class of field extensions are those obtained by trying to solve equations over a given field $F$. For example, if $F = \mathbb{R}$, then the simple equation $x^2 + 1 = 0$ does not have a solution in $F$. The question arises whether there is some larger field containing $\mathbb{R}$ in which this equation does have a solution, and it was this question that led to the introduction of the complex numbers $\mathbb{C}$.

Given any field $F$ and any polynomial $p(x) \in F[x]$ one can ask a similar question: does there exist an extension $K$ of $F$ containing a solution of the equation $p(x) = 0$ (i.e., containing a root of $p(x)$)? Note that we may assume here that the polynomial $p(x)$ is irreducible in $F[x]$ since a root of any factor of $p(x)$ is certainly a root of $p(x)$ itself. The answer to this is yes:

**Proposition 9.1.10.** *Let $F$ be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field $K$ containing an isomorphic copy of $F$ in which $p(x)$ has a root.*

*Identifying $F$ with this isomorphic copy shows that there exists an extension of $F$ in which $p(x)$ has a root.*

*Proof.* Consider the ring $K = F[x]/(p(x))$. Note that $K$ is a field, since $p(x)$ is irreducible, and hence it is a prime element, moreover $F[x]$ is a PID, so the prime ideal $(p(x))$ is maximal.

The composition $F \to F[x] \to K$ of the embedding of $F$ into $F[x]$ with the quotient map to $K$ is a nonzero map of fields, so $K$ is an extension of $F$, making $F[x]$ a subring in $K[x]$. Thus, one can think about $p(x)$ as an element in $K[x]$.

Moreover let $\alpha = \overline{x} \in K$ be the image of $x$ in $K$ under the quotient map. Then $p(\alpha) = 0$ in $K$, so $\alpha$ is a root of $p(x) \in K[x]$. ∎

**Proposition 9.1.11.** *Let $p(x) \in F[x]$ be an irreducible polynomial of degree $n$ and let $K = F[x]/(p(x))$. Then $K/F$ is a field extension of degree $n$. Moreover, if $\alpha = \overline{x} \in K$ then elements*

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

*form a basis of $K$ over $F$. Thus,*

$$K = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in F\},$$

*so elements of $K$ are polynomials in $\alpha$ of degree at most $n - 1$.*

*Proof.* This is a restatement of our description of $F[x]/(p(x))$ in terms of remainders modulo $p(x)$. ∎

**Definition 9.1.12.** Let $K$ be an extension of the field $F$ and let $\alpha, \beta, \ldots$ be a collection of elements of $K$. Then the smallest subfield of $K$ containing both $F$ and the elements $\alpha, \beta, \ldots$ denoted $F(\alpha, \beta, \ldots)$ is called the field generated by $\alpha, \beta, \ldots$ over $F$.

**Example 9.1.13.**

1. $\mathbb{C} = \mathbb{R}(i) \simeq \mathbb{R}[x]/(x^2 + 1)$.
2. Let $\mathbb{Q}(\sqrt{2})$ be the smallest subfield in $\mathbb{R}$ containing $\sqrt{2}$. Then $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$.

**Proposition 9.1.14.** *Let $p(x) \in F[x]$ be an irreducible polynomial and suppose $K$ is an extension of $F$ containing a root $\alpha$ of $p(x)$ (i.e. $p(x) \in \operatorname{Ker} ev_\alpha$, where $ev_\alpha : K[x] \to K$). Then the subfield $F(\alpha) \subset K$ is isomorphic to the quotient*

$$F[x]/(p(x)).$$

*Proof.* Consider the ring homomorphism

$$\phi : F[x] \to F(\alpha),$$

$$f(x) \mapsto f(\alpha).$$

By assumption, $p(x) \in \operatorname{Ker}\phi$, so $(p(x)) \subset \operatorname{Ker}\phi$. Since $p(x)$ is irreducible, the ideal $(p(x))$ is maximal, and since $\phi$ is nonzero, we get that $(p(x)) = \operatorname{Ker}\phi$. We get an injective map of fields

$$F[x]/(p(x)) \to F(\alpha),$$

which must be surjective, since the image of the field $F[x]/(p(x))$ is a subfield, and it contains both $F$ and $\alpha$. ■

## 9.2 Classical straightedge and compass constructions

**Proposition 9.2.1.** *Let $K$ be a finite extension of $F$, and let $L$ be a finite extension of $K$. Then $L$ is a finite extension of $F$ and*

$$[L : F] = [L : K] \cdot [K : F].$$

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be a basis of $K$ over $F$, and let $\beta_1, \ldots, \beta_m$ be a basis of $L$ over $K$.

We know that any $\theta \in L$ can be expressed as

$$\theta = b_1 \cdot \beta_1 + \ldots + b_m \cdot \beta_m,$$

for some uniquely determined $b_1, \ldots, b_m \in K$. Then we have

$$b_i = a_{i1} \cdot \alpha_1 + \ldots + a_{in} \cdot \alpha_n$$

for some unique constants $a_{ij} \in F$. Thus,

$$\theta = \sum_{i \leq m, j \leq n} a_{ij} \cdot \alpha_j \cdot \beta_i,$$

which means that elements $\alpha_j \cdot \beta_i$ form a basis of $L$ over $F$. ■

As a simple application of the results we have obtained on algebraic extensions, and in particular on the multiplicativity of extension degrees, we can answer (in the negative) the following geometric problems posed by the Greeks:

**I.** (Doubling the Cube) Is it possible using only straightedge and compass to construct a cube with precisely twice the volume of a given cube?

**II.** (Trisecting an Angle) Is it possible using only straightedge and compass to trisect any given angle $\theta$?

**III.** (Squaring the Circle) Is it possible using only straightedge and compass to construct a square whose area is precisely the area of a given circle?

To answer these questions we must translate the construction of lengths by compass and straightedge into algebraic terms. Let 1 denote a fixed given unit distance. Then any distance is determined by its length $a \in \mathbb{R}$, which allows us to view geometric distances as elements of the real numbers $\mathbb{R}$. Using the given unit distance 1 to define the scale on the axes, we can then construct the usual Cartesian plane $\mathbb{R}^2$ and view all of our constructions as occurring in $\mathbb{R}^2$. A point $(x, y) \in \mathbb{R}^2$ is then constructible starting with the given distance 1 if and only if its coordinates $x$ and $y$ are constructible elements of $\mathbb{R}$.

The problems above then amount to determining whether particular lengths in $\mathbb{R}$ can be obtained by compass and straightedge constructions from a fixed unit distance. The collection of such real numbers together with their negatives will be called the **constructible elements** of $\mathbb{R}$, and we shall not distinguish between the lengths that are constructible and the real numbers that are constructible.

Each straightedge and compass construction consists of a series of operations of the following four types:

(1) connecting two given points by a straight line,

(2) finding a point of intersection of two straight lines,

(3) drawing a circle with given radius and center,

(4) finding the point(s) of intersection of a straight line and a circle or the intersection of two circles.

**Exercise 9.2.2.** Given two lengths $a$ and $b$ in $\mathbb{R}_{>0}$, one may construct using straightedge and compass the lengths $a \pm b, ab, \frac{a}{b}, \sqrt{a}$.

**Corollary 9.2.3.** *The set of constructible real numbers is a subfield of $\mathbb{R}$ (we allow negative coordinates).*

Since the equation of a circle on a plane is quadratic, whereas the equation of a line is linear, the process of finding intersection points boils down to solving linear and quadratic equations.

**Definition 9.2.4.** An extension $K/F$ is called **quadratic** if $[K : F] = 2$, i.e. if $K$ is obtained from $F$ by adjoining a root of a quadratic equation.

It follows that if a collection of constructible elements is given, then one can construct all the elements in the subfield $F$ of $\mathbb{R}$ generated by these elements and that any straightedge and compass operation on elements of $F$ produces elements in at worst a quadratic extension of $F$. Since quadratic extensions have degree 2 and extension degrees are multiplicative, it follows that if $a \in \mathbb{R}$ is obtained from elements in a field $F$ by a (finite) series of straightedge and compass operations then $a$ is an element of an extension $K$ of $F$ of degree a power of 2: $[K : F] = 2^m$ for some $m$. Since $[F(a) : F]$ divides this extension degree, it must also be a power of 2.

**Proposition 9.2.5.** *If the element $a \in \mathbb{R}$ is obtained from a field $F \subset \mathbb{R}$ by a series of compass and straightedge constructions then $[F(a) : F] = 2^k$ for some integer $k \geq 0$.*

**Theorem 9.2.6.** *None of the classical Greek problems: **(I)** Doubling the Cube, **(II)** Trisecting an Angle, and **(III)** Squaring the Circle, is possible.*

*Proof.* **(I)** Doubling the cube amounts to constructing $\sqrt[3]{2}$ in the reals starting with the unit 1. Since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of 2, this is impossible.

**(II)** An angle $\theta$ can be constructed if and only if $\cos(\theta)$ can be constructed. So the problem is, given $\cos(\theta)$ to construct $\cos(\theta/3)$.

To see that this is not always possible (it is certainly occasionally possible, for example for $\theta = 180°$), consider $\theta = 60°$. Then $\cos(\theta) = \frac{1}{2}$. By the triple angle formula for cosines:

$$\cos(\theta) = 4\cos^3(\theta/3) - 3\cos(\theta/3),$$

substituting $\theta = 60°$, we see that $\beta = \cos 20°$ satisfies the equation

$$4\beta^3 - 3\beta - \frac{1}{2} = 0.$$

It can be shown that this polynomial is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, and as before we see that $\beta$ is not constructible.

**(III)** Squaring the circle is equivalent to determining whether the real number $\pi$ is constructible. It is a difficult problem even to prove that this number is not rational. It is in fact transcendental (which we shall assume without proof), which means that $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is not even finite, showing the impossibility of squaring the circle by straightedge and compass. ■