



# algebra note

**Author:** isomo

**Date:** January 4, 2025

## Preface

These abstract algebra notes primarily focus on self-study, with a writing style that deliberately maintains low information density and includes some redundancy for clarity.

My first encounter with abstract algebra was through an English textbook, which was heavily focused on theorem proofs. Progress was slow, and I struggled to see practical applications. After spending considerable time with this approach, I sought Chinese resources for potentially better learning methods. On Bilibili, I discovered Maki's abstract algebra lectures and accompanying notes, which provided an excellent introduction to the subject. However, the content still had some gaps. Later, after finding a recommended algebra book, "Methods of Algebra" by Professor Li Wenwei, I began compiling these notes based on that foundation to aid my future studies. The "Methods of Algebra" book is difficult, we math level maybe on the freshman level, so we find the "Algebra Note" by the Professor Li Wenwei, which is more suitable for us.

# Contents

<b>Chapter 1</b>	<b>Introduction</b>	<b>1</b>
1.1	What is Algebra? . . . . .	1
<b>Chapter 2</b>	<b>Sets mappings and relationships</b>	<b>2</b>
2.1	Set Theory . . . . .	2
2.2	Mappings . . . . .	3
2.3	Product of Sets & Disjoint Union . . . . .	5
2.4	Structure of Order . . . . .	5
2.5	Equivalence Relations and Quotient Sets . . . . .	6
2.6	positive integer to rational number . . . . .	8
2.7	arithmetical . . . . .	9
2.8	Congruence Relation . . . . .	11
2.9	radix . . . . .	12
<b>Chapter 3</b>	<b>Ring, Field and Polynomial</b>	<b>14</b>
3.1	Ring & Field . . . . .	14
3.2	homomorphism & isomorphism . . . . .	15
3.3	Polynomial Ring . . . . .	16
3.4	Monoid Group . . . . .	18
3.5	Group . . . . .	21

# Chapter 1 Introduction

## 1.1 What is Algebra?

In light of this, classical algebra can be understood as the art of solving equations by:

- Replacing specific numbers with variables
- Using operations such as transposition of terms

This traditional approach forms the foundation of algebraic manipulation and equation solving.

### Theorem 1.1 (Fundamental Theorem of Algebra)

Let  $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$  be a polynomial in  $X$  with complex coefficients, where  $n \in \mathbb{Z}_{\geq 1}$ . Then there exist  $x_1, \dots, x_n \in \mathbb{C}$  such that:

$$f = \prod_{k=1}^n (X - x_k)$$

These  $x_1, \dots, x_n$  are precisely the complex roots of  $f$  (counting multiplicity); they are unique up to reordering.



Now let us further explain the previously raised question: What is algebra?

#### • What is an equation?

An expression obtained through a finite number of basic operations: addition, subtraction, multiplication, and division (with non-zero denominators).

#### • What are numbers?

At minimum, this includes common number systems like  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$ . All these systems support four basic operations, though division requires non-zero denominators. Note that  $\mathbb{Z}$  is not included in this list, as division is not freely applicable in  $\mathbb{Z}$ .

#### • What is the art of solving?

This involves:

- Determining whether equations have solutions
- Finding exact solutions when possible
- Developing efficient algorithms, Providing methods for approximating solutions

# Chapter 2 Sets mappings and relationships

## 2.1 Set Theory

**Remark** Element of Set also one of Set.

### Axiom 2.1 (Axiom of Extensionality)

If two sets have the same elements, then they are equal.

$$A = B \iff (A \subset B) \wedge (B \subset A)$$



### Axiom 2.2 (Axiom of Pairing)

For any elements  $x$  and  $y$ , there exists a set  $\{x, y\}$  whose elements are exactly  $x$  and  $y$ .



### Axiom 2.3 (Axiom Schema of Separation)

Let  $\mathcal{P}$  be a property of sets, and let  $\mathcal{P}(u)$  denote that set  $u$  satisfies property  $\mathcal{P}$ . Then for any set  $X$ , there exists a set  $Y$  such that:

$$Y = \{u \in X : \mathcal{P}(u)\}$$



### Axiom 2.4 (Axiom of Union)

For any set  $X$ , there exists its union set  $\bigcup X$  defined as:

$$\bigcup X := \{u : \exists v \in X, u \in v\}$$



### Axiom 2.5 (Axiom of Power Set)

For any set  $X$ , there exists its power set  $P(X)$  defined as:

$$P(X) := \{u : u \subset X\}$$



### Axiom 2.6 (Axiom of Infinity)

There exists an infinite set. More precisely, there exists a set  $X$  such that:

1.  $\emptyset \in X$
2. If  $y \in X$ , then  $y \cup \{y\} \in X$



### Axiom 2.7 (Axiom Schema of Replacement)

Let  $\mathcal{F}$  be a function with domain set  $X$ . Then there exists a set  $\mathcal{F}(X)$  defined as:

$$\mathcal{F}(X) = \{\mathcal{F}(x) : x \in X\}$$



**Remark** The Replacement Axiom and the Separation Axiom Schema are to construct new sets from existing sets. Different is the Replacement can equal size of the set, but the Separation is a subset numbers of the set.

### Definition 2.1 (Cartesian Product)

For any two sets  $A$  and  $B$ , their Cartesian product  $A \times B$  (also called simply the product) consists of all ordered pairs  $(a, b)$  where  $a \in A$  and  $b \in B$ . In other words:

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



**Axiom 2.8 (Axiom of Regularity)**

Every non-empty set contains an element which is minimal with respect to the membership relation  $\in$ . 

**Axiom 2.9 (Axiom of Choice)**

Let  $X$  be a set of non-empty sets. Then there exists a function  $g : X \rightarrow \bigcup X$  (called a choice function) such that:

$$\forall x \in X, g(x) \in x$$


**Example 2.1 Symmetric Difference** The symmetric difference of sets  $X$  and  $Y$  is defined as  $X \triangle Y := (X \setminus Y) \cup (Y \setminus X)$ . Let's verify that  $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$ .

**Proof** Let  $z$  be an arbitrary element. Then:

$$\begin{aligned} z \in X \triangle Y &\iff z \in (X \setminus Y) \cup (Y \setminus X) \\ &\iff z \in X \setminus Y \text{ or } z \in Y \setminus X \\ &\iff (z \in X \text{ and } z \notin Y) \text{ or } (z \in Y \text{ and } z \notin X) \\ &\iff z \in X \cup Y \text{ and } z \notin X \cap Y \\ &\iff z \in (X \cup Y) \setminus (X \cap Y) \end{aligned}$$

Therefore,  $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$ . □

## 2.2 Mappings

**Definition 2.2 (Mapping)**

Let  $A$  and  $B$  be sets. A mapping from  $A$  to  $B$  is written as  $f : A \rightarrow B$  or  $A \xrightarrow{f} B$ .

In set-theoretic language, we understand a mapping  $f : A \rightarrow B$  as a subset of  $A \times B$ , denoted  $\Gamma_f$ , satisfying the following condition: for each  $a \in A$ , the set

$$\{b \in B : (a, b) \in \Gamma_f\}$$

is a singleton, whose unique element is denoted  $f(a)$  and called the image of  $a$  under  $f$ . 

**Definition 2.3 (Left and Right Inverses)**

Consider a pair of mappings  $A \xrightarrow{f} B \xrightarrow{g} A$ . If  $g \circ f = \text{id}_A$ , then:

- We call  $g$  the left inverse of  $f$
- We call  $f$  the right inverse of  $g$

A mapping with a left inverse (or right inverse) is called left invertible (or right invertible). 

**Example 2.2 Composition of Invertible Maps** Let us show that the composition of two left (or right) invertible mappings is again left (or right) invertible.

**Proof** Let  $f : A \rightarrow B$  and  $f' : B \rightarrow C$  be left invertible mappings. Then:

- Let  $g$  be left inverse of  $f$ , so  $g \circ f = \text{id}_A$ . Let  $g'$  be left inverse of  $f'$ , so  $g' \circ f' = \text{id}_B$
- Then for composition  $f' \circ f$ :

$$(g \circ g') \circ (f' \circ f) = g \circ (g' \circ f') \circ f = g \circ f = \text{id}_A$$

- Therefore  $g \circ g'$  is a left inverse of  $f' \circ f$



The proof for right invertible mappings is similar.  $\square$

### Proposition 2.1

For a mapping  $f : A \rightarrow B$  where  $A$  is non-empty, the following are equivalent:

- (i)  $f$  is injective
- (ii)  $f$  has a left inverse
- (iii)  $f$  satisfies the left cancellation law

Similarly, where  $B$  is non-empty, the following are equivalent:

- (i)'  $f$  is surjective
- (ii)'  $f$  has a right inverse
- (iii)'  $f$  satisfies the right cancellation law



**Proof** First, we prove the equivalence for injective properties:

(i)  $\implies$  (ii): Assume  $f$  is injective.  $\forall b \in \text{Im}(f), \exists a \in A, f(a) = b$ . Define  $g : B \rightarrow A$  by  $g(b) = a$  if  $b \in \text{Im}(f)$ , and arbitrary otherwise. Then  $g \circ f = \text{id}_A$ , so  $g$  is left inverse.

(ii)  $\implies$  (iii): Assume  $g \circ f = \text{id}_A$ . If  $f g_1 = f g_2$ , then  $g(f g_1) = g(f g_2) \iff (g f) g_1 = (g f) g_2 \iff g_1 = g_2$


(iii)  $\implies$  (i): Assume left cancellation,  $f g_1 = f g_2 \implies g_1 = g_2$ , if  $\forall a_1, a_2 \in A, f(a_1) = f(a_2)$ , then  $f(a_1) = f(a_2) \implies a_1 = a_2$ .

the proof for surjective properties is similar.  $\square$

### Definition 2.4 (Invertible Mapping)

A mapping  $f$  is called invertible if it is both left and right invertible. In this case, there exists a unique mapping  $f^{-1} : B \rightarrow A$  such that:

$$f^{-1} \circ f = \text{id}_A \quad \text{and} \quad f \circ f^{-1} = \text{id}_B$$

This mapping  $f^{-1}$  is called the inverse of  $f$ . 

### Proposition 2.2

Let  $f : A \rightarrow B$  be an invertible mapping. Then:

1.  $f^{-1} : B \rightarrow A$  is also invertible, and  $(f^{-1})^{-1} = f$
2. If  $g : B \rightarrow C$  is also invertible, then the composition  $g \circ f : A \rightarrow C$  is invertible, and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$



**Proof**

1. Since  $f \circ f^{-1} = \text{id}_B$  and  $f^{-1} \circ f = \text{id}_A$ ,  $f$  is both left and right inverse of  $f^{-1}$ , so  $(f^{-1})^{-1} = f$


2. For composition:

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ f = \text{id}_A$$

$$\text{Similarly, } (g \circ f) \circ (f^{-1} \circ g^{-1}) = \text{id}_C$$

$\square$

### Proposition 2.3

A mapping  $f$  is bijective if and only if it is invertible, in which case its inverse mapping is precisely the previously defined  $f^{-1}$ . 

**Proof** There are easy to prove by the proposition 2.1

(  $\implies$  ) If  $f$  is bijective: Being injective implies  $f$  has a left inverse, Being surjective implies  $f$  has a right inverse, Therefore  $f$  is invertible.

(  $\impliedby$  ) If  $f$  is invertible: Having left inverse implies  $f$  is injective, Having right inverse implies  $f$  is surjective, Therefore  $f$  is bijective.  $\square$

#### Definition 2.5 (Preimage)

For a mapping  $f : A \rightarrow B$  and  $b \in B$ , we denote:

$$f^{-1}(b) := f^{-1}(\{b\}) = \{a \in A : f(a) = b\}$$

**Remark** Note that this notation  $f^{-1}(b)$  represents the preimage of  $b$  under  $f$ , which exists even when  $f$  is not invertible.

## 2.3 Product of Sets & Disjoint Union

#### Definition 2.6 (Generalized Cartesian Product)

Using the language of mappings, we define:

$$\prod_{i \in I} A_i := \{f : I \rightarrow \bigcup_{i \in I} A_i \mid \forall i \in I, f(i) \in A_i\}$$

Henceforth, we may write  $f(i)$  as  $a_i$ , so elements of  $\prod_{i \in I} A_i$  can be reasonably denoted as  $(a_i)_{i \in I}$ .

For any  $i \in I$ , there is a mapping  $p_i : \prod_{j \in I} A_j \rightarrow A_i$  defined by  $p_i((a_j)_{j \in I}) = a_i$ , called the  $i$ -th projection.

**Remark** For easy to understand, The  $\prod_{i \in I} A_i$  as the three domain space, the  $(a_i)_{i \in I}$  as the one point in the three domain space, the  $p_i$  as the projection from the three domain space to the one point.

#### Definition 2.7 (Disjoint Union and Partition)

Let set  $A$  be the union of a family of subsets  $(A_i)_{i \in I}$ , and suppose these subsets are pairwise disjoint, that is:

$$\forall i, j \in I, i \neq j \implies A_i \cap A_j = \emptyset$$

In this case, we say  $A$  is the disjoint union of  $(A_i)_{i \in I}$ , or  $(A_i)_{i \in I}$  is a partition of  $A$ , written as:

$$A = \coprod_{i \in I} A_i$$

## 2.4 Structure of Order

#### Definition 2.8 (Binary Relation)

A binary relation between sets  $A$  and  $B$  is any subset of  $A \times B$ . Let  $R \subset A \times B$  be a binary relation. Then for all  $a \in A$  and  $b \in B$ , we use the notation:

$$aRb \text{ to represent } (a, b) \in R$$

For convenience, when  $A = B$ , we call this a binary relation on  $A$ .



**Definition 2.9 (Order Relations)**

Let  $\preceq$  be a binary relation on set  $A$ . We call  $\preceq$  a preorder and  $(A, \preceq)$  a preordered set when:

- Reflexivity: For all  $a \in A$ ,  $a \preceq a$
- Transitivity: For all  $a, b, c \in A$ , if  $a \preceq b$  and  $b \preceq c$ , then  $a \preceq c$

If it also satisfies:

- Antisymmetry: For all  $a, b \in A$ , if  $a \preceq b$  and  $b \preceq a$ , then  $a = b$

then  $\preceq$  is called a partial order and  $(A, \preceq)$  is called a partially ordered set.

A partially ordered set  $(A, \preceq)$  is called a totally ordered set or chain if any two elements  $a, b \in A$  are comparable, that is, either  $a \preceq b$  or  $b \preceq a$  holds.

**Definition 2.10 (Order-Preserving Maps)**

Let  $f : A \rightarrow B$  be a mapping between preordered sets. Then:

- $f$  is called order-preserving if:

$$a \preceq a' \implies f(a) \preceq f(a') \text{ for all } a, a' \in A$$

- $f$  is called strictly order-preserving if:

$$a \preceq a' \iff f(a) \preceq f(a') \text{ for all } a, a' \in A$$

**Definition 2.11 (Maximal, Minimal Elements and Bounds)**

Let  $(A, \preceq)$  be a partially ordered set.

- An element  $a_{\max} \in A$  is called a maximal element of  $A$  if: there exists no  $a \in A$  such that  $a \succ a_{\max}$
- An element  $a_{\min} \in A$  is called a minimal element of  $A$  if: there exists no  $a \in A$  such that  $a \prec a_{\min}$

Furthermore, let  $A'$  be a subset of  $A$ .

- An element  $a \in A$  is called an upper bound of  $A'$  in  $A$  if: for all  $a' \in A'$ ,  $a' \preceq a$
- An element  $a \in A$  is called a lower bound of  $A'$  in  $A$  if: for all  $a' \in A'$ ,  $a' \succeq a$



**Remark** we can use the tree structure to understand the maximal, minimal elements and bounds. the partial order like the link between the nodes, the maximal, minimal elements like the root nodes and leaf nodes.

**Definition 2.12 (Well-Ordered Set)**

A totally ordered set  $(A, \preceq)$  is called a well-ordered set if every non-empty subset  $S \subseteq A$  has a minimal element.



## 2.5 Equivalence Relations and Quotient Sets

**Definition 2.13 (Equivalence Relation)**

A binary relation  $\sim$  on set  $A$  is called an equivalence relation if it satisfies:

- Reflexivity: For all  $a \in A$ ,  $a \sim a$
- Symmetry: For all  $a, b \in A$ , if  $a \sim b$  then  $b \sim a$
- Transitivity: For all  $a, b, c \in A$ , if  $a \sim b$  and  $b \sim c$  then  $a \sim c$



**Definition 2.14 (Equivalence Class)**

Let  $\sim$  be an equivalence relation on set  $A$ . A non-empty subset  $C \subset A$  is called an equivalence class if:

- Elements in  $C$  are mutually equivalent: for all  $x, y \in C$ ,  $x \sim y$
- $C$  is closed under  $\sim$ : for all  $x \in C$  and  $y \in A$ , if  $x \sim y$  then  $y \in C$

If  $C$  is an equivalence class and  $a \in C$ , then  $a$  is called a representative element of  $C$ .

**Proposition 2.4 (Partition by Equivalence Classes)**

Let  $\sim$  be an equivalence relation on set  $A$ . Then  $A$  is the disjoint union of all its equivalence classes.



**Proof** Let  $\{C_i\}_{i \in I}$  be the collection of all equivalence classes of  $A$ .

1. First,  $A = \bigcup_{i \in I} C_i$  since every element belongs to its equivalence class
2. For any distinct equivalence classes  $C_i$  and  $C_j$ : If  $x \in C_i \cap C_j$  and  $x \neq \emptyset$ , then  $C_i = C_j$ , this is a contradiction, so  $C_i \cap C_j = \emptyset$ .
3. Therefore,  $A = \bigsqcup_{i \in I} C_i$

**Definition 2.15 (Quotient Set)**

Let  $\sim$  be an equivalence relation on a non-empty set  $A$ . The quotient set is defined as the following subset of the power set  $\mathcal{P}(A)$ :

$$A/\sim := \{C \subset A : C \text{ is an equivalence class with respect to } \sim\}$$

The quotient set comes with a quotient map  $q : A \rightarrow A/\sim$  that maps each  $a \in A$  to its unique equivalence class.



**Remark** here to find the quotient set, we can use the boolean function symmetric for the equivalence relation, then we only travel the quotient set, which can reduce the travel space.

**Proposition 2.5 (Universal Property of Quotient Maps)**

Let  $\sim$  be an equivalence relation on set  $A$  and  $q : A \rightarrow A/\sim$  be the corresponding quotient map. If a mapping  $f : A \rightarrow B$  satisfies:

$$a \sim a' \implies f(a) = f(a')$$

then there exists a unique mapping  $\bar{f} : (A/\sim) \rightarrow B$  such that:

$$\bar{f} \circ q = f$$



**Proof** First,  $\bar{f}$  is well-defined: for any  $c \in A/\sim$ . Then:

$$\bar{f}(c) := f(a), a = q^{-1}(c)$$

The proof of uniqueness: Assume  $\bar{f}$  and  $\bar{f}'$ , then  $\bar{f} \circ q = \bar{f}' \circ q$ , the  $q$  is surjective, so  $\bar{f} = \bar{f}'$ .

**Proposition 2.6**

For any mapping  $f : A \rightarrow B$ , define an equivalence relation  $\sim_f$  on  $A$  by:

$$a \sim_f a' \iff f(a) = f(a')$$

Then by Proposition 2.5, there exists a bijection:

$$\bar{f} : (A/\sim_f) \xrightarrow{1:1} \text{im}(f)$$



**Proof** Let  $q : A \rightarrow A/\sim_f$  be the quotient map. By the universal property:

1. Well-defined: If  $[a] = [a']$ , then  $a \sim_f a'$ , so  $f(a) = f(a')$
2. Injective: If  $\bar{f}([a]) = \bar{f}([a'])$ , then  $f(a) = f(a')$ , so  $a \sim_f a'$ , thus  $[a] = [a']$
3. Surjective: For any  $b \in \text{im}(f)$ , there exists  $a \in A$  with  $f(a) = b$ , so  $\bar{f}([a]) = b$

Therefore,  $\bar{f}$  is a bijection between  $A/\sim_f$  and  $\text{im}(f)$ . □

## 2.6 positive integer to rational number

### Definition 2.16 (Integers as Quotient Set)

The set of integers  $\mathbb{Z}$  is defined as the quotient set of  $\mathbb{Z}_{\geq 0}^2$  under  $\sim$ . We temporarily denote the equivalence class containing  $(m, n)$  in  $\mathbb{Z}_{\geq 0}^2$  as  $[m, n]$ . ♣

**Remark** the  $\sim$  relation is defined as  $(m, n) \sim (m', n') \iff m + n' = m' + n \iff m - n = m' - n'$ .

### Definition 2.17 (Operations on Integer Equivalence Classes)

For any elements  $[m, n]$  and  $[r, s]$  in  $\mathbb{Z}$ , define:

$$\begin{aligned} [m, n] + [r, s] &:= [m + r, n + s] \\ [m, n] \cdot [r, s] &:= [mr + ns, nr + ms] \end{aligned}$$

By convention, multiplication  $x \cdot y$  is often written simply as  $xy$ . ♣

### Definition 2.18 (Total Order on Integers)

Define a total order  $\leq$  on  $\mathbb{Z}$  by:

$$x \leq y \iff y - x \in \mathbb{Z}_{\geq 0}$$
♣

### Definition 2.19 (Rational Numbers)

Define the set of rational numbers  $\mathbb{Q}$  as the quotient set of  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  under the equivalence relation:

$$(r, s) \sim (r', s') \iff rs' = r's$$

We temporarily denote the equivalence class containing  $(r, s)$  as  $[r, s]$ . Through the mapping  $x \mapsto [x, 1]$ , we view  $\mathbb{Z}$  as a subset of  $\mathbb{Q}$ . ♣

### Definition 2.20 (Total Order and Absolute Value on $\mathbb{Q}$ )

Define a total order on  $\mathbb{Q}$  by:

$$\begin{aligned} [r, s] \geq 0 &\iff rs \geq 0 \\ x \geq y &\iff x - y \geq 0 \end{aligned}$$

For any  $x \in \mathbb{Q}$ , its absolute value  $|x|$  is defined as:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$
♣

### Proposition 2.7

Let  $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ . For any  $x \in \mathbb{Q}^\times$ , there exists a unique  $x^{-1} \in \mathbb{Q}^\times$  such that  $xx^{-1} = 1$ . ♠

**Proof** For  $x = [r, s] \in \mathbb{Q}^\times$ , define  $x^{-1} = [s, r]$  when  $r > 0$  and  $x^{-1} = [-s, -r]$  when  $r < 0$ . Then  $xx^{-1} = 1$  and the uniqueness, here have the  $x', x''$ , then  $x'x = 1 = x''x$ , the  $x$  have the right inverse, so  $x' = x''$ .  $\square$

## 2.7 arithmetical

### Definition 2.21 (Integer Multiples and Divisibility)

For any  $x \in \mathbb{Z}$ , define:

$$x\mathbb{Z} := \{xd : d \in \mathbb{Z}\}$$

which consists of all multiples of  $x$ .

For  $x, y \in \mathbb{Z}$ :

- We say  $x$  divides  $y$ , written  $x \mid y$ , if  $y \in x\mathbb{Z}$
- Otherwise, we write  $x \nmid y$
- When  $x \mid y$ , we call  $x$  a factor or divisor of  $y$



### Proposition 2.8 (Division Algorithm)

For any integers  $a, d \in \mathbb{Z}$  where  $d \neq 0$ , there exist unique integers  $q, r \in \mathbb{Z}$  such that:

$$\begin{aligned} a &= dq + r \\ 0 &\leq r < |d| \end{aligned}$$



**Proof Existence:**  $\forall a, b, \exists q \in \mathbb{Z}$ , let exist  $r = a - dq$  (here can use the modular equivalence relation), and  $0 \leq r < |d|$ .

**Uniqueness:** Suppose  $a = dq_1 + r_1 = dq_2 + r_2$  with  $0 \leq r_1, r_2 < |d|$

- Then  $d(q_1 - q_2) = r_2 - r_1$
- $|r_2 - r_1| < |d|$
- Therefore  $q_1 = q_2$  and  $r_1 = r_2$

$\square$

### Lemma 2.1 (Generator of Integer Ideals)

Let  $I$  be a non-empty subset of  $\mathbb{Z}$  satisfying:

1. If  $x, y \in I$ , then  $x + y \in I$
2. If  $a \in \mathbb{Z}$  and  $x \in I$ , then  $ax \in I$

Then there exists a unique  $g \in \mathbb{Z}_{\geq 0}$  such that  $I = g\mathbb{Z}$ .



**Proof** If  $I = \{0\}$ , take  $g = 0$ . Otherwise, let  $g$  be the smallest positive element in  $I$ .

For any  $x \in I$ , by division algorithm:

$$x = gq + r \text{ where } 0 \leq r < g$$

Then  $r = x - gq \in I$  by properties of  $I$ . By minimality of  $g$ , we must have  $r = 0$ . Therefore  $x \in g\mathbb{Z}$ , so  $I \subseteq g\mathbb{Z}$ .

Since  $g \in I$ , we have  $g\mathbb{Z} \subseteq I$ . Thus  $I = g\mathbb{Z}$ .

Uniqueness follows from the fact that  $g$  must be the smallest positive element in  $I$ .  $\square$

**Definition 2.22 (Greatest Common Divisor)**

For any integers  $a, b \in \mathbb{Z}$ , the greatest common divisor of  $a$  and  $b$ , denoted  $\gcd(a, b)$ , is the unique positive integer  $d$  such that:

- $d \mid a$  and  $d \mid b$
- For any  $d' \in \mathbb{Z}$ , if  $d' \mid a$  and  $d' \mid b$ , then  $d' \mid d$

**Proposition 2.9 (Bézout's Identity)**

For integers  $x_1, \dots, x_n$ :

$$\mathbb{Z}x_1 + \dots + \mathbb{Z}x_n = \gcd(x_1, \dots, x_n)\mathbb{Z}$$

Consequently,  $x_1, \dots, x_n$  are coprime if and only if there exist  $a_1, \dots, a_n \in \mathbb{Z}$  such that:

$$a_1x_1 + \dots + a_nx_n = 1$$



**Proof** We proceed by induction on  $n$ .

For  $n = 2$ : Let  $d = \gcd(x_1, x_2)$ . By Euclidean algorithm, there exist  $a_1, a_2 \in \mathbb{Z}$  such that:

$$d = a_1x_1 + a_2x_2 \in \mathbb{Z}x_1 + \mathbb{Z}x_2$$

Therefore  $d\mathbb{Z} \subseteq \mathbb{Z}x_1 + \mathbb{Z}x_2$ .

Conversely, since  $d \mid x_1$  and  $d \mid x_2$ , we have  $\mathbb{Z}x_1 + \mathbb{Z}x_2 \subseteq d\mathbb{Z}$ .

For  $n > 2$ : Let  $g = \gcd(x_1, \dots, x_{n-1})$ . By induction:

$$\mathbb{Z}x_1 + \dots + \mathbb{Z}x_{n-1} = g\mathbb{Z}$$

Then:

$$\mathbb{Z}x_1 + \dots + \mathbb{Z}x_n = g\mathbb{Z} + \mathbb{Z}x_n = \gcd(g, x_n)\mathbb{Z} = \gcd(x_1, \dots, x_n)\mathbb{Z}$$

The corollary follows directly since  $\gcd(x_1, \dots, x_n) = 1$  if and only if they are coprime. □

**Definition 2.23 (Prime Numbers)**

Let  $p \in \mathbb{Z} \setminus \{0, \pm 1\}$ . We say  $p$  is a prime element if its only divisors are  $\pm 1$  and  $\pm p$ . A positive prime element is called a prime number.

**Proposition 2.10 (Euclid's Lemma)**

Let  $p$  be a prime element. If  $a, b \in \mathbb{Z}$  such that  $p \mid ab$ , then either  $p \mid a$  or  $p \mid b$ .



**Proof** If  $p \nmid a$ , then  $\gcd(p, a) = 1$  since  $p$  is prime. By proposition 2.9, there exist  $x, y \in \mathbb{Z}$  such that:

$$px + ay = 1$$

Multiply both sides by  $b$ :

$$pbx + aby = b$$

Since  $p \mid ab$ ,  $pbx + aby \in p\mathbb{Z}$ , so  $p \mid b$ . □

**Theorem 2.1 (Fundamental Theorem of Arithmetic)**

Every non-zero integer  $n \in \mathbb{Z}$  has a prime factorization:

$$n = \pm p_1^{a_1} \dots p_r^{a_r}$$

where  $r \in \mathbb{Z}_{\geq 0}$  (with the convention that the right side equals  $\pm 1$  when  $r = 0$ ),  $p_1, \dots, p_r$  are distinct

prime numbers,  $a_1, \dots, a_r \in \mathbb{Z}_{\geq 1}$ , and this factorization is unique up to ordering.



**Proof Existence:** By induction on  $|n|$

- Base case: When  $|n| = 1$ , take  $r = 0$
- For  $|n| > 1$ : Let  $p$  be the smallest prime divisor of  $n$
- Then  $n = pm$  where  $|m| < |n|$
- By induction,  $m$  has prime factorization
- Combine  $p$  with  $m$ 's factorization

**Uniqueness:** Suppose we have two factorizations:

$$p_1^{a_1} \cdots p_r^{a_r} = q_1^{b_1} \cdots q_s^{b_s}$$

- By proposition 2.10,  $p_1$  divides some  $q_i$
- Since both are prime,  $p_1 = q_i$
- Cancel and continue by induction
- Therefore  $r = s$  and factorizations are same up to ordering

□

**Remark** For a prime number  $p$ , we use the notation  $p^a \parallel n$  to indicate that  $p^a | n$  but  $p^{a+1} \nmid n$  (i.e.,  $p^a$  is the exact power of  $p$  dividing  $n$ ).

### Corollary 2.1

Consider integers  $n = \pm \prod_{i=1}^r p_i^{a_i}$  and  $m = \pm \prod_{i=1}^r p_i^{b_i}$ , where  $p_1, \dots, p_r$  are distinct primes and  $a_i, b_i \in \mathbb{Z}_{\geq 0}$ . Then:

$$\gcd(n, m) = \prod_{i=1}^r p_i^{\min\{a_i, b_i\}}, \quad \text{lcm}(n, m) = \prod_{i=1}^r p_i^{\max\{a_i, b_i\}}$$

Similar results hold for GCD and LCM of any number of positive integers.



### Theorem 2.2 (Euclid)

There are infinitely many prime numbers.



**Proof** Let  $p_1, \dots, p_n$  be any finite collection of primes. Consider  $N = p_1 \cdots p_n + 1$ . Any prime factor  $p$  of  $N$  must be different from all  $p_i$  (since dividing  $N$  by any  $p_i$  leaves remainder 1). Therefore, no finite collection can contain all primes.

□

## 2.8 Congruence Relation

### Definition 2.24 (Congruence Relation)

Let  $N \in \mathbb{Z}$ . Two integers  $a, b \in \mathbb{Z}$  are called congruent modulo  $N$  if  $N \mid (a - b)$ . This relation is written as:

$$a \equiv b \pmod{N}$$



**Definition 2.25 (Congruence Classes)**

For a fixed  $N \in \mathbb{Z}$ , we denote the quotient set of  $\mathbb{Z}$  under the equivalence relation modulo  $N$  (Definition 2.5.4) as  $\mathbb{Z}/N\mathbb{Z}$ , or abbreviated as  $\mathbb{Z}/N$ . The equivalence classes are called congruence classes modulo  $N$ .

**Proposition 2.11 (Multiplicative Inverses Modulo N)**

Let  $N \in \mathbb{Z}_{\geq 1}$ . For any  $x \in \mathbb{Z}$ :

$$(\exists y \in \mathbb{Z}, xy \equiv 1 \pmod{N}) \iff \gcd(N, x) = 1$$



**Proof** ( $\implies$ ) If  $xy \equiv 1 \pmod{N}$ , then  $xy = kN + 1$  for some  $k \in \mathbb{Z}$ . Therefore  $xy - kN = 1$ , showing  $\gcd(N, x) = 1$  by properties 2.9.

( $\impliedby$ ) If  $\gcd(N, x) = 1$ , then by properties 2.9:  $\exists y, k \in \mathbb{Z}$  such that  $xy + kN = 1$ . Therefore  $xy \equiv 1 \pmod{N}$ .  $\square$

**Theorem 2.3 (Fermat's Little Theorem)**

Let  $p$  be a prime number. Then for all  $x \in \mathbb{Z}$ :

$$\gcd(p, x) = 1 \implies x^{p-1} \equiv 1 \pmod{p}$$

Consequently, for all  $x \in \mathbb{Z}$ :

$$x^p \equiv x \pmod{p}$$



**Proof** Consider the sequence  $x, 2x, \dots, (p-1)x \pmod{p}$ . When  $\gcd(p, x) = 1$ , then by proposition 2.11,  $\exists y, xy \equiv 1 \pmod{p}$ , then  $xy, 2xy, \dots, (p-1)xy \pmod{p}$ , these are all distinct and nonzero modulo  $p$ , thus they also mean for the  $x, 2x, \dots, (p-1)x \pmod{p}$ . Their product is congruent to  $(p-1)! \cdot x^{p-1}$ . Therefore  $(p-1)! \cdot x^{p-1} \equiv (p-1)! \pmod{p}$ . Since  $\gcd(p, (p-1)!) = 1$ , we can cancel to get  $x^{p-1} \equiv 1 \pmod{p}$  by proposition 2.11 to reduce the  $(p-1)!$ .  $\square$

**Definition 2.26 (Euler's Totient Function)**

For  $n \in \mathbb{Z}_{\geq 1}$ , define  $\varphi(n)$  as the number of positive integers not exceeding  $n$  that are coprime to  $n$ .



## 2.9 radix

**Definition 2.27 (Equipotent Sets)**

Two sets  $A$  and  $B$  are called equipotent (or have the same cardinality) if there exists a bijection  $f : A \xrightarrow{1:1} B$ . We denote this as  $|A| = |B|$ .

**Definition 2.28 (Cardinality Comparison)**

For sets  $A$  and  $B$ , if there exists an injection  $f : A \hookrightarrow B$ , we write  $|A| \leq |B|$ . We write  $|A| < |B|$  when  $|A| \leq |B|$  but  $|A| \neq |B|$ .

**Proposition 2.12 (Pigeonhole Principle)**

Let  $A$  and  $B$  be finite sets with the same cardinality. Then any injection (or surjection)  $f : A \rightarrow B$  is automatically a bijection.





**Proposition 2.13 (Characterization of Infinite Sets)**

A set  $A$  is infinite if and only if there exists an injection  $\mathbb{Z}_{\geq 0} \hookrightarrow A$ .



**Proof** ( $\implies$ ) If  $A$  is infinite, by axiom of choice we can construct an injection.

( $\impliedby$ ) If such injection exists, then  $|A| \geq |\mathbb{Z}_{\geq 0}|$ , so  $A$  must be infinite. □

**Definition 2.29 (Countable Sets)**

Let  $\aleph_0 := |\mathbb{Z}_{\geq 0}|$ . A set  $A$  is called countable (or enumerable) if  $|A| = \aleph_0$ . A set  $A$  is called at most countable if  $|A| \leq \aleph_0$ , meaning  $A$  is either finite or countable.

**Proposition 2.14**

The union and product of finitely many countable sets are countable. That is, if  $A_1, \dots, A_n$  are countable sets, then:

1.  $\bigcup_{i=1}^n A_i$  is countable
2.  $\prod_{i=1}^n A_i$  is countable



**Proof** For union: Let  $f_i : \mathbb{Z}_{\geq 0} \rightarrow A_i$  be bijections. Define  $f : \mathbb{Z}_{\geq 0} \rightarrow \bigcup_{i=1}^n A_i$  by:

$$f(k) = f_i(m) \text{ where } k = in + m, 0 \leq m < n$$

This is surjective as each element appears in some  $A_i$ .

For product: Let  $g_i : \mathbb{Z}_{\geq 0} \rightarrow A_i$  be bijections. Use Cantor's pairing function to construct bijection:

$$g : \mathbb{Z}_{\geq 0} \rightarrow \prod_{i=1}^n A_i$$

given by  $g(k) = (g_1(k_1), \dots, g_n(k_n))$  where  $k_i$  are obtained from  $k$  by repeated pairing. □

**Theorem 2.4 (Cantor's Theorem)**

For any set  $A$ :

$$2^{|A|} = |\mathcal{P}(A)| > |A|$$

where  $\mathcal{P}(A)$  is the power set of  $A$ .



**Proof** First show  $|\mathcal{P}(A)| \geq 2^{|A|}$  by constructing characteristic function. Then prove  $|\mathcal{P}(A)| > |A|$  by diagonal argument: Assume  $f : A \rightarrow \mathcal{P}(A)$  is surjective. Consider  $B = \{x \in A : x \notin f(x)\}$ . Then  $B \in \mathcal{P}(A)$  but  $B \neq f(a)$  for any  $a \in A$ . □

## Chapter 3 Ring, Field and Polynomial

### 3.1 Ring & Field

#### Definition 3.1 (Ring)

A ring is a tuple  $(R, +, \cdot, 0_R, 1_R)$  where  $R$  is a set,  $0_R, 1_R \in R$ , and  $+: R \times R \rightarrow R$  and  $\cdot: R \times R \rightarrow R$  are binary operations satisfying:

1. Addition satisfies:
  - Associativity:  $(x + y) + z = x + (y + z)$
  - Identity:  $x + 0_R = x = 0_R + x$
  - Commutativity:  $x + y = y + x$
  - Inverse: For all  $x$  there exists  $-x$  with  $x + (-x) = 0_R$
2. Multiplication (written as  $xy$  for  $x \cdot y$ ) satisfies:
  - Associativity:  $(xy)z = x(yz)$
  - Identity:  $x \cdot 1_R = x = 1_R \cdot x$
3. Distributive Laws:
  - $(x + y)z = xz + yz$
  - $z(x + y) = zx + zy$

Where  $x, y, z$  represent arbitrary elements of  $R$ . When no confusion arises, we write  $0_R, 1_R$  as  $0, 1$  and denote the ring by  $R$ . We write  $x + (-y)$  as  $x - y$ .



#### Definition 3.2 (Subring)

Let  $R$  be a ring. A subset  $R_0 \subseteq R$  containing  $0_R, 1_R$  is called a subring of  $R$  if it is closed under:

- Addition:  $x, y \in R_0 \implies x + y \in R_0$
- Multiplication:  $x, y \in R_0 \implies xy \in R_0$
- Additive inverse:  $x \in R_0 \implies -x \in R_0$

Then  $(R_0, +, \cdot, 0_R, 1_R)$  forms a ring.



#### Definition 3.3 (Ring Invertibility)

Let  $x$  be an element of a ring  $R$ .

- If there exists  $y \in R$  such that  $xy = 1$  (resp.  $yx = 1$ ), then  $y$  is called a right inverse (resp. left inverse) of  $x$
- $x$  is called right invertible (resp. left invertible) if it has a right (resp. left) inverse
- $x$  is called invertible if it has both left and right inverses

The set of invertible elements in  $R$  is denoted by  $R^\times$ .



#### Proposition 3.1 (Uniqueness of Ring Inverses)

If an element  $x$  in a ring  $R$  is invertible, then:

1. Its left inverse is also its right inverse
2. There exists a unique  $x^{-1} \in R$  such that  $x^{-1}x = 1 = xx^{-1}$
3.  $(x^{-1})^{-1} = x$



**Proof** Let  $y$  be a left inverse and  $z$  a right inverse of  $x$ . Then  $y = y(xz) = (yx)z = z$ . Therefore,  $y = z = x^{-1}$  is the unique two-sided inverse. Clearly  $(x^{-1})^{-1} = x$  by definition.  $\square$


#### Definition 3.4 (Commutative Ring)

A ring  $R$  is called commutative if its multiplication is commutative, i.e.,

$$xy = yx \text{ for all } x, y \in R$$



#### Definition 3.5 (Division Ring and Field)

A ring  $R$  is called a division ring if  $R^\times = R \setminus \{0\}$  (i.e., every non-zero element is invertible). A commutative division ring is called a field. A subring of a field that is itself a field is called a subfield. 

#### Definition 3.6 (Integral Domain)

A non-zero commutative ring  $R$  is called an integral domain if for all  $x, y \in R$ :

$$x, y \neq 0 \implies xy \neq 0$$




## 3.2 homomorphism & isomorphism

#### Definition 3.7 (Ring Homomorphism)

Let  $f : R \rightarrow R'$  be a mapping between rings. We call  $f$  a ring homomorphism if:


- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1_R) = 1_{R'}$

for all  $x, y \in R$ . A homomorphism from a ring to itself is called an endomorphism. 

#### Definition 3.8 (Ring Isomorphism)

Let  $f : R \rightarrow R'$  be a ring homomorphism. We call  $f$  a ring isomorphism if there exists a ring homomorphism  $g : R' \rightarrow R$  such that:

$$g \circ f = id_R \text{ and } f \circ g = id_{R'}$$

In this case,  $g$  is called the inverse of  $f$ , and we say  $R$  and  $R'$  are isomorphic. 

#### Proposition 3.2

If  $f : R \rightarrow R'$  is a ring homomorphism that is bijective as a set mapping, then  $f$  is a ring isomorphism. 

**Proof** Let  $g : R' \rightarrow R$  be the inverse of  $f$  as a set mapping. We need to show  $g$  is a ring homomorphism:

- For addition:  $g(x' + y') = g(f(g(x')) + f(g(y'))) = g(x') + g(y')$
- For multiplication:  $g(x'y') = g(f(g(x'))f(g(y'))) = g(x')g(y')$
- For identity:  $g(1_{R'}) = g(f(1_R)) = 1_R$

Therefore  $g$  is a ring homomorphism and  $f$  is an isomorphism.  $\square$

#### Proposition 3.3 (Chinese Remainder Theorem - Ring Version)

Let  $N \in \mathbb{Z}_{\geq 1}$  factor as  $N = n_1 \cdots n_k$  where  $n_1, \dots, n_k$  are pairwise coprime. Then there exists a ring

isomorphism:

$$\varphi : \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$$

given by  $[x]_N \mapsto ([x]_{n_i})_{i=1}^k$



### Proof

1. **Well-defined:** If  $x \equiv y \pmod{N}$ , then  $x \equiv y \pmod{n_i}$  for all  $i$
2. **Ring homomorphism:**
  - $\varphi([x]_N + [y]_N) = \varphi([x+y]_N) = ([x+y]_{n_i}) = ([x]_{n_i} + [y]_{n_i})$
  - $\varphi([x]_N [y]_N) = \varphi([xy]_N) = ([xy]_{n_i}) = ([x]_{n_i} [y]_{n_i})$
3. **Injective:** If  $\varphi([x]_N) = \varphi([y]_N)$ , then  $x \equiv y \pmod{n_i}$  for all  $i$ . Since  $n_i$  are coprime,  $x \equiv y \pmod{N}$
4. **Surjective:** Given  $([a_i]_{n_i})$ , by CRT there exists  $x$  with  $x \equiv a_i \pmod{n_i}$ . Then  $\varphi([x]_N) = ([a_i]_{n_i})$

□

**Example 3.1 Application of Chinese Remainder Theorem** Find  $x$  satisfying the system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Solution:

1.  $N = 3 \cdot 5 \cdot 7 = 105$
2. Find  $M_i$ :
  - $M_1 = 35$  (for mod 3)
  - $M_2 = 21$  (for mod 5)
  - $M_3 = 15$  (for mod 7)
3. Find  $y_i$  where  $M_i y_i \equiv 1 \pmod{n_i}$ :
  - $35y_1 \equiv 1 \pmod{3} \implies y_1 = 2$
  - $21y_2 \equiv 1 \pmod{5} \implies y_2 = 1$
  - $15y_3 \equiv 1 \pmod{7} \implies y_3 = 1$
4.  $x = (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \pmod{105} = 23$   
 Verify:  $23 \equiv 2 \pmod{3}$ ,  $23 \equiv 3 \pmod{5}$ ,  $23 \equiv 2 \pmod{7}$

## 3.3 Polynomial Ring

### Definition 3.9 (Polynomial Ring)

Let  $R$  be a non-zero ring. A polynomial in variable  $X$  with coefficients in  $R$  is defined as a formal sum:

$$f = \sum_{n \geq 0} a_n X^n, \quad a_n \in R$$

where only finitely many  $a_n$  are non-zero. Terms with  $a_n = 0$  may be omitted. When emphasis on the variable is needed, we write  $f(X)$ . The set of all such polynomials is denoted  $R[X]$ .



**Definition 3.10 (Operations on Polynomials)**

Addition of polynomials is defined term by term:

$$\sum_{n \geq 0} a_n X^n + \sum_{n \geq 0} b_n X^n := \sum_{n \geq 0} (a_n + b_n) X^n$$

Multiplication is defined by convolution:

$$\left( \sum_{n \geq 0} a_n X^n \right) \cdot \left( \sum_{n \geq 0} b_n X^n \right) := \sum_{n \geq 0} \left( \sum_{h+k=n} a_h b_k \right) X^n$$

**Proposition 3.4 (Ring Structure of Polynomials)**

With the above operations,  $R[X]$  forms a ring where:

1. The zero polynomial is  $0_{R[X]}$
2. The unit polynomial is the constant polynomial  $1_{R[X]}$  corresponding to  $1_R$
3.  $R$  embeds as a subring of  $R[X]$
4. If  $R$  is commutative, then  $R[X]$  is also commutative

**Lemma 3.1 (Degree Properties in Integral Domains)**

Let  $R$  be an integral domain (Definition 3.6). Then for all non-zero  $f, g \in R[X]$ :

$$\deg(fg) = \deg f + \deg g$$

Consequently:

1.  $R[X]$  is also an integral domain
2.  $R[X]^\times = R^\times$

**Definition 3.11 (Homogeneous Polynomials)**

Let  $f = \sum_{a_1, \dots, a_n \geq 0} c_{a_1, \dots, a_n} X_1^{a_1} \cdots X_n^{a_n}$  be an element of  $R[X_1, \dots, X_n]$ .

$f$  is called homogeneous of degree  $N$  if there exists  $N \in \mathbb{Z}_{\geq 0}$  such that  $c_{a_1, \dots, a_n} \neq 0$  implies  $a_1 + \cdots + a_n = N$ .



**Remark** This concept extends naturally to polynomial rings with infinitely many variables, as they can be written as unions of subrings with finitely many variables.

**Definition 3.12 (Polynomial Composition)**

Let  $R$  be a commutative ring. For  $n, m \in \mathbb{Z}_{\geq 1}$ , given:

$$f = \sum_{a_1, \dots, a_n \geq 0} c_{a_1, \dots, a_n} X_1^{a_1} \cdots X_n^{a_n} \in R[X_1, \dots, X_n]$$

and  $g_1, \dots, g_n \in R[Y_1, \dots, Y_m]$

Let  $g := (g_1, \dots, g_n) \in R[Y_1, \dots, Y_m]^n$ . The composition is defined as:

$$f \circ g := \sum_{a_1, \dots, a_n \geq 0} c_{a_1, \dots, a_n} g_1^{a_1} \cdots g_n^{a_n} \in R[Y_1, \dots, Y_m]$$



### 3.4 Monoid Group

#### Definition 3.13 (monoid)

We say that  $(S, *)$  is a monoid if the binary operation satisfies the associative law and has an identity element. That is,

$$\forall x, y, z \in S, \quad x * (y * z) = (x * y) * z$$

and

$$\exists e \in S, \forall x \in S, \quad e * x = x * e = x$$



#### Definition 3.14 (commutative monoid)

We say that  $(S, *)$  is a commutative monoid if it is a monoid and the operation satisfies the commutative law. That is,

$$\forall x, y \in S, \quad x * y = y * x$$



#### Proposition 3.5 (unique of identity element)

Let  $(S, \cdot)$  be a monoid. Then the identity element is unique.



**Proof** Suppose that  $e$  and  $e'$  are both identity elements of  $S$ . Then

$$e = e \cdot e' = e'$$

so  $e = e'$ . □

#### Proposition 3.6 (expand of associative law)

Let  $x_1, \dots, x_n, y_1, \dots, y_m \in S$ . Then

$$x_1 \cdot x_2 \cdot \dots \cdot x_n \cdot y_1 \cdot y_2 \cdot \dots \cdot y_m = (x_1 \cdot x_2 \cdot \dots \cdot x_n) \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_m)$$



**Proof** We prove this by induction on  $n$ .

**Base Case** ( $n = 1$ ): When  $n = 1$ , the statement simplifies to:

$$x_1 \cdot y_1 \cdot y_2 \cdot \dots \cdot y_m = x_1 \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_m)$$

This is clearly true by the associative property of multiplication.

**Inductive Step:** Assume the statement holds for  $n = k$ , that is:

$$x_1 \cdot x_2 \cdot \dots \cdot x_k \cdot y_1 \cdot y_2 \cdot \dots \cdot y_m = (x_1 \cdot x_2 \cdot \dots \cdot x_k) \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_m)$$

We need to show that the statement holds for  $n = k + 1$ . Consider:

$$x_1 \cdot x_2 \cdot \dots \cdot x_k \cdot x_{k+1} \cdot y_1 \cdot y_2 \cdot \dots \cdot y_m$$

By the associative property, we can regroup the terms as:

$$(x_1 \cdot x_2 \cdot \dots \cdot x_k) \cdot (x_{k+1} \cdot y_1 \cdot y_2 \cdot \dots \cdot y_m)$$

Using the inductive hypothesis on the first  $k$  terms, we have:

$$(x_1 \cdot x_2 \cdot \dots \cdot x_k) \cdot x_{k+1} \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_m) = (x_1 \cdot x_2 \cdot \dots \cdot x_k \cdot x_{k+1}) \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_m)$$

Thus, the statement holds for  $n = k + 1$ . □

**Proposition 3.7**

Let  $x \in S$  and  $m, n \in \mathbb{N}$ . Then

$$x^{m+n} = x^m \cdot x^n$$



**Proof** We will prove this in three steps:

**Step 1:** First, recall from Proposition 3.6 that for any elements in  $S$ :

$$x_1 \cdot x_2 \cdot \dots \cdot x_n \cdot y_1 \cdot y_2 \cdot \dots \cdot y_m = (x_1 \cdot x_2 \cdot \dots \cdot x_n) \cdot (y_1 \cdot y_2 \cdot \dots \cdot y_m)$$

**Step 2:** Now, consider the special case where all elements are equal to  $x$ :

- Let  $x_1 = x_2 = \dots = x_m = x$
- Let  $y_1 = y_2 = \dots = y_n = x$

**Step 3:** By definition of exponentiation in a monoid:

$$\begin{aligned} x^{m+n} &= \underbrace{x \cdot x \cdot \dots \cdot x}_{m+n \text{ times}} \\ &= (\underbrace{x \cdot x \cdot \dots \cdot x}_m) \cdot (\underbrace{x \cdot x \cdot \dots \cdot x}_n) \\ &= x^m \cdot x^n \end{aligned}$$

Therefore, we have proved that  $x^{m+n} = x^m \cdot x^n$  for all  $x \in S$  and  $m, n \in \mathbb{N}$ . □

**Definition 3.15 (Submonoid)**

Let  $(S, \cdot)$  be a monoid. If  $T \subset S$ , we say that  $(T, \cdot)$  is a submonoid of  $(S, \cdot)$  if:

1. The identity element  $e \in T$
2.  $T$  is closed under multiplication, that is:

$$\forall x, y \in T, \quad x \cdot y \in T$$

**Proposition 3.8**

If  $(T, \cdot)$  is a submonoid of  $(S, \cdot)$ , then  $(T, \cdot)$  is a monoid. ♠

**Proof** We need to verify two properties:

1. The operation is associative in  $T$ :

Since  $T \subset S$  and  $\cdot$  is associative in  $S$ , it is also associative in  $T$ .

2.  $T$  has an identity element:

By definition of submonoid, the identity element  $e \in T$ .

Therefore,  $(T, \cdot)$  satisfies all properties of a monoid. □

**Definition 3.16 (Monoid Homomorphism)**

Let  $(S, \cdot)$  and  $(T, *)$  be monoids, and let  $f : S \rightarrow T$  be a mapping. We say  $f$  is a monoid homomorphism if  $f$  preserves multiplication and maps the identity element to the identity element. That is:

1. For all  $x, y \in S$ :

$$f(x \cdot y) = f(x) * f(y)$$

2. For the identity elements  $e \in S$  and  $e' \in T$ :

$$f(e) = e'$$



**Remark** While a homomorphism preserves operations, an isomorphism represents complete structural equiv-



alence. An isomorphism is first a **bijjective mapping**, meaning it establishes a one-to-one correspondence between elements - essentially “relabeling” elements uniquely. Beyond being bijective, an isomorphism preserves operations under this relabeling, implying that the only difference between two structures (like monoids) is their labeling.

**Example 3.2 Different Types of Monoid Maps** Let's examine several maps between monoids:

1. **A homomorphism that is not an isomorphism:** Consider  $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$  defined by  $f(n) = 2n$ 
  - Preserves operation:  $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$
  - Is injective:  $f(a) = f(b) \implies 2a = 2b \implies a = b$
  - Not surjective: odd numbers are not in the image
  - Therefore: homomorphism but not isomorphism
2. **Non-isomorphic homomorphism:** Consider  $h : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_2, +)$  defined by  $h(n) = n \bmod 2$ 
  - Preserves operation:  $h(a + b) = (a + b) \bmod 2 = (a \bmod 2 + b \bmod 2) \bmod 2 = h(a) + h(b)$
  - Not injective:  $h(0) = h(2) = 0$
  - Surjective: image is all of  $\mathbb{Z}_2$
  - Therefore: homomorphism but not isomorphism

#### Definition 3.17 (Generated Submonoid)

Let  $(S, \cdot)$  be a monoid and  $A \subset S$  be a subset. The submonoid generated by  $A$ , denoted by  $\langle A \rangle$ , is defined as the intersection of all submonoids of  $S$  containing  $A$ . That is:

$$\langle A \rangle = \bigcap \{T \subset S : T \supset A, T \text{ is a submonoid}\}$$



#### Proposition 3.9

Let  $(S, \cdot)$  be a monoid and  $A \subset S$  be a subset. Then  $\langle A \rangle$  is also a submonoid. Therefore, it is the smallest submonoid containing  $A$ .



**Proof** We will prove this in two steps:

**Step 1:** Show  $\langle A \rangle$  contains the identity element

Let  $\{T_\alpha\}_{\alpha \in I}$  be the collection of all submonoids containing  $A$ . Each  $T_\alpha$  contains the identity  $e$  (by definition of submonoid), Therefore  $e \in \bigcap_{\alpha \in I} T_\alpha = \langle A \rangle$

**Step 2:** Show closure under multiplication

Let  $x, y \in \langle A \rangle = \bigcap_{\alpha \in I} T_\alpha$ . Then  $x, y \in T_\alpha$  for all  $\alpha \in I$ . Since each  $T_\alpha$  is a submonoid,  $x \cdot y \in T_\alpha$  for all  $\alpha \in I$ . Therefore  $x \cdot y \in \bigcap_{\alpha \in I} T_\alpha = \langle A \rangle$ .

□

#### Definition 3.18 (Monoid Isomorphism)

Let  $(S, \cdot)$  and  $(T, *)$  be monoids, and let  $f : S \rightarrow T$  be a mapping. We say  $f$  is a monoid isomorphism if  $f$  is bijective and a homomorphism. That is:

1.  $f$  is bijective (one-to-one and onto)
2. For all  $x, y \in S$ :


$$f(x \cdot y) = f(x) * f(y)$$

3. For the identity elements  $e \in S$  and  $e' \in T$ :

$$f(e) = e'$$



**Proposition 3.10**

If  $f : (S, \cdot) \rightarrow (T, *)$  is a monoid isomorphism, then  $f^{-1} : T \rightarrow S$  is a monoid homomorphism. Therefore,  $f^{-1}$  is also a monoid isomorphism. 


**Proof** Since  $f$  is an isomorphism,  $f^{-1}$  exists and is bijective. We need to show:

1.  $f^{-1}$  preserves operation:

$$\begin{aligned} f^{-1}(a * b) &= f^{-1}(f(f^{-1}(a)) * f(f^{-1}(b))) \\ &= f^{-1}(f(f^{-1}(a) \cdot f^{-1}(b))) \\ &= f^{-1}(a) \cdot f^{-1}(b) \end{aligned}$$

2.  $f^{-1}$  preserves identity:

$$f^{-1}(e') = e \text{ where } e' \text{ and } e \text{ are identity elements}$$


Therefore,  $f^{-1}$  is both a homomorphism and bijective, making it an isomorphism. 

## 3.5 Group


**Definition 3.19 (Invertible Element)**

Let  $(S, \cdot)$  be a monoid and  $x \in S$ . We say  $x$  is invertible if and only if

$$\exists y \in S, x \cdot y = y \cdot x = e$$


where  $y$  is called the inverse of  $x$ , denoted as  $x^{-1}$ . 

**Proposition 3.11 (Uniqueness of Inverse)**

Let  $(S, \cdot)$  be a monoid. If  $x \in S$  is invertible, then its inverse is unique. That is, if  $y, y' \in S$  are both inverses of  $x$ , then  $y = y'$ . 

**Proof** Let  $y$  and  $y'$  be inverses of  $x$ . Then:

$$\begin{aligned} y &= y \cdot e \\ &= y \cdot (x \cdot y') \\ &= (y \cdot x) \cdot y' \\ &= e \cdot y' \\ &= y' \end{aligned}$$

Therefore, the inverse is unique. 

**Definition 3.20 (Group)**

Let  $(G, \cdot)$  be a monoid. We say it is a group if every element in  $G$  is invertible.

Equivalently, if  $\cdot$  is a binary operation on  $G$ , we say  $(G, \cdot)$  is a group, or  $G$  forms a group under  $\cdot$ , when this operation satisfies:

1. *Associativity:* For all  $x, y, z \in G$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

2. Identity element: There exists  $e \in G$  such that for all  $x \in G$

$$x \cdot e = e \cdot x = x$$

3. Inverse elements: For each  $x \in G$ , there exists  $y \in G$  such that

$$x \cdot y = y \cdot x = e$$



### Proposition 3.12

Let  $(G, \cdot)$  be a group and  $x \in G$ . Then  $(x^{-1})^{-1} = x$ .



**Proof** Let  $y = x^{-1}$ . Then:

$$y \cdot x = x \cdot y = e$$

This shows that  $x$  is the inverse of  $y = x^{-1}$ . Therefore,  $(x^{-1})^{-1} = x$ . □

### Proposition 3.13 (Inverse of Product)

Let  $(G, \cdot)$  be a group and  $x, y \in G$ . Then  $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ .



**Proof** We will show that  $y^{-1} \cdot x^{-1}$  is the inverse of  $x \cdot y$ :

$$\begin{aligned} (x \cdot y)(y^{-1} \cdot x^{-1}) &= x \cdot (y \cdot y^{-1}) \cdot x^{-1} \\ &= x \cdot e \cdot x^{-1} \\ &= x \cdot x^{-1} \\ &= e \end{aligned}$$

Similarly,  $(y^{-1} \cdot x^{-1})(x \cdot y) = e$ . Therefore,  $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ . □

### Definition 3.21 (Abelian Group)

Let  $(G, \cdot)$  be a group. We say it is an abelian group, or commutative group, if the operation satisfies the commutative law:

$$\forall x, y \in G, \quad x \cdot y = y \cdot x$$



### Lemma 3.2

Let  $(S, \cdot)$  be a monoid and let  $G$  be the subset of all invertible elements in  $S$ . Then  $(G, \cdot)$  is a group. ♥

**Proof** We need to verify three group axioms:

1. Closure: If  $x, y \in G$ , then  $x \cdot y \in G$  (as product of invertible elements is invertible)
2. Identity:  $e \in G$  (as  $e$  is invertible)
3. Inverse: If  $x \in G$ , then  $x^{-1} \in G$  (by definition of invertible elements)

Associativity is inherited from  $S$ . Therefore,  $(G, \cdot)$  is a group. □

### Definition 3.22 (General Linear Group)

The group of  $n \times n$  invertible real matrices under matrix multiplication is called the general linear group of degree  $n$  over the real numbers, denoted as  $(GL(n, \mathbb{R}), \cdot)$ . Since a matrix is invertible if and only if its determinant is nonzero:

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) : \det(A) \neq 0\}$$



**Definition 3.23 (Special Linear Group)**

The special linear group of degree  $n$  over the real numbers is the group of  $n \times n$  real matrices with determinant exactly 1 under matrix multiplication, denoted as  $(SL(n, \mathbb{R}), \cdot)$ . That is:

$$SL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) : \det(A) = 1\}$$

**Definition 3.24 (Subgroup)**

Let  $(G, \cdot)$  be a group and  $H \subset G$ . We say  $H$  is a subgroup of  $G$ , denoted as  $H < G$ , if it contains the identity element and is closed under multiplication and inverse operations. That is:

1.  $\forall x, y \in H, \quad x \cdot y \in H$  (closure under multiplication)
2.  $\forall x \in H, \quad x^{-1} \in H$  (closure under inverse)
3.  $e \in H$  (contains identity)

**Proposition 3.14**

Let  $(G, \cdot)$  be a group. If  $H$  is a subgroup of  $G$ , then  $(H, \cdot)$  is also a group.



**Proof** Since  $H$  is a subgroup:

1. Associativity: Inherited from  $G$
2. Identity:  $e \in H$  by definition of subgroup
3. Inverse: For all  $x \in H, x^{-1} \in H$  by definition of subgroup
4. Closure: For all  $x, y \in H, x \cdot y \in H$  by definition of subgroup

Therefore,  $(H, \cdot)$  satisfies all group axioms. □

**Proposition 3.15**

For convenience, we can combine the first two conditions of a subgroup definition 3.24 into one, reducing to two conditions:

1.  $\forall x, y \in H, \quad x \cdot y^{-1} \in H$
2.  $e \in H$

These conditions are equivalent to the original subgroup definition. □

**Proof**

$(\Rightarrow) \forall y \in H, y^{-1} \in H$ , then the closure under multiplication,  $\forall x, y, y^{-1} \in H, x \cdot y^{-1} \in H$

$(\Leftarrow) \forall x, y \in H, x \cdot y^{-1} \in H$ , let  $x = e$ , then have  $\forall y \in H, y^{-1} \in H$ ; so  $\forall x, y^{-1} \in H, x \cdot (y^{-1})^{-1} \in H$ , then  $x \cdot y \in H$ . □

**Proposition 3.16**

$(SL(n, \mathbb{R}), \cdot)$  is a group. □

**Proof** We verify the group axioms:

1. Closure: If  $A, B \in SL(n, \mathbb{R})$ , then  $\det(AB) = \det(A) \det(B) = 1 \cdot 1 = 1$ , so  $AB \in SL(n, \mathbb{R})$
2. Identity: The identity matrix  $I_n \in SL(n, \mathbb{R})$  since  $\det(I_n) = 1$
3. Inverse: If  $A \in SL(n, \mathbb{R})$ , then  $\det(A^{-1}) = \frac{1}{\det(A)} = 1$ , so  $A^{-1} \in SL(n, \mathbb{R})$
4. Associativity: Inherited from matrix multiplication

Therefore,  $(SL(n, \mathbb{R}), \cdot)$  is a group. □

**Definition 3.25 (Group Homomorphism)**

Let  $(G, \cdot)$  and  $(G', *)$  be groups, and let  $f : G \rightarrow G'$  be a mapping. We say  $f$  is a group homomorphism if it preserves the operation, that is:

$$\forall x, y \in G, \quad f(x \cdot y) = f(x) * f(y)$$

**Proposition 3.17**

Let  $f : (G, \cdot) \rightarrow (G', *)$  be a group homomorphism. Then:

1.  $f(e) = e'$  (preserves identity)
2.  $f(x^{-1}) = f(x)^{-1}$  (preserves inverses)

**Proof**

1. For identity element:

$$\begin{aligned} f(e) * f(e) &= f(e \cdot e) = f(e) \quad \text{left multiply by } f(e)^{-1} \\ \therefore f(e) &= e' \end{aligned}$$

2. For inverse elements:

$$\begin{aligned} f(x) * f(x^{-1}) &= f(x \cdot x^{-1}) = f(e) = e' \quad \text{left multiply by } f(x)^{-1} \\ \therefore f(x^{-1}) &= f(x)^{-1} \end{aligned}$$

