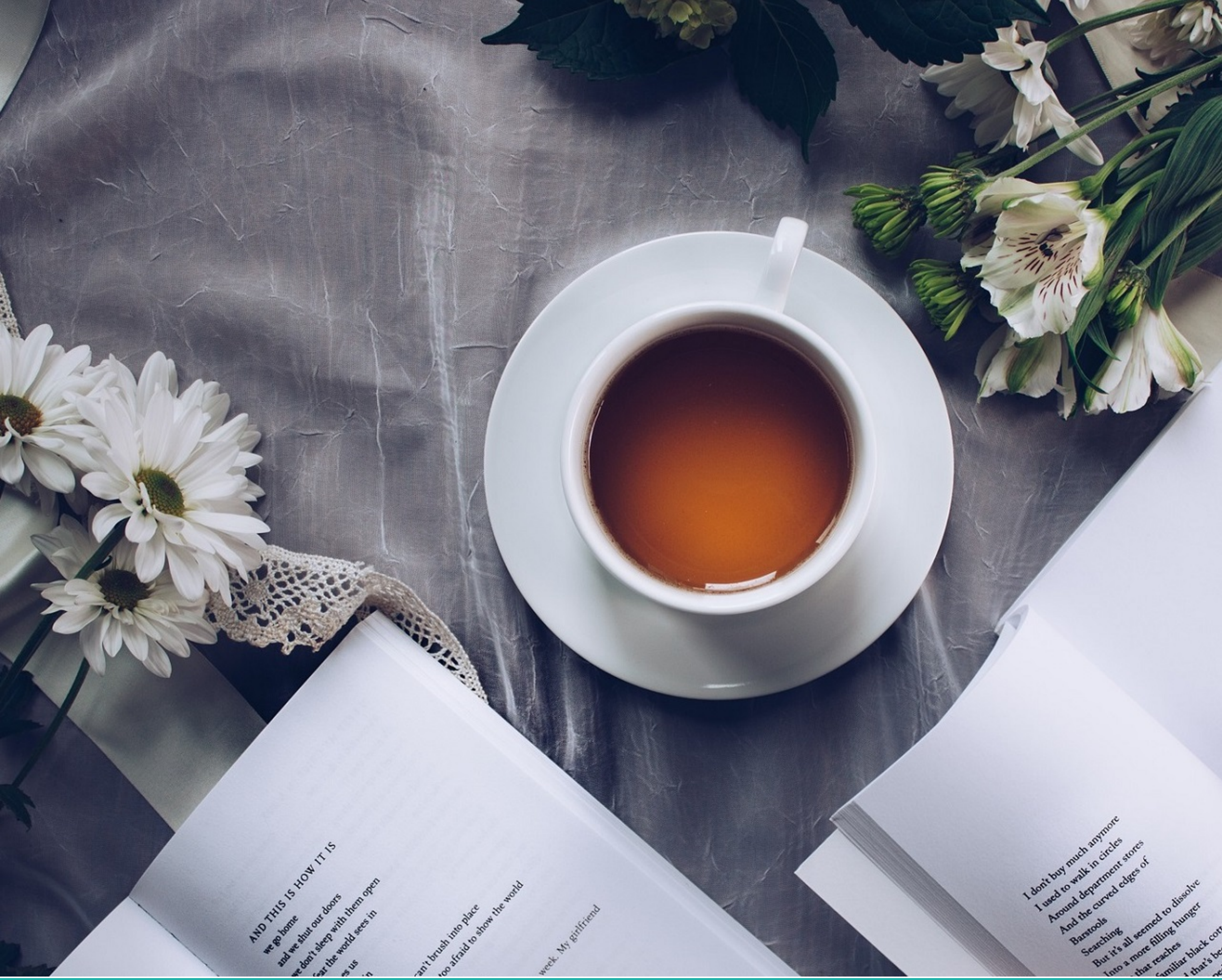

algebra note

Author: isomo

Date: May 5, 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

Chapter 1 Introduction **1**

1.1 What is Algebra? 1

Chapter 2 Sets mappings and relationships **2**

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

Chapter 3 Ring, Field and Polynomial **14**

3.1 Ring & Field 14

3.2 homomorphism & isomorphism 15

3.3 Polynomial Ring 16

3.4 Fractional field to rational function field 19

3.5 Monoid Group 21

3.6 Group 24

Chapter 4 Vector Spaces and linear mappings **28**

4.1 Introduction: Back to the system of linear equations 28

4.2 Vector spaces 29

4.3 Matrix & calculate 29

4.4 Bases & Dimensions 30

4.5 Linear mappings 31

4.6 Linear mappings to Matrix 32

4.7 Transpose of a Matrix and Dual Spaces 33

4.8 Kernel, Image, and Gaussian Elimination 35

4.9 Change of Basis: Matrix Conjugation and Equivalence 36

4.10 Direct Sum Decomposition 37

4.11 Block Matrix Operations 37

4.12 Quotient Spaces 38

Chapter 5 Determinant **40**

5.1 Permutations Introduction 40

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 $x_1, \ldots, x_n \in \mathbb{C}$ such that:

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

These $x_1, \ldots, x_n$ 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* $g : X \to \bigcup X$ *(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* $f : A \to B$ *or* $A \xrightarrow{f} B$.
In set-theoretic language, we understand a mapping $f : A \to B$ *as a subset of* $A \times B$*, denoted* Γ_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* $g \circ f = \mathrm{id}_A$*, 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 $f : A \to B$ and $f' : B \to C$ be left invertible mappings. Then:

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

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

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

The proof for right invertible mappings is similar. □

Proposition 2.1

For a mapping $f : A \to B$ 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 A 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. $\forall b \in \mathrm{Im}(f)$, $\exists a \in A$, $f(a) = b$. Define $g : B \to A$ by $g(b) = a$ if $b \in \mathrm{Im}(f)$, and arbitrary otherwise. Then $g \circ f = \mathrm{id}_A$, so g is left inverse.

(ii) $\implies$ (iii): Assume $g \circ f = \mathrm{id}_A$. If $fg_1 = fg_2$, then $g(fg_1) = g(fg_2) \iff (gf)g_1 = (gf)g_2 \iff g_1 = g_2$

(iii) $\implies$ (i): Assume left cancellation, $fg_1 = fg_2 \implies g_1 = g_2$, 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. □

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 $f^{-1} : B \to A$ such that:

$$f^{-1} \circ f = id_A \quad \text{and} \quad f \circ f^{-1} = id_B$$

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

Proposition 2.2

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

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

Proof

1. Since $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$, f is both left and right inverse of f^{-1}, so $(f^{-1})^{-1} = f$
2. For composition:
$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ f = \mathrm{id}_A$$
Similarly, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C$

□

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

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

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

Definition 2.5 (Preimage)

For a mapping $f : A \to B$ 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:

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

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 $p_i : \prod_{j \in I} A_j \to A_i$ 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 $f : A \to B$ 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, $A = \coprod_{i \in I} C_i$

□

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 $q : A \to A/{\sim}$ that maps each $a \in A$ to its unique equivalence class. ♣

Remark here the 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 $q : A \to A/{\sim}$ be the corresponding quotient map. If a mapping $f : A \to B$ satisfies:

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

then there exists a unique mapping $\bar{f} : (A/{\sim}) \to B$ 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 $f : A \to B$, 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:

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

♠

Proof Let $q : A \to A/\sim_f$ 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 $b \in \mathrm{im}(f)$, 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 $\mathrm{im}(f)$. □

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 $\mathbb{Z}^2_{\geq 0}$ under $\sim$. We temporarily denote the equivalence class containing (m, n) in $\mathbb{Z}^2_{\geq 0}$ 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:

$$[m, n] + [r, s] := [m + r, n + s]$$

$$[m, n] \cdot [r, s] := [mr + ns, nr + ms]$$

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:

$$[r, s] \geq 0 \iff rs \geq 0$$

$$x \geq y \iff x - y \geq 0$$

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 $x' = x''$. □

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:

$$a = dq + r$$
$$0 \leq r < |d|$$

♠

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 $r_1 = r_2$

□

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. □

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 $x_1, \dots, x_n$:

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

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

$$a_1x_1 + \cdots + a_nx_n = 1$$

♠

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 $d|x_1$ and $d|x_2$, 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:

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

Then:

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

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 ± 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:

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

where $r \in \mathbb{Z}_{\geq 0}$ (with the convention that the right side equals ± 1 when $r = 0$), $p_1, \dots, p_r$ are distinct *prime numbers, $a_1, \ldots, a_r \in \mathbb{Z}_{\geq 1}$, 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 $p_1, \ldots, p_r$ are distinct primes and $a_i, b_i \in \mathbb{Z}_{\geq 0}$. Then:

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

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 $p_1, \ldots, p_n$ 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 $xy \equiv 1 \pmod{N}$ □

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 $x, 2x, \ldots, (p-1)x \pmod{p}$. When $\gcd(p, x) = 1$, then by proposition 2.11, $\exists y, xy \equiv 1 \pmod{p}$, then $xy, 2xy, \ldots, (p-1)xy \pmod{p}$, these are all distinct and nonzero modulo p, thus they also mean for the $x, 2x, \ldots, (p-1)x \pmod{p}$. 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 $(p-1)!$. □

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) $f : A \to B$ 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 ($\Longrightarrow$) If A is infinite, by axiom of choice we can construct an injection.

($\Longleftarrow$) 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 $A_1, \ldots, A_n$ 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 $f_i : \mathbb{Z}_{\geq 0} \to A_i$ be bijections. Define $f : \mathbb{Z}_{\geq 0} \to \bigcup_{i=1}^n A_i$ 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 $g_i : \mathbb{Z}_{\geq 0} \to A_i$ be bijections. Use Cantor's pairing function to construct bijection:

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

given by $g(k) = (g_1(k_1), \ldots, g_n(k_n))$ 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 $f : A \to \mathcal{P}(A)$ 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 $+ : R \times R \to R$ and $\cdot : R \times R \to R$ 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. □

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 $f : R \to R'$ 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 $f : R \to R'$ be a ring homomorphism. We call f a ring isomorphism if there exists a ring homomorphism $g : R' \to R$ 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 $f : R \to R'$ is a ring homomorphism that is bijective as a set mapping, then f is a ring isomorphism. ♠

Proof Let $g : R' \to R$ 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. □

Proposition 3.3 (Chinese Remainder Theorem - Ring Version)

Let $N \in \mathbb{Z}_{\geq 1}$ factor as $N = n_1 \cdots n_k$ where $n_1, \ldots, n_k$ 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:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

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 $f = \sum_{a_1,\ldots,a_n\geq 0} c_{a_1,\ldots,a_n} X_1^{a_1}\cdots X_n^{a_n}$ be an element of $R[X_1,\ldots,X_n]$.
f is called homogeneous of degree N if there exists $N \in \mathbb{Z}_{\geq 0}$ such that $c_{a_1,\ldots,a_n} \neq 0$ 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:

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

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

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

Proposition 3.5 (Polynomial Ring Isomorphisms)

For any ring R, there exists a natural ring isomorphism:

$$R[X,Y] \simeq (R[X])[Y]$$

More generally, for any $n \geq 2$, there are ring isomorphisms:

$$R[X_1, \dots, X_n] \simeq R[X_1, \dots, X_{n-1}][X_n] \simeq \cdots \simeq R[X_1] \cdots [X_n]$$

Proof Let's prove for $R[X, Y] \simeq (R[X])[Y]$. Define:

$$\varphi : R[X, Y] \to (R[X])[Y]$$

by sending $\sum_{i,j} a_{ij} X^i Y^j$ to $\sum_j (\sum_i a_{ij} X^i) Y^j$

1. Ring homomorphism:
   - Addition: Clear from coefficients reorganization
   - Multiplication: Terms with same total degree in Y combine
2. Bijective:
   - Injective: Different polynomials map to different arrangements
   - Surjective: Any element in $(R[X])[Y]$ comes from rearranging terms

The general case follows by induction on n. □

Corollary 3.1

If R is an integral domain, then any polynomial ring $R[X, Y, \dots]$ with any number of variables is also an integral domain, and $R[X, Y, \dots]^\times = R^\times$.

Proof By induction on the number of variables:

1. Base case: For $R[X]$, already proved in previous lemma 3.1
2. Inductive step: Assume true for n variables
3. For $n + 1$ variables, use isomorphism:

$$R[X_1, \dots, X_{n+1}] \simeq (R[X_1, \dots, X_n])[X_{n+1}]$$

4. By induction hypothesis, $R[X_1, \dots, X_n]$ is an integral domain
5. Apply one-variable case to get result

□

Proposition 3.6 (Polynomial Division Algorithm)

For any polynomials $a, d \in F[X]$ where $d \neq 0$, there exist unique polynomials $q, r \in F[X]$ such that:

$$a = dq + r \quad \textit{with} \quad \deg(r) < \deg(d)$$

where we define $\deg(0) := -\infty$.

Proof **Existence:** By induction on $\deg(a)$

- If $\deg(a) < \deg(d)$: Take $q = 0, r = a$
- If $\deg(a) \geq \deg(d)$:
  - Let $c = \text{lc}(a)/\text{lc}(d)$ and $n = \deg(a) - \deg(d)$
  - Set $a_1 = a - dcX^n$
  - Note $\deg(a_1) < \deg(a)$
  - By induction: $a_1 = dq_1 + r$
  - Then $a = d(q_1 + cX^n) + r$

Uniqueness: If $a = dq_1 + r_1 = dq_2 + r_2$, then:

- $d(q_1 - q_2) = r_2 - r_1$

- If $q_1 \neq q_2$, then $\deg(r_2 - r_1) \geq \deg(d)$
- But $\deg(r_2 - r_1) < \deg(d)$
- Therefore $q_1 = q_2$ and $r_1 = r_2$

□

Definition 3.13 (Root of Polynomial)

Let $f \in F[X]$ and $a \in F$. We say a is a root of f if $f(a) = 0$.
More generally, for a commutative ring R, if $f \in R[X]$ and $a \in R$ satisfy $f(a) = 0$, then a is called a root of f, or more precisely, a root of f in R.

Proposition 3.7 (Bound on Number of Roots)

Let $f \in F[X] \setminus \{0\}$. Then f has at most $\deg f$ distinct roots in F.

Proof By induction on $\deg f$:

- Base case: If $\deg f = 0$, then f is constant and non-zero, so has no roots
- Inductive step: Let a be a root of f
  - Then $X - a$ divides f, so $f = (X - a)g$ for some g
  - $\deg g = \deg f - 1$
  - Any root of f different from a must be a root of g
  - By induction, g has at most $\deg g$ distinct roots
  - Therefore f has at most $1 + \deg g = \deg f$ distinct roots

□

3.4 Fractional field to rational function field

Definition 3.14 (Rational Functions)

A rational function over R is defined as a quotient $\frac{f}{g}$ where:

- *$f, g \in R[X]$*
- *g is not the zero polynomial (i.e., $g \neq 0_{R[X]}$)*

Proposition 3.8 (Fraction Field)

Let R be an integral domain. Then:

1. *Frac(R) forms a field under the given operations*
2. *The map $f \mapsto [f, 1]$ embeds R as a subring of Frac(R)*

Proposition 3.9 (Universal Property of Fraction Field)

Let R be an integral domain, R' a commutative ring, and $\varphi : R \to R'$ a ring homomorphism such that $\varphi(R \setminus \{0\}) \subset (R')^\times$. Then there exists a unique ring homomorphism $\Phi : \mathit{Frac}(R) \to R'$ making the following diagram commute:

$$
\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d] & R' \\
\mathit{Frac}(R) \arrow[ur, "\Phi"'] &
\end{tikzcd}
$$

Explicitly, $\Phi(f/g) = \varphi(f)\varphi(g)^{-1}$.

Corollary 3.2

Let F be a field containing an integral domain R as a subring. If every element of F can be expressed as fg^{-1} where $f, g \in R$ and $g \neq 0$, then there exists a unique ring isomorphism $\Phi : Frac(R) \to F$ making the following diagram commute:

$$\begin{tikzcd} R \arrow[r, "\text{inclusion}"] \arrow[d] & F \\ Frac(R) \arrow[ur, "\sim"', "\Phi"] & \end{tikzcd}$$

Proof By universal property, there exists unique $\Phi : \text{Frac}(R) \to F$.

- Injective: As composition of non-zero elements remains non-zero
- Surjective: Every element in F has form fg^{-1} with $f, g \in R$
- Therefore Φ is an isomorphism

□

Definition 3.15 (Field of Rational Functions)

Let F be a field. The field of fractions of $F[X, Y, \ldots]$ is called the field of rational functions in variables $X, Y, \ldots$, denoted $F(X, Y, \ldots)$. It contains $F[X, Y, \ldots]$ as a subring.
Elements of $F(X, Y, \ldots)$ are called rational functions in variables $X, Y, \ldots$ with coefficients in F.

Definition 3.16 (Degree of Rational Functions)

Let F be a field. For any $h = \frac{f}{g} \in F(X)$ where $h \neq 0$, define:

$$\deg h := \deg f - \deg g$$

Additionally, define $\deg(0) := -\infty$.

Corollary 3.3 (Bound on Roots in Integral Domain)

Let R be an integral domain and $f \in R[X] \setminus \{0\}$. Then f has at most $\deg f$ distinct roots in R.

Proof Let $F = \text{Frac}(R)$ be the fraction field of R. Since R is a subring of F, any root of f in R is also a root in F. By the previous proposition, f has at most $\deg f$ distinct roots in F. Therefore, f has at most $\deg f$ distinct roots in R. □

Proposition 3.10 (Function Evaluation Map)

Let R be an integral domain and $n \in \mathbb{Z}_{\geq 1}$. The function evaluation map:

$$Fcn : R[X_1, \ldots, X_n] \to \{\textit{functions } R^n \to R\}$$

is injective if and only if R has infinitely many elements.

Theorem 3.1 (Extension Principle for Algebraic Equations)

Let R be an infinite integral domain, $f, g_1, \ldots, g_m \in R[X_1, \ldots, X_n]$, where $g_1, \ldots, g_m$ are non-zero. If for all $(x_1, \ldots, x_n) \in R^n$:

$$(g_1(x_1, \ldots, x_n) \neq 0 \wedge \cdots \wedge g_m(x_1, \ldots, x_n) \neq 0) \implies f(x_1, \ldots, x_n) = 0$$

then $f = 0$.

Proof By contradiction, assume $f \neq 0$.

1. Let $U = \{x \in R^n : g_1(x) \neq 0, \ldots, g_m(x) \neq 0\}$
2. Since R is infinite and g_i are non-zero, U is non-empty
3. By hypothesis, f vanishes on U
4. But $f \neq 0$ implies f can only vanish at finitely many points
5. This contradicts R being infinite

Therefore $f = 0$. □

3.5 Monoid Group

Definition 3.17 (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 3.18 (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 3.11 (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 3.12 (expand of associative law)

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

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

Proof We prove this by induction on n.

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

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

This is clearly true by the associative property of multiplication.

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

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

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

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

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

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

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

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

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

□

Proposition 3.13

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 3.12 that for any elements in S:

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

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

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

Step 3: By definition of exponentiation in a monoid:

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

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 3.19 (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 3.14

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 3.20 (Monoid Homomorphism)

Let $(S, \cdot)$ and $(T, *)$ be monoids, and let $f : S \to T$ 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 equivalence. An isomorphism is first a **bijective 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 $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ 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 $h : (\mathbb{Z}, +) \to (\mathbb{Z}_2, +)$ 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 3.21 (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 3.15

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_α 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_α 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 3.22 (Monoid Isomorphism)

Let $(S, \cdot)$ and $(T, *)$ be monoids, and let $f : S \to T$ 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 3.16

If $f : (S, \cdot) \to (T, *)$ is a monoid isomorphism, then $f^{-1} : T \to S$ 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. □

3.6 Group

Definition 3.23 (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 3.17 (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 3.24 (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 3.18

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 3.19 (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 3.25 (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 3.26 (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 3.27 (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 3.28 (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 3.20

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 3.21

For convenience, we can combine the first two conditions of a subgroup definition 3.28 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 3.22

$(SL(n, \mathbb{R}), \cdot)$ 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 3.29 (Group Homomorphism)

Let $(G, \cdot)$ and $(G', *)$ be groups, and let $f : G \to G'$ 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 3.23

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

□

Chapter 4 Vector Spaces and linear mappings

Broadly speaking, a vector space over a field F refers to a set V together with two operations:

- Vector addition $+ : V \times V \to V$, denoted $(v_1, v_2) \mapsto v_1 + v_2$, satisfying associativity, commutativity, and the existence of inverses;
- Scalar multiplication $\cdot : F \times V \to V$, denoted $(t, v) \mapsto t \cdot v = tv$, satisfying associativity and distributivity over addition.

If a mapping $T : V \to W$ between vector spaces satisfies the identities

$$T(v_1 + v_2) = T(v_1) + T(v_2),$$
$$T(tv) = tT(v),$$

then T is called a linear mapping.

4.1 Introduction: Back to the system of linear equations

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + \cdots + a_{2n}X_n &= b_2 \\ &\vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n &= b_m \end{aligned} \tag{4.1}$$

Definition 4.1

Consider a system of n linear equations over a field F in the form (4.1). If $b_1 = \cdots = b_m = 0$, then the system is called homogeneous. ♣

Given $n, m \in \mathbb{Z}_{\geq 1}$ and a family of coefficients $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$ where $a_{ij} \in F$, define the mapping

$$\begin{aligned} T : F^n &\to F^m \\ (x_j)_{j=1}^n &\mapsto \left(\sum_{j=1}^n a_{1j}x_j, \ldots, \sum_{j=1}^n a_{mj}x_j \right). \end{aligned}$$

Definition 4.2

Let $T : F^n \to F^m$ correspond to a homogeneous system of linear equations as described above. If $v_1, \ldots, v_h \in F^n$ are all solutions of the system, and every solution $x \in F^n$ can be uniquely expressed through addition and scalar multiplication as

$$x = \sum_{i=1}^h t_i v_i, \quad t_1, \ldots, t_h \in F, \tag{4.2}$$

where the tuple $(t_1, \ldots, t_h)$ is uniquely determined by x, then $v_1, \ldots, v_h$ is called a fundamental system of solutions for the homogeneous system. ♣

Proposition 4.1

Consider a homogeneous system of n linear equations in the form (Eq.4.1), where $\mathbf{b} = \mathbf{0}$. If the reduced row echelon matrix obtained by elimination has r pivot elements, then the corresponding homogeneous system has a fundamental system of solutions $v_1, \ldots, v_{n-r}$.

4.2 Vector spaces

Definition 4.3

A vector space over a field F, also called an F-vector space, is a tuple $(V, +, \cdot, 0_V)$ where V is a set, $0_V \in V$, and operations $+ : V \times V \to V$ and $\cdot : F \times V \to V$ are written as $(u, v) \mapsto u + v$ and $(t, v) \mapsto t \cdot v$ respectively, satisfying the following conditions:

1. *Addition satisfies:*
   - *Associativity: $(u + v) + w = u + (v + w)$;*
   - *Identity element: $v + 0_V = v = 0_V + v$;*
   - *Commutativity: $u + v = v + u$;*
   - *Additive inverse: For every v, there exists $-v$ such that $v + (-v) = 0_V$.*
2. *Scalar multiplication, often written as tv instead of $t \cdot v$, satisfies:*
   - *Associativity: $s \cdot (t \cdot v) = (st) \cdot v$;*
   - *Identity property: $1 \cdot v = v$, where 1 is the multiplicative identity in F.*
3. *Scalar multiplication distributes over addition:*
   - *First distributive property: $(s + t) \cdot v = s \cdot v + t \cdot v$;*
   - *Second distributive property: $s \cdot (u + v) = s \cdot u + s \cdot v$.*

Where u, v, w (or s, t) represent arbitrary elements of V (or F). When there is no risk of confusion, we denote 0_V simply as 0, write $u + (-v)$ as $u - v$, and refer to the structure $(V, +, \cdot, 0)$ simply as V.

Definition 4.4

Let V be an F-vector space. If a subset V_0 of V contains 0 and is closed under addition and scalar multiplication, then $(V_0, +, \cdot, 0)$ is also an F-vector space, called a subspace of V.

4.3 Matrix & calculate

Definition 4.5

Let $m, n \in \mathbb{Z}_{\geq 1}$. An $m \times n$ matrix over a field F is a rectangular array

$$A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} = \begin{bmatrix} \cdots & \cdots & a_{ij} & \cdots & \cdots \end{bmatrix}$$

where $a_{ij} \in F$ is called the (i, j)-entry or (i, j)-element of matrix A, with i indicating the row and j indicating the column. An $n \times n$ matrix is called a square matrix of order n.

We denote the set of all $m \times n$ matrices over F by $M_{m \times n}(F)$.

Proposition 4.2

The set $M_{m\times n}(F)$ equipped with standard addition and scalar multiplication forms an F-vector space. The zero element is the zero matrix, and the additive inverse of a matrix $A = (a_{ij})_{i,j}$ is $-A = (-a_{ij})_{i,j}$. ♠

Definition 4.6 (Matrix Multiplication)

Matrix multiplication is a mapping defined as:

$$M_{m\times n}(F) \times M_{n\times r}(F) \to M_{m\times r}(F)$$
$$(A, B) \mapsto AB$$

If $A = (a_{ij})_{1\le i\le m, 1\le j\le n}$ and $B = (b_{jk})_{1\le j\le n, 1\le k\le r}$, then $AB = (c_{ik})_{1\le i\le m, 1\le k\le r}$, where:

$$c_{ik} := \sum_{j=1}^{n} a_{ij}b_{jk} = \begin{pmatrix} a_{i1} & \cdots & a_{in} \end{pmatrix} \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix}$$

This represents the dot product of the i^{th} row of A with the k^{th} column of B. ♣

Proposition 4.3

Matrix multiplication satisfies the following properties:

- *Associativity: $(AB)C = A(BC)$;*
- *Distributivity: $A(B + C) = AB + AC$ and $(B + C)A = BA + CA$;*
- *Linearity: $A(tB) = t(AB) = (tA)B$;*

where $t \in F$ and matrices A, B, C are arbitrary, provided their dimensions make these operations valid. ♠

4.4 Bases & Dimensions

Definition 4.7

Let S be a subset of an F-vector space V.

- *If $\langle S\rangle = V$, then S is said to generate V, or S is called a generating set of V.*
- *A linear relation in S is an equation of the form*

$$\sum_{s\in S} a_s s = 0$$

  This relation is called trivial if all coefficients a_s are zero; otherwise, it is non-trivial. The set S is linearly dependent if there exists a non-trivial linear relation among its elements; otherwise, S is linearly independent.
- *If S is a linearly independent generating set, then S is called a basis of V.* ♣

Lemma 4.1

For any subset S of an F-vector space V, the following statements are equivalent:

1. *S is a minimal generating set.*
2. *S is a basis.*
3. *S is a maximal linearly independent subset.* ♡

Proof Let's prove the equivalence by showing $(1) \Rightarrow (2)$, $(2) \Rightarrow (3)$, and $(3) \Rightarrow (1)$.

(1) $\Rightarrow$ (2): If S is a minimal generating set, then $\langle S\rangle = V$. Suppose S is not linearly independent. Then there exists some $s_0 \in S$ that can be expressed as a linear combination of other elements in S. But this means $S\setminus\{s_0\}$ still generates V, contradicting the minimality of S. Therefore, S must be linearly independent, making it a basis.

(2) $\Rightarrow$ (3): Let S be a basis. Then S is linearly independent and $\langle S\rangle = V$. To show that S is maximal, suppose we add any vector $v \notin S$ to form $S' = S \cup \{v\}$. Since $\langle S\rangle = V$, we have $v \in \langle S\rangle$, meaning v can be written as a linear combination of elements in S. Therefore, S' must be linearly dependent, proving that S is a maximal linearly independent set.

(3) $\Rightarrow$ (1): Let S be a maximal linearly independent set. If $\langle S\rangle \neq V$, then there exists some $v \in V \setminus \langle S\rangle$. The set $S \cup \{v\}$ would still be linearly independent, contradicting the maximality of S. Therefore $\langle S\rangle = V$. Now suppose S is not minimal. Then there exists a proper subset $S' \subset S$ with $\langle S'\rangle = V$. But this means some element in $S \setminus S'$ can be expressed as a linear combination of elements in S', making S linearly dependent, which is a contradiction. Thus, S is a minimal generating set. □

Proposition 4.4

Consider a family of F-vector spaces V_i, each with a given basis B_i, where i ranges over a given index set I. Embed each V_i as a subspace of the direct sum $\bigoplus_{j\in I} V_j$. Correspondingly, view each B_i as a subset of $\bigoplus_{j\in I} V_j$. These subsets B_i are pairwise disjoint, and $\bigcup_{i\in I} B_i$ forms a basis for $\bigoplus_{i\in I} V_i$. ♠

Definition 4.8

Every F-vector space V has a basis. In fact, any linearly independent subset of V can be extended to a basis.

Furthermore, all bases of V have the same cardinality. This common cardinality is called the dimension of V, denoted by $\dim_F V$ or simply $\dim V$. ♣

Lemma 4.2

Let $\{s_1, ..., s_n\}$ be a generating set for an F-vector space V. If $m > n$, then any collection of m vectors $v_1, ..., v_m \in V$ is linearly dependent. ♡

4.5 Linear mappings

Definition 4.9 (Linear Mapping)

Let V and W be F-vector spaces. A mapping $T : V \to W$ is called a linear mapping (also known as a linear transformation or linear operator) if it satisfies:

$$T(v_1 + v_2) = T(v_1) + T(v_2), \qquad \forall v_1, v_2 \in V,$$
$$T(tv) = tT(v), \qquad \forall t \in F, v \in V.$$
♣

Lemma 4.3

If $T : U \to V$ and $S : V \to W$ are linear mappings, then their composition $S \circ T : U \to W$ is also a linear mapping. ♡

Proof We need to verify that $S \circ T$ satisfies the two defining properties of linear mappings:

1. For any $u_1, u_2 \in U$:

$$
\begin{aligned}
(S \circ T)(u_1 + u_2) &= S(T(u_1 + u_2)) \\
&= S(T(u_1) + T(u_2)) \quad \text{(by linearity of } T\text{)} \\
&= S(T(u_1)) + S(T(u_2)) \quad \text{(by linearity of } S\text{)} \\
&= (S \circ T)(u_1) + (S \circ T)(u_2)
\end{aligned}
$$

2. For any $t \in F$ and $u \in U$:

$$
\begin{aligned}
(S \circ T)(tu) &= S(T(tu)) \\
&= S(tT(u)) \quad \text{(by linearity of } T\text{)} \\
&= tS(T(u)) \quad \text{(by linearity of } S\text{)} \\
&= t(S \circ T)(u)
\end{aligned}
$$

Therefore, $S \circ T$ is a linear mapping. □

Definition 4.10

If a linear mapping $T : V \to W$ is both left and right invertible, it is called an invertible linear mapping or an isomorphism.

In this case, there exists a unique linear mapping $T^{-1} : W \to V$ such that $T^{-1} \circ T = \mathrm{id}_V$ and $T \circ T^{-1} = \mathrm{id}_W$. This mapping T^{-1} is called the inverse of T; it is simultaneously the unique left inverse and the unique right inverse of T. ♣

Definition 4.11

Let V and W be F-vector spaces. Define $\mathrm{Hom}(V, W)$ as the set of all linear mappings from V to W. Addition and scalar multiplication are defined by:

$$
\begin{aligned}
(T_1 + T_2)(v) &= T_1(v) + T_2(v) \\
(tT)(v) &= t \cdot T(v)
\end{aligned}
$$

The zero element of $\mathrm{Hom}(V, W)$ is the zero mapping $0 : V \to W$. ♣

4.6 Linear mappings to Matrix

Definition 4.12

Let V be an F-vector space. We denote $\mathrm{End}(V) := \mathrm{Hom}(V, V)$, whose elements are called endomorphisms of V. ♣

Corollary 4.1

Let V be an F-vector space. Then $\mathrm{End}(V)$ forms a ring where addition is the addition of linear maps, and multiplication is the composition of linear maps $(S, T) \mapsto ST$. The zero element is the zero mapping, and the multiplicative identity is the identity mapping id_V. Moreover, $\mathrm{End}(V)$ is the zero ring if and only if $V = \{0\}$. ♡

Theorem 4.1

Let V and W be finite-dimensional vector spaces with ordered bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_m$ respectively, where $n, m \in \mathbb{Z}_{\geq 1}$. Then there exists a vector space isomorphism:

$$\mathcal{M} : \operatorname{Hom}(V, W) \xrightarrow{1:1} M_{m \times n}(F)$$

mapping $T \mapsto (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$, where $(a_{ij})_{i,j} = \mathcal{M}(T)$ is characterized by the property:

$$T(v_j) = \sum_{i=1}^{m} a_{ij} w_i, \quad 1 \leq j \leq n.$$

Consequently, $\dim \operatorname{Hom}(V, W) = \dim V \cdot \dim W$.

♡

Theorem 4.2

Let U, V, and W be finite-dimensional vector spaces with ordered bases $u_1, \ldots, u_r$, $v_1, \ldots, v_n$, and $w_1, \ldots, w_m$ respectively. The following diagram commutes:

$$\begin{tikzcd}
\operatorname{Hom}(V, W) \times \operatorname{Hom}(U, V) \arrow[r, "\text{Map composition}"] \arrow[d, "M \times M"'] & \operatorname{Hom}(U, W) \arrow[d, "M"] \\
M_{m \times n}(F) \times M_{n \times r}(F) \arrow[r, "\text{Matrix multiplication}"'] & M_{m \times r}(F)
\end{tikzcd}$$

In other words, $M(S \circ T) = M(S) \cdot M(T)$, where the left side represents composition of maps and the right side represents matrix multiplication.

♡

Definition 4.13

A matrix $A \in M_{m \times n}(F)$ is called left invertible (or right invertible) if there exists $B \in M_{n \times m}(F)$ such that $BA = 1_{n \times n}$ (or $AB = 1_{m \times m}$). Such a matrix B is called a left inverse (or right inverse) of A.
If $m = n$ and A is both left and right invertible, then A is called an invertible $n \times n$ matrix. In this case, there exists a unique matrix $A^{-1} \in M_{n \times n}(F)$ such that $A^{-1}A = 1_{n \times n} = AA^{-1}$. This matrix A^{-1} serves simultaneously as both the unique left inverse and the unique right inverse of A.
In other words, invertible matrices are precisely the invertible elements in the ring $M_{m \times m}(F)$.

♣

4.7 Transpose of a Matrix and Dual Spaces

Definition 4.14

Let R be a ring. For any $A = (a_{ij}) \in M_{m \times n}(R)$, the transpose of A, denoted ${}^tA$, is the $n \times m$ matrix (a_{ji}). That is,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \implies {}^tA = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

♣

Proposition 4.5

Let $A \in M_{m\times m}(F)$. Then A is invertible if and only if ${}^tA$ is invertible. Moreover, in this case,

$$({}^tA)^{-1} = {}^t(A^{-1}).$$

Proof Suppose A is invertible, so $A^{-1}A = AA^{-1} = I$. Taking transposes, $({}^tA^{-1})({}^tA) = {}^t(AA^{-1}) = {}^tI = I$, and $({}^tA)({}^tA^{-1}) = {}^t(A^{-1}A) = I$. Thus, ${}^tA$ is invertible and $({}^tA)^{-1} = {}^t(A^{-1})$.

Conversely, if ${}^tA$ is invertible, the same argument applied to ${}^tA$ shows A is invertible. □

Definition 4.15

Let V be a vector space over a field F. The dual space of V, denoted $V^\vee$, is defined as

$$V^\vee := \mathrm{Hom}(V, F),$$

the set of all linear functionals from V to F.

Definition 4.16

Let $T : V \to W$ be a linear map between vector spaces over F. The transpose (dual) map of T, denoted ${}^tT : W^\vee \to V^\vee$, is defined by

$${}^tT(\lambda) = \lambda \circ T, \quad \forall \lambda \in W^\vee.$$

That is, for any $v \in V$,

$$({}^tT(\lambda))(v) = \lambda(T(v)).$$

Proposition 4.6

Let U, V, W be vector spaces over F, and let $T : U \to V$, $S : V \to W$ be linear maps. Then

$${}^t(ST) = {}^tT \circ {}^tS \in \mathrm{Hom}(W^\vee, U^\vee).$$

Proof For any $\lambda \in W^\vee$ and $u \in U$,

$$({}^t(ST)(\lambda))(u) = \lambda((ST)(u)) = \lambda(S(T(u))) = ({}^tS(\lambda))(T(u)) = ({}^tT({}^tS(\lambda)))(u).$$

Thus, ${}^t(ST) = {}^tT \circ {}^tS$. □

Proposition 4.7

Let V be a finite-dimensional vector space with basis $v_1, \ldots, v_n$. For each $1 \le i \le n$, define $\check{v}_i \in V^\vee$ by

$$\check{v}_i\left(\sum_{j=1}^n x_j v_j\right) = x_i.$$

Then $\check{v}_1, \ldots, \check{v}_n$ form a basis of $V^\vee$, called the dual basis of $v_1, \ldots, v_n$.

Proof Each $\check{v}_i$ is linear, and for any v_j we have $\check{v}_i(v_j) = \delta_{ij}$. Any $f \in V^\vee$ is determined by its values $f(v_j)$, so $f = \sum_{i=1}^n f(v_i)\check{v}_i$. Thus, $\{\check{v}_1, \ldots, \check{v}_n\}$ is a basis for $V^\vee$. □

4.8 Kernel, Image, and Gaussian Elimination

Definition 4.17

*Let $T : V \to W$ be a linear map between vector spaces. The **kernel** of T is*

$$\ker T := \{v \in V : T(v) = 0\} = T^{-1}(0).$$

*The **image** of T is*

$$\operatorname{im} T := \{w \in W : \exists v \in V,\, T(v) = w\}.$$

Proposition 4.8

Let $T : V \to W$ be a linear map. Then $\ker T$ is a subspace of V, and $\operatorname{im} T$ is a subspace of W.

Proof For $\ker T$: Let $u, v \in \ker T$ and $a, b \in F$. Then $T(au + bv) = aT(u) + bT(v) = a \cdot 0 + b \cdot 0 = 0$, so $au + bv \in \ker T$. Thus, $\ker T$ is a subspace of V.

For $\operatorname{im} T$: Let $w_1, w_2 \in \operatorname{im} T$, so $w_1 = T(v_1)$, $w_2 = T(v_2)$ for some $v_1, v_2 \in V$. For $a, b \in F$, $aw_1 + bw_2 = aT(v_1) + bT(v_2) = T(av_1 + bv_2) \in \operatorname{im} T$. Thus, $\operatorname{im} T$ is a subspace of W. □

Proposition 4.9

A linear map $T : V \to W$ is injective if and only if $\ker T = \{0\}$.

Theorem 4.3

Let $T : V \to W$ be a linear map between vector spaces, with V finite-dimensional. Then

$$\dim V = \dim(\ker T) + \dim(\operatorname{im} T).$$

Definition 4.18 (Rank)

*Let $T : V \to W$ be a linear map between finite-dimensional vector spaces. The **rank** of T, denoted $\operatorname{rk}(T)$, is defined as*

$$\operatorname{rk}(T) := \dim(\operatorname{im} T).$$

For a matrix $A \in M_{m\times n}(F)$, the rank $\operatorname{rk}(A)$ is defined as the rank of the associated linear map $T_A : F^n \to F^m$.

Proposition 4.10

Let $A' \in M_{m\times n}(F)$ be the row echelon form of $A \in M_{m\times n}(F)$ obtained by elementary row operations. Then the rank of A, $\operatorname{rk}(A)$, equals the number r of pivots (leading ones) in A'.

Proof Elementary row operations do not change the row space of A, so $\operatorname{rk}(A) = \operatorname{rk}(A')$. In row echelon form, the number of pivots equals the dimension of the row (or column) space, which is the rank. □

Proposition 4.11

Let $A \in M_{m\times m}(F)$. The following statements are equivalent:

(i) A is invertible;

(ii) For any column vector $v \in F^m$, $Av = 0$ if and only if $v = 0$;

(iii) $\operatorname{rk}(A) = m$;

(iv) A can be written as a product of elementary matrices.

Therefore, $A \in M_{m\times m}(F)$ is invertible if and only if it is left invertible, if and only if it is right invertible.

Proof (i) $\Rightarrow$ (ii): If A is invertible and $Av = 0$, then $v = A^{-1}Av = A^{-1}0 = 0$.

(ii) $\Rightarrow$ (iii): If $Av = 0$ only for $v = 0$, the columns of A are linearly independent, so $\mathrm{rk}(A) = m$.

(iii) $\Rightarrow$ (iv): If $\mathrm{rk}(A) = m$, A can be reduced to the identity matrix by elementary row operations, so A is a product of elementary matrices.

(iv) $\Rightarrow$ (i): Elementary matrices are invertible, so their product A is invertible.

The equivalence of left and right invertibility for square matrices follows from these properties. $\square$

4.9 Change of Basis: Matrix Conjugation and Equivalence

Lemma 4.4

The map $P_{\mathbf{v}}^{\mathbf{v}'} : F^n \to F^n$ defined by change of basis from $\mathbf{v}$ to $\mathbf{v}'$ is a vector space automorphism of F^n. Its inverse is $P_{\mathbf{v}'}^{\mathbf{v}}$.

Proof By definition, $P_{\mathbf{v}}^{\mathbf{v}'}$ is invertible, with $P_{\mathbf{v}'}^{\mathbf{v}}$ as its inverse, since changing from basis $\mathbf{v}$ to $\mathbf{v}'$ and then back recovers the original coordinates. Thus, $P_{\mathbf{v}}^{\mathbf{v}'}$ is an automorphism. $\square$

Theorem 4.4

Let V and W be finite-dimensional vector spaces with ordered bases $\mathbf{v}, \mathbf{v}'$ for V and $\mathbf{w}, \mathbf{w}'$ for W. For any $T \in \mathrm{Hom}(V, W)$, we have

$$\mathcal{M}_{\mathbf{w}'}^{\mathbf{v}'}(T) = P_{\mathbf{w}}^{\mathbf{w}'}\,\mathcal{M}_{\mathbf{w}}^{\mathbf{v}}(T)\,P_{\mathbf{v}}^{\mathbf{v}'} = (P_{\mathbf{w}'}^{\mathbf{w}})^{-1}\mathcal{M}_{\mathbf{w}}^{\mathbf{v}}(T)P_{\mathbf{v}}^{\mathbf{v}'}.$$

Definition 4.19 (Matrix Conjugation (Similarity))

Let $\mathbf{A}, \mathbf{B} \in M_{n\times n}(F)$. If there exists an invertible matrix $P \in M_{n\times n}(F)$ such that

$$\mathbf{B} = P^{-1}\mathbf{A}P,$$

*then $\mathbf{A}$ and $\mathbf{B}$ are called **conjugate** or **similar** matrices.*

Proposition 4.12

Conjugation is an equivalence relation on $M_{n\times n}(F)$.

Definition 4.20 (Matrix Equivalence)

*Matrices $A, B \in M_{m\times n}(F)$ are called **equivalent** if there exist invertible matrices $Q \in M_{m\times m}(F)$ and $P \in M_{n\times n}(F)$ such that*

$$B = QAP.$$

Proposition 4.13

Two matrices $A, B \in M_{m\times n}(F)$ are equivalent if and only if $\mathrm{rk}(A) = \mathrm{rk}(B)$.

Theorem 4.5

For any matrix $A \in M_{m\times n}(F)$, the row rank of A equals the column rank of A.

Definition 4.21

*A matrix $A \in M_{m\times n}(F)$ is called **full rank** if* $\operatorname{rk}(A) = \min\{m, n\}$.

4.10 Direct Sum Decomposition

Definition 4.22

Let V be a vector space over a field F, and let $(V_i)_{i\in I}$ be a family of subspaces of V. The sum of these subspaces is defined as

$$\sum_{i\in I} V_i := \left\{ \sum_{i\in I} v_i \in V : v_i \in V_i, \text{ and only finitely many } v_i \neq 0 \right\}.$$

For finitely many subspaces, we write $V_1 + \cdots + V_n$ for their sum. By convention, the sum over the empty index set $I = \emptyset$ is the zero subspace $\{0\}$.

Proposition 4.14

Let $(V_i)_{i\in I}$ be a family of subspaces of an F-vector space V, with $I \neq \emptyset$. If for every $i \in I$,

$$V_i \cap \sum_{j\neq i} V_j = \{0\},$$

*then we denote $\sum_{i\in I} V_i$ by $\bigoplus_{i\in I} V_i$, called the (internal) **direct sum** of $(V_i)_{i\in I}$, and each V_i is called a **direct summand**.*

This condition holds if and only if the canonical map from the external direct sum $\bigoplus_{i\in I} V_i$ to $\sum_{i\in I} V_i$ is an isomorphism.

Proposition 4.15

Let V be a vector space over a field F, and $V_0 \subset V$ any subspace. Then there exists a subspace $V_1 \subset V$ such that

$$V = V_0 \oplus V_1.$$

Proof Let $\{v_1, \ldots, v_k\}$ be a basis for V_0. Extend this to a basis $\{v_1, \ldots, v_k, w_1, \ldots, w_m\}$ for V. Let $V_1 = \operatorname{span}\{w_1, \ldots, w_m\}$. Then every $v \in V$ can be uniquely written as $v = v_0 + v_1$ with $v_0 \in V_0$, $v_1 \in V_1$, so $V = V_0 \oplus V_1$. □

4.11 Block Matrix Operations

Definition 4.23

Let $T : V \to W$ be a linear map, where $V = V_1 \oplus \cdots \oplus V_n$ and $W = W_1 \oplus \cdots \oplus W_m$ are direct sum decompositions. The matrix $A := M(T)$, with respect to these decompositions, can be partitioned into $m \times n$ blocks as follows:

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mn} \end{pmatrix}$$

where $A_{ij} := M(T_{ij})$ is the matrix of the component map $T_{ij} : V_j \to W_i$.

*A matrix A with such a partition is called a **block matrix**, and each A_{ij} is called its (i,j)-block.* ♣

Let V be a vector space over F and U a subspace. For any $v \in V$, the equivalence class of v modulo U is denoted by

$$v + U := \{v + u : u \in U\}.$$

Such subsets are called **cosets** of U in V, and v is called a representative of the coset. We have $v + U = v' + U$ if and only if $v - v' \in U$.

4.12 Quotient Spaces

Definition 4.24 (Quotient Space)

*Let U be a subspace of an F-vector space V. Define the **quotient space***

$$V/U := \{v + U : v \in V\}$$

as the set of all cosets of U in V.

On V/U, define the following operations:

- *Addition: $(v_1 + U) + (v_2 + U) := (v_1 + v_2) + U$, for $v_1, v_2 \in V$;*
- *Scalar multiplication: $t(v + U) := (tv) + U$, for $t \in F$, $v \in V$;*
- *Zero element: $0_{V/U} := U = 0_V + U$ (the coset of 0).*

*With these operations, $(V/U, +, \cdot, 0_{V/U})$ is a vector space over F, called the **quotient space** of V by U.* ♣

Definition 4.25 (Cokernel)

*Let $T : V \to W$ be a linear map. The **cokernel** of T is defined as the quotient space of W by the image of T:*

$$\operatorname{coker}(T) := W/\operatorname{im}(T).$$

♣

Proposition 4.16

A linear map $T : V \to W$ is surjective if and only if $\operatorname{coker}(T) = \{0\}$. ♠

Proof If T is surjective, then $\operatorname{im}(T) = W$, so $W/\operatorname{im}(T) = W/W = \{0\}$.

Conversely, if $\operatorname{coker}(T) = \{0\}$, then $W/\operatorname{im}(T) = \{0\}$, so $\operatorname{im}(T) = W$, i.e., T is surjective. □

Proposition 4.17

Let U be a subspace of a vector space V, and let $T : V \to W$ be a linear map.

(i) If $U \subset \ker(T)$, then there exists a unique linear map $\overline{T} : V/U \to W$ such that the following diagram commutes:

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "q"'] & W \\ V/U \arrow[ur, dashed, "\overline{T}"'] & \end{tikzcd}$$

where $q : V \to V/U$ is the quotient map. Explicitly, $\overline{T}(v + U) = T(v)$.

(ii) If $U = \ker(T)$ and $W = \operatorname{im}(T)$, then $\overline{T} : V/U \to W$ is an isomorphism of vector spaces. ♠

Proof (i) If $U \subset \ker(T)$, then $T(v) = T(v')$ whenever $v - v' \in U$, so T is constant on cosets $v + U$. Thus, $\overline{T}(v + U) := T(v)$ is well-defined and linear. Uniqueness follows since q is surjective.

(ii) If $U = \ker(T)$ and $W = \operatorname{im}(T)$, then $\overline{T}$ is injective (since $\ker(\overline{T}) = \{U\}$) and surjective (since T is surjective onto W), so it is an isomorphism. □

Proposition 4.18

Let U be a subspace of V. Let $\overline{V} := V/U$, and let $q : V \to \overline{V}$ be the quotient map. There is a bijection

$$\{W \subset V : W \text{ is a subspace}, W \supset U\} \longleftrightarrow \{\overline{W} \subset \overline{V} : \overline{W} \text{ is a subspace}\}$$

given by $W \mapsto \overline{W} := q(W)$ and $\overline{W} \mapsto W := q^{-1}(\overline{W})$.

This bijection has the following properties:

- *It is strictly order-preserving: $W_1 \supset W_2$ if and only if $\overline{W}_1 \supset \overline{W}_2$.*
- *If W corresponds to $\overline{W}$, then there is a natural isomorphism*

$$V/W \cong \overline{V}/\overline{W}, \quad v + W \mapsto q(v) + \overline{W}.$$

If we write $\overline{W} = W/U$, this isomorphism can be viewed as

$$V/W \cong (V/U)/(W/U).$$

Proposition 4.19

Let V, W be subspaces of a vector space. Then there is a natural isomorphism

$$V/(V \cap W) \cong (V + W)/W$$

given by $v + (V \cap W) \mapsto v + W$ for $v \in V$.

Chapter 5 Determinant

5.1 Permutations Introduction

Definition 5.1

Let X be a non-empty set. The set of permutations on X is defined as

$$S_X := \{\text{ bijections } \sigma : X \to X \}.$$

It contains the identity mapping $\mathrm{id} = \mathrm{id}_X \in S_X$. These permutations can be composed as functions, $(\sigma, \sigma') \mapsto \sigma\sigma'$, or inverted, $\sigma \mapsto \sigma^{-1}$, and the result still belongs to S_X. ♣

Definition 5.2

Fix $n \in \mathbb{Z}_{\geq 1}$. For $1 \leq i \neq j \leq n$, the corresponding transposition $(i\ j) \in S_n$ is defined as the following permutation:

$$(i\ j) : \quad k \mapsto \begin{cases} j, & \text{if } k = i, \\ i, & \text{if } k = j, \\ k, & \text{if } k \neq i, j. \end{cases}$$

In other words, $(i\ j)$ swaps i and j, and leaves all other elements unchanged. ♣

Definition 5.3

Let $\sigma \in S_n$. The elements of the following set are called the inversions of σ:

$$\mathrm{Inv}_\sigma := \{ (i, j) \in \mathbb{Z}^2 : 1 \leq i < j \leq n,\ \sigma(i) > \sigma(j) \}.$$

The number of inversions of σ is defined as $\ell(\sigma) := |\, \mathrm{Inv}_\sigma \,|$. ♣

Proposition 5.1

Let $\sigma \in S_n$. Then there exists $\ell \in \mathbb{Z}_{\geq 0}$ and a sequence of transpositions $\tau_1, \ldots, \tau_\ell \in S_n$ such that

$$\sigma = \tau_1 \cdots \tau_\ell;$$

when $\ell = 0$, the product on the right is understood as the identity id. We call ℓ the length of the above decomposition. Among all decompositions of σ into transpositions, the minimal possible length is $\ell(\sigma)$. ♠

Proposition 5.2

There exists a unique map $\mathrm{sgn} : S_n \to \{\pm 1\}$ such that the following properties hold:

(i) For all $\sigma, \xi \in S_n$, we have $\mathrm{sgn}(\sigma\xi) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\xi)$,

(ii) If $\tau \in S_n$ is a transposition, then $\mathrm{sgn}(\tau) = -1$.

The above map sgn satisfies $\mathrm{sgn}(\mathrm{id}) = 1$ and $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1} = \mathrm{sgn}(\sigma)$. Its value can further be expressed in terms of the number of inversions as

$$\mathrm{sgn}(\sigma) = (-1)^{\ell(\sigma)}.$$

♠

Definition 5.4

Let $\sigma \in S_n$. If there exists a sequence of transpositions $\tau_1, \ldots, \tau_\ell$ such that $\sigma = \tau_1 \cdots \tau_\ell$, where $\ell \in \mathbb{Z}_{\geq 0}$ is even (respectively, odd), then σ is called an even permutation *(respectively,* odd permutation*).* ♣