Modern Mathematics

- A Journey from Concretization to Abstraction -

Ji, Yong-Hyeon

A document presented for
the Modern Mathematics

Department of Information Security, Cryptology, and Mathematics
College of Science and Technology
Kookmin University

July 1, 2024

Contents

Chapter 1

Introduction

1.1 Axiom

Chapter 2

Quadratic Formula and Peano Axiom

2.1 Quadratic Formula

Note. We want to find the roots of the quadratic equation: for $a \neq 0$,

$$ax^2 + bx + c = 0.$$

Sol.

$$\begin{aligned}
ax^2 + bx + c = 0 &\iff ax^2 + bx = -c \\
&\iff x^2 + \frac{b}{a}x = -\frac{c}{a} && \text{Divide every term by } a \neq 0 \\
&\iff x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 = -\frac{c}{a} && \text{Complete the square on the left side} \\
&\iff \left(x + \frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
&\iff x + \frac{b}{2a} = \pm\sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}} && \text{Take the square root on both sides} \\
&\iff x = -\frac{b}{2a} \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}} && \text{Simplify to solve for } x \\
&\iff x = -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \\
&\iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} && \text{Quadratic formula}
\end{aligned}$$

This expression provides the solutions for x in the quadratic equation $ax^2+bx+c = 0\,(a \neq 0)$. □

2.2 Peano Axiom and Natural Number

2.2.1 Peano Axiom and Successor Function

The set of natural numbers, denoted by $\mathbb{N}$, is defined by the following axioms:

1. **Zero is a natural number**: $0 \in \mathbb{N}$.

   There exists a natural number 0.

2. **Successor**: $n \in \mathbb{N} \implies S(n) \in \mathbb{N}$.

   For every natural number n, there exists a natural number $S(n)$, called the successor of n.

   (i) (✓) $0 \longrightarrow S(0) \longrightarrow S(S(0)) \longrightarrow \cdots$

   (ii) (×) $k \in \mathbb{N} \longrightarrow S(k) = 0 \longrightarrow S0 \longrightarrow SS0 \longrightarrow \cdots$

   (iii) (×)

$$\begin{tikzcd}
0 \arrow[r] & S0 \arrow[r] & SS0 \arrow[d] \\
 & SSSS0 \arrow[u] & SSS0 \arrow[l]
\end{tikzcd}$$

   (iv) (×)

$$\begin{tikzcd}
0 \arrow[r] & S0 \arrow[r] & SS0 \arrow[r] & SSS0 \\
 & & S(k) \arrow[u] & \\
 & & k \in \mathbb{N} \arrow[u] &
\end{tikzcd}$$

   (v) (×)

$$\begin{tikzcd}
0 \arrow[r] & S0 \arrow[r] & SS0 \arrow[r] & SSS0 \arrow[r] & SSSS0
\end{tikzcd}$$

$$k \in \mathbb{N}$$

3. **No natural number has 0 as its successor**: $n \in \mathbb{N} \implies S(n) \neq 0$.

   There is no natural number whose successor is 0. (It solves 2-(ii))

4. **Distinctness**: $\forall m, n \in \mathbb{N} : [S(m) = S(n) \implies m = n]$.Define addition to the set of natural numbers and define integers based on the concepts of identity and inverse. Also define rational numbers based on the multiplication of integers. In this way, derive the group structure and define the group. Give me the ratex code to be a professional mathematician.

   Distinct natural numbers have distinct successors. (It solves 2-(iii) and (iv))

5. Induction: $(0 \in M) \wedge (n \in M \Rightarrow S(n) \in M) \implies \mathbb{N} \subseteq M$

If a set M of natural numbers contains 0 and is closed under the successor function (i.e., $n \in M \implies S(n) \in M$), then M contains all natural numbers. (It solves 2-(v))

Remark 2.0.1 (**Successor Function $S(n)$**).
The successor function $S(n)$ can be understood through these principles:

1. **Uniqueness and Existence**: For each natural number n, there exists a unique natural number $S(n)$. This means $S(n)$ is well-defined and there is no ambiguity about what the successor of n is.

2. **Construction of Natural Numbers**: The successor function constructs the sequence of natural numbers starting from 0. For example:

$$S(0) = 1, \quad S(1) = 2, \quad S(2) = 3, \quad \text{and so on.}$$

   Here, 1 is the successor of 0, 2 is the successor of 1, and so forth. Each natural number n can be reached by repeatedly applying the successor function starting from 0.

3. **Non-circularity** No natural number n has 0 as its successor. This avoids circular definitions and ensures a clear progression of numbers:

$$\forall n \in \mathbb{N} : S(n) \neq 0.$$

4. **Injectivity**: The axiom $S(m) = S(n) \implies m = n$ ensures that the successor function is injective, meaning different numbers have different successors. This property is essential for maintaining the distinctness of natural numbers.

5. **Basis of Induction**: The induction axiom relies on the successor function. It states that if a property holds for 0 and holds for $S(n)$ whenever it holds for n, then the property holds for all natural numbers. This principle is the foundation of mathematical induction.

A visual representation of the successor function can help understand its role:

$$0 \xrightarrow{S} 1 \xrightarrow{S} 2 \xrightarrow{S} 3 \xrightarrow{S} 4 \xrightarrow{S} \cdots$$

Each arrow represents the application of the successor function, moving from one natural number to the next.

In summary, the successor function $S(n)$ in Peano's axioms is a fundamental operation that:

- Provides a way to generate the next natural number from a given one.
- Ensures the natural numbers are distinct and ordered.
- erves as the basis for defining natural numbers and performing induction.

These properties make the successor function an essential component in the foundation of arithmetic and number theory.

2.3 Group Structure

2.3.1 Addition and Multiplication on Natural Numbers

Observation.

- $1 + 1 = 2$
- $(-1) \times (-1) = 1$

Addition on Natural Numbers

Addition on the set of natural numbers $\mathbb{N}$ is defined recursively:

- **(Base Case)**
$$n \in \mathbb{N} \implies 0 + n = n.$$
- **(Recursive Step)**
$$m, n \in \mathbb{N} \implies S(m) + n = S(m + n).$$

Remark 2.0.2.

$$\begin{aligned} 1 &= S0 & \\ 2 &= SS0 & &= S^2 0 \\ 3 &= SSS0 & &= S^3 0 \\ &\vdots & \\ n &= \underbrace{S \cdots S}_{n} 0 & &= S^n 0 \end{aligned}$$

Example 2.1. Prove that $1 + 1 = 2$.

Proof. Consider $1 = S(0)$. Then

$$1 + 1 = S(0) + S(0) = S(S(0) + 0) = S(S0) = 2.$$

□

Multiplication on Natural Numbers

Multiplication on the set of natural numbers $\mathbb{N}$ is defined recursively:

- **(Base Case)**
$$n \in \mathbb{N} \implies 0 \cdot n = n.$$
- **(Recursive Step)**
$$m, n \in \mathbb{N} \implies S(m) \cdot n = (m \cdot n) + n.$$

Example 2.2. Prove that $n \times 1 = n$ for all $n \in \mathbb{N}$.

Proof. Consider $n, 1 \in \mathbb{N}$, i.e., $n = S^n 0$, $1 = S0$. Then

$$\begin{aligned} n \times 1 = S^n 0 \times S0 &= S(S^{n-1}0) \times S0 \\ &= (S^{n-1}0 \times S0) + S0 \\ &= (S^{n-2}0 \times S0) + (S0 + S0) \\ &= (0 \times S0) + (\underbrace{S0 + S0 + \cdots + S0}_{n}) \\ &= 0 + n \\ &= n. \end{aligned}$$

□

Construction of Integer

The set of integers $\mathbb{Z}$ includes identity and inverse elements.

- **Identity**: $\forall a \in \mathbb{Z},\ a + 0 = a$
- **Inverses**: $\forall n \in \mathbb{N},\ \exists - n \in \mathbb{Z}$ such that $n + (-n) = 0$

Formally, the set of integers $\mathbb{Z}$ is:

$$\begin{aligned} \mathbb{Z} &= -\mathbb{N} \cup \{0\} \cup \mathbb{N} \\ &= \{-1, -2, -3, \dots\} \cup \{0\} \cup \{1, 2, 3, \dots\} \\ &= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}. \end{aligned}$$

Example 2.3. Prove that $(-1) \times (-1) = 1$.

Proof.

$$\begin{aligned} 0 &= 0 \times (-1) \\ &= S(-1) \times (-1) \\ &= ((-1) \times (-1)) + (-1). \end{aligned}$$

Thus, $(-1) \times (-1) = 1$. □

2.3.2 Rational Number and Equivalence Relation

Observation.

- $\frac{1}{2} = 0.5$
- $\frac{1}{2} = \frac{2}{4} = \cdots = \frac{1622660}{3245320}$

Rational Numbers

A rational number $\mathbb{Q}$ is defined as an ordered pair of integers (a, b) where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$. This pair represents the fraction $\frac{a}{b}$.

Note. We introduce an equivalence relation on the set of pairs of integers:

$$(a,b) \sim (c,d) \iff ad = bc$$

This relation ensures that different pairs of integers representing the same rational number are considered equivalent.

The set of rational numbers $\mathbb{Q}$ is the set of equivalence classes of the pairs (a,b):

$$\mathbb{Q} = \left\{ \frac{a}{b} \,\middle|\, a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}, (a,b) \sim (c,d) \iff ad = bc \right\}$$

2.3.3 Groups

Observation.

$(\mathbb{Z},+)$

- $\forall a,b \in \mathbb{Z},\ a+b \in \mathbb{Z}$
- $\forall a,b,c \in \mathbb{Z},\ (a+b)+c = a+(b+c)$
- $\exists 0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z},\ a+0 = a$
- $\forall a \in \mathbb{Z},\ \exists -a \in \mathbb{Z}$ such that $a+(-a) = 0$

$(\mathbb{Q}^*,\cdot)$

- $\forall a,b \in \mathbb{Q}^*,\ a \cdot b \in \mathbb{Q}^*$
- $\forall a,b,c \in \mathbb{Q}^*,\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$
- $\exists 1 \in \mathbb{Q}^*$ such that $\forall a \in \mathbb{Q}^*,\ a \cdot 1 = a$
- $\forall a \in \mathbb{Q}^*,\ \exists a^{-1} \in \mathbb{Q}^*$ such that $a \cdot a^{-1} = 1$

Group

Definition 2.1. A **group** is a set G equipped with a binary operation $* : G \times G \to G$ that combines any two elements a and b to form another element denoted $a * b$. The set and operation, $(G,*)$, must satisfy four fundamental properties known as the group axioms:

1. **Closure**:
$$a,b \in G \implies a*b \in G$$
2. **Associativity**:
$$a,b,c \in G \implies (a*b)\cdot c = a*(b*c)$$
3. **Identity Element**:
$$\exists e \in G : [a \in G \implies e*a = a = a*e]$$
4. **Inverse Element**:
$$a \in G \implies [\exists a^{-1} \in G : a*a^{-1} = e = a^{-1}*a]$$

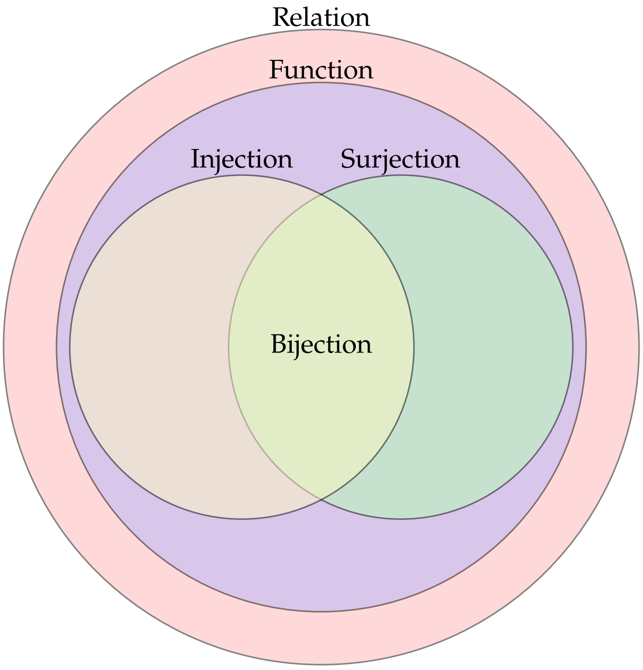
Chapter 3

Functions

Observation.

$$\begin{tikzcd}
 & \text{Relation} \arrow[d, bend right, "\text{Many-to-one}"'] \arrow[d, bend left, "\text{Left-Total}"] & \\
 & \text{Function} \arrow[dl, "\text{One-to-Many}"'] \arrow[dr, "\text{Right-Total}"] & \\
\text{Injection} \arrow[dr] & & \text{Surjection} \arrow[dl] \\
 & \text{Bijection} &
\end{tikzcd}$$

$$\begin{tikzcd}
 & f \subseteq S \times T \arrow[d, bend right, "\frac{s\ f\ t_1 \quad s\ f\ t_2}{t_1 = t_2}"'] \arrow[d, bend left, "\frac{s \in S}{\exists t \in T \text{ s.t. } s\ f\ t}"] & \\
 & S \xrightarrow{f} T \arrow[dl, "\frac{s_1\ f\ t \quad s_2\ f\ t}{s_1 = s_2}"'] \arrow[dr, "\frac{t \in T}{\exists s \in S \text{ s.t. } t\ f\ s}"] & \\
S \overset{f}{\rightarrowtail} T \arrow[dr] & & S \overset{f}{\twoheadrightarrow} T \arrow[dl] \\
 & S \overset{f}{\leftrightarrow} T &
\end{tikzcd}$$



3.1 Functions

Function

Definition 3.1. Let S and T be sets. A **function** f **from** S **to** T is a relation on $S \times T$ satisfying as follows:

(i) (**Left-Total**[a]) $\mathsf{Dom} f = S$, i.e.,

$$s \in S \implies \exists t \in T : f(s) = t.$$

(ii) (**Many-to-one**[b]) Let $s \in \mathsf{Dom} f$ and $t_1, t_2 \in \mathsf{Cdm} f$. Then

$$f(s) = t_1 \wedge f(s) = t_2 \implies s_1 = s_2.$$

[a] Every element of S relates to some element of T.
[b] Every element of $\mathsf{Dom} f$ relates to no more than one element of its $\mathsf{Cdm} f$.

Domain, Codomain, and Range

Definition 3.2.

- **Domain:** The domain of a function $f : A \to B$ is the set A of all possible input values for which the function is defined. Formally:

$$\text{Domain}(f) = A$$

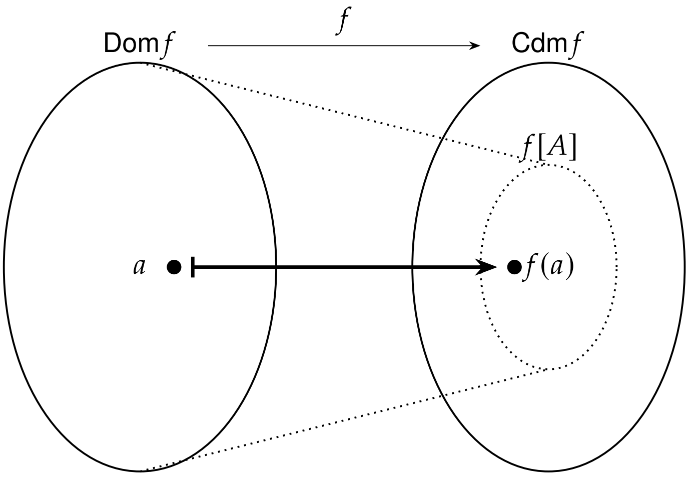
- **Co-domain:** The co-domain of a function $f : A \to B$ is the set B which includes all potential output values. It is the target set for the function. Formally:

$$\text{Co-domain}(f) = B$$

- **Range:** The range (or image) of a function f is the set of all actual output values produced by the function. It is a subset of the co-domain B. Formally:

$$\text{Range}(f) = f[A] = \{f(a) \mid a \in A\} \subseteq B$$

Remark 3.2.1.



3.2 Composition

Composition of Functions

Definition 3.3. Given two functions f and g, where $f : A \longrightarrow B$ and $g : B \longrightarrow C$, the **composition** of g and f, denoted by $g \circ f$, is a function from A to C defined as follows:

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$. That is,

$$\begin{array}{rcccl} g \circ f & : & A & \longrightarrow & C \\ & & a & \longmapsto & (g \circ f)(a) \end{array}$$

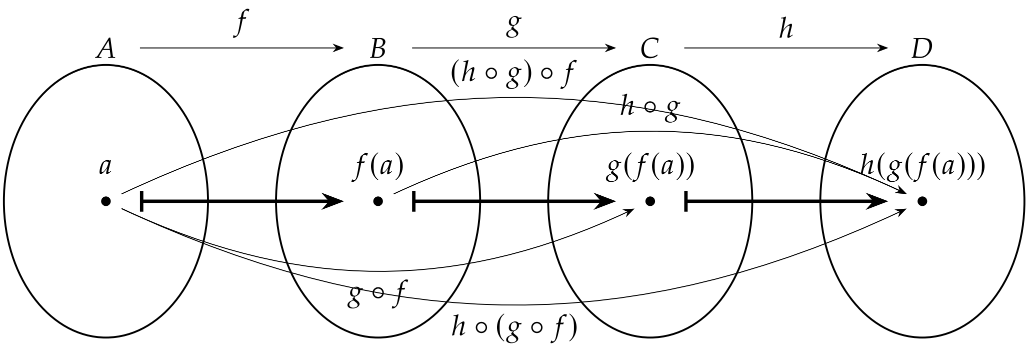
Remark 3.3.1.

- **Functions**:
  - Let $f : B \longrightarrow C$ be a function from set B to set C.
  - Let $g : A \longrightarrow B$ be a function from set A to set B.
- **Composition Definition**:
  - The composition $f \circ g$ is a function from A to C.
  - For each $x \in A$, $(f \circ g)(x)$ is defined as $f(g(x))$.
- **Domain and Range**:
  - The domain of the composite function $f \circ g$ is A.
  - The range of the composite function $f \circ g$ is a subset of C.

Remark 3.3.2. Let G be a set of bijective functions from a set X to itself. Define the binary operation $\circ$ to be the composition of functions. Then G under this operation is a group.

1. **Closure**: If $f, g \in G$, then $f \circ g \in G$ because the composition of two bijective functions is bijective.
2. **Associativity**: Function composition is associative. For any $f, g, h \in G$,

$$(f \circ g) \circ h = f \circ (g \circ h)$$



3. **Identity Element**: The identity function $\mathrm{id}_A : A \to A$, defined by $\mathrm{id}_A(a) = a$ for all $a \in A$, is the identity element in G. For any $f \in G$,

$$f \circ \mathrm{id}_A = f = \mathrm{id}_A \circ f$$

   $f \circ \mathrm{id}_A$:
   $\mathrm{id}_A \circ f$:
   f :

4. **Inverse Element**: For each $f \in G$, its inverse f^{-1} exists and is also a bijection from A to A. It satisfies

$$f \circ f^{-1} = \mathrm{id}_A = f^{-1} \circ f$$

3.3 Symmetric Group

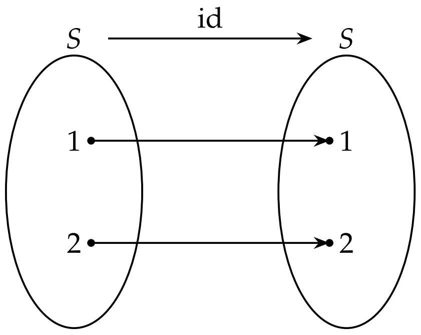
Exercise 3.1 (Symmetric Group S_2)**.** The **symmetric group** S_2 is the group of all permutations of a two-element set. For a set $X = \{1, 2\}$, the symmetric group S_2 consists of all bijective functions (permutations) from X to itself.

There are exactly two permutations of the set $S = \{1, 2\}$:

- **Identity Permutation** id:

$$\mathrm{id}(1) = 1, \quad \mathrm{id}(2) = 2$$

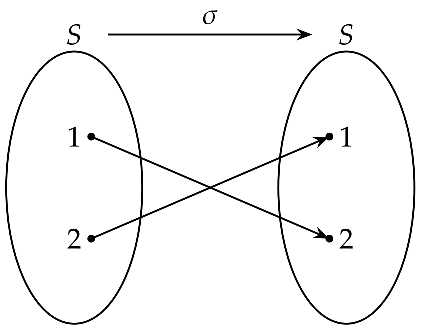
  This permutation leaves every element in its original position.



- **Transposition** σ:

$$\sigma(1) = 2, \quad \sigma(2) = 1$$

  This permutation swaps the two elements.



Therefore, the elements of S_2 can be written as:

$$S_2 = \{\mathrm{id}, \sigma\}$$

Exercise 3.2 (Symmetric Group S_3)**.** content...

Group Operation

The group operation in S_2 is the composition of permutations. Given two permutations f and g, their composition $f \circ g$ is defined as:

$$(f \circ g)(x) = f(g(x))$$

for all $x \in X$.

Group Table (Cayley Table)

The Cayley table for S_2 describes the result of composing any two permutations:

$\circ$	id	σ
id	id	σ
σ	σ	id

Group Axioms Verification

- **Closure**:
  - The composition of any two elements in S_2 is also an element of S_2.
- **Associativity**:
  - Function composition is associative. For all $f, g, h \in S_2$,

    $$(f \circ g) \circ h = f \circ (g \circ h)$$
- **Identity Element**:
  - The identity permutation id acts as the identity element. For all $f \in S_2$,

    $$f \circ \mathrm{id} = \mathrm{id} \circ f = f$$
- **Inverse Element**:
  - Each element in S_2 has an inverse in S_2. Specifically,

    $$\mathrm{id}^{-1} = \mathrm{id}, \quad \sigma^{-1} = \sigma$$

Chapter 4

Group Homomorphism

4.1 Exponentiation Function

Consider the following groups:

- The **additive group on integers** $(\mathbb{Z}, +)$:
  - Set: $\mathbb{Z}$
  - Operation: Addition $(+)$
  - Identity Element: 0
  - Inverses: For each $a \in \mathbb{Z}$, the inverse is $-a$.
- The **multiplicative group on nonzero rational numbers** $(\mathbb{Q}^*, \cdot)$:
  - Set: $\mathbb{Q}^*$
  - Operation: Multiplication $(\cdot)$
  - Identity Element: 1
  - Inverses: For each $q \in \mathbb{Q}^*$, the inverse is $q^{-1} = \frac{1}{q}$.

We define the exponential function $\exp : \mathbb{Z} \longrightarrow \mathbb{Q}^*$ by:

$$\exp(n) = 2^n \quad \text{for all } n \in \mathbb{Z}.$$

Verification

Homomorphism Property:

$$\exp(a + b) = 2^{a+b} = 2^a \cdot 2^b = \exp(a) \cdot \exp(b).$$

Identity Element:

- In $(\mathbb{Z}, +)$, the identity element is 0.
- In $(\mathbb{Q}^*, \cdot)$, the identity element is 1.

$$\exp(0) = 2^0 = 1.$$

Inverses:

- For each $n \in \mathbb{Z}$, the inverse of n in $\mathbb{Z}$ is $-n$.
- The inverse of $\exp(n) = 2^n$ in $\mathbb{Q}^*$ should be $\exp(-n) = 2^{-n}$.

$$\exp(-n) = 2^{-n} = \frac{1}{2^n} = (\exp(n))^{-1}.$$

Thus, the exponential function $\exp(n) = 2^n$ preserves the group structure between the additive group on integers $(\mathbb{Z}, +)$ and the multiplicative group on nonzero rational numbers $(\mathbb{Q}^*, \cdot)$.