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 7, 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) (×)

   $$\begin{array}{ccccc} 0 & \longrightarrow & S0 & \longrightarrow & SS0 \\ & & \uparrow & & \downarrow \\ & & SSSS0 & \longleftarrow & SSS0 \end{array}$$

   (iv) (×)

   $$\begin{array}{ccccccc} 0 & \longrightarrow & S0 & \longrightarrow & SS0 & \longrightarrow & SSS0 \\ & & & & \uparrow & & \\ & & & & S(k) & & \\ & & & & \uparrow & & \\ & & & & k \in \mathbb{N} & & \end{array}$$

   (v) (×)

   $$0 \longrightarrow S0 \longrightarrow SS0 \longrightarrow SSS0 \longrightarrow SSSS0$$

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

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

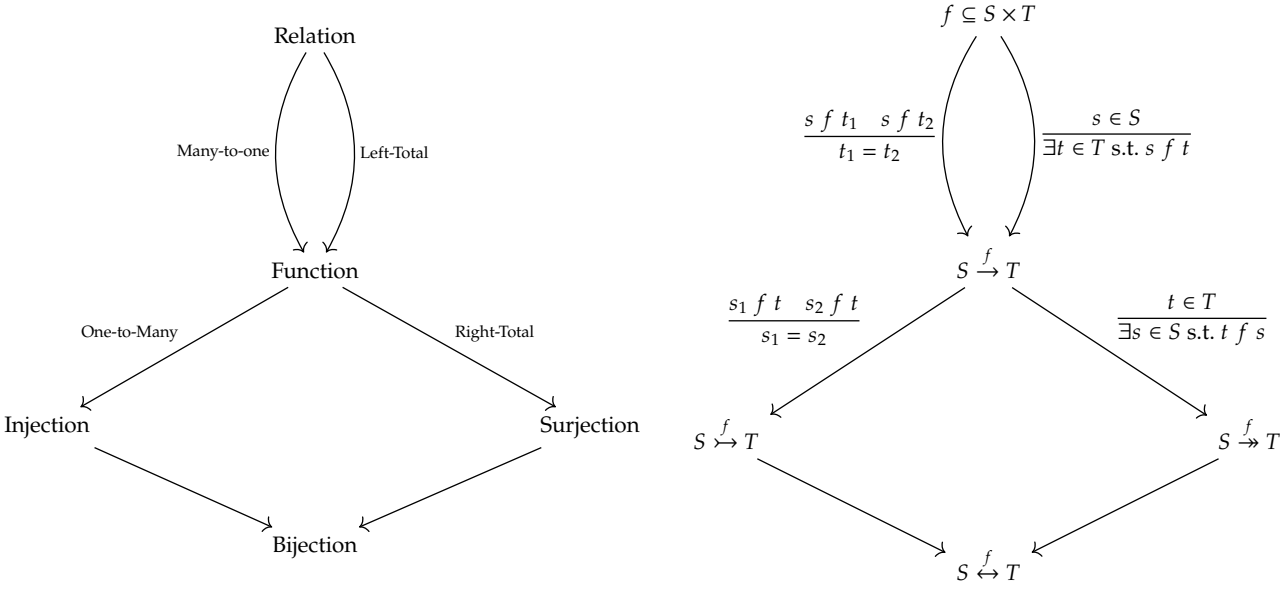
Definition 2.1. A **group** is a set G equipped with a binary operation $* : G \times G \to G$ that combines any two elements a and b to form another element denoted $a * b$. The set and operation, $(G, *)$, must satisfy four fundamental properties known as the group axioms:

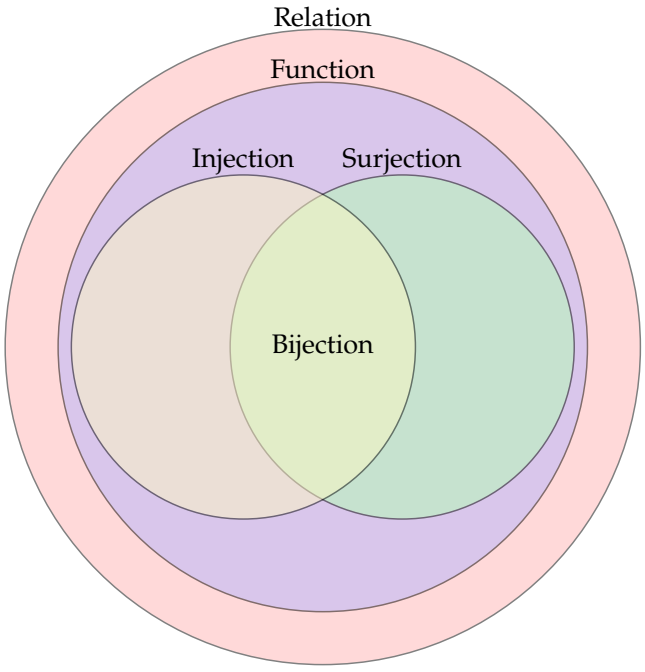
1. **Closure**:
$$a, b \in G \implies a * b \in G$$
2. **Associativity**:
$$a, b, c \in G \implies (a * b) \cdot c = a * (b * c)$$
3. **Identity Element**:
$$\exists e \in G : [a \in G \implies e * a = a = a * e]$$
4. **Inverse Element**:
$$a \in G \implies [\exists a^{-1} \in G : a * a^{-1} = e = a^{-1}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

Chapter 3

Functions

Observation.





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:

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

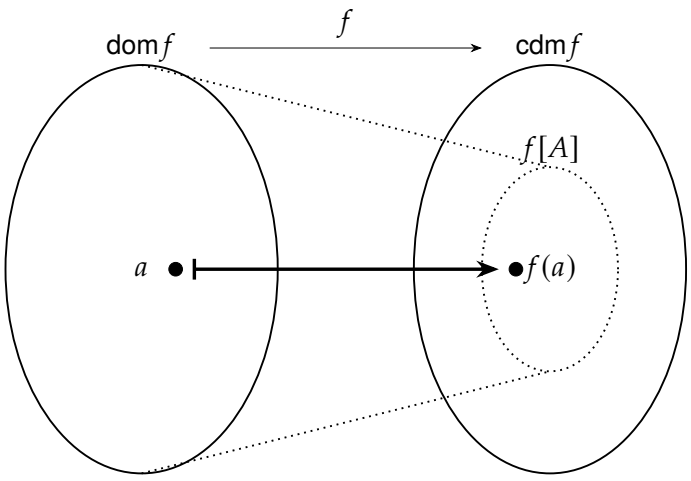
- **Co-domain:** The co-domain of a function $f : A \to B$ is the set B which includes all potential output values. It is the target set for the function. Formally:

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

- **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 $f : A \to B$ and $g : B \to C$, 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,

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

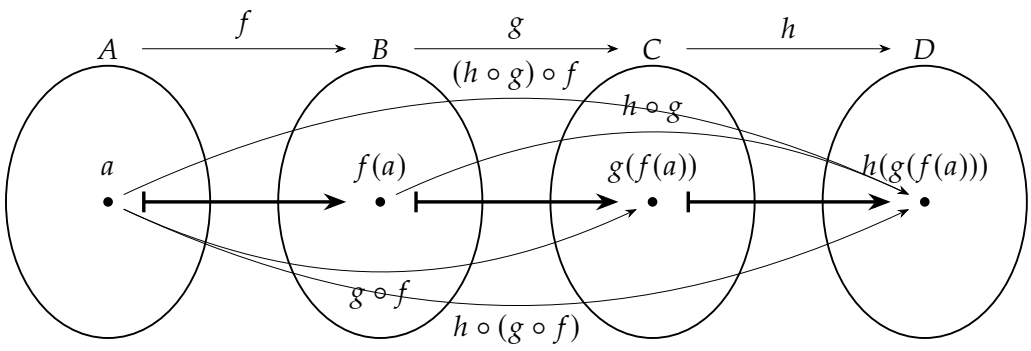
Remark 3.3.1.

- **Functions**:
  - Let $f : B \to C$ be a function from set B to set C.
  - Let $g : A \to B$ 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 :

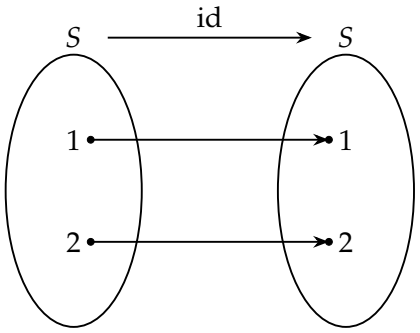
4. **Inverse Element**: For each $f \in G$, its inverse f^{-1} exists and is also a bijection from A to A. It satisfies
$$f \circ f^{-1} = \mathrm{id}_A = f^{-1} \circ f$$

3.3 Symmetric Group

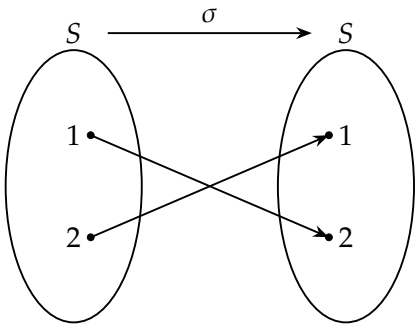
Exercise 3.1 (Symmetric Group S_2)**.** The **symmetric group** S_2 is the group of all permutations of a two-element set. For a set $X = \{1, 2\}$, the symmetric group S_2 consists of all bijective functions (permutations) from X to itself.

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 $f \in S_2$,

$$f \circ \text{id} = \text{id} \circ f = f$$

- **Inverse Element**:
  - Each element in S_2 has an inverse in S_2. Specifically,

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

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 $\exp : \mathbb{Z} \to \mathbb{Q}^*$ 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 $(\mathbb{Q}^*, \cdot)$.

Chapter 5

Linear Algebra and Group

Note (General Definition of Vector Space)**.** The operations + and · must satisfy the following properties for all $\mathbf{u}, \mathbf{v} \in V$ and $\alpha, \beta \in \mathbb{F}$:

1. **Associativity of Addition**:
$$(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$$

2. **Commutativity of Addition**:
$$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$$

3. **Existence of Additive Identity**:
$$\mathbf{u} \in V \implies \exists \mathbf{0} \in V : \mathbf{u} + \mathbf{0} = \mathbf{u}$$

4. **Existence of Additive Inverse**:
$$\mathbf{u} \in V \implies \exists -\mathbf{u} \in V : \mathbf{u} + (-\mathbf{u}) = \mathbf{0}$$

5. **Distributivity of Scalar Multiplication over Vector Addition**:
$$\alpha \cdot (\mathbf{u} + \mathbf{v}) = (\alpha \cdot \mathbf{u}) + (\alpha \cdot \mathbf{v})$$

6. **Distributivity of Scalar Multiplication over Field Addition**:
$$(\alpha + \beta) \cdot \mathbf{u} = (\alpha \cdot \mathbf{u}) + (\beta \cdot \mathbf{u})$$

7. **Compatibility of Scalar Multiplication with Field Multiplication**:
$$(\alpha\beta) \cdot \mathbf{u} = \alpha \cdot (\beta \cdot \mathbf{u})$$

8. **Identity Element of Scalar Multiplication**:
$$1 \cdot \mathbf{u} = \mathbf{u}$$

Linear Operation

Definition 5.1. Let V be a set over a field $\mathbb{F}$. We define the following linear operations on V:

1. An **addition operation**

$$\begin{aligned} + : V \times V &\to V \\ (\mathbf{u}, \mathbf{v}) &\mapsto \mathbf{u} + \mathbf{v} \end{aligned}$$

on V such that $(V, +)$ is an abelian group.

2. A **scalar multiplication operation**

$$\begin{aligned} \cdot : \mathbb{F} \times V &\to V \\ (\alpha, \mathbf{u}) &\mapsto \alpha \cdot \mathbf{u} \end{aligned}$$

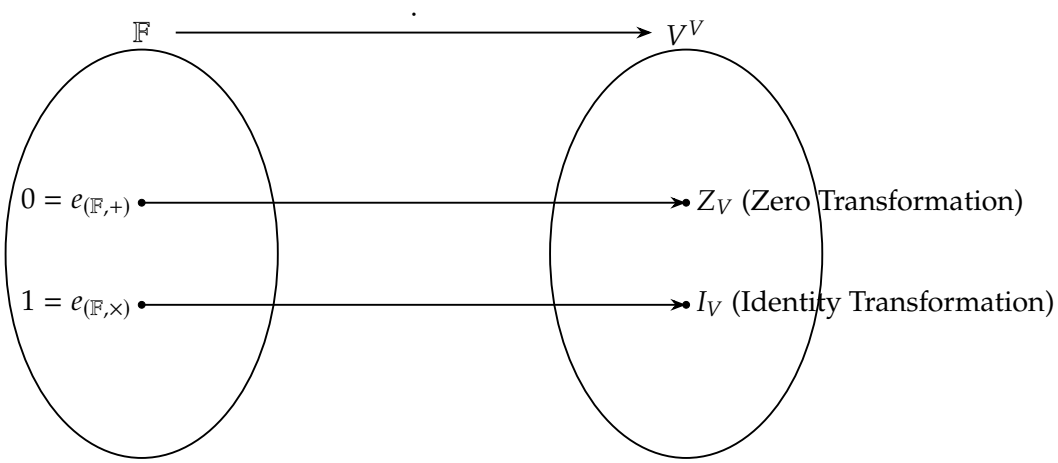
on V. Here $0 \cdot \mathbf{u} := \mathbf{0}$ and $1 \cdot \mathbf{u} := \mathbf{u}$, i.e.,

$$\begin{aligned} \cdot : \mathbb{F} \times V &\to V \\ (0, \mathbf{u}) &\mapsto \mathbf{0} \end{aligned} \qquad \begin{aligned} \cdot : \mathbb{F} \times V &\to V \\ (1, \mathbf{u}) &\mapsto \mathbf{u} \end{aligned}$$

Remark 5.1.1. Consider

$$\cdot : \mathbb{F} \to [V \to V].$$

Then



Remark 5.1.2. Let V be a set over a field $\mathbb{F}$. Assume that, for $\mathbf{x}, \mathbf{y} \in V$ and $\alpha, \beta \in F$,

$$\alpha \cdot \mathbf{x} + \beta \cdot \mathbf{y} \in V.$$

Then

$$\begin{aligned} \alpha = 1 = \beta &\implies \mathbf{x} + \mathbf{y} \in V \quad \cdots\cdots \text{(Additivity)} \\ \beta = 0 &\implies \alpha \cdot \mathbf{x} \in V \quad \cdots\cdots \text{(Homogeneity)} \end{aligned}$$

Vector Space

Definition 5.2. A **vector space** $(V, +, \cdot)$, simply V, over a field F is a set V together with two operations:

1. **Vector Addition:**
$$\begin{array}{rccc} + & : & V \times V & \longrightarrow & V \\ & & (\mathbf{u}, \mathbf{v}) & \longmapsto & \mathbf{u} + \mathbf{v} \end{array}'$$
such that $(V, +)$ forms an abelian group.

2. **Scalar Multiplication:**
$$\begin{array}{rccc} \cdot & : & F \times V & \longrightarrow & V \\ & & (a, \mathbf{u}) & \longmapsto & a \cdot \mathbf{u} \end{array}'$$
such that $(V, \cdot)$ satisfies the following properties:

   (a) **Distributivity of Scalar Multiplication with Respect to Vector Addition:**
$$a \cdot (\mathbf{u} + \mathbf{v}) = (a \cdot \mathbf{u}) + (a \cdot \mathbf{v}).$$

   (b) **Distributivity of Scalar Multiplication with Respect to Field Addition:**
$$(a + b) \cdot \mathbf{v} = (a \cdot \mathbf{v}) + (b \cdot \mathbf{v}).$$

   (c) **Associativity of Scalar Multiplication:**
$$a \cdot (b \cdot \mathbf{v}) = (a \cdot b) \cdot \mathbf{v}.$$

   (d) **Multiplicative Identity:**
$$\mathbf{v} \in V \implies 1 \cdot \mathbf{v} = \mathbf{v},$$
   where 1 is the multiplicative identity in F.

Linear Transformation

Definition 5.3. Let V and W be vector spaces over the same field F. A function $T : V \to W$ is called a **linear transformation** (or linear map) if for all $\mathbf{u}, \mathbf{v} \in V$ and all scalars $a \in F$, the following two conditions are satisfied:

1. **Additivity:**
$$T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v}).$$

2. **Homogeneity of Scalar Multiplication:**
$$T(a \cdot \mathbf{u}) = a \cdot T(\mathbf{u}).$$

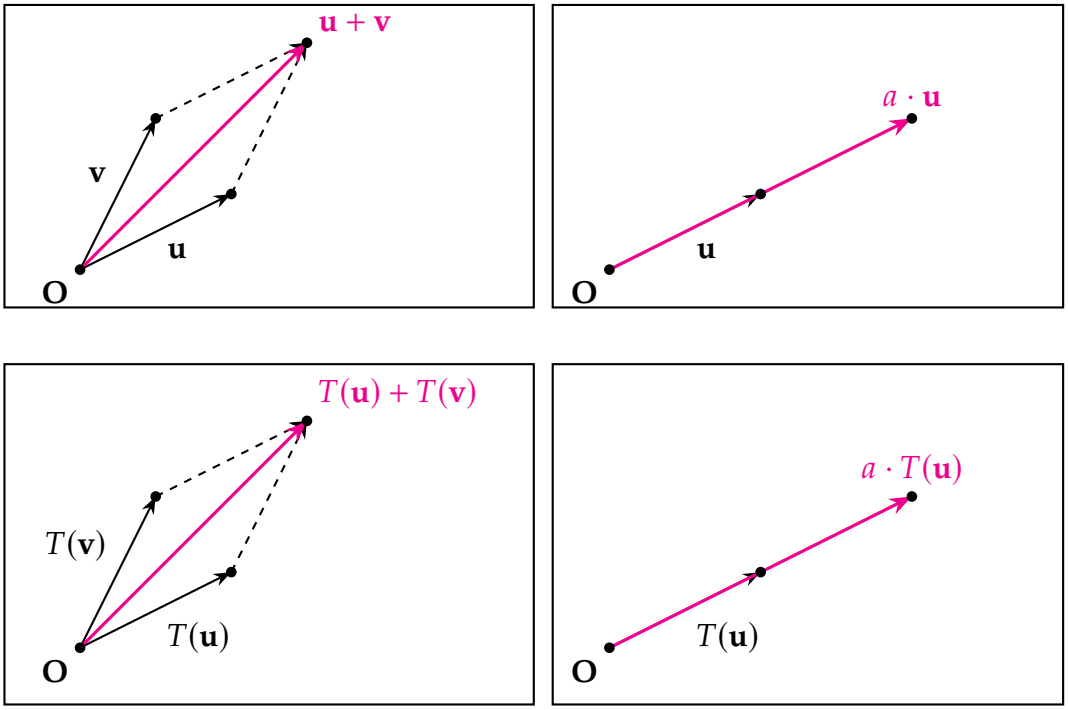
That is, T preserves the operations of vector addition and scalar multiplication.

Remark 5.3.1.
$$\begin{cases} \mathbf{u}, \mathbf{v} \in V \\ a, b \in F \end{cases} \implies \begin{array}{rccc} T & : & V & \longrightarrow & W \\ & & a \cdot \mathbf{u} + b \cdot \mathbf{v} & \longmapsto & T(a \cdot \mathbf{u} + b \cdot \mathbf{v}) = a \cdot T(\mathbf{u}) + b \cdot T(\mathbf{v}) \end{array}$$

Remark 5.3.2. Given that $T : V \to W$ is a linear transformation, the following properties hold:

1. $T(\mathbf{0}_V) = \mathbf{0}_W$, where $\mathbf{0}_V$ and $\mathbf{0}_W$ are the zero vectors in V and W, respectively.
2. $T\left(\sum_{i=1}^{n} a_i \mathbf{u}_i\right) = \sum_{i=1}^{n} a_i T(\mathbf{u}_i)$ for any finite set of vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n \in V$ and scalars $a_1, a_2, \ldots, a_n \in F$.

Remark 5.3.3.



Remark 5.3.4 (Dimension).

- (**Finite-Dimensional Vector Spaces**) A finite-dimensional vector space V over a field F with dimension n is always isomorphic to F^n.
- (**Basis and Isomorphism**)
  - Let $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ be a basis for V.
  - Any vector $\mathbf{v} \in V$ can be uniquely expressed as:

    $$\mathbf{v} = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \cdots + a_n\mathbf{e}_n,$$

    where $a_i \in F$ for $i = 1, 2, \ldots, n$.
  - The map:

    $$\varphi : V \to F^n, \quad \mathbf{v} \mapsto (a_1, a_2, \ldots, a_n)$$

    is a linear isomorphism.
- (**Infinite-Dimensional Vector Spaces**) Infinite-dimensional vector spaces are more complex and are not isomorphic to F^n for any finite n.
- (**Examples and Considerations**)
  - **Function Spaces**: Spaces like the set of all polynomials $\mathbb{P}$ or the space of continuous functions $C([0, 1])$.

- **Hilbert Spaces**: Spaces such as ℓ^2 (space of square-summable sequences).
- **Isomorphisms**: Infinite-dimensional vector spaces may be isomorphic to structures like F^∞ (sequences with only finitely many non-zero entries) or $F^{(\infty)}$ (the direct sum of infinitely many copies of F).

From the standpoint of solving equations, the algebraic structures we have discussed are interconnected in the following ways:

Group

A **group** provides a foundation for solving equations involving a single operation. The group structure ensures that every element has an inverse, allowing us to "undo" operations and solve equations. For instance, in the group of integers $(\mathbb{Z}, +)$, the equation $x + a = b$ can be solved as $x = b - a$.

Ring

A **ring** extends the concept of a group by introducing a second operation, typically multiplication, in addition to addition. Rings allow us to solve more complex equations that involve both addition and multiplication. For example, solving polynomial equations $f(x) = 0$ where $f(x)$ is a polynomial with coefficients in a ring R.

Field

A **field** is a ring with additional properties that make division possible (except by zero). This structure is crucial for solving linear equations and systems of linear equations. In a field F, any linear equation $ax = b$ (where $a \neq 0$) can be solved as $x = a^{-1}b$, where a^{-1} is the multiplicative inverse of a.

Vector Space

A **vector space** over a field F is a set of vectors that can be added together and scaled by elements of F. Vector spaces provide a framework for solving linear systems of equations. Solutions to systems of linear equations can be understood as finding vectors $\mathbf{x} \in V$ such that $A\mathbf{x} = \mathbf{b}$, where A is a matrix and $\mathbf{b}$ is a vector in V.

Module

A **module** is a generalization of vector spaces where the scalars come from a ring instead of a field. Modules allow us to solve equations in contexts where the coefficients are not from a field, such as systems of linear equations with integer coefficients. For example, solving $A\mathbf{x} = \mathbf{b}$ where A is a matrix with entries from a ring R and $\mathbf{x}, \mathbf{b} \in M$.

Algebra

An **algebra** over a field F combines the structures of a vector space and a ring. Algebras provide a framework for solving polynomial equations and other equations involving both addition and multiplication of vectors. In an algebra A, we can solve equations like $x^2 + ax + b = 0$ using techniques from both linear algebra and ring theory.

Summary

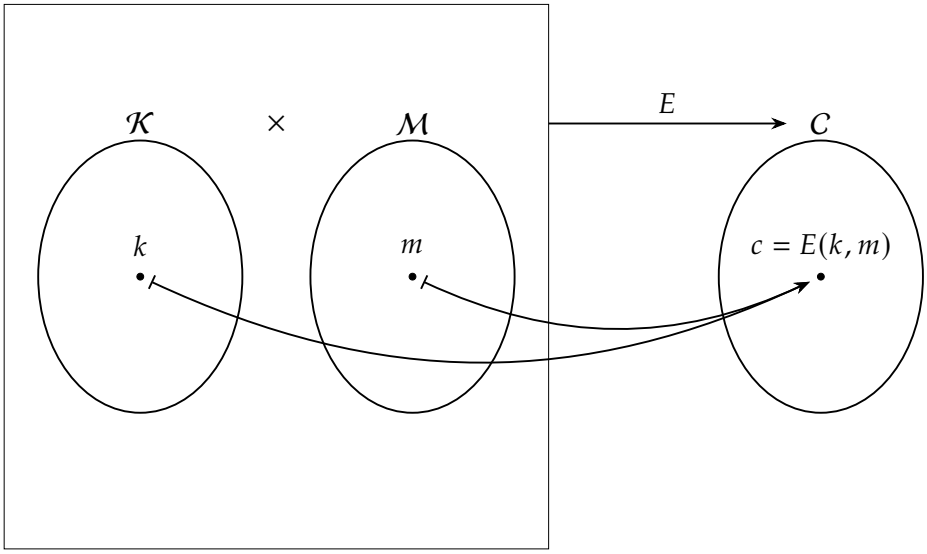
The conceptual connection between these structures is rooted in the increasing complexity and capability they offer for solving equations:

- **Groups** provide a way to solve equations with a single operation.
- **Rings** introduce a second operation, allowing for more complex equations.
- **Fields** enable division, which is essential for solving linear equations.
- **Vector spaces** over fields extend these concepts to systems of linear equations.
- **Modules** generalize vector spaces to allow coefficients from rings.
- **Algebras** integrate vector space and ring structures, enabling the solution of polynomial and other complex equations.

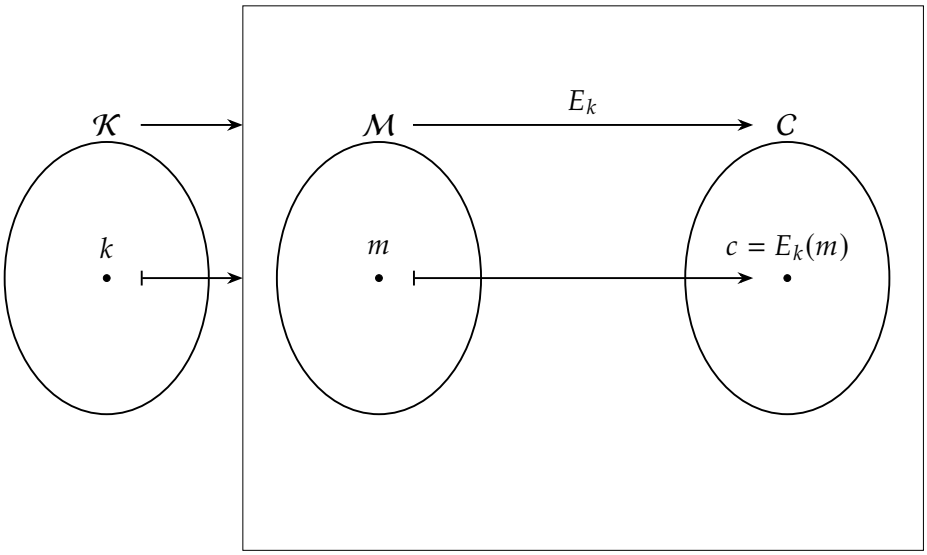
LaTex Practice

- **Block Size**: n (number of bits in a block)
- **Key Size**: k (number of bits in the key)

$$E : \boxed{\{0,1\}^k \times \{0,1\}^n} \rightarrow \{0,1\}^n$$
$$D : \boxed{\{0,1\}^k \times \{0,1\}^n} \rightarrow \{0,1\}^n$$



$$E : \{0,1\}^k \rightarrow \boxed{\{0,1\}^n \rightarrow \{0,1\}^n}$$
$$D : \{0,1\}^k \rightarrow \boxed{\{0,1\}^n \rightarrow \{0,1\}^n}$$



Appendix A

Preliminaries

A.1 Sets, Cartesian Products, and Relations

A.1.1 Sets and Ordered Pairs

Set

A **set** is a well-defined collection of distinct objects, called elements or members of the set. Sets are one of the most fundamental concepts in mathematics.

Set

Definition A.1. A **set** is a well-defined collection of distinct objects, considered as an object in its own right. Sets are usually denoted by capital letters, and the elements are listed within curly braces.

Example A.1. For example:

$$A = \{1, 2, 3\}$$

This denotes a set A containing the elements 1, 2, and 3.

Note (Properties)**.**

- **No Repetition**: Each element in a set appears only once.
- **Order Irrelevance**: The order of elements in a set does not matter. For instance, $\{1, 2, 3\} = \{3, 2, 1\}$.
- **Membership**: If an element a is in a set A, we write $a \in A$.

Note (Types of Sets)**.**

- **Finite and Infinite Sets**: A set with a finite number of elements is finite; otherwise, it is infinite.
- **Subset**: A set A is a subset of a set B if every element of A is also an element of B, denoted $A \subseteq B$.
- **Power Set**: The power set of A is the set of all subsets of A, denoted $\mathcal{P}(A)$.

Ordered Pair

An **ordered pair** is a fundamental concept in mathematics used to combine two elements in a specific order. The notation for an ordered pair is (a, b), where a is the first element and b is the second element.

Ordered Pair

Definition A.2. An **ordered pair** (a, b) is a collection of two elements where the order of the elements matters. This is in contrast to a set, where the order of elements does not matter.

Remark A.2.1.

- The ordered pair (a, b) is not the same as (b, a) unless $a = b$.
- Formally, the ordered pair (a, b) can be defined using sets to ensure the distinction from unordered pairs. One common definition is:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

This definition ensures that:

$$(a, b) = (c, d) \iff a = c \text{ and } b = d$$

Note (Properties).

- **Uniqueness**: Each ordered pair (a, b) is unique if either a or b is unique.
- **Order**: The order of elements in an ordered pair is significant.

A.1.2 Cartesian Product and Relation

Cartesian Product

The **Cartesian product** is a fundamental concept in set theory, used to define the set of all possible ordered pairs from two sets.

Cartesian Product

Given two sets A and B, the Cartesian product $A \times B$ is defined as the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. Formally,

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

Note (Properties).

- **Order Matters**: The pair (a, b) is different from the pair (b, a) unless $a = b$.
- **Empty Set**: If either A or B is the empty set $\emptyset$, then $A \times B$ is also empty:

$$A \times \emptyset = \emptyset \quad \text{and} \quad \emptyset \times B = \emptyset$$

Example A.2.

1. If $A = \{1, 2\}$ and $B = \{x, y\}$, then

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$$

2. If $A = \{a, b\}$ and $B = \{1, 2, 3\}$, then

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

Relation

A **relation** generalizes the concept of Cartesian product to establish connections between elements of two sets.

Relation

Definition A.3. A relation R from a set A to a set B is a subset of the Cartesian product $A \times B$. Formally,

$$R \subseteq A \times B$$

This means that a relation R consists of ordered pairs (a, b) where $a \in A$ and $b \in B$.

Note (Properties of Relations)**.**

- **Domain and Range**:
  - The **domain** of R is the set of all $a \in A$ such that there exists $b \in B$ with $(a, b) \in R$.

$$\text{Domain}(R) = \{a \in A \mid \exists b \in B,\ (a, b) \in R\}$$

  - The **range** of R is the set of all $b \in B$ such that there exists $a \in A$ with $(a, b) \in R$.

$$\text{Range}(R) = \{b \in B \mid \exists a \in A,\ (a, b) \in R\}$$

- **Inverse Relation**: The inverse of a relation R, denoted R^{-1}, is the set of all pairs (b, a) such that $(a, b) \in R$:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

- **Composition of Relations**: Given a relation R from A to B and a relation S from B to C, the composition $S \circ R$ is a relation from A to C defined by:

$$S \circ R = \{(a, c) \mid \exists b \in B,\ (a, b) \in R \text{ and } (b, c) \in S\}$$

Note (Types of Relations)**.**

- **Binary Relation**: A relation involving two sets, as defined above.
- **Unary Relation**: A relation on a single set A is simply a subset of A.
- **Ternary and Higher Relations**: Relations involving three or more sets, defined as subsets of the Cartesian product of those sets.

Example A.3.

1. If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, a possible relation R from A to B could be:

$$R = \{(1, a), (2, b), (3, a)\}$$

   - Domain: $\{1, 2, 3\}$
   - Range: $\{a, b\}$

2. Consider the relation R on set $A = \{1, 2, 3\}$ defined by:

$$R = \{(1, 2), (2, 3), (3, 1)\}$$

   - Domain: $\{1, 2, 3\}$
   - Range: $\{1, 2, 3\}$
   - Inverse Relation: $R^{-1} = \{(2, 1), (3, 2), (1, 3)\}$

A.2 Rational Number and Equivalence Class

We define the equivalence relation $(a, b) \sim (c, d)$ on the set $\mathbb{Z} \times \mathbb{Z}^*$ as:

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

Proof. To prove that $\sim$ is an equivalence relation, we must show it is reflexive, symmetric, and transitive.

- **Reflexive**: A relation $\sim$ is reflexive if every element is related to itself.
  For any $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, we need to show that $(a, b) \sim (a, b)$.

$$(a, b) \sim (a, b) \iff ab = ba$$

  This is true because $ab = ba$ holds for all integers a and b. Thus, the relation is reflexive.

- **Symmetric**: A relation $\sim$ is symmetric if whenever $(a, b) \sim (c, d)$, then $(c, d) \sim (a, b)$.
  Assume $(a, b) \sim (c, d)$. This means:

$$ad = bc$$

  We need to show that $(c, d) \sim (a, b)$.

$$(c, d) \sim (a, b) \iff cd = da$$

  Since $ad = bc$, we have $cd = da$ by the commutative property of multiplication. Thus, the relation is symmetric.

- **Transitive**: A relation $\sim$ is transitive if whenever $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $(a, b) \sim (e, f)$.
  Assume $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. This means:

$$ad = bc \quad \text{and} \quad cf = de$$

  We need to show that $(a, b) \sim (e, f)$.

$$(a, b) \sim (e, f) \iff af = be$$

From $ad = bc$, we have $d = \frac{bc}{a}$ (assuming $a \neq 0$). Substituting d into $cf = de$:

$$cf = \left(\frac{bc}{a}\right)e$$

Multiplying both sides by a:

$$acf = bce$$

Since $c \neq 0$:

$$af = be$$

Thus, $(a, b) \sim (e, f)$, proving that the relation is transitive.

□

Since the relation $(a, b) \sim (c, d) \iff ad = bc$ is reflexive, symmetric, and transitive, it is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.

The equivalence relation $(a, b) \sim (c, d) \iff ad = bc$ naturally connects to the division of the set of pairs of integers into equivalence classes, where each equivalence class represents a unique rational number.

An equivalence class $[(a, b)]$ under this relation consists of all pairs (c, d) such that $(a, b) \sim (c, d)$. This can be interpreted as:

$$[(a, b)] = \{(c, d) \mid ad = bc\}$$

Each equivalence class $[(a, b)]$ corresponds to the rational number $\frac{a}{b}$, and different pairs (a, b) and (c, d) represent the same rational number if and only if they belong to the same equivalence class.

Example A.4. Consider $(1, 2), (2, 4), (3, 6), (-1, -2), (1, -2)$

- (Class of $(1, 2)$)

  $$[1, 2] = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid 1d = 2c\} = \{(1, 2), (2, 4), (3, 6), (-1, -2), \ldots\}$$

  This class represents the rational number $\frac{1}{2}$.

- (Class of $(2, 3)$)

  $$[2, 3] = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid 2d = 3c\} = \{(2, 3), (4, 6), (-2, -3), \ldots\}$$

  This class represents the rational number $\frac{2}{3}$.

- (Class of $(1, -2)$)

  $$[1, -2] = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid 1d = -2c\} = \{(1, -2), (2, -4), (-1, 2), \ldots\}$$

  This class represents the rational number $\frac{1}{-2}$.

Remark A.3.1 (Properties of Partition)**.**

- (Disjoint) Each element of $\mathbb{Z} \times \mathbb{Z}^*$ belongs to exactly one equivalence class. If $(a, b) \in [c, d]$, then $[a, b] = [c, d]$.

- (Exhaustive) The union of all equivalence classes covers the entire set $\mathbb{Z} \times \mathbb{Z}^*$. Every pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ is in some equivalence class.

Bijection Between $\mathbb{Z} \times \mathbb{Z}^*$ and $\mathbb{N}$

To establish a bijection between $\mathbb{Z} \times \mathbb{Z}^*$ and $\mathbb{N}$, we construct a function that maps each pair (a, b) in $\mathbb{Z} \times \mathbb{Z}^*$ to a unique natural number.

Encoding Integers as Natural Numbers

Define the encoding function $e : \mathbb{Z} \to \mathbb{N}$ as follows:

$$e(a) = \begin{cases} 2a & \text{if } a \geq 0 \\ -2a - 1 & \text{if } a < 0 \end{cases}$$

Define the encoding function $e^* : \mathbb{Z}^* \to \mathbb{N}$ similarly:

$$e^*(b) = \begin{cases} 2b & \text{if } b > 0 \\ -2b - 1 & \text{if } b < 0 \end{cases}$$

Pairing Function

Define a pairing function $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by:

$$\pi(n_1, n_2) = \frac{(n_1 + n_2)(n_1 + n_2 + 1)}{2} + n_2$$

Mapping Function

Define the mapping function $f : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{N}$ by:

$$f(a, b) = \pi(e(a), e^*(b))$$

Bijection

To show that f is a bijection, we need to prove that it is both injective and surjective.

Injectivity

Assume $f(a, b) = f(c, d)$. This implies:

$$\pi(e(a), e^*(b)) = \pi(e(c), e^*(d))$$

Since π is injective, we have:

$$(e(a), e^*(b)) = (e(c), e^*(d))$$

This implies $e(a) = e(c)$ and $e^*(b) = e^*(d)$, which in turn implies $a = c$ and $b = d$.

Thus, f is injective.

Surjectivity

Let $n \in \mathbb{N}$. We need to find $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ such that $f(a, b) = n$.

Since π is surjective, there exist $n_1, n_2 \in \mathbb{N}$ such that:

$$n = \pi(n_1, n_2)$$

Using the inverse of e and e^*, we can find a and b such that:

$$e(a) = n_1 \quad \text{and} \quad e^*(b) = n_2$$

Thus, $f(a, b) = n$, and f is surjective.

Conclusion

Since f is both injective and surjective, it is a bijection. Therefore, $\mathbb{Z} \times \mathbb{Z}^*$ is in one-to-one correspondence with $\mathbb{N}$.

Invalid Equivalence Classes and Proof Using Natural Numbers and Integers

Consider the equivalence relation $(a, b) \sim (c, d)$ defined by:

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

where $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ and $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Invalid Equivalence Classes

Equivalence Classes Overview

In mathematics, an equivalence class under a given equivalence relation is a subset formed by grouping all elements related to each other by that relation. For the relation $(a, b) \sim (c, d) \iff ad = bc$ on $\mathbb{Z} \times \mathbb{Z}^*$, each equivalence class represents a unique rational number.

Valid Equivalence Classes

Under the relation $(a, b) \sim (c, d) \iff ad = bc$ with $b \neq 0$ and $d \neq 0$, each equivalence class $[a, b]$ includes all pairs (c, d) such that $ad = bc$. Formally:

$$[a, b] = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}^* \mid ad = bc\}$$

These equivalence classes correspond to unique relationships between pairs of integers.

Invalid Equivalence Classes with Zero Denominator

When $b = 0$ or $d = 0$, the equivalence relation breaks down because:

- **Undefined Products**: A pair $(a, 0)$ does not represent a valid mathematical entity since $a \cdot 0$ is not meaningful in the context of this relation.
- **Equivalence Condition Breakdown**: If $b = 0$ or $d = 0$, the condition $ad = bc$ can lead to contradictions or meaningless comparisons.

Proof: If $b = 0$ or $d = 0$, Then (a, b) is Not Equivalent to (c, d)

Case 1: $b = 0$ and $d \neq 0$

Suppose $(a, 0) \sim (c, d)$. According to the equivalence relation:

$$a \cdot d = 0 \cdot c \implies ad = 0$$

For this to hold, at least one of a or d must be zero. Given that $d \neq 0$, we must have $a = 0$. Thus:

$$(a, 0) \sim (0, d)$$

This implies that $(a, 0)$ can only be equivalent to pairs of the form $(0, d)$.

Case 2: $d = 0$ and $b \neq 0$

Suppose $(a, b) \sim (c, 0)$. According to the equivalence relation:

$$a \cdot 0 = b \cdot c \implies 0 = bc$$

For this to hold, at least one of b or c must be zero. Given that $b \neq 0$, we must have $c = 0$. Thus:

$$(a, b) \sim (0, 0)$$

This implies that $(c, 0)$ can only be equivalent to pairs of the form $(a, 0)$.

Case 3: Both $b = 0$ and $d = 0$

Suppose $(a, 0) \sim (c, 0)$. According to the equivalence relation:

$$a \cdot 0 = 0 \cdot c \implies 0 = 0$$

This is trivially true, so pairs of the form $(a, 0)$ are all equivalent to each other, regardless of the value of a or c.

Conclusion

When $b = 0$ or $d = 0$, the equivalence relation $(a, b) \sim (c, d) \iff ad = bc$ does not define valid equivalence classes that can represent meaningful relationships between pairs of integers. These invalid equivalence classes do not correspond to well-defined mathematical entities because they involve undefined or meaningless products.