

# A Concise Note on Set Theory

Samena Bahleri

`samenabahleri09@gmail.com`

September 20, 2025

*This page left intentionally blank*

# Contents

<b>1</b>	<b>A Brief History of the Development of Set Theory</b>	<b>7</b>
<b>2</b>	<b>Defining and Constructing</b>	<b>7</b>
<b>3</b>	<b>Methods of Specifying Sets</b>	<b>8</b>
3.1	Roster (Tabular) Method . . . . .	8
3.2	Set-Builder Notation . . . . .	8
3.3	Descriptive Method . . . . .	8
3.4	Predicate-Logic Method . . . . .	8
3.5	Recursive Definition . . . . .	9
3.6	Definition via Set Operations . . . . .	9
<b>4</b>	<b>Defining versus Constructing Sets</b>	<b>9</b>
<b>5</b>	<b>Sets and Classes</b>	<b>10</b>
<b>6</b>	<b>Von Neumann Hierarchy</b>	<b>11</b>
<b>7</b>	<b>The Language of Set Theory</b>	<b>14</b>
7.1	The Symbols . . . . .	14
7.2	Mathematical Contexts . . . . .	14
7.3	Types of Vocabulary Symbols . . . . .	14
7.4	Terms . . . . .	15
7.5	Atomic Formulas . . . . .	15
7.6	Compound Formulas . . . . .	15
7.7	Logical Equivalences . . . . .	16
7.8	Set-Theoretic Abbreviations . . . . .	16
7.9	Additional Common Abbreviations . . . . .	16
7.10	Semantics . . . . .	16
<b>8</b>	<b>Axioms of Set Theory</b>	<b>17</b>
8.1	Axiom of Extensionality . . . . .	17
8.2	Axiom of the Empty Set . . . . .	17
8.3	Axiom of Pairing . . . . .	17
8.4	Axiom Schema of Separation . . . . .	17
8.5	Axiom of Union . . . . .	17
8.6	Axiom of Power Set . . . . .	17
8.7	Axiom of Infinity . . . . .	17
8.8	Axiom Schema of Replacement . . . . .	17
8.9	Axiom of Regularity (Foundation) . . . . .	18
8.10	Axiom of Choice . . . . .	18
<b>9</b>	<b>Union</b>	<b>18</b>
<b>10</b>	<b>Intersection</b>	<b>22</b>
<b>11</b>	<b>Difference</b>	<b>27</b>

<b>12 Symmetric Difference</b>	<b>30</b>
<b>13 Complement</b>	<b>32</b>
<b>14 Cartesian Product</b>	<b>34</b>
<b>15 Subset</b>	<b>39</b>
<b>16 Power Set</b>	<b>42</b>
<b>17 Properties and Laws</b>	<b>45</b>
17.1 Commutative Laws . . . . .	45
17.2 Associative Laws . . . . .	45
17.3 Distributive Laws . . . . .	45
17.4 De Morgan's Laws . . . . .	46
17.5 Identity Laws . . . . .	46
17.6 Idempotent Laws . . . . .	46
17.7 Complement Laws . . . . .	47
17.8 Absorption Laws . . . . .	47
<b>18 Relations As a Sets</b>	<b>47</b>
18.1 Binary Relations . . . . .	48
18.2 Unnatural Relations . . . . .	50
<b>19 Properties of Relations</b>	<b>50</b>
19.1 Reflexivity . . . . .	51
19.2 Irreflexivity . . . . .	51
19.3 Asymmetry . . . . .	51
19.4 Symmetry . . . . .	51
19.5 Antisymmetry . . . . .	51
19.6 Transitivity . . . . .	52
19.7 Connectivity . . . . .	52
19.8 Reflexive and Symmetric But Not Transitive . . . . .	53
19.9 Reflexive and Antisymmetric But Not Transitive . . . . .	53
19.10 Antisymmetric and Transitive But Not Reflexive . . . . .	54
19.11 Reflexive, Symmetric, and Transitive . . . . .	54
<b>20 Equivalence Classes and Partitions</b>	<b>55</b>
<b>21 Order Relations</b>	<b>57</b>
21.1 Preorder . . . . .	57
21.2 Partial Order . . . . .	58
21.3 Linear Order . . . . .	59
21.4 Strict Order . . . . .	59
21.5 Strict Linear Order . . . . .	60
<b>22 Graph</b>	<b>62</b>

<b>23 Operations on Relations</b>	<b>64</b>
23.1 Inverse of a Relation . . . . .	64
23.2 Relative Product of Relations . . . . .	65
23.3 Restriction of a Relation . . . . .	65
23.4 Application of a Relation to a Set . . . . .	67
23.5 Transitive Closure . . . . .	67
23.6 Reflexive Transitive Closure . . . . .	68
<b>24 Functions</b>	<b>68</b>
24.1 Domain, Codomain, Range, and Preimage . . . . .	68
<b>25 Kinds of Functions</b>	<b>73</b>
25.1 Injective . . . . .	73
25.2 Surjective . . . . .	74
25.3 Bijective . . . . .	75
25.4 Combinations . . . . .	76
25.4.1 Bijective (Both injective and surjective) . . . . .	76
25.4.2 Injective but not surjective . . . . .	76
25.4.3 Surjective but not injective . . . . .	77
25.4.4 Neither injective nor surjective . . . . .	77
25.5 Equivalence Relation with Function Properties . . . . .	78
<b>26 Functions as Relations</b>	<b>81</b>
26.1 Graph of a Function . . . . .	81
26.2 Restriction and Image . . . . .	83
26.3 Composition of Functions . . . . .	84
26.4 Partial Function . . . . .	86
26.5 Graph of a Partial Function . . . . .	87
<b>27 Inverses of Functions</b>	<b>87</b>
27.1 Left and Right Inverse . . . . .	88
27.2 Injective Case . . . . .	90
27.3 Surjective Case . . . . .	90
27.4 Bijective Case . . . . .	91
27.5 Uniqueness of Inverse . . . . .	92
<b>28 Enumerations and Countable Sets</b>	<b>93</b>
28.1 Enumeration . . . . .	93
28.2 Countable Sets . . . . .	95
<b>29 Cantor's Zig-Zag Method</b>	<b>96</b>
<b>30 Pairing Functions and Codes</b>	<b>98</b>
<b>31 Uncountable Sets</b>	<b>102</b>
<b>32 Reduction and Equinumerosity</b>	<b>107</b>
32.1 Reduction . . . . .	107
32.2 2Equinumerosity . . . . .	109

<b>33 Sets of Different Sizes</b>	<b>110</b>
<b>34 Cantor's Theorem</b>	<b>111</b>
<b>35 Cantor–Schröder–Bernstein</b>	<b>112</b>

# 1 A Brief History of the Development of Set Theory

When it comes to the concept of sets, humans essentially possess this knowledge intuitively. However, when discussing the cardinality of a set mathematically and rigorously, Georg Cantor is considered a pioneer in the development of set theory, particularly in analyzing the sizes of the sets  $\mathbb{R}$  and  $\mathbb{N}$ . On the other hand, set theory also contains inherent gaps that forced the discipline to undergo refinement. Specifically, Bertrand Russell demonstrated that naive set theory syntactically allows us to construct a set that leads to a contradiction. The set in question is:

$$R = \{x : x \notin x\}.$$

As an example, consider some simple sets:

- 1)  $A = \{1, 2, 3\}$
- 2)  $B = \{4\}$
- 3)  $C = \{C\}$

Now we define:

$$R = \{x \mid x \text{ does not contain itself}\}.$$

With this definition,  $A \in R$  and  $B \in R$ , because they do not contain themselves. Now the question arises: is  $R \in R$ ?

- 1) If  $R \in R$ , then  $R$  contains itself, but  $R$  is only supposed to contain sets that do not contain themselves, which yields a contradiction.
- 2) If  $R \notin R$ , then  $R$  does not contain itself, and therefore by definition  $R$  must be in  $R$ , which again yields a contradiction.

As we have seen, the set developed by Russell is self-referential, meaning it refers to itself. Therefore, this set inherently contains a contradiction and cannot be consistent; it is always *false* with respect to itself. Moreover, identifying this paradox, Ernst Zermelo proposed axiomatic set theory to avoid this kind of construction by introducing axioms that restrict how sets can be constructed. Subsequently, Abraham Fraenkel and Thoralf Skolem further refined Zermelo's axioms, resulting in Zermelo–Fraenkel (ZF) set theory, which was later extended to ZFC with the inclusion of the Axiom of Choice.

Finally, beyond Russell's paradox, the development of set theory also saw momentous contributions from Kurt Gödel and Paul Cohen, who analyzed the foundational challenges posed by the Continuum Hypothesis (*CH*), demonstrating its consistency and independence relative to ZFC set theory.

## 2 Defining and Constructing

Firstly, a set is a collection of objects, considered as a single object. The objects making up a set are called its *elements* or *members*.

For example, if  $x$  is an element of a set  $U$ , we write:

$$x \in U.$$

Conversely, if  $x$  is not an element of  $U$ , we write:

$$x \notin U.$$

We can specify a set either by listing its elements explicitly or by defining a property that determines membership. In fact, sets may be specified in several different ways.

## 3 Methods of Specifying Sets

### 3.1 Roster (Tabular) Method

This method lists all the elements of the set explicitly:

$$A = \{1, 2, 3, 4, 5\}.$$

**Example.**

The first five natural numbers are

$$\mathbb{N}_5 = \{1, 2, 3, 4, 5\}.$$

### 3.2 Set-Builder Notation

This method defines a set by specifying a property that its members must satisfy:

$$B = \{x \in \mathbb{N} \mid x \text{ is even}\}.$$

**Example.**

All positive even natural numbers:

$$E = \{x \in \mathbb{N} \mid x \leftrightarrow 0 \pmod{2}\}.$$

### 3.3 Descriptive Method

This method describes the set in words:

$$C = \{\text{all real numbers greater than zero}\}.$$

### 3.4 Predicate-Logic Method

This is a formal version of set-builder notation using logical expressions:

$$D = \{x \in \mathbb{Z}^+ \mid x^2 < 10\}.$$

Explicitly, this set is

$$D = \{1, 2, 3\}.$$

### 3.5 Recursive Definition

Sets can be defined recursively, where each stage is built from the previous one:

$$S_0 = \emptyset, \quad S_{n+1} = \mathcal{P}(S_n).$$

**Example.**

The von Neumann ordinals:

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \dots$$

### 3.6 Definition via Set Operations

Sets can also be defined in terms of other sets, using operations such as union, intersection, and difference.

**Example 1.**

$$A = \{1, 2, 3, 4\}, \quad B = \{3, 4, 5, 6\}.$$

Then:

$$A \cup B = \{1, 2, 3, 4, 5, 6\},$$

$$A \cap B = \{3, 4\},$$

$$A \setminus B = \{1, 2\}.$$

**Example 2.**

The set of rational numbers:

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, \quad q \in \mathbb{Z} \setminus \{0\} \right\}.$$

Some rational numbers are

$$\left\{ -\frac{3}{2}, -1, 0, \frac{1}{2}, \frac{2}{3}, 1, \frac{5}{4} \right\}.$$

## 4 Defining versus Constructing Sets

To *define* a set means to specify a membership condition or description. A definition does not actually produce the set; it merely characterizes its members. By contrast, to *construct* a set means to build it from existing sets using axioms of set theory such as union and intersection. When defining a set, one assumes its existence; when constructing a set, one must establish its existence from the axioms.

Because we will mostly be dealing with sets whose elements are mathematical objects, it is important to keep in mind the following sets:

- 1)  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ , the set of natural numbers

- 2)  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ , the set of integers
- 3)  $\mathbb{Q} = \left\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\right\}$ , the set of rationals
- 4)  $\mathbb{R} = (-\infty, \infty)$ , the set of real numbers (the continuum)

## 5 Sets and Classes

In axiomatic set theory, one distinguishes between *sets* and *classes*. A set is a collection that may itself be an element of another collection. A class is a collection of sets defined by a property. If a class can be an element, it is a set; otherwise, it is a *proper class*.

The axiom schema of separation introduces the notation for set abstraction:

$$\{x \in a \mid \varphi(x, p_1, \dots, p_n)\},$$

where  $a$  is a set and  $\varphi$  is a formula. The restriction  $x \in a$  is essential; without it one obtains contradictions such as Russell's paradox. For example, the collection

$$\{x \mid x = x\}$$

would be the collection of all sets. If it were a set  $v$ , then

$$r = \{x \in v \mid x \notin x\}$$

would also be a set, yielding the contradiction  $r \in r \leftrightarrow r \notin r$ .

As an example of a genuine set, consider

$$\mathbb{N} = \{0, 1, 2, 3, \dots\},$$

which may occur as an element of another collection. Another example is

$$E = \{n \in \mathbb{N} \mid n \text{ is even}\},$$

which is obtained by separation from  $\mathbb{N}$ .

As examples of proper classes, consider

$$V = \{x \mid x = x\}, \quad \text{Ord} = \{\alpha \mid \alpha \text{ is an ordinal}\}.$$

These are not sets, since assuming they were leads to contradictions.

Proper classes cannot occur on the left of  $\in$ , but they can occur on the right and in equality or inclusion statements, interpreted schematically. For example,

$$a \in \{x \mid \varphi(x)\} \leftrightarrow \varphi(a),$$

$$\{x \mid \varphi(x)\} = \{x \mid \psi(x)\} \leftrightarrow \forall x (\varphi(x) \leftrightarrow \psi(x)),$$

$$\{x \mid \varphi(x)\} \subseteq \{x \mid \psi(x)\} \leftrightarrow \forall x (\varphi(x) \rightarrow \psi(x)).$$

In summary, every set is a class, but not every class is a set. Sets such as  $\mathbb{N}$  and  $E$  can occur as elements of other collections, while proper classes such as  $V$  and  $\text{Ord}$  describe collections too large to be sets.

## 6 Von Neumann Hierarchy

The *cumulative hierarchy* ( $V_\alpha$ ) is defined by transfinite recursion on ordinals  $\alpha$ . This construction builds the universe of sets in stages, where each stage contains all sets that can be formed from the previous stages. For any ordinal  $\alpha$ , we define  $V_\alpha$  as follows.

1. Base Cases (Finite Ordinals)

1. Stage 1: The empty set

$$V_0 = \emptyset$$

2. Stage 2: All subsets of  $V_0$

$$V_1 = \mathcal{P}(V_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$$

3. Stage 3: All subsets of  $V_1$

$$V_2 = \mathcal{P}(V_1) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

4. Stage 4: All subsets of  $V_2$

$$V_3 = \mathcal{P}(V_2) = \mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$$

5. Stage 5: All subsets of  $V_3$

$$V_4 = \mathcal{P}(V_3)$$

$\vdots$

In general, for finite  $n$ ,

$$V_{n+1} = \mathcal{P}(V_n).$$

The cardinalities of these stages satisfy:

1.  $|V_0| = 0$
2.  $|V_1| = 1$
3.  $|V_2| = 2$
4.  $|V_3| = 4$
5.  $|V_4| = 16$
6.  $|V_n| = 2^{2^{\cdot^{\cdot^2}}}$  (a tower of  $n$  exponentials)

Here,  $|V|$  denotes the *cardinality* of the set  $V$ .

## 2. Cardinality and Power Sets

Consider the set

$$A = \{x, y, z\}.$$

This set has three elements, so

$$|A| = 3.$$

The *power set* of  $A$ , denoted  $\mathcal{P}(A)$ , is the set of all subsets of  $A$ :

$$\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}.$$

Thus,  $|\mathcal{P}(A)| = 8$ . In general, if  $|A| = n$ , then

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

## 3. First Limit Ordinal

1. Stage  $\omega$ :

$$V_\omega = \bigcup_{n < \omega} V_n = V_0 \cup V_1 \cup V_2 \cup V_3 \cup \dots$$

2. Stage  $\omega + 1$ :

$$V_{\omega+1} = \mathcal{P}(V_\omega)$$

3. Stage  $\omega + 2$ :

$$V_{\omega+2} = \mathcal{P}(V_{\omega+1})$$

## 4. General Recursive Definition

For any ordinal  $\alpha$ :

1. Successor case.

If  $\alpha = \beta + 1$ , then

$$V_\alpha = \mathcal{P}(V_\beta).$$

2. Limit case

If  $\alpha$  is a limit ordinal, then

$$V_\alpha = \bigcup_{\beta < \alpha} V_\beta.$$

3. Zero case

$$V_0 = \emptyset.$$

## 5. Rank Function

Every set  $x$  has a *rank*  $\Sigma(x)$ , defined as the least ordinal  $\alpha$  such that  $x \in V_{\alpha+1}$ :

$$\Sigma(x) = \min\{\alpha \mid x \in V_{\alpha+1}\},$$

equivalently,

$$\Sigma(x) = \sup\{\Sigma(y) + 1 \mid y \in x\}.$$

### Example 1:

Let

$$L = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

The ranks of its elements are:

$$\Sigma(\emptyset) = 0, \quad \Sigma(\{\emptyset\}) = 1, \quad \Sigma(\{\emptyset, \{\emptyset\}\}) = 2.$$

Thus,

$$\sup\{\Sigma(y) + 1 \mid y \in L\} = \sup\{1, 2, 3\} = 3,$$

and hence

$$\boxed{\Sigma(L) = 3}.$$

### Example 2:

Let

$$M = \{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\}.$$

The ranks of the elements are:

$$\Sigma(\emptyset) = 0, \quad \Sigma(\{\emptyset, \{\emptyset\}\}) = 2, \quad \Sigma(\{\emptyset, \{\emptyset, \{\emptyset\}\}\}) = 3.$$

Hence,

$$\sup\{\Sigma(y) + 1 \mid y \in M\} = \sup\{1, 3, 4\} = 4,$$

and therefore

$$\boxed{\Sigma(M) = 4}.$$

### Example 3:

Let

$$B = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

This set has neither a minimum nor a maximum element. Its bounds satisfy:

$$\boxed{\min\{x \mid x \in B\} \text{ does not exist, } \sup\{x \mid x \in B\} = 1}.$$

## 6. Universe of Sets

The universe of all sets is given by

$$V = \bigcup_{\alpha \in \text{Ord}} V_\alpha,$$

where Ord denotes the class of all ordinals. This construction exhibits the universe of sets as a well-ordered cumulative hierarchy, with each stage built systematically from all preceding stages.

# 7 The Language of Set Theory

The way we describe a set is primarily through the language of *First-Order Logic* (FOL). This formal language provides a precise syntactic framework for expressing mathematical statements about sets.

## 7.1 The Symbols

The basic alphabet of our logical language consists of:

1. Equality:  $=, \neq$
2. Logical connectives:  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
3. Quantifiers:  $\forall, \exists$
4. Membership / relations:  $\in$
5. Variables:  $x, y, z, \dots$
6. Punctuation symbols:  $( ), ,, .$

## 7.2 Mathematical Contexts

1. Groups:  $e$  (identity),  $*$  (operation),  $^{-1}$  (inverse)
2. Fields:  $0, 1, +, \cdot$
3. Arithmetic:  $0, 1, +, -, \cdot, /, <, >, \leq, \geq$

## 7.3 Types of Vocabulary Symbols

Each vocabulary symbol has an associated *arity* (number of arguments):

1. Constants:  $c_0, c_1, c_2, \dots$  (0-ary symbols)
2. Functions:  $f_0, f_1, f_2, \dots$  ( $n$ -ary for  $n \geq 1$ )
3. Relations:  $R_0, R_1, R_2, \dots$  ( $n$ -ary for  $n \geq 1$ )

## 7.4 Terms

Terms are expressions that refer to objects in the domain. They are defined recursively:

1. Constant symbols  $c_0, c_1, \dots$  are terms
2. Variable symbols  $x, y, z, \dots$  are terms
3. If  $f_i$  is an  $n$ -ary function symbol and  $t_1, \dots, t_n$  are terms, then

$$f_i(t_1, \dots, t_n)$$

is a term

### Examples:

1. Variables:  $x, y, z$
2. Constants:  $\emptyset$
3. Function applications:  $f(x, y), g(h(z))$

## 7.5 Atomic Formulas

The basic building blocks of formulas:

1. Equality:  $t_1 = t_2$
2. Relations:  $R(t_1, \dots, t_n)$

## 7.6 Compound Formulas

If  $X$  and  $Y$  are formulas, then so are:

1.  $\neg X$
2.  $(X \wedge Y)$
3.  $(X \vee Y)$
4.  $(X \rightarrow Y)$
5.  $(X \leftrightarrow Y)$
6.  $\forall x X$
7.  $\exists x X$

## 7.7 Logical Equivalences

The following equivalences hold:

1.  $\neg(\neg a) \leftrightarrow a$
2.  $(a \wedge b) \leftrightarrow \neg((\neg a) \vee (\neg b))$
3.  $(a \rightarrow b) \leftrightarrow ((\neg a) \vee b)$
4.  $(a \leftrightarrow b) \leftrightarrow ((a \rightarrow b) \wedge (b \rightarrow a))$
5.  $\exists v_i a \leftrightarrow \neg \forall v_i (\neg a)$
6.  $\forall v_i a \leftrightarrow \neg \exists v_i (\neg a)$
7.  $(a \leftrightarrow b) \leftrightarrow (b \leftrightarrow a)$

## 7.8 Set-Theoretic Abbreviations

1. Bounded existential quantifier:

$$\exists x \in y X(x) \leftrightarrow \exists x (x \in y \wedge X(x))$$

2. Bounded universal quantifier:

$$\forall x \in y X(x) \leftrightarrow \forall x (x \in y \rightarrow X(x))$$

3. Unique existence:

$$\exists! x X(x) \leftrightarrow \exists x (X(x) \wedge \forall y (X(y) \rightarrow y = x))$$

## 7.9 Additional Common Abbreviations

1.  $x \notin y \leftrightarrow \neg(x \in y)$
2.  $x \subseteq y \leftrightarrow \forall z \in x (z \in y)$
3.  $x \subsetneq y \leftrightarrow (x \subseteq y) \wedge (x \neq y)$

## 7.10 Semantics

The language described above is purely syntactic. Semantics assigns meaning by interpreting formulas in a structure.

1. Existence of the empty set:

$$\exists x \forall y (y \notin x)$$

2. Intermediate membership:

$$\forall x \forall y (x \in y \rightarrow \exists z (x \in z \wedge z \in y))$$

3. Reflexivity of equality:

$$\forall x (x = x)$$

4. Existence of distinct sets:

$$\exists x \exists y (x \neq y)$$

## 8 Axioms of Set Theory

### 8.1 Axiom of Extensionality

$$\forall x \forall y (\forall a (a \in x \leftrightarrow a \in y) \rightarrow x = y)$$

Two sets are equal if and only if they have exactly the same elements.

### 8.2 Axiom of the Empty Set

$$\exists x \forall a (a \notin x)$$

There exists a set with no elements, called the empty set  $\emptyset$ .

### 8.3 Axiom of Pairing

$$\forall a \forall \omega \exists x \forall \gamma (\gamma \in x \leftrightarrow (\gamma = a \vee \gamma = \omega))$$

For any two sets, there exists a set containing exactly those two sets as elements.

### 8.4 Axiom Schema of Separation

$$\forall a \forall p_1 \dots \forall p_n \exists b \forall x (x \in b \leftrightarrow (x \in a \wedge \varphi(x, p_1, \dots, p_n)))$$

From any set  $a$ , one can form a subset  $b$  consisting of exactly those elements of  $a$  that satisfy the property  $\varphi(x, p_1, \dots, p_n)$ . Each choice of formula  $\varphi$  yields a distinct axiom; together these form the axiom schema of separation.

### 8.5 Axiom of Union

$$\forall x \exists y \forall a (a \in y \leftrightarrow \exists z (z \in x \wedge a \in z))$$

For any set, there exists a set containing exactly all elements of the elements of that set, called its union.

### 8.6 Axiom of Power Set

$$\forall x \exists y \forall a (a \in y \leftrightarrow a \subseteq x)$$

For any set, there exists a set of all its subsets, called the power set.

### 8.7 Axiom of Infinity

$$\exists x (\emptyset \in x \wedge \forall a \in x (a \cup \{a\} \in x))$$

There exists a set that contains the empty set and is closed under the successor operation, guaranteeing the existence of an infinite set (for example, the natural numbers).

### 8.8 Axiom Schema of Replacement

$$\forall x \exists y \forall \omega (\omega \in y \leftrightarrow \exists a \in x (\omega = F(a)))$$

The image of a set under any definable function is itself a set.

## 8.9 Axiom of Regularity (Foundation)

$$\forall x (x \neq \emptyset \rightarrow \exists a \in x \forall \omega \in x (\omega \notin a))$$

Every nonempty set has an element disjoint from the set, ruling out infinite descending membership chains and preventing sets from containing themselves.

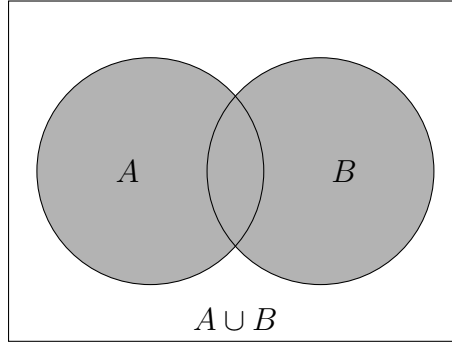
## 8.10 Axiom of Choice

$$\forall \mathcal{C} \left( \forall A \in \mathcal{C} (A \neq \emptyset) \rightarrow \exists f : \mathcal{C} \rightarrow \bigcup \mathcal{C}, f(A) \in A \right)$$

## 9 Union

The symbolic notation for union is:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$



### 1. Example 1:

Let

$$A = \{1, 2, 3\}, \quad B = \{3, 4, 5\}.$$

Then the union of  $A$  and  $B$  is

$$A \cup B = \{1, 2, 3, 4, 5\}.$$

Notice that the element 3, which is in both sets, only appears once in the union.

### 2. Example 2:

Let

$$A = \{1, 2, 3, 4, 5\}, \quad B = \{3, 4, 5, 6, 7\}, \quad C = \{5, 6, 7, 8, 9\}.$$

We ask for

$$U = A \cup B \cup C.$$

first,

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}.$$

Second,

$$(A \cup B) \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Hence,

$$\boxed{U = A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}}$$

### 3. Example 3:

Let

$$A = \left\{ x \in \mathbb{N}^+ \mid \frac{x^2}{10} < 1 \right\}$$
$$B = \{x \in \mathbb{Z} \mid -7 < x \leq -6\}$$

Since,

$$A = \{1, 2, 3\}, \quad \text{and} \quad B = \{-6\}$$

Therefore,

$$\boxed{A \cup B = \{-6, 1, 2, 3\}}$$

### 4. Example 4:

Let  $\mathcal{A}$  be a set whose elements are themselves sets. Then the union of all sets in  $\mathcal{A}$ , denoted  $\bigcup \mathcal{A}$ , is defined as:

$$\bigcup \mathcal{A} = \{x \mid \exists B \in \mathcal{A} \text{ such that } x \in B\}$$

Examples:

1.  $\mathcal{A}_1 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$

$$\bigcup \mathcal{A}_1 = \{1, 2, 3, 4\}$$

2.  $\mathcal{A}_2 = \{\{\{1\}, \{2\}\}, \{\{2\}, \{3\}\}\}$

$$\bigcup \mathcal{A}_2 = \{\{1\}, \{2\}, \{3\}\}$$

3.  $\mathcal{A}_3 = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, a\}\}$

$$\bigcup \mathcal{A}_3 = \{a, b, c, d\}$$

**5. Example 5:**

Let

$$A = \left\{ x \in \mathbb{R} \mid -8 - x > -\frac{x}{4} - 12 \right\}$$
$$B = \left\{ x \in \mathbb{R} \mid 30 - 2x < -\frac{x}{2} + 1 - 2x \right\}$$

Since,

$$A = \left( -\infty, \frac{16}{3} \right), \quad B = (-\infty, -58)$$

Therefore,

$$A \cup B = \left( -\infty, \frac{16}{3} \right)$$

**6. Example 6:**

Let

$$X = \{ \alpha \mid \alpha \in \mathbb{Z} \}.$$

In this case, because the interval of  $\mathbb{Z}$  is  $(-\infty, \infty)$ , we can systematically enumerate the set of integers by pairing each positive integer with its negative counterpart. Explicitly,

$$X = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}.$$

More formally, we can express this as

$$X = \{0\} \cup \bigcup_{n=1}^{\infty} \{-n, n\}.$$

This approach allows us to systematically enumerate all integers by pairing positive and negative integers together, ensuring we cover the entire infinite set  $\mathbb{Z}$ . Moreover, note that  $\{0\}$  is a singleton set with exactly one element, and for each natural number  $n \geq 1$ , the set  $\{-n, n\}$  has exactly two elements. In this way,  $X$  is obtained by taking infinitely many of these finite pieces and joining them together using union operations, one for each  $n \in \mathbb{N}$ .

Since the union runs over all natural numbers, we are forming what is called a countable union of finite sets. This construction demonstrates how union operations can systematically combine finite pieces to build infinite structures. Although this union process never ends, it grows step by step in correspondence with the natural numbers. We can think of this construction as building our set incrementally:

$$X_0 = \{0\}$$

$$X_1 = X_0 \cup \{-1, 1\}$$

$$X_2 = X_1 \cup \{-2, 2\}$$

$$X_3 = X_2 \cup \{-3, 3\}$$

$\vdots$

So in general,

$$X_n = \{0\} \cup \bigcup_{k=1}^n \{-k, k\}$$

Therefore,

$$X = \bigcup_{n=0}^{\infty} X_n = \mathbb{Z}.$$

Because this construction systematically organizes every integer through union operations indexed by the natural numbers, we can see how infinite unions work in practice. Each step adds new elements while preserving all previous ones, and the union operation ensures that every integer appears exactly once in the final set. This example illustrates the power of union operations in constructing complex infinite sets from simple finite components.

## 7. Example 7:

Let

$$\mathbb{Z} \cup \mathbb{N}.$$

Therefore, the union of  $\mathbb{Z}$  and  $\mathbb{N}$  is clearly  $\mathbb{Z}$ .

*Proof.*

By using the Axiom of Union:

$$\forall x \exists y \forall \alpha (\alpha \in y \leftrightarrow \exists z (z \in x \wedge \alpha \in z)).$$

Intuitively, for any set  $x$ , there exists a set  $y$  (its union) containing exactly those elements that belong to at least one member of  $x$ .

Now take  $x = \{\mathbb{Z}, \mathbb{N}\}$ . Then the axiom guarantees the existence of a set  $y$  such that:

$$\forall \alpha (\alpha \in y \leftrightarrow (\alpha \in \mathbb{Z} \vee \alpha \in \mathbb{N})).$$

Thus  $y = \mathbb{Z} \cup \mathbb{N}$ .

But since  $\mathbb{N} \subseteq \mathbb{Z}$ , we have:

$$\forall \alpha \ (\alpha \in \mathbb{N} \rightarrow \alpha \in \mathbb{Z}).$$

Hence,

$$\alpha \in \mathbb{Z} \cup \mathbb{N} \leftrightarrow (\alpha \in \mathbb{Z} \vee \alpha \in \mathbb{N}) \leftrightarrow \alpha \in \mathbb{Z}.$$

As a result,

$$\boxed{\mathbb{Z} \cup \mathbb{N} = \mathbb{Z}. \text{ QED}}$$

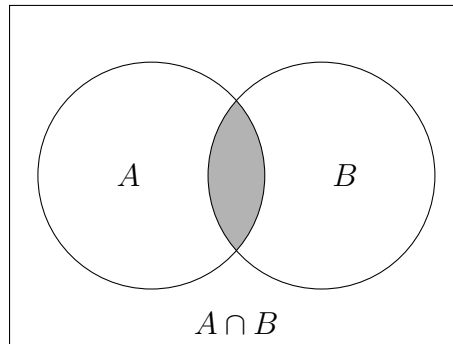
## 10 Intersection

The symbolic notation for intersection is:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Moreover, if two sets have no common element, then the two sets are *disjoint*. Formally:

$$A \cap B = \emptyset$$



### 1. Example 1:

Let

$$P = \{a, b, c, d\}, \quad Q = \{b, d, e, f\}.$$

The intersection of  $P$  and  $Q$  contains only the elements that are in both sets:

$$\boxed{P \cap Q = \{b, d\}}$$

Notice that  $a$ ,  $c$ ,  $e$ , and  $f$  are excluded because they are not in both sets.

**2. Example 2:**

Consider three sets:

$$M = \{1, 3, 5, 7\}, \quad N = \{3, 4, 5, 6\}, \quad O = \{0, 2, 5, 8\}.$$

We want the elements that all three sets share:

Only the number 5 appears in  $M$ ,  $N$ , and  $O$ :

$$M \cap N \cap O = \{5\}.$$

Hence, the intersection is:

$$\boxed{M \cap N \cap O = \{5\}}$$

**3. Example 3:**

Let

$$A = \{x \in \mathbb{Z} \mid 0 \leq x \leq 10\}$$

$$B = \{x \in \mathbb{Z} \mid 7 \leq x \leq 12\}$$

Since the set  $A$  is

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

and the set  $B$  is

$$B = \{7, 8, 9, 10, 11, 12\},$$

we have

$$\boxed{A \cap B = \{7, 8, 9, 10\}}$$

**4. Example 4:**

Let

$$C = \{x \in \mathbb{N}^+ \mid |x - 5| < 4\}$$

$$D = \{x \in \mathbb{Z} \mid 3x - 7 = 2\}$$

$$E = \{x \in \mathbb{N}^+ \mid |2x - 10| \leq 6\}$$

$$F = \{x \in \mathbb{Z} \mid |x + 1| = 7\}$$

$$G = \{x \in \mathbb{N}^+ \mid |x - 12| > 5\}.$$

Since,

$$C = \{2, 3, 4, 5, 6, 7, 8\}$$

$$D = \{3\}$$

$$E = \{2, 3, 4, 5, 6, 7, 8\}$$

$$F = \{-8, 6\}$$

For  $G$ , since  $x \in \mathbb{N}^+$ ,

$$G = \{1, 2, 3, 4, 5, 6\} \cup \{18, 19, 20, \dots\}$$

Hence

1.  $C \cap D = \{3\}$
2.  $C \cap E = \{2, 3, 4, 5, 6, 7, 8\}$  (same set)
3.  $C \cap F = \{6\}$
4.  $E \cap F = \{6\}$
5.  $C \cap G = \{2, 3, 4, 5, 6\}$
6.  $E \cap G = \{2, 3, 4, 5, 6\}$
7.  $D \cap G = \{3\}$

We conclude that,

$$\boxed{C \cap D \cap E \cap F \cap G = \emptyset}$$

## 5. Example 5:

Let

$$A = \left\{ x \in \mathbb{N}^+ \mid \frac{3x-4}{5} \leq 7 \right\}$$

$$B = \left\{ x \in \mathbb{Z} \mid \frac{2x+9}{4} = \frac{5x-1}{6} \right\}$$

Since the set  $A$  is

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

and the set  $B$  is

$$B = \emptyset \quad (\text{since } \frac{29}{4} \notin \mathbb{Z}),$$

we have

$$\boxed{A \cap B = \emptyset}$$

**6. Example 6:**

Suppose

$$A = \{\{a, b\}, \{a, d, e\}, \{a, d\}\}$$

In this case, we will answer by using intersection over the set. Therefore, the intersection over all subsets of  $A$  is:

$$\bigcap A = \bigcap_{X \in A} X$$

The element common to all subsets is  $a$ , so:

$$\boxed{\bigcap A = \{a\}}$$

**7. Example 7:**

We can also define union and intersection over an indexed collection of sets  $A_1, A_2, \dots$ :

$$\bigcup_i A_i = \{x \mid x \in A_i \text{ for some } i\}$$

$$\bigcap_i A_i = \{x \mid x \in A_i \text{ for all } i\}$$

If  $I$  is an index set and we are considering  $A_i$  for each  $i \in I$ , then:

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\}$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i \in I\}$$

Let the index set be:

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

Define a family of sets  $\{A_i\}_{i \in I}$ :

$$\begin{aligned} A_1 &= \left\{ x \in \mathbb{Z} \mid \frac{x-1}{x} = \frac{6}{3} \right\} \\ A_2 &= \left\{ y \in \mathbb{R} \mid \frac{y+8}{12} = \frac{5y+6}{4} \right\} \\ A_3 &= \left\{ z \in \mathbb{N} \mid -11(z+9) = -6 + 5 \left[ -z - \frac{99}{5} \right] \right\} \end{aligned}$$

Then we compute:

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup A_3, \quad \bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3$$

Since the sets are

$$A_1 = \{-1\}, \quad A_2 = \left\{-\frac{5}{7}\right\}, \quad A_3 = \{1\},$$

Hence,

$$\bigcup_{i \in I} A_i = \left\{-1, -\frac{5}{7}, 1\right\}, \quad \bigcap_{i \in I} A_i = \emptyset$$

## 8. Example 8:

Example 1:

Let the index set be:

$$I = \mathbb{N}$$

Define a family of sets:

$$A_i = \{i, i+1, \dots, i^2\}$$

Therefore, the first few sets are:

$$\begin{aligned} A_1 &= \{1\}, \\ A_2 &= \{2, 3, 4\}, \\ A_3 &= \{3, 4, 5, 6, 7, 8, 9\}, \\ &\vdots \end{aligned}$$

Finally, the intersection remains:

$$\bigcap_{i \in \mathbb{N}} A_i = \emptyset$$

while the union of all sets in the family is:

$$\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N}$$

Example 2:

Let the index set be:

$$I = \mathbb{Z}$$

Define a family of sets:

$$A_i = (i-1, i)$$

Therefore, the first few sets are:

$$\begin{aligned} A_{-2} &= (-3, -2), \\ A_{-1} &= (-2, -1), \\ A_0 &= (-1, 0), \\ A_1 &= (0, 1), \\ A_2 &= (1, 2), \\ A_3 &= (2, 3), \\ &\vdots \end{aligned}$$

Finally, the intersection of all sets is:

$$\bigcap_{i \in \mathbb{Z}} A_i = \emptyset$$

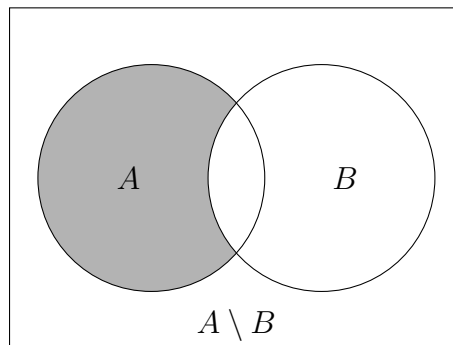
and the union of all sets is:

$$\bigcup_{i \in \mathbb{Z}} A_i = \mathbb{R}.$$

## 11 Difference

The difference of sets  $A$  and  $B$ , written  $A \setminus B$  or  $A - B$  is the set of all elements of  $A$  that are not in  $B$ :

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$



### 1. Example 1:

Let

$$A = \{apple, banana, cherry, date\}, \quad B = \{banana, date, fig\}.$$

The difference  $A - B$  consists of elements in  $A$  that are not in  $B$ :

$$\boxed{A - B = \{apple, cherry\}}$$

Here, *banana* and *date* are removed because they are present in  $B$ .

## 2. Example 2:

Consider three sets:

$$X = \{red, blue, green, yellow\}, \quad Y = \{blue, yellow, purple\}, \quad Z = \{yellow, orange\}.$$

We want the elements in  $X$  that are not in  $Y$  or  $Z$ :

Remove elements of  $Y$  from  $X$  first:

$$X - Y = \{red, green\}.$$

Then remove elements of  $Z$  (no change since *red* and *green* are not in  $Z$ ):

$$(X - Y) - Z = \{red, green\}.$$

Hence, the difference is:

$$\boxed{X - Y - Z = \{red, green\}}$$

## 3. Example 3:

Let

$$A = \{x \in \mathbb{Z} \mid -1 \leq x \leq 6\}$$

$$B = \{x \in \mathbb{Z} \mid x \geq 2\}$$

Since the set  $A$  is

$$A = \{-1, 0, 1, 2, 3, 4, 5, 6\}$$

and the set  $B$  is

$$B = \{2, 3, 4, 5, 6, 7, 8, \dots\},$$

we have

$$\boxed{A \setminus B = \{-1, 0, 1\}}$$

**4. Example 4:**

Let

$$\mathbb{Z} = \bigcup_{k=-\infty}^{\infty} \{k\}, \quad \mathbb{N}^+ = \bigcup_{k=0}^{\infty} \{k+1\}.$$

Then the difference is

$$\mathbb{Z} \setminus \mathbb{N}^+ = \{z \in \mathbb{Z} \mid z \leq 0\}.$$

So the result is the set of all non-positive integers:

$$\bigcup_{k=-\infty}^0 \{k\} = (-\infty, 0] \cap \mathbb{Z}$$

**5. Example 5:**

Let the index set be:

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

Define the family of sets  $\{A_i\}_{i \in I}$ :

$$\begin{aligned} A_1 &= \left\{ x \in \mathbb{N} \mid \frac{3x-7}{4} = \frac{6x}{2} + \frac{49}{7} \right\} \\ A_2 &= \left\{ y \in \mathbb{Z} \mid \frac{2y+9}{3} \leq 6 \right\} \\ A_3 &= \left\{ z \in \mathbb{R} \mid \frac{5z-11}{2} > 4 \right\} \end{aligned}$$

Since:

$$A_1 = \emptyset, \quad A_2 = \{x \in \mathbb{Z} \mid x \leq 4\}, \quad A_3 = \{x \in \mathbb{R} \mid x > \frac{19}{5}\}$$

Therefore:

$$\bigcup_{i \in I} A_i = \{x \in \mathbb{R} \mid x > \frac{19}{5}\} \cup \{x \in \mathbb{Z} \mid x \leq 4\}, \quad \bigcap_{i \in I} A_i = \emptyset$$

We conclude:

$$\left( \bigcup_{i \in I} A_i \right) \setminus \left( \bigcap_{i \in I} A_i \right) = \{x \in \mathbb{R} \mid x > \frac{19}{5}\} \cup \{x \in \mathbb{Z} \mid x \leq 4\}$$

## 6. Example 6:

Let

$$\begin{aligned} A &= \left\{ x \in \mathbb{R} \mid \frac{x}{2} + \frac{1}{3} < \frac{2x}{5} \right\} \\ B &= \left\{ y \in \mathbb{N} \mid 2 < \frac{y-1}{3} \leq 6 \right\} \\ C &= \{ z \in \mathbb{Z} \mid -5 \leq z \leq 10 \} \end{aligned}$$

Since

$$A = \left( -\infty, -\frac{10}{3} \right), \quad B = (7, 19] \cap \mathbb{N}, \quad C = [-5, 10] \cap \mathbb{Z}$$

Thus,

$$A \cap B = \emptyset$$

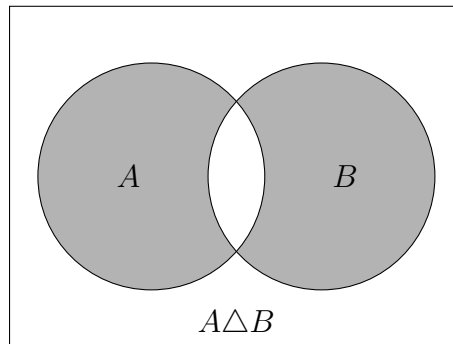
We conclude that,

$$\boxed{(A \cap B) \setminus C = \emptyset}$$

## 12 Symmetric Difference

The symmetric difference of sets  $A$  and  $B$ , written  $A \Delta B$ , is the set of all elements that are in either  $A$  or  $B$  but not in both:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$



### 1. Example 1:

Let

$$A = \{1, 2, 3, 4\}, \quad B = \{3, 4, 5, 6\}.$$

The symmetric difference consists of elements that belong to exactly one of the two sets. Hence,

$$\boxed{A \Delta B = \{1, 2, 5, 6\}}$$

The elements 3 and 4 are excluded since they appear in both  $A$  and  $B$ .

## 2. Example 2:

Consider three sets:

$$X = \{1, 2, 3, 4\}, \quad Y = \{3, 4, 5, 6\}, \quad Z = \{4, 5, 6, 7\}.$$

First, compute the symmetric difference of  $X$  and  $Y$ :

$$X \Delta Y = \{1, 2, 5, 6\}.$$

Next, compute the symmetric difference with  $Z$ :

$$\{1, 2, 5, 6\} \Delta \{4, 5, 6, 7\} = \{1, 2, 4, 7\}.$$

Therefore,

$$\boxed{X \Delta Y \Delta Z = \{1, 2, 4, 7\}}$$

## 3. Example 3:

Let

$$A = \left\{ (p, q) \in \mathbb{N}^2 \mid \frac{3p + 2q}{p} \geq 9, p \neq 0 \right\},$$
$$B = \left\{ x \in \mathbb{Z}^+ \mid \frac{x - 1}{x} = x + 1 \right\}.$$

Since

$$A = \bigcup_{p=1}^{\infty} \{p\} \times ([3p, \infty) \cap \mathbb{N}),$$

and

$$B = \emptyset,$$

we have

$$A \cap B = \emptyset.$$

Since the sets are disjoint,

$$A \Delta B = A.$$

Thus,

$$\boxed{A \Delta B = \bigcup_{p=1}^{\infty} \{p\} \times ([3p, \infty) \cap \mathbb{N})}$$

## 4. Example 4:

Let

$$A = \{p \in \mathbb{R} \mid -4(p - 4) \geq -2(p + 1)\},$$
$$B = \{q \in \mathbb{R} \mid -46 < 4q - 6 \leq -26\},$$
$$C = \{r \in \mathbb{R} \mid -(1 + 2r) > -6(r - 4) - 1\}.$$

Solving the inequalities gives

$$A = (-\infty, 9], \quad B = (-10, -5], \quad C = (6, \infty).$$

Hence,

$$A \cup B = (-\infty, 9], \quad C \setminus A = (9, \infty).$$

Since these sets are disjoint,

$$(A \cup B) \Delta (C \setminus A) = (-\infty, 9] \cup (9, \infty) = (-\infty, \infty).$$

Therefore,

$$(A \cup B) \Delta (C \setminus A) = (-\infty, \infty)$$

### 5. Example 5:

Let

$$A = \bigcup_{n \in \mathbb{N}} \{f^k(n) : k \geq 0\}, \quad B = \bigcup_{k \in \mathbb{N}} \{k^2 - k + 1\},$$

where

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even,} \\ 3n + 1, & \text{if } n \text{ is odd.} \end{cases}$$

Since  $f^0(n) = n$ , every natural number belongs to  $A$ , hence

$$A = \mathbb{N}.$$

Therefore,

$$A \cup B = \mathbb{N}, \quad A \cap B = B.$$

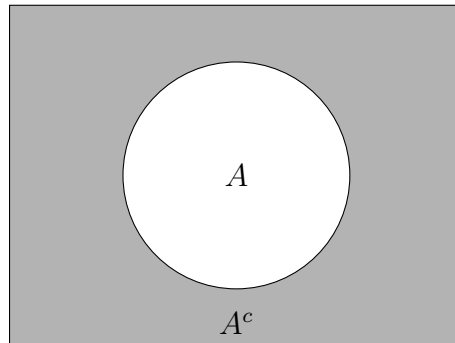
We conclude that,

$$A \Delta B = \{m \in \mathbb{N} \mid m \neq k^2 - k + 1 \text{ for any } k \in \mathbb{N}\}$$

## 13 Complement

The symbolic notation for Complement is:

$$A^c = \{x \in U \mid x \notin A\}$$



**1. Example 1:**

Let

$$U = \{1, 2, 3, 4, 5, 6\} \quad (\text{the universal set}), \quad A = \{2, 4, 6\}.$$

Hence,

$$A^c = \{1, 3, 5\}$$

The elements 2, 4, and 6 are excluded since they belong to  $A$ .

**2. Example 2:**

Consider the universal set and two subsets:

$$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, \quad B = \{1, 3, 5, 7, 9\}, \quad C = \{2, 3, 4, 5\}.$$

The complement of  $B$  in  $U$  is

$$B^c = \{2, 4, 6, 8\}.$$

The complement of  $C$  in  $U$  is

$$C^c = \{1, 6, 7, 8, 9\}.$$

**3. Example 3:**

Let

$$A = \bigcup_{k \in \mathbb{N}} \{2k + 1\}, \quad B = \bigcup_{k \in \mathbb{N}} \{2k\}.$$

Since  $A$  is the set of odd natural numbers and  $B$  is the set of even natural numbers, we have

$$B^c = \mathbb{N} \setminus B = A.$$

**4. Example 4:**

Let

$$A = \{p \in \mathbb{P} \mid p + 2 \in \mathbb{P}\},$$

that is,  $A$  is the set of primes  $p$  such that  $p + 2$  is also prime.

Let

$$U = \bigcup_{k \in \mathbb{N}} \{2k + 1\} = \{1, 3, 5, 7, 9, 11, 13, \dots\}.$$

Then the complement of  $A$  relative to  $U$  is

$$A^c = U \setminus A.$$

Hence,

$$A^c = \{2k + 1 \mid k \in \mathbb{N}\} \setminus \{p \in \mathbb{P} \mid p + 2 \in \mathbb{P}\}$$

5. **Example 5:**

Let

$$L = \{ (x, y) \in \mathbb{R}^2 \mid y - 3 = x - 2 \}.$$

Thus,  $L$  is the line of slope 1 passing through the point  $(2, 3)$ .

Let

$$A = \{ (x, y) \in \mathbb{R}^2 \mid y > x + 1 \},$$

the set of points strictly above the line  $y = x + 1$ .

The complement of  $A$  relative to  $\mathbb{R}^2$  is

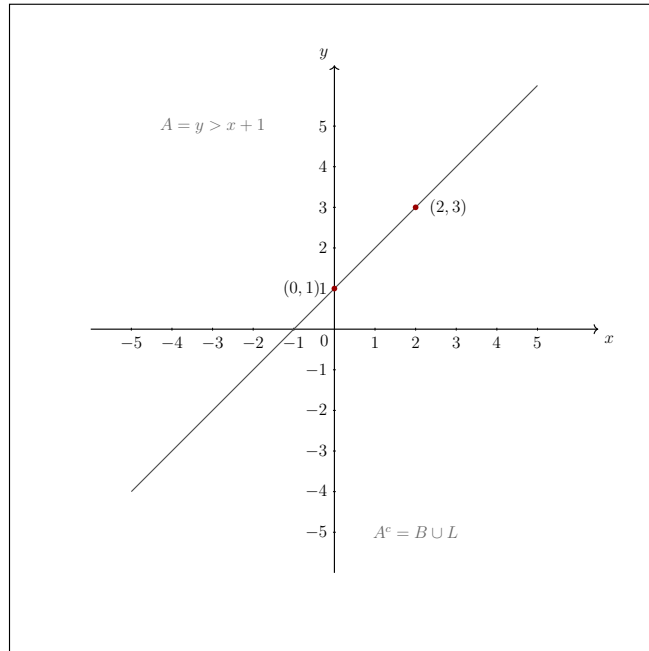
$$A^c = \mathbb{R}^2 \setminus A.$$

That is,

$$A^c = \bigcup_{x \in \mathbb{R}} \{ (x, y) \in \mathbb{R}^2 \mid y \leq x + 1 \} = B \cup L$$

where

$$B = \{ (x, y) \in \mathbb{R}^2 \mid y < x + 1 \}, \quad L = \{ (x, y) \in \mathbb{R}^2 \mid y = x + 1 \}.$$



## 14 Cartesian Product

It follows from the Axiom of Extensionality that sets have no intrinsic order to their elements. For instance, in an unordered pair

$$\{x, y\} = \{y, x\}$$

the order does not matter.

However, when we need to represent ordered structures, we use ordered pairs, written  $\langle x, y \rangle$ . Here, order does matter:

$$\langle x, y \rangle \neq \langle y, x \rangle \quad \text{if } x \neq y$$

An ordered pair  $\langle a, b \rangle$  is defined in set theory using the *Wiener–Kuratowski* definition:

$$\langle a, b \rangle := \{\{a\}, \{a, b\}\}$$

This definition guarantees that

$$\langle a, b \rangle = \langle c, d \rangle \leftrightarrow a = c \text{ and } b = d$$

*Proof.*

Suppose

$$\langle a, b \rangle = \langle c, d \rangle.$$

By definition, this means

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}.$$

So the two sets have the same elements. There are two cases:

1. If  $\{a\} = \{c\}$ , then  $a = c$ . Then  $\{a, b\} = \{c, d\}$ , so  $\{a, b\} = \{a, d\}$ . This forces  $b = d$ .
2. If  $\{a\} = \{c, d\}$ , then  $\{a\}$  must have two elements unless  $c = d$ . But  $\{a\}$  has only one element, so  $c = d$  and  $a = c = d$ . Then from  $\{a, b\} = \{c\} = \{a\}$ , we get  $b = a = d$ .

Thus in either case,  $a = c$  and  $b = d$ .

If  $a = c$  and  $b = d$ , then clearly

$$\langle a, b \rangle = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = \langle c, d \rangle.$$

Hence,

$$\langle a, b \rangle = \langle c, d \rangle \leftrightarrow a = c \text{ and } b = d. \quad Q.E.D.$$

The idea of ordered pairs can be extended to longer sequences. For example, a triple  $\langle x, y, z \rangle$  is represented as  $\langle \langle x, y \rangle, z \rangle$ , and a quadruple  $\langle x, y, z, u \rangle$  is  $\langle \langle \langle x, y \rangle, z \rangle, u \rangle$ .

In general, an ordered  $n$ -tuple is defined as nested ordered pairs:

$$\langle x_1, x_2, \dots, x_n \rangle$$

With this in mind, we can now define the Cartesian product. Since order matters, we collect all possible ordered pairs with the first element taken from  $A$  and the second from  $B$ :

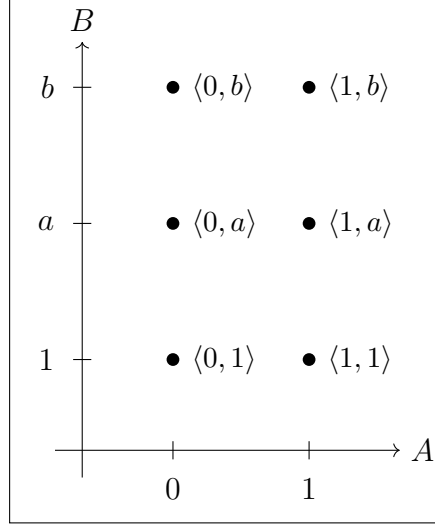
$$A \times B = \{\langle a, b \rangle \mid a \in A \wedge b \in B\}$$

For example, let

$$\begin{aligned} A &= \{0, 1\} \\ B &= \{1, a, b\} \end{aligned}$$

Then the Cartesian product is

$\langle 0, 1 \rangle$	$\langle 0, a \rangle$	$\langle 0, b \rangle$
$\langle 1, 1 \rangle$	$\langle 1, a \rangle$	$\langle 1, b \rangle$



As we have seen, the cardinality  $|A| = 2$  and  $|B| = 3$ . Hence,

$$|A \times B| = 6.$$

Note that the Cartesian product is not commutative:

$$A \times B \neq B \times A.$$

Indeed,

$$A \times B = \{\langle 0, 1 \rangle, \langle 0, a \rangle, \langle 0, b \rangle, \langle 1, 1 \rangle, \langle 1, a \rangle, \langle 1, b \rangle\},$$

whereas

$$B \times A = \{\langle 1, 0 \rangle, \langle 1, 1 \rangle, \langle a, 0 \rangle, \langle a, 1 \rangle, \langle b, 0 \rangle, \langle b, 1 \rangle\}.$$

Both sets have six elements, but they are different because order matters. The Cartesian product can be extended to products of a set with itself. For a set  $A$ ,

$$\begin{aligned} A^1 &= A, \\ A^2 &= A \times A, \\ A^3 &= A^2 \times A, \\ &\vdots \\ A^{k+1} &= A^k \times A. \end{aligned}$$

If  $|A| = n$ , then  $|A^k| = n^k$  for all  $k \geq 1$ , as shown by induction. More generally, if  $|A| = n$  and  $|B| = m$ , then

$$|A \times B| = n \cdot m.$$

Let

$$C_x = \{\langle x, y \rangle \mid y \in B\}, \quad x \in A.$$

Each set  $C_x$  has  $m$  elements, the family  $\{C_x\}_{x \in A}$  is pairwise disjoint, and

$$A \times B = \bigcup_{x \in A} C_x.$$

Cartesian powers naturally lead to the notion of words. A word of length  $n$  over  $A$  is an element of  $A^n$ . The set of all finite words over  $A$  is the *Kleene star*:

$$A^* = \bigcup_{k=0}^{\infty} A^k,$$

where  $A^0 = \{\emptyset\}$  is the empty word.

### 1. Example 1.

Let

$$A = \{1, 2\}, \quad B = \{3, 4\}.$$

Then

$\langle 1, 3 \rangle$	$\langle 1, 4 \rangle$
$\langle 2, 3 \rangle$	$\langle 2, 4 \rangle$

Note that  $\langle 1, 3 \rangle \neq \langle 3, 1 \rangle$ .

### 2. Example 2.

Let

$$X = \{1, 2\}, \quad Y = \{a, b\}, \quad Z = \{0, 9\}.$$

First,

$$X \times Y = \{\langle 1, a \rangle, \langle 1, b \rangle, \langle 2, a \rangle, \langle 2, b \rangle\}.$$

Then

$\langle \langle 1, a \rangle, 0 \rangle$	$\langle \langle 1, a \rangle, 9 \rangle$
$\langle \langle 1, b \rangle, 0 \rangle$	$\langle \langle 1, b \rangle, 9 \rangle$
$\langle \langle 2, a \rangle, 0 \rangle$	$\langle \langle 2, a \rangle, 9 \rangle$
$\langle \langle 2, b \rangle, 0 \rangle$	$\langle \langle 2, b \rangle, 9 \rangle$

### 3. Example 3.

Let

$$A = \{1, 2\}, \quad B = \{3, 4\}, \quad C = \{5, 6\}, \quad D = \{7, 8\}.$$

The Cartesian product  $A \times B \times C \times D$  consists of ordered quadruples:

$\langle \langle \langle 1, 3 \rangle, 5 \rangle, 7 \rangle$	$\langle \langle \langle 1, 3 \rangle, 5 \rangle, 8 \rangle$	$\langle \langle \langle 1, 3 \rangle, 6 \rangle, 7 \rangle$	$\langle \langle \langle 1, 3 \rangle, 6 \rangle, 8 \rangle$
$\langle \langle \langle 1, 4 \rangle, 5 \rangle, 7 \rangle$	$\langle \langle \langle 1, 4 \rangle, 5 \rangle, 8 \rangle$	$\langle \langle \langle 1, 4 \rangle, 6 \rangle, 7 \rangle$	$\langle \langle \langle 1, 4 \rangle, 6 \rangle, 8 \rangle$
$\langle \langle \langle 2, 3 \rangle, 5 \rangle, 7 \rangle$	$\langle \langle \langle 2, 3 \rangle, 5 \rangle, 8 \rangle$	$\langle \langle \langle 2, 3 \rangle, 6 \rangle, 7 \rangle$	$\langle \langle \langle 2, 3 \rangle, 6 \rangle, 8 \rangle$
$\langle \langle \langle 2, 4 \rangle, 5 \rangle, 7 \rangle$	$\langle \langle \langle 2, 4 \rangle, 5 \rangle, 8 \rangle$	$\langle \langle \langle 2, 4 \rangle, 6 \rangle, 7 \rangle$	$\langle \langle \langle 2, 4 \rangle, 6 \rangle, 8 \rangle$

4. **Example 4.**

$$A = \{(x, y) \in \mathbb{R}^2 \mid y = \frac{3}{2}x - 1\},$$

$$B = \{(m, n) \in \mathbb{Z}^2 \mid m \geq 6n, m \neq 0\}.$$

Thus,

$$A \times B = \left\{ \left( (x, \frac{3}{2}x - 1), (m, n) \right) \mid x \in \mathbb{R}, m, n \in \mathbb{Z}, m \geq 6n, m \neq 0 \right\}.$$

5. **Example 5.**

Let

$$A = \{\langle x \rangle \mid x \in \{p, q, r\}\}, \quad B = \{\langle y \rangle \mid y \in \{0, 1, 2\}\}.$$

Then

$C_{\langle p \rangle} = \{\langle p, 0 \rangle, \langle p, 1 \rangle, \langle p, 2 \rangle\}$		0	1	2
$C_{\langle q \rangle} = \{\langle q, 0 \rangle, \langle q, 1 \rangle, \langle q, 2 \rangle\}$	$p$	$\langle p, 0 \rangle$	$\langle p, 1 \rangle$	$\langle p, 2 \rangle$
$C_{\langle r \rangle} = \{\langle r, 0 \rangle, \langle r, 1 \rangle, \langle r, 2 \rangle\}$	$q$	$\langle q, 0 \rangle$	$\langle q, 1 \rangle$	$\langle q, 2 \rangle$
	$r$	$\langle r, 0 \rangle$	$\langle r, 1 \rangle$	$\langle r, 2 \rangle$

6. **Example 6.**

Let

$$I = [0, 1], \quad A_\alpha = [\alpha, 2] \times [0, \alpha].$$

For selected values of  $\alpha$ :

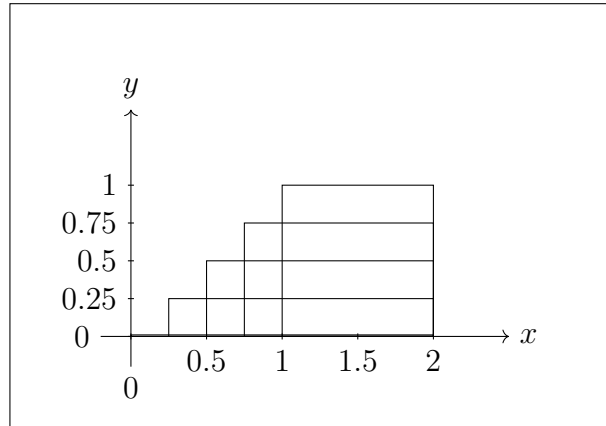
$$A_0 = [0, 2] \times \{0\},$$

$$A_{0.25} = [0.25, 2] \times [0, 0.25],$$

$$A_{0.5} = [0.5, 2] \times [0, 0.5],$$

$$A_{0.75} = [0.75, 2] \times [0, 0.75],$$

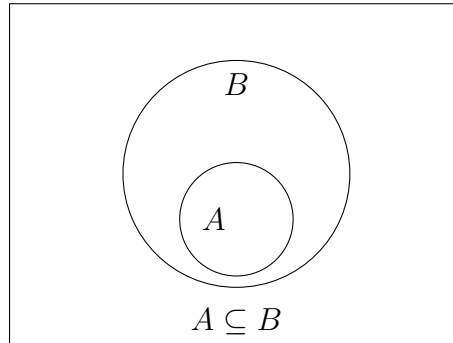
$$A_1 = [1, 2] \times [0, 1].$$



## 15 Subset

The symbolic notation for subset is:

$$A \subseteq B \leftrightarrow \forall x (x \in A \rightarrow x \in B)$$



If  $A$  is not a subset of  $B$ , we write  $A \not\subseteq B$ . This means that there exists at least one element in  $A$  that is not in  $B$ :

$$A \not\subseteq B \leftrightarrow \exists x (x \in A \wedge x \notin B)$$

Furthermore, It's crucial to distinguish between an element of a set and a subset of a set:

1.  $2 \in \mathbb{Z}$
2.  $\mathbb{E} \subseteq \mathbb{Z}$  (the set of even numbers is a subset of the integers)
3. A set can be both an element and a subset of another set.

For example:

$$\{1\} \in \{1, \{1\}\} \quad \text{and} \quad \{1\} \subseteq \{1, \{1\}\}$$

This shows that a set can be both an element and a subset of another set:

1.  $\{1\} \in \{1, \{1\}\}$ , which means that the set  $\{1\}$  appears as an element of the larger set.
2.  $\{1\} \subseteq \{1, \{1\}\}$ , since every element of  $\{1\}$  (namely 1) is also an element of the larger set.

In contrast, the number 1 itself is only an element and not a subset:

1.  $1 \in \{1, \{1\}\}$ , because 1 is an element of the set.
2.  $1 \not\subseteq \{1, \{1\}\}$ , since 1 is not a set and therefore cannot be a subset.

### 1. Example 1

$$A \subseteq B \rightarrow A \cup B = B$$

*Proof.*

By definition of subset,

$$A \subseteq B \leftrightarrow \forall x (x \in A \rightarrow x \in B).$$

By definition of union,

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Thus,

$$x \in A \cup B \leftrightarrow (x \in A \vee x \in B).$$

Since  $A \subseteq B$ , we have  $x \in A \rightarrow x \in B$ , and therefore

$$(x \in A \vee x \in B) \leftrightarrow (x \in B \vee x \in B) \leftrightarrow x \in B.$$

Hence,

$$\boxed{A \cup B = B. \quad \text{QED}}$$

### 2. Example 2

$$A \subseteq B \rightarrow A \cap B = A$$

*Proof.*

By definition of intersection,

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Thus,

$$x \in A \cap B \leftrightarrow (x \in A \wedge x \in B).$$

Since  $A \subseteq B$ ,  $x \in A$  implies  $x \in B$ , so

$$(x \in A \wedge x \in B) \leftrightarrow x \in A.$$

Therefore,

$$\boxed{A \cap B = A. \quad \text{QED}}$$

### 3. Example 3

Let

$$A \in B.$$

Then,

$$A \subseteq \bigcup B.$$

*Proof.*

By definition,

$$\bigcup B = \{x \mid \exists C \in B (x \in C)\}.$$

If  $x \in A$  and  $A \in B$ , then taking  $C = A$  gives  $x \in \bigcup B$ . Hence,

$$\boxed{A \subseteq \bigcup B. \quad \text{QED}}$$

### 4. Example 4

Let

$$A = \{1, 2, 3, 4, 5\}, \quad B = \{2, 4\}.$$

Every element of  $B$  is an element of  $A$ , so

$$\boxed{B \subseteq A}.$$

### 5. Example 5

Let

$$X = \{10, 20, 30, 40\}, \quad Y = \{10, 20, 30, 40\}, \quad Z = \{20, 30\}.$$

Then,

$$\boxed{Y \subseteq X \quad \text{and} \quad Z \subseteq X}.$$

### 6. Example 6

Let

$$A = \{1, 2, 3\}, \quad B = \{3, 2, 1\}.$$

By extensionality,

$$A = B \leftrightarrow A \subseteq B \text{ and } B \subseteq A.$$

Moreover, every set satisfies

$$A \subseteq A,$$

and for every set  $A$ ,

$$\boxed{\emptyset \subseteq A}.$$

## 7. Example 7

$$\mathbb{N}^+ \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Each inclusion is proper:

$$\boxed{\mathbb{N}^+ \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}}.$$

Let

$$\mathbb{B} = \{0, 1\}.$$

Then the Kleene star is

$$\mathbb{B}^* = \{\Lambda, 0, 1, 00, 01, 10, 11, 000, \dots\}.$$

For any string  $x \in A^*$  with

$$x = x_1x_2 \dots x_n,$$

its length is defined by

$$\boxed{\text{len}(x) = n}.$$

## 16 Power Set

The symbolic notation for the power set of a set  $A$  is:

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}$$

### 1. Example 1.

Let

$$S = \{a, b\}.$$

Then the power set of  $S$  is

$$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Since  $|S| = 2$ , we have

$$|\mathcal{P}(S)| = 2^{|S|} = 2^2.$$

**2. Example 2.**

Let

$$Y = \emptyset.$$

Then

$$\mathcal{P}(Y) = \{\emptyset\}.$$

Hence,

$$|\mathcal{P}(Y)| = 2^{|Y|} = 2^0 = 1.$$

**3. Example 3.**

Let

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

Then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Thus,

$$|\mathcal{P}(A)| = 2^{|A|} = 2^3.$$

Let

$$B = \mathcal{P}(\mathcal{P}(A)).$$

Therefore,

$$|\mathcal{P}(\mathcal{P}(A))| = 2^{|\mathcal{P}(A)|} = 256.$$

4. **Example 4.**

Let

$$A = \{1, 2\}, \quad B = \{3, 4\}.$$

Define

$$C = \mathcal{P}(A) \times \mathcal{P}(B).$$

Since

$$|\mathcal{P}(A)| = 2^{|A|}, \quad |\mathcal{P}(B)| = 2^{|B|},$$

it follows that

$$|C| = 2^{|A|+|B|} = 16.$$

Explicitly,

$(\emptyset, \emptyset)$	$(\emptyset, \{3\})$	$(\emptyset, \{4\})$	$(\emptyset, \{3, 4\})$
$(\{1\}, \emptyset)$	$(\{1\}, \{3\})$	$(\{1\}, \{4\})$	$(\{1\}, \{3, 4\})$
$(\{2\}, \emptyset)$	$(\{2\}, \{3\})$	$(\{2\}, \{4\})$	$(\{2\}, \{3, 4\})$
$(\{1, 2\}, \emptyset)$	$(\{1, 2\}, \{3\})$	$(\{1, 2\}, \{4\})$	$(\{1, 2\}, \{3, 4\})$

5. **Example 5.**

Let

$$A = \{x \in \mathcal{P}(\{1, 2, 3, 4\}) \mid 2 \in x\}.$$

The power set of  $\{1, 2, 3, 4\}$  is

$\emptyset$	$\{1\}$	$\{2\}$	$\{3\}$
$\{4\}$	$\{1, 2\}$	$\{1, 3\}$	$\{1, 4\}$
$\{2, 3\}$	$\{2, 4\}$	$\{3, 4\}$	$\{1, 2, 3\}$
$\{1, 2, 4\}$	$\{1, 3, 4\}$	$\{2, 3, 4\}$	$\{1, 2, 3, 4\}$

Selecting only those subsets that contain 2,

$\{2\}$	$\{1, 2\}$	$\{2, 3\}$	$\{2, 4\}$
$\{1, 2, 3\}$	$\{1, 2, 4\}$	$\{2, 3, 4\}$	$\{1, 2, 3, 4\}$

Hence,

$$|A| = 8.$$

## 17 Properties and Laws

### 17.1 Commutative Laws

1.  $A \cup B = B \cup A$
2.  $A \cap B = B \cap A$

Let

$$A = \{1, 2, 3\}, \quad B = \{3, 4, 5\}.$$

Operation	Result
$A \cup B$	$\{1, 2, 3, 4, 5\}$
$B \cup A$	$\{1, 2, 3, 4, 5\}$
$A \cap B$	$\{3\}$
$B \cap A$	$\{3\}$

### 17.2 Associative Laws

1.  $(A \cup B) \cup C = A \cup (B \cup C)$
2.  $(A \cap B) \cap C = A \cap (B \cap C)$

Let

$$A = \{1, 2\}, \quad B = \{2, 3\}, \quad C = \{3, 4\}.$$

Operation	Result
$(A \cup B) \cup C$	$\{1, 2, 3, 4\}$
$A \cup (B \cup C)$	$\{1, 2, 3, 4\}$
$(A \cap B) \cap C$	$\emptyset$
$A \cap (B \cap C)$	$\emptyset$

### 17.3 Distributive Laws

1.  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
2.  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Let

$$A = \{1, 2\}, \quad B = \{2, 3\}, \quad C = \{3, 4\}.$$

Operation	Result
$A \cup (B \cap C)$	$\{1, 2, 3\}$
$(A \cup B) \cap (A \cup C)$	$\{1, 2, 3\}$
$A \cap (B \cup C)$	$\{2\}$
$(A \cap B) \cup (A \cap C)$	$\{2\}$

## 17.4 De Morgan's Laws

1.  $(A \cup B)^c = A^c \cap B^c$
2.  $(A \cap B)^c = A^c \cup B^c$

Let

$$U = \{1, 2, 3, 4, 5\}, \quad A = \{1, 2\}, \quad B = \{2, 3\}.$$

$$A^c = \{3, 4, 5\}, \quad B^c = \{1, 4, 5\}.$$

Operation	Result
$(A \cup B)^c$	$\{4, 5\}$
$A^c \cap B^c$	$\{4, 5\}$
$(A \cap B)^c$	$\{1, 3, 4, 5\}$
$A^c \cup B^c$	$\{1, 3, 4, 5\}$

## 17.5 Identity Laws

1.  $A \cup \emptyset = A$
2.  $A \cap U = A$

Let

$$U = \{1, 2, 3, 4, 5\}, \quad A = \{2, 3, 4\}.$$

Operation	Result
$A \cup \emptyset$	$\{2, 3, 4\}$
$A \cap U$	$\{2, 3, 4\}$

## 17.6 Idempotent Laws

1.  $A \cup A = A$
2.  $A \cap A = A$

Let

$$A = \{1, 3, 5\}.$$

Operation	Result
$A \cup A$	$\{1, 3, 5\}$
$A \cap A$	$\{1, 3, 5\}$

## 17.7 Complement Laws

1.  $A \cup A^c = U$
2.  $A \cap A^c = \emptyset$
3.  $(A^c)^c = A$

Let

$$U = \{1, 2, 3, 4, 5\}, \quad A = \{1, 3, 5\}.$$

$$A^c = \{2, 4\}.$$

Operation	Result
$A \cup A^c$	$U$
$A \cap A^c$	$\emptyset$
$(A^c)^c$	$A$

## 17.8 Absorption Laws

1.  $A \cup (A \cap B) = A$
2.  $A \cap (A \cup B) = A$

Let

$$A = \{1, 2, 3\}, \quad B = \{2, 3, 4\}.$$

Operation	Result
$A \cup (A \cap B)$	$\{1, 2, 3\}$
$A \cap (A \cup B)$	$\{1, 2, 3\}$

## 18 Relations As a Sets

Recall these sets,

1.  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ , *the set of natural numbers.*
2.  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ , *the set of integers.*
3.  $\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$ , *the set of rational numbers.*
4.  $\mathbb{R} = (-\infty, \infty)$ , *the set of real numbers (the continuum).*

One of the standard relations we can define on these sets is the order relation ( $\geq, \leq, <, >$ ). For example, let us define the relation  $<$  on  $\mathbb{N}$ :

Definition of  $R$ :

$$R = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n < m \}$$

This means  $R$  is the set of all ordered pairs  $\langle n, m \rangle$  where both  $n$  and  $m$  are natural numbers and  $n$  is less than  $m$ .

In detail:

1.  $\langle 0, 1 \rangle \in R$  since  $0 < 1$ .
2.  $\langle 1, 5 \rangle \in R$  since  $1 < 5$ .
3.  $\langle 2, 3 \rangle \in R$  since  $2 < 3$ .

This relations capture the idea that:

$$n < m \leftrightarrow \langle n, m \rangle \in R$$

## 18.1 Binary Relations

A binary relation on a set  $A$  is any subset of  $A^2$ . If  $R \subseteq A^2$  is a binary relation, and  $x, y \in A$ , we write:

$$xRy \quad \text{to mean} \quad \langle x, y \rangle \in R$$

For example:

We can think of  $\mathbb{N}^2$  as an infinite matrix of ordered pairs:

$$\begin{array}{lcl} 0 : & \langle 0, 0 \rangle, \langle 0, 1 \rangle, \dots, \langle 0, m \rangle \dots \\ 1 : & \langle 1, 0 \rangle, \langle 1, 1 \rangle, \dots, \langle 1, m \rangle \dots \\ & \vdots \\ & \vdots \\ n : & \langle n, 0 \rangle, \langle n, 1 \rangle, \dots, \langle n, m \rangle \dots \end{array}$$

Moreover, for Subsets of  $\mathbb{N}^2$  with  $n, m \in \{0, 1, 2, 3, \dots\}$ :

1. Identity relation

$$I = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n = m \}$$

Explicitly,

$$I = \{ \langle 0, 0 \rangle, \langle 1, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 3 \rangle, \dots \}.$$

2. Less-than relation

$$L = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n < m \}$$

$\langle 0, 1 \rangle$	$\langle 0, 2 \rangle$	$\langle 0, 3 \rangle$
	$\langle 1, 2 \rangle$	$\langle 1, 3 \rangle$
		$\langle 2, 3 \rangle$
$\vdots$	$\vdots$	$\vdots$

### 3. Greater-than relation

$$G = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n > m \}$$

$\langle 1, 0 \rangle$		
$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$	
$\langle 3, 0 \rangle$	$\langle 3, 1 \rangle$	$\langle 3, 2 \rangle$
$\vdots$	$\vdots$	$\vdots$

### 4. Less-than-or-equal relation

$$K = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n \leq m \}$$

Equivalently,

$$K = L \cup I,$$

where

$$I = \{ \langle n, n \rangle \mid n \in \mathbb{N} \}$$

is the identity relation.

$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 0, 2 \rangle$	$\langle 0, 3 \rangle$
	$\langle 1, 1 \rangle$	$\langle 1, 2 \rangle$	$\langle 1, 3 \rangle$
		$\langle 2, 2 \rangle$	$\langle 2, 3 \rangle$
			$\langle 3, 3 \rangle$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

### 5. Greater-than-or-equal relation

$$H = \{ \langle n, m \rangle \in \mathbb{N}^2 \mid n \geq m \}$$

Equivalently,

$$H = G \cup I.$$

$\langle 0, 0 \rangle$			
$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$		
$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 2, 2 \rangle$	
$\langle 3, 0 \rangle$	$\langle 3, 1 \rangle$	$\langle 3, 2 \rangle$	$\langle 3, 3 \rangle$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

The relations  $L$  and  $G$  are *strict orders*. They are irreflexive, since for no  $n \in \mathbb{N}$  do we have  $nLn$  or  $nGn$ .

## 18.2 Unnatural Relations

Any subset of  $A^2$  is a relation on  $A$ . This means that relations can be formed not only from familiar notions such as  $<$  or  $=$ , but also from arbitrary conditions.

### 1. Empty relation

This is the relation that contains no ordered pairs. For every  $x, y \in A$ , we have

$$\langle x, y \rangle \notin \emptyset.$$

In other words, nothing is related to anything else.

### 2. Universal relation

This is the relation that contains all possible ordered pairs from  $A$ . For every  $x, y \in A$ , we have

$$\langle x, y \rangle \in A^2.$$

In other words, everything is related to everything else.

Example of an arbitrary relation

$$E = \{ \langle n, m \rangle \mid n > 5 \text{ or } m \cdot n \geq 34 \}$$

Some explicit examples are:

1.  $\langle 6, 0 \rangle \in E$  since  $6 > 5$ .
2.  $\langle 2, 17 \rangle \in E$  since  $2 \cdot 17 = 34 \geq 34$ .
3.  $\langle 4, 5 \rangle \notin E$  since  $4 \not> 5$  and  $4 \cdot 5 = 20 < 34$ .

## 19 Properties of Relations

Let  $R \subseteq A^2$  be a binary relation on a set  $A$ :

## 19.1 Reflexivity

$$\forall x \in A, xRx$$

### Example:

The relation  $\leq$  on  $\mathbb{R}$  is reflexive because  $3 \leq 3$ . Likewise, the subset relation  $\subseteq$  is reflexive:  $\{1\} \subseteq \{1\}$ . In both cases, every element is related to itself.

## 19.2 Irreflexivity

$$\forall x \in A, \neg(xRx)$$

### Example:

The relation  $<$  on  $\mathbb{N}$  is irreflexive because no number is less than itself:  $5 < 5$  is false, so  $\neg(5 < 5)$ .

## 19.3 Asymmetry

$$\forall x, y \in A, xRy \rightarrow \neg(yRx)$$

### Example:

The relation  $<$  on  $\mathbb{N}$  is asymmetric because  $2 < 3$ , but  $3 < 2$  is false. There is no pair such that both  $xRy$  and  $yRx$  hold. Therefore,  $<$  is asymmetric. Any asymmetric relation is automatically irreflexive.

## 19.4 Symmetry

$$\forall x, y \in A, xRy \rightarrow yRx$$

### Example:

Let

$$A = \{1, 2, 3\} \quad \text{and} \quad R = \{1R2, 2R1, 2R3, 3R2\}$$

This relation is symmetric because:

$$1R2 \quad \text{and} \quad 2R1$$

$$2R3 \quad \text{and} \quad 3R2$$

Every pair has its mirror image in the relation. Therefore,  $R$  is symmetric.

## 19.5 Antisymmetry

$$\forall x, y \in A, (xRy \wedge yRx) \rightarrow x = y$$

### 1. Example 1: (on $\mathbb{N}$ ):

Let  $R = \leq$ . If  $x \leq y$  and  $y \leq x$ , then  $x = y$ . Therefore,  $\leq$  is antisymmetric.

2. **Example 2:** (on  $\subseteq$ ):

Let

$$A = \{1, 2\} \quad \text{and} \quad \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

If  $X \subseteq Y$  and  $Y \subseteq X$ , then  $X = Y$ . Therefore,  $\subseteq$  is antisymmetric on  $\mathcal{P}(A)$ .

3. **Example 3:**

Let

$$A = \{1, 2, 3\} \quad \text{and} \quad R = \{1R1, 2R2, 3R3, 1R2\}$$

Since  $2R1 \notin R$ , no pair of distinct elements appears in both directions. Therefore,  $R$  is antisymmetric.

## 19.6 Transitivity

$$\forall x, y, z \in A, (xRy \wedge yRz) \rightarrow xRz$$

1. **Example 1:**

The relation  $<$  on  $\mathbb{N}$  is transitive:

$$2 < 4 \wedge 4 < 5 \rightarrow 2 < 5$$

2. **Example 2:**

The subset relation  $\subseteq$  is transitive:

$$\{1\} \subseteq \{1, 2\}, \{1, 2\} \subseteq \{1, 2, 3\} \rightarrow \{1\} \subseteq \{1, 2, 3\}.$$

3. **Counterexample:**

Let  $A = \{1, 2, 3\}$  and  $R = \{1R2, 2R3\}$ . Here,  $1R3 \notin R$  despite  $1R2$  and  $2R3$  being in  $R$ . Therefore,  $R$  is not transitive.

## 19.7 Connectivity

$$\forall x, y \in A, x \neq y \rightarrow (xRy \vee yRx)$$

1. **Example 1 (on  $\mathbb{N}$ ):**

The relation  $\leq$  is connected because for any distinct  $x, y$ , either  $x \leq y$  or  $y \leq x$ .

2. **Example 2 (on  $<$ ):**

The relation  $<$  on  $\mathbb{N}$  is connected because for  $x \neq y$ , either  $x < y$  or  $y < x$ .

### 3. Example 3 (counterexample for $\subseteq$ ):

Let

$$A = \{1, 2\} \quad \text{with} \quad \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Since  $\{1\} \not\subseteq \{2\}$  and  $\{2\} \not\subseteq \{1\}$ , the relation  $\subseteq$  is not connected on  $\mathcal{P}(A)$ .

### 4. Another Counterexample:

Let  $A = \{1, 2\}$  and  $R = \{1R1\}$ . Since neither  $1R2$  nor  $2R1$  is in  $R$ , the relation is not connected.

## 19.8 Reflexive and Symmetric But Not Transitive

**Example:**

Let

$$A = \{1, 2, 3\} \quad \text{and} \quad R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$$

This relation is reflexive because:

$$(1, 1), (2, 2), (3, 3) \in R$$

This relation is symmetric because:

$$(1, 2) \in R \quad \text{and} \quad (2, 1) \in R$$

$$(2, 3) \in R \quad \text{and} \quad (3, 2) \in R$$

This relation is not transitive because:

$$(1, 2) \in R \quad \text{and} \quad (2, 3) \in R \quad \text{but} \quad (1, 3) \notin R$$

## 19.9 Reflexive and Antisymmetric But Not Transitive

**Example:**

Let

$$A = \{1, 2, 3, 4\} \quad \text{and} \quad R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3), (3, 4)\}$$

This relation is reflexive because:

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

This relation is antisymmetric because:

$$(1, 2) \in R \quad \text{but} \quad (2, 1) \notin R$$

$$(2, 3) \in R \quad \text{but} \quad (3, 2) \notin R$$

$$(3, 4) \in R \quad \text{but} \quad (4, 3) \notin R$$

No pair of distinct elements appears in both directions.  
This relation is not transitive because:

$$(1, 2) \in R \quad \text{and} \quad (2, 3) \in R \quad \text{but} \quad (1, 3) \notin R$$

## 19.10 Antisymmetric and Transitive But Not Reflexive

**Example:**

Let

$$A = \{1, 2, 3\} \quad \text{and} \quad R = \{(1, 1), (2, 2), (1, 2), (2, 3), (1, 3)\}$$

This relation is antisymmetric because:

$$(1, 2) \in R \quad \text{but} \quad (2, 1) \notin R$$

$$(2, 3) \in R \quad \text{but} \quad (3, 2) \notin R$$

$$(1, 3) \in R \quad \text{but} \quad (3, 1) \notin R$$

No pair of distinct elements appears in both directions.  
This relation is transitive because:

$$(1, 2) \in R \quad \text{and} \quad (2, 3) \in R \quad \text{and} \quad (1, 3) \in R$$

$$(1, 2) \in R \quad \text{and} \quad (2, 2) \in R \quad \text{and} \quad (1, 2) \in R$$

All required transitive pairs are present.  
This relation is not reflexive because:

$$(3, 3) \notin R$$

Not all elements are related to themselves.

## 19.11 Reflexive, Symmetric, and Transitive

**Example:**

Let

$$A = \{1, 2, 3\} \quad \text{and} \quad R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2), (1, 3), (3, 1)\}$$

This relation is reflexive because:

$$(1, 1), (2, 2), (3, 3) \in R$$

Every element is related to itself.  
This relation is symmetric because:

$$(1, 2) \in R \quad \text{and} \quad (2, 1) \in R$$

$$(2, 3) \in R \quad \text{and} \quad (3, 2) \in R$$

$$(1, 3) \in R \quad \text{and} \quad (3, 1) \in R$$

Every pair has its mirror image in the relation.

This relation is transitive because:

$$(1, 2) \in R \quad \text{and} \quad (2, 3) \in R \quad \text{and} \quad (1, 3) \in R$$

$$(2, 3) \in R \quad \text{and} \quad (3, 1) \in R \quad \text{and} \quad (2, 1) \in R$$

$$(3, 1) \in R \quad \text{and} \quad (1, 2) \in R \quad \text{and} \quad (3, 2) \in R$$

All required transitive pairs are present.

## 20 Equivalence Classes and Partitions

Let  $R \subseteq A^2$ . Then  $R$  is an equivalence relation iff Reflexive, Symmetric, Transitive. Elements  $x, y \in A$  are  $R$ -equivalent iff  $xRy$ .

Let  $R \subseteq A^2$  be an equivalence relation. For each  $x \in A$ , the equivalence class of  $x$  is:

$$[x]_R = \{y \in A \mid xRy\}$$

The quotient set of  $A$  under  $R$  is:

$$A/R = \{[x]_R \mid x \in A\}$$

Moreover, if  $R \subseteq A^2$  is an equivalence relation on  $A$ , then

$$xRy \leftrightarrow [x]_R = [y]_R$$

### 1. Example 1:

Let  $A = \mathcal{P}(\{1, 2, 3\})$ . Define the relation  $R \subseteq A^2$  by:

$$XRY \leftrightarrow |X| = |Y|$$

This relation is an equivalence relation because:

$$\begin{aligned} [\emptyset] &= \{\emptyset\} \\ [\{1\}] &= \{\{1\}, \{2\}, \{3\}\} \\ [\{1, 2\}] &= \{\{1, 2\}, \{1, 3\}, \{2, 3\}\} \\ [\{1, 2, 3\}] &= \{\{1, 2, 3\}\} \end{aligned}$$

## 2. Example 2:

Let  $n \in \mathbb{Z}^+$  and define an equivalence relation  $R$  on  $\mathbb{Z}$  as follows:

$$aRb \leftrightarrow a \equiv b \pmod{n}$$

The equivalence classes are:

- (a)  $[0]_4 = \{4k : k \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\}$
- (b)  $[1]_4 = \{4k + 1 : k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}$
- (c)  $[2]_4 = \{4k + 2 : k \in \mathbb{Z}\} = \{\dots, -6, -2, 2, 6, 10, \dots\}$
- (d)  $[3]_4 = \{4k + 3 : k \in \mathbb{Z}\} = \{\dots, -5, -1, 3, 7, 11, \dots\}$

The quotient set is:

$$\mathbb{Z}/\equiv_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

## 3. Example 4:

Let  $X = \mathbb{N}^2$  and define an equivalence relation  $R$  on  $X$  as follows:

$$(x_1, y_1) R (x_2, y_2) \leftrightarrow x_1 + y_2 = y_1 + x_2$$

Equivalently, this can be written as:

$$(x_1, y_1) R (x_2, y_2) \leftrightarrow x_1 - y_1 = x_2 - y_2$$

The equivalence class of a pair  $(x_1, y_1)$  is:

$$[(x_1, y_1)]_R = \{(x_2, y_2) \in \mathbb{N}^2 \mid x_2 - y_2 = x_1 - y_1\}$$

Some specific equivalence classes:

- (a)  $[(3, 1)]_R = \{(x, y) \in \mathbb{N}^2 \mid x - y = 2\} = \{(2, 0), (3, 1), (4, 2), (5, 3), \dots\}$
- (b)  $[(1, 3)]_R = \{(x, y) \in \mathbb{N}^2 \mid x - y = -2\} = \{(0, 2), (1, 3), (2, 4), (3, 5), \dots\}$
- (c)  $[(2, 2)]_R = \{(x, y) \in \mathbb{N}^2 \mid x - y = 0\} = \{(0, 0), (1, 1), (2, 2), (3, 3), \dots\}$

Each equivalence class is determined uniquely by the value  $x_1 - y_1$ .

Mapping to  $\mathbb{Z}$ :

Define a mapping from equivalence classes to integers:

$$\varphi : \mathbb{N}^2/R \rightarrow \mathbb{Z}, \quad [(x_1, y_1)]_R \mapsto x_1 - y_1$$

If  $(x_1, y_1) R (x_2, y_2)$ , then

$$x_1 + y_2 = y_1 + x_2 \quad \rightarrow \quad x_1 - y_1 = x_2 - y_2$$

so the mapping is well-defined. Moreover, this mapping is a bijection, establishing:

$$\mathbb{N}^2/R \cong \mathbb{Z}$$

Each integer  $n \in \mathbb{Z}$  corresponds to the equivalence class of all pairs  $(x, y) \in \mathbb{N}^2$  with  $x - y = n$ . For instance:

$$0 \leftrightarrow [(0, 0)]_R, \quad 2 \leftrightarrow [(3, 1)]_R, \quad -2 \leftrightarrow [(1, 3)]_R$$

## 21 Order Relations

### 21.1 Preorder

A relation  $R \subseteq A^2$  is a preorder if reflexive and transitive.

Let  $A = \{a, b, c\}$ . The Cartesian product is

$A^2$	$a$	$b$	$c$
$a$	$(a, a)$	$(a, b)$	$(a, c)$
$b$	$(b, a)$	$(b, b)$	$(b, c)$
$c$	$(c, a)$	$(c, b)$	$(c, c)$

#### 1. Example 1:

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

Reflexive:

$$\forall x \in A, (x, x) \in R$$

Transitive:

$$\forall x, y, z \in A, (xRy \wedge yRz) \rightarrow xRz$$

But not antisymmetric:

$$aRb \wedge bRa \quad \text{but} \quad a \neq b$$

#### 2. Example 2:

Universal relation on  $L = \{a, b\}$

$$R = L^2$$

Reflexive, transitive, but not antisymmetric if  $|L| > 1$ .

### 3. Example 3:

Relation on  $\mathbb{B}^*$ :

$$x \preceq y \leftrightarrow \text{len}(x) \leq \text{len}(y)$$

Reflexive, transitive, connected, but not antisymmetric:

$$01 \preceq 10 \wedge 10 \preceq 01 \quad \text{but} \quad 01 \neq 10$$

## 21.2 Partial Order

A relation  $R \subseteq A^2$  is a partial order if reflexive, transitive, and antisymmetric.

### 1. Example 1:

Let  $A = \{a, b, c\}$

$A^2$	$a$	$b$	$c$
$a$	$(a, a)$	$(a, b)$	$(a, c)$
$b$	$(b, a)$	$(b, b)$	$(b, c)$
$c$	$(c, a)$	$(c, b)$	$(c, c)$

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

Reflexive, transitive, antisymmetric, but not connected:

$$\neg(bRc) \wedge \neg(cRb)$$

### 2. Example 2:

$$A = \mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$A^2$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$(\emptyset, \emptyset)$	$(\emptyset, \{a\})$	$(\emptyset, \{b\})$	$(\emptyset, \{a, b\})$
$\{a\}$	$(\{a\}, \emptyset)$	$(\{a\}, \{a\})$	$(\{a\}, \{b\})$	$(\{a\}, \{a, b\})$
$\{b\}$	$(\{b\}, \emptyset)$	$(\{b\}, \{a\})$	$(\{b\}, \{b\})$	$(\{b\}, \{a, b\})$
$\{a, b\}$	$(\{a, b\}, \emptyset)$	$(\{a, b\}, \{a\})$	$(\{a, b\}, \{b\})$	$(\{a, b\}, \{a, b\})$

$$R = \subseteq$$

Reflexive, transitive, antisymmetric, but not connected:

$$\{a\} \not\subseteq \{b\}, \quad \{b\} \not\subseteq \{a\}$$

### 3. Example 3:

Divisibility on  $\mathbb{N}$

$$n \mid m \leftrightarrow \exists k \in \mathbb{N}, m = kn$$

Partial order, not linear:

$$2 \nmid 3, \quad 3 \nmid 2$$

On  $\mathbb{Z}$ , not antisymmetric:

$$1 \mid -1 \wedge -1 \mid 1 \quad \text{but} \quad 1 \neq -1$$

## 21.3 Linear Order

A relation  $R \subseteq A^2$  is a linear order if it is a partial order and connected.

### 1. Example 1:

Let  $A = \{a, b, c\}$

$A^2$	$a$	$b$	$c$
$a$	$(a, a)$	$(a, b)$	$(a, c)$
$b$	$(b, a)$	$(b, b)$	$(b, c)$
$c$	$(c, a)$	$(c, b)$	$(c, c)$

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

Connected: corresponds to  $a < b < c$ .

### 2. Example 2:

$$x \leq y \leftrightarrow x = y \vee x < y$$

Reflexive, transitive, antisymmetric, connected:  $(\mathbb{N}, \leq)$  is a linear order.

## 21.4 Strict Order

A relation  $R \subseteq A^2$  is a strict order if irreflexive, asymmetric, and transitive.

### 1. Example 1:

Let  $A = \{a, b, c\}$

$A^2$	$a$	$b$	$c$
$a$	$(a, a)$	$(a, b)$	$(a, c)$
$b$	$(b, a)$	$(b, b)$	$(b, c)$
$c$	$(c, a)$	$(c, b)$	$(c, c)$

where,

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

2. **Example 2:**

$$x < y \leftrightarrow \exists k \in \mathbb{N}^+, y = x + k$$

Irreflexive, asymmetric, transitive:  $(\mathbb{N}, <)$  is a strict order.

## 21.5 Strict Linear Order

A strict linear order is a strict order that is connected:

$$\forall x, y \in A, x \neq y \rightarrow (xRy \vee yRx)$$

1. **Example 1:**

Let  $A = \{a, b, c\}$

$A^2$	$a$	$b$	$c$
$a$	$(a, a)$	$(a, b)$	$(a, c)$
$b$	$(b, a)$	$(b, b)$	$(b, c)$
$c$	$(c, a)$	$(c, b)$	$(c, c)$

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

Irreflexive, asymmetric, transitive, connected: corresponds to  $a < b < c$ .

2. **Example 2:**

$$x < y \leftrightarrow \exists k \in \mathbb{N}^+, y = x + k$$

Irreflexive, asymmetric, transitive, connected:  $(\mathbb{N}, <)$  is a strict linear order.

- (a)  $3 \not< 3$
- (b)  $2 < 5$ , then  $5 \not< 2$
- (c)  $1 < 4 \wedge 4 < 7 \rightarrow 1 < 7$
- (d)  $6 \neq 10 \rightarrow (6 < 10 \vee 10 < 6)$

3. **Example 3:**

$$X \subsetneq Y \leftrightarrow X \subseteq Y \wedge X \neq Y$$

- (a)  $\{1\} \subsetneq \{1, 2\}$
- (b)  $\{1, 2\} \subsetneq \{1, 2, 3\}$
- (c)  $\{1, 2\} \not\subsetneq \{1, 2\}$

If  $<$  is a strict linear order on  $A$ , then

$$\forall a, b \in A, \quad [(\forall x \in A, x < a \leftrightarrow x < b) \rightarrow a = b]$$

**Example:**

For  $A = \{a, b, c\}$  with  $< = \{(a, b), (a, c), (b, c)\}$ :

$$\{x \in A \mid x < a\} = \emptyset, \quad \{x \in A \mid x < b\} = \{a\}, \quad \{x \in A \mid x < c\} = \{a, b\}$$

Properties:

1. If  $R$  is a strict order on  $A$ , then

$$R^+ = R \cup \text{Id}_A$$

is a partial order. Moreover, if  $R$  is a strict linear order, then  $R^+$  is a linear order.

2. If  $R$  is a partial order on  $A$ , define

$$R^- = R \setminus \text{Id}_A$$

$R^-$  is a strict order (irreflexive, asymmetric, transitive). Moreover, if  $R$  is a linear order, then  $R^-$  is a strict linear order.

**Example:**

Let  $A = \{a, b, c\}$  and

$$R = \{(a, b), (a, c), (b, c)\} \quad (\text{strict linear order})$$

The Cartesian product  $A^2$ :

$A^2$	$a$	$b$	$c$
$a$	$(a, a)$	$(a, b)$	$(a, c)$
$b$	$(b, a)$	$(b, b)$	$(b, c)$
$c$	$(c, a)$	$(c, b)$	$(c, c)$

Identity relation:

$$\text{Id}_A = \{(a, a), (b, b), (c, c)\}$$

Then

$$R^+ = R \cup \text{Id}_A = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, c)\}$$

$$R^- = R^+ \setminus \text{Id}_A = \{(a, b), (a, c), (b, c)\}$$

$R^+$  is a linear order, and  $R^-$  is a strict linear order.

## 22 Graph

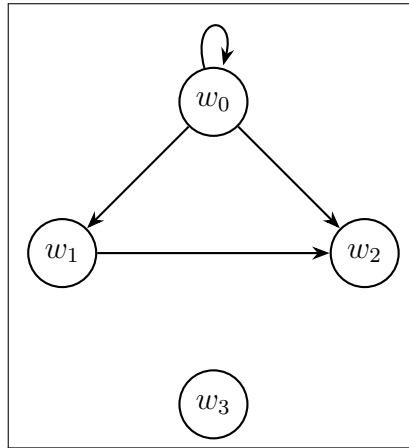
A graph is an ordered pair  $G = \langle V, E \rangle$ , where:

1.  $V$  is a non-empty set of vertices.
2.  $E \subseteq V^2$  is a set of edges, where each edge is an ordered pair  $\langle v_1, v_2 \rangle \in V^2$  representing a directed connection from  $v_1$  to  $v_2$ .

### 1. Example 1:

Let  $G = \langle V, E \rangle$  be a directed graph with:

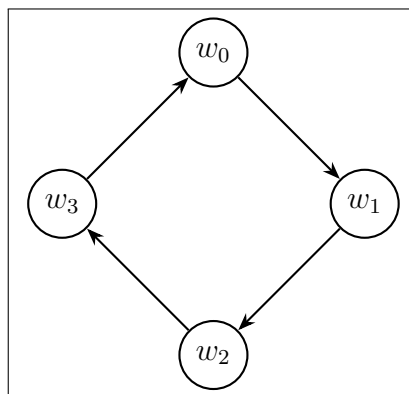
$$V = \{w_0, w_1, w_2, w_3\} \quad E = \{\langle w_0, w_0 \rangle, \langle w_0, w_1 \rangle, \langle w_0, w_2 \rangle, \langle w_1, w_2 \rangle\}$$



### 2. Example 2:

Consider the directed graph  $G_2 = \langle V_2, E_2 \rangle$  with:

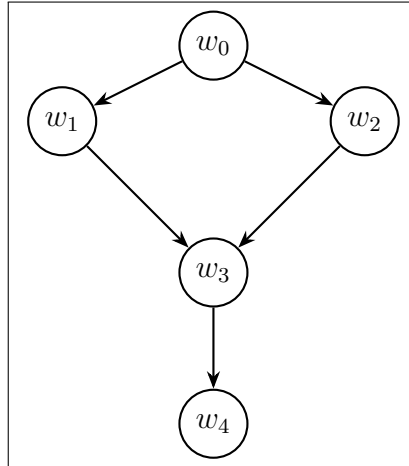
$$V_2 = \{w_0, w_1, w_2, w_3\}, \quad E_2 = \{\langle w_0, w_1 \rangle, \langle w_1, w_2 \rangle, \langle w_2, w_3 \rangle, \langle w_3, w_0 \rangle\}$$



3. **Example 3:**

Consider the directed graph  $G_3 = \langle V_3, E_3 \rangle$  with:

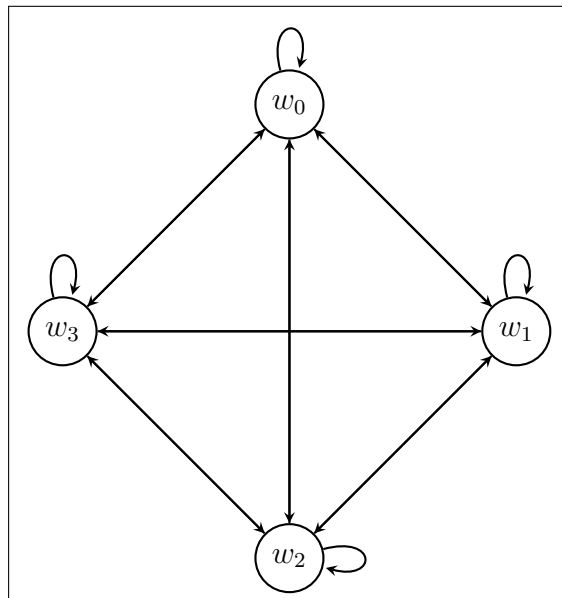
$$V_3 = \{w_0, w_1, w_2, w_3, w_4\}, \quad E_3 = \{\langle w_0, w_1 \rangle, \langle w_0, w_2 \rangle, \langle w_1, w_3 \rangle, \langle w_2, w_3 \rangle, \langle w_3, w_4 \rangle\}$$



4. **Example 4:**

Consider the directed graph  $G_4 = \langle V_4, E_4 \rangle$  with:

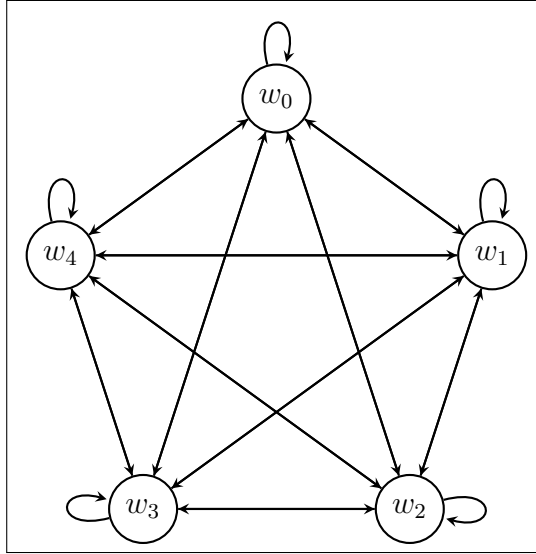
$$V_4 = \{w_0, w_1, w_2, w_3\}, \quad E_4 = \{\langle w_i, w_j \rangle \mid w_i, w_j \in V_4\}$$



### 5. Example 5:

Consider the directed graph  $G_5 = \langle V_5, E_5 \rangle$  with:

$$V_5 = \{w_0, w_1, w_2, w_3, w_4\}, \quad E_5 = \{\langle w_i, w_j \rangle \mid w_i, w_j \in V_5\}$$



## 23 Operations on Relations

Let  $R, S \subseteq A^2$  be binary relations on a set  $A$ . The following are standard operations on relations:

### 23.1 Inverse of a Relation

Definition:

$$R^{-1} = \{\langle y, x \rangle \mid \langle x, y \rangle \in R\}$$

In general, if  $R \subseteq \mathbb{N}^2$ , the inverse relation  $R^{-1}$  contains all pairs of  $R$  with their coordinates swapped:

$$R^{-1} = \{(y, x) \in \mathbb{N}^2 \mid (x, y) \in R\}$$

**Example:**

Let

$$S = \{\langle x, y \rangle \in \mathbb{Z}^2 \mid x + 1 = y\}$$

that is,

$S$	$\dots$	$-1$	$0$	$1$	$2$	$3$	$\dots$
$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$-1$	$\dots$		$(-1, 0)$				$\dots$
$0$	$\dots$			$(0, 1)$			$\dots$
$1$	$\dots$				$(1, 2)$		$\dots$
$2$	$\dots$					$(2, 3)$	$\dots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

then

$S^{-1}$	$\dots$	$-2$	$-1$	$0$	$1$	$2$	$\dots$
$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$0$	$\dots$		$(0, -1)$				$\dots$
$1$	$\dots$			$(1, 0)$			$\dots$
$2$	$\dots$				$(2, 1)$		$\dots$
$3$	$\dots$					$(3, 2)$	$\dots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

## 23.2 Relative Product of Relations

Definition:

$$(R \mid S) = \{\langle x, z \rangle \mid \exists y (xRy \wedge ySz)\}$$

**Example:**

Suppose we have

$$R = \{(1, 2), (2, 3), (3, 4)\}, \quad S = \{(2, 5), (3, 6), (4, 7)\}$$

Then the composition of relations is

$$R \mid S = \{(x, z) \mid \exists y ((x, y) \in R \wedge (y, z) \in S)\}$$

Thus

1.  $((1, 2) \in R) \text{ and } ((2, 5) \in S) \rightarrow ((1, 5) \in R \mid S)$
2.  $((2, 3) \in R) \text{ and } ((3, 6) \in S) \rightarrow ((2, 6) \in R \mid S)$
3.  $((3, 4) \in R) \text{ and } ((4, 7) \in S) \rightarrow ((3, 7) \in R \mid S)$

Consequently

$$R \mid S = \{(1, 5), (2, 6), (3, 7)\}$$

## 23.3 Restriction of a Relation

Definition:

$$R \upharpoonright A = R \cap A^2$$

In general, if  $R \subseteq \mathbb{N}^2$  and  $A \subseteq \mathbb{N}$ , the restriction of  $R$  to  $A$  keeps only those pairs in  $R$  where both elements are in  $A$ :

$$R \upharpoonright A = \{(x, y) \in R \mid (x, y) \in A\}$$

Hence

$A^2$	$a_1$	$a_2$	$\dots$	$a_n$
$a_1$	$(a_1, a_1)$	$(a_1, a_2)$	$\dots$	$(a_1, a_n)$
$a_2$	$(a_2, a_1)$	$(a_2, a_2)$	$\dots$	$(a_2, a_n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_n$	$(a_n, a_1)$	$(a_n, a_2)$	$\dots$	$(a_n, a_n)$

**Example 1:**

Given

$$R = \{(1, 2), (2, 4), (3, 6), (4, 8), (5, 10), (6, 12)\} \subseteq \mathbb{Z}^2$$

Restriction to even numbers  $E = \{2, 4, 6, 8, 10, 12, \dots\}$ :

$$R \upharpoonright_E = \{(2, 4), (4, 8), (6, 12)\}$$

**Example 2:**

Given

$$f = \{(x, x^2) \mid x \in \mathbb{R}\}$$

Restriction to  $\mathbb{Z} \cap [0, 3]$ :

$f \upharpoonright_{\mathbb{Z} \cap [0, 3]}$	0	1	2	3
0	(0, 0)			
1		(1, 1)		
2			(2, 4)	
3				(3, 9)

**Example 3:**

Let

$\mathbb{R}^2$	$\dots$	$a_{ijk}$	$\dots$	$b_{lmn}$	$\dots$	$c_{pqr}$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_{ijk}$	$\dots$	$(a_{ijk}, a_{ijk})$	$\dots$	$(a_{ijk}, b_{lmn})$	$\dots$	$(a_{ijk}, c_{pqr})$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$b_{lmn}$	$\dots$	$(b_{lmn}, a_{ijk})$	$\dots$	$(b_{lmn}, b_{lmn})$	$\dots$	$(b_{lmn}, c_{pqr})$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$c_{pqr}$	$\dots$	$(c_{pqr}, a_{ijk})$	$\dots$	$(c_{pqr}, b_{lmn})$	$\dots$	$(c_{pqr}, c_{pqr})$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Restriction to  $\mathbb{N}^2$ :

$\mathbb{N}^2$	1	2	3	$\dots$
1	(1, 1)	(1, 2)	(1, 3)	$\dots$
2	(2, 1)	(2, 2)	(2, 3)	$\dots$
3	(3, 1)	(3, 2)	(3, 3)	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Given relation

$$R = \{(a_{ijk}, c_{pqr}), (b_{lmn}, 2), (2, 3), (\pi, e), (3, 5)\} \subseteq \mathbb{R}^2$$

Restriction to  $\mathbb{N}^2$ :

$$R \upharpoonright_{\mathbb{N}^2} = \{(2, 3), (3, 5)\}$$

## 23.4 Application of a Relation to a Set

Definition:

$$R[A] = \{y \in A \mid \exists x \in A, \langle x, y \rangle \in R\}$$

**Example:**

Let

$$S = \{(a, b), (b, c), (c, d)\}$$

and consider the set  $P = \{a, b, c\}$ .

Where

$$\begin{aligned} (a, b) &\rightarrow b \in S[\cdot] \\ (b, c) &\rightarrow c \in S[\cdot] \\ (c, d) &\rightarrow d \notin S[P] \text{ since } d \notin P \end{aligned}$$

then

$$S[P] = \{b, c\}$$

## 23.5 Transitive Closure

Definition:

$$R^1 = R, \quad R^{n+1} = R^n \mid R$$

$$R^+ = \bigcup_{n=1}^{\infty} R^n$$

**Example:**

Let

$$R = \{(1, 2), (2, 3), (3, 4)\}$$

Since

$$\begin{aligned} R^1 &= \{(1, 2), (2, 3), (3, 4)\} \\ R^2 &= R \mid R = \{(1, 3), (2, 4)\} \\ R^3 &= R^2 \mid R = \{(1, 4)\} \end{aligned}$$

Therefore

$R^+$	1	2	3	4
1		(1, 2)	(1, 3)	(1, 4)
2			(2, 3)	(2, 4)
3				(3, 4)
4				

## 23.6 Reflexive Transitive Closure

Let

$$\text{Id}_A = \{\langle x, x \rangle \mid x \in A\}$$

then

$$R^* = R^+ \cup \text{Id}_A$$

**Example:**

Since  $\text{Id}_A$ :

$\text{Id}_A$	1	2	3	4
1	(1, 1)			
2		(2, 2)		
3			(3, 3)	
4				(4, 4)

We conclude that,  $R^* = R^+ \cup \text{Id}_A$ :

$R^*$	1	2	3	4
1	(1, 1)	(1, 2)	(1, 3)	(1, 4)
2		(2, 2)	(2, 3)	(2, 4)
3			(3, 3)	(3, 4)
4				(4, 4)

## 24 Functions

A function  $f$  from set  $A$  to set  $B$  is a relation that assigns to each element of  $A$  exactly one element of  $B$ .

Let  $A$  and  $B$  be sets. A function  $f : A \rightarrow B$  is a subset  $f \subseteq A \times B$  such that

$$f = \{(x, y) \in A \times B \mid f(x) = y\}$$

This is a subset of  $A \times B$  such that for every  $x \in A$ , there exists a unique  $y \in B$  with  $(x, y) \in f$ .

### 24.1 Domain, Codomain, Range, and Preimage

1. Domain:

$$\text{dom}(f) = A = \{x \mid \exists y \in B : (x, y) \in f\}$$

2. Codomain:

$$\text{cod}(f) = B$$

3. Range (Image):

$$\text{range}(f) = \text{im}(f) = \{y \in B \mid \exists x \in A : f(x) = y\}$$

4. Image of a subset:

For  $S \subseteq A$ :

$$f(S) = \{f(x) \mid x \in S\} = \{y \in B \mid \exists x \in S : f(x) = y\}$$

5. Preimage (Inverse Image):

For  $T \subseteq B$ :

$$f^{-1}(T) = \{x \in A \mid f(x) \in T\}$$

**Example:**

Let

$$A = \{1, 2, 3, 4, 5\}$$

$$B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Define

$$f : A \rightarrow B, \quad f(x) = 2x$$

Let

$$S = \{1, 3, 5\} \subseteq A$$

Then

$$f(S) = \{f(x) \mid x \in S\}$$

$$f(1) = 2$$

$$f(3) = 6$$

$$f(5) = 10$$

Therefore

$$\boxed{f(S) = \{2, 6, 10\}}$$

**1. Example 1:**

Let  $f : \mathbb{R} \rightarrow \mathbb{R}$  be defined by  $f(x) = x^2$ .

$$\text{range}(f) = \{y \in \mathbb{R} \mid y \geq 0\} = [0, \infty)$$

Image of a set:

$$f(\{-2, 3\}) = \{(-2)^2, 3^2\} = \{4, 9\}$$

Preimage of a set:

$$f^{-1}(\{4\}) = \{x \in \mathbb{R} \mid x^2 = 4\} = \{-2, 2\}$$

## 2. Example 2:

Let

$$\times : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

be the usual multiplication function defined by

$$\times(a, b) = a \times b$$

Then:

$$\text{dom}(\times) = \mathbb{N} \times \mathbb{N}, \quad \text{cod}(\times) = \mathbb{N}, \quad \text{range}(\times) = \mathbb{N}$$

For example:

$$(3, 4) \in \mathbb{N} \times \mathbb{N}$$

and

$$3 \times 4 = 12$$

Therefore,

$$\times(3, 4) = 12$$

We also have the identity property:

$$\forall n \in \mathbb{N}, \exists (n, 1) \in \mathbb{N} \times \mathbb{N} : n \times 1 = n$$

## 3. Example 3:

Let

$$f(x) = x^2 - 3x + 2$$

We want to find

$$f(2 + x)$$

Substitute

$$2 + x \text{ for } x$$

Hence

$$f(2 + x) = (2 + x)^2 - 3(2 + x) + 2$$

Expand and simplify:

$$\begin{aligned}
 f(2+x) &= (x^2 + 4x + 4) - 3(2+x) + 2 \\
 &= x^2 + 4x + 4 - 6 - 3x + 2 \\
 &= x^2 + x
 \end{aligned}$$

Thus,

$$\boxed{f(2+x) = x^2 + x}$$

#### 4. Example 4:

Let

$$f(x) = 2x + 3$$

We want to find

$$f^{-1}(x)$$

we define

$$\begin{aligned}
 y &= 2x + 3 \\
 y - 3 &= 2x \\
 x &= \frac{y - 3}{2}
 \end{aligned}$$

Now, interchange

$x$  and  $y$

Hence:

$$\boxed{f^{-1}(x) = \frac{x - 3}{2}}$$

#### 5. Example 5:

Let

$$f : \mathbb{N} \rightarrow \mathbb{N}$$

be defined by

$$f(x) = x + 1$$

Then:

$$\text{range}(f) = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$$

For example:

$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 3$$

Hence,

$$0 \notin \text{range}(f) \text{ since } \nexists x \in \mathbb{N} : f(x) = 0$$

**6. Example 6:**

Let  $g : \mathbb{N} \rightarrow \mathbb{N}$  be defined by:

$$g(x) = x + 2 - 1$$

Then:

$$\forall x \in \mathbb{N}, f(x) = x + 1 = x + 2 - 1 = g(x)$$

By the principle of extensionality for functions:

$$\forall x \in \text{dom}(f) : f(x) = g(x) \rightarrow f = g$$

provided  $\text{dom}(f) = \text{dom}(g)$  and  $\text{cod}(f) = \text{cod}(g)$ .

**7. Example 7:**

Let  $h : \mathbb{N} \rightarrow \mathbb{N}$  be defined by:

$$h(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd} \end{cases}$$

Since:

$$\forall x \in \mathbb{N}, (\text{even}(x) \vee \text{odd}(x))(x) \wedge \neg(\text{even}(x) \wedge \text{odd}(x))$$

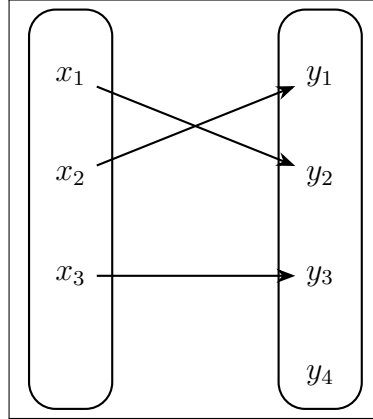
the function  $h$  is well-defined and  $h(x) \in \mathbb{N}$  for all  $x \in \mathbb{N}$ .

## 25 Kinds of Functions

### 25.1 Injective

A function  $f : A \rightarrow B$  is injective or one-to-one if and only if:

$$\forall x_1, x_2 \in A, f(x_1) = f(x_2) \rightarrow x_1 = x_2.$$



Equivalently, for each  $y \in B$ , there is at most one  $x \in A$  such that  $f(x) = y$ . We call such a function an injection from  $A$  to  $B$ .

**1. Example 1:**

$$f : \mathbb{R} \rightarrow \mathbb{R}, \text{ where } f(x) = 2x + 3$$

If  $2x_1 + 3 = 2x_2 + 3$ , then  $x_1 = x_2$ .

Exponential function is strictly increasing.

**2. Example 2:**

$f : \mathbb{Z} \rightarrow \mathbb{N}$ , defined by

$$f(x) = \begin{cases} 2x, & \text{if } x \geq 0, \\ -2x - 1, & \text{if } x < 0 \end{cases}$$

**3. Example 3:**

There exist injective functions from  $\mathbb{N}$  into each of  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ . Formally:

$$\exists f_i : \mathbb{N} \rightarrow S_i, \quad S_i \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}, \text{ such that } f_i \text{ is injective.}$$

$$f_1 : \mathbb{N} \rightarrow \mathbb{N}, \quad f_1(x) = x + 1$$

$$f_2 : \mathbb{N} \rightarrow \mathbb{Z}, \quad f_2(x) = \begin{cases} \frac{x}{2}, & \text{if } x \text{ is even} \\ -\frac{x+1}{2}, & \text{if } x \text{ is odd} \end{cases}$$

$$f_3 : \mathbb{N} \rightarrow \mathbb{Q}, \quad f_3(x) = \frac{x}{x+1}$$

$$f_4 : \mathbb{N} \rightarrow \mathbb{R}, \quad f_4(x) = x.$$

Each  $f_i$  is injective, since distinct natural numbers map to distinct elements of the codomain.

#### 4. Example 4:

Let

$$f : \{2n + 1 \mid n \in \mathbb{N}\} \longrightarrow \mathbb{Q}, \quad f(2n + 1) = \frac{2n + 1}{2n + 2}$$

$$\text{Im}(f) = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a \in \{2n + 1 \mid n \in \mathbb{N}\}, b = a + 1 \right\}$$

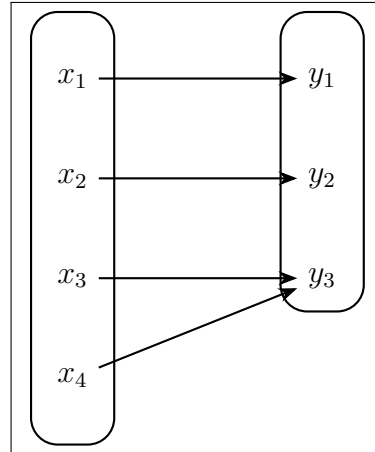
Hence,

$$\begin{aligned} f(1) &= 1/2 \\ f(3) &= 3/4 \\ f(5) &= 5/6 \\ f(7) &= 7/8 \\ f(9) &= 9/10 \\ &\vdots \end{aligned}$$

## 25.2 Surjective

A function  $f : A \rightarrow B$  is surjective or onto if and only if  $B$  is the range of  $f$ , i.e.,

$$\forall y \in B, \exists x \in A \mid f(x) = y.$$



We call such a function a surjection from  $A$  to  $B$ .

#### 1. Example 1:

$$f : \mathbb{Z} \rightarrow \mathbb{N}, \text{ where } f(x) = |x|$$

$x$	-3	-2	-1	0	1	2	3
$ x $	3	2	1	0	1	2	3

#### 2. Example 2:

$$f : \mathbb{R} \rightarrow \mathbb{R}, \text{ where } f(x) = x^3$$

$$\forall y \in \mathbb{R}, \exists x = \sqrt[3]{y} \in \mathbb{R} \mid f(x) = y$$

3. **Example 3:**

$f : \mathbb{R} \rightarrow [0, \infty)$ , where  $f(x) = x^2$

$$f(\sqrt{x}) = (\sqrt{x})^2 = x$$

4. **Example 4:**

Floor function:  $f : \mathbb{R} \rightarrow \mathbb{Z}$ , where  $f(x) = \lfloor x \rfloor$

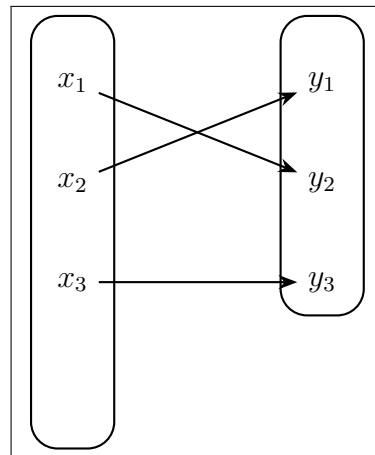
$x$	-2.7	-1.2	0.5	1.0	2.9
$\lfloor x \rfloor$	-3	-2	0	1	2

## 25.3 Bijective

A function  $f : A \rightarrow B$  is bijective if and only if it is both injective and surjective. We call such a function a bijection from  $A$  to  $B$ , or a one-to-one correspondence.

Equivalently:

$$\forall y \in B, \exists! x \in A \mid f(x) = y.$$



(For every element in  $B$ , there exists exactly one element in  $A$  that maps to it.)

1. **Example:**

Let

$$A = \{1, 2, 3\}, \quad B = \{a, b, c\}.$$

Define a function

$$f : A \rightarrow B$$

by

$$f(1) = a, \quad f(2) = b, \quad f(3) = c.$$

Each element of  $A$  maps to a unique element of  $B$ , so  $f$  is injective. Every element of  $B$  is the image of some element of  $A$ , so  $f$  is surjective. Therefore,  $f$  is bijective.

## 25.4 Combinations

### 25.4.1 Bijective (Both injective and surjective)

#### 1. Example 1:

Identity function:  $f : \mathbb{R} \rightarrow \mathbb{R}$ , where  $f(x) = x$

Injective and surjective, therefore bijective:

$$\forall y \in \mathbb{R}, \exists! x \in \mathbb{R} \mid f(x) = y$$

#### 2. Example 2:

$f : [0, \infty) \rightarrow [0, \infty)$ , where  $f(x) = x^2$

Injective:

$$\forall x_1, x_2 \in [0, \infty), x_1^2 = x_2^2 \implies x_1 = x_2$$

Surjective:

$$\forall y \in [0, \infty), \exists x \in [0, \infty) \mid f(x) = y$$

Therefore bijective.

### 25.4.2 Injective but not surjective

Recall the Von Neumann Ordinal,

$$\begin{aligned} 0 &= \emptyset = \{\} \\ 1 &= \{\emptyset\} = \emptyset \cup \{\emptyset\} \\ 2 &= \{\emptyset, \{\emptyset\}\} = 1 \cup \{1\} \\ &\vdots \\ n &= n-1 \cup \{n-1\} \end{aligned}$$

Based on this notion, we can define a function that is injective but not surjective:

#### 1. Example:

Let  $A = \{1, 2, 3\}$  and define  $f : A \rightarrow \mathcal{P}(A)$  by  $F(x) = \{x\}$ .

Then:

$$f(1) = \{1\}, \quad f(2) = \{2\}, \quad f(3) = \{3\}$$

Hence:

$$\text{Im}(f) = \{\{1\}, \{2\}, \{3\}\} \subset \mathcal{P}(A)$$

Since  $\emptyset \in \mathcal{P}(A)$  but  $\emptyset \notin \text{Im}(f)$ , we conclude that  $f$  is injective but not surjective

### 25.4.3 Surjective but not injective

#### 1. Example:

Piecewise function:  $f : \mathbb{N} \rightarrow \mathbb{N}$ , where

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd} \end{cases}$$

Surjective:

$$\forall y \in \mathbb{N}, \exists x \in \mathbb{N} : f(x) = y$$

Not injective:

$$f(1) = f(2) = 1 \text{ but } 1 \neq 2$$

### 25.4.4 Neither injective nor surjective

#### 1. Example 1:

Constant function:  $f : \mathbb{N} \rightarrow \mathbb{N}$ , where  $f(x) = 1$  for all  $x$

Not injective:

$$f(1) = f(2) = 1 \text{ but } 1 \neq 2$$

Not surjective:

$$\nexists x \in \mathbb{N} \mid f(x) = 2$$

#### 2. Example 2:

$f : \mathbb{R} \rightarrow \mathbb{R}$ , where  $f(x) = x^2$

Not injective:

$$f(-2) = f(2) = 4 \text{ but } -2 \neq 2$$

Not surjective:

$$\nexists x \in \mathbb{R} \mid f(x) = -1$$

## 25.5 Equivalence Relation with Function Properties

### 1. Example 1:

Let  $E = \{a, b, c, d, e, f\}$ . Define  $R \subseteq E^2$ :

$R$	$a$	$b$	$c$	$d$	$e$	$f$
$a$	$(a, a)$	$(a, b)$				
$b$	$(b, a)$	$(b, b)$				
$c$			$(c, c)$	$(c, d)$		
$d$			$(d, c)$	$(d, d)$		
$e$					$(e, e)$	$(e, f)$
$f$					$(f, e)$	$(f, f)$

Reflexive:

$$\forall x \in E, (x, x) \in R$$

Symmetric:

$$\forall x, y \in E, (x, y) \in R \rightarrow (y, x) \in R$$

Transitive:

$$\forall x, y, z \in E, (x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$$

Equivalence classes:

$$[a] = \{a, b\}, \quad [c] = \{c, d\}, \quad [e] = \{e, f\}$$

Thus:

$$E/R = \{[a], [c], [e]\}$$

Function  $f : E \rightarrow E/R$

Defined by:

$$f(x) = [x]$$

Not injective:

$$a \neq b \wedge f(a) = f(b)$$

Surjective:

$$\forall y \in E/R, \exists x \in E : f(x) = y$$

Not bijective:

$$\neg \text{Injective} \rightarrow \neg \text{Bijective}$$

Therefore:

$$E \not\cong E/R$$

Bijective Function Defined on Quotient Classes

Let:

$$S = \{a, c, e\}$$

Define:

$$g : E/R \rightarrow S, \quad g([a]) = a, \quad g([c]) = c, \quad g([e]) = e$$

Injective:

$$\forall x_1, x_2 \in E/R, \quad g(x_1) = g(x_2) \rightarrow x_1 = x_2$$

Surjective:

$$\forall y \in S, \quad \exists x \in E/R, \quad g(x) = y$$

Bijective:

$$\text{Injective} \wedge \text{Surjective} \rightarrow \text{Bijective}$$

Therefore:

$$E/R \cong S$$

## 2. Example 2:

Let  $X = \mathbb{N}^2$ . Define  $R \subseteq X^2$  by:

$$(x_1, y_1) R (x_2, y_2) \leftrightarrow x_1 + y_2 = y_1 + x_2$$

By definition of equivalence:

Reflexive:

$$\forall (x, y) \in X, \quad (x, y) R (x, y)$$

Symmetric:

$$\forall (x_1, y_1), (x_2, y_2) \in X, \quad ((x_1, y_1) R (x_2, y_2) \rightarrow (x_2, y_2) R (x_1, y_1))$$

Transitive:

$$\forall (x_1, y_1), (x_2, y_2), (x_3, y_3) \in X, ((x_1, y_1) R (x_2, y_2) \wedge (x_2, y_2) R (x_3, y_3) \rightarrow (x_1, y_1) R (x_3, y_3))$$

Equivalence Classes:

$$[(x_1, y_1)] = \{(x_2, y_2) : x_2 - y_2 = x_1 - y_1\}$$

Quotient set:

$$X/R = \{[(x, y)] : (x, y) \in \mathbb{N}^2\}$$

Define:

$$\Sigma : X/R \rightarrow \mathbb{Z}, \quad \Sigma([(x, y)]) = x - y$$

Values:

$\Sigma(x, y)$	1	2	3	4	5
1	0	-1	-2	-3	-4
2	1	0	-1	-2	-3
3	2	1	0	-1	-2
4	3	2	1	0	-1
5	4	3	2	1	0

Injective

$$\Sigma([(x_1, y_1)]) = \Sigma([(x_2, y_2)]) \rightarrow x_1 - y_1 = x_2 - y_2 \rightarrow (x_1, y_1) R (x_2, y_2) \rightarrow [(x_1, y_1)] = [(x_2, y_2)]$$

$\Sigma([(x, y)])$	-2	-1	0	1	2	...
Pairs	(0, 2)	(0, 1)	(0, 0)	(1, 0)	(2, 0)	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Surjective

$$\forall z \in \mathbb{Z}, \exists (x, y) \in \mathbb{N}^2, \Sigma([(x, y)]) = z$$

$z \in \mathbb{Z}$	-2	-1	0	1	2	...
Pair	(0, 2)	(0, 1)	(0, 0)	(1, 0)	(2, 0)	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Bijjective

$$\text{Injective} \wedge \text{Surjective} \rightarrow \text{Bijjective}$$

We conclude that:

$$X/R \cong \mathbb{Z}$$

## 26 Functions as Relations

A function  $f : A \rightarrow B$  defines a relation between  $A$  and  $B$ :

$$x \in A \ R \ y \in B \leftrightarrow f(x) = y$$

We identify  $f$  with its set of ordered pairs:

$$f = \{(x, y) \mid x \in A \wedge f(x) = y\} \subseteq A \times B$$

### 26.1 Graph of a Function

Let  $R \subseteq A \times B$  satisfy:

$$(xRy \wedge xRz) \rightarrow y = z, \quad \text{and} \quad \forall x \in A, \exists y \in B \mid \langle x, y \rangle \in R.$$

Then  $R$  is the graph of a function  $f : A \rightarrow B$  defined by  $f(x) = y \leftrightarrow xRy$ .

Let  $f : A \rightarrow B$  be a function. The graph of  $f$  is the relation  $R_f \subseteq A \times B$  defined by:

$$R_f = \{\langle x, y \rangle \mid f(x) = y\}.$$

#### 1. Example 1:

Define a function  $f : \mathbb{N} \rightarrow \mathbb{Z}$  by

$$f(n) = (-1)^n \cdot \left\lfloor \frac{n+1}{2} \right\rfloor$$

Explicitly:

$$\begin{aligned} n = 0 : \quad & \left\lfloor \frac{0+1}{2} \right\rfloor = \lfloor 0.5 \rfloor = 0 \rightarrow f(0) = (-1)^0 \cdot 0 = 0 \\ n = 1 : \quad & \left\lfloor \frac{1+1}{2} \right\rfloor = \lfloor 1 \rfloor = 1 \rightarrow f(1) = (-1)^1 \cdot 1 = -1 \\ n = 2 : \quad & \left\lfloor \frac{2+1}{2} \right\rfloor = \lfloor 1.5 \rfloor = 1 \rightarrow f(2) = (-1)^2 \cdot 1 = 1 \\ n = 3 : \quad & \left\lfloor \frac{3+1}{2} \right\rfloor = \lfloor 2 \rfloor = 2 \rightarrow f(3) = (-1)^3 \cdot 2 = -2 \\ n = 4 : \quad & \left\lfloor \frac{4+1}{2} \right\rfloor = \lfloor 2.5 \rfloor = 2 \rightarrow f(4) = (-1)^4 \cdot 2 = 2 \end{aligned}$$

Therefore:  $f(0) = 0, \quad f(1) = -1, \quad f(2) = 1, \quad f(3) = -2, \quad f(4) = 2, \dots$

Then the graph is:

$$R_f = \{(0, 0), (1, -1), (2, 1), (3, -2), (4, 2), \dots\}$$

Each element in  $\mathbb{N}$  maps to exactly one element in  $\mathbb{Z}$ .

## 2. Example 2:

Let

$$A = \{a_i \mid i \geq 1\}, \quad B = \{b_k \mid k \geq 1\}, \quad C = \{c_j \mid j \geq 1\}.$$

Define functions

$$f : A \rightarrow B, \quad f(a_i) = b_i \quad \forall i \geq 1,$$

$$g : B \rightarrow C, \quad g(b_k) = c_k \quad \forall k \geq 1.$$

Their graphs are

$$R_f = \{(a_i, b_i) \mid i \geq 1\},$$

$$R_g = \{(b_k, c_k) \mid k \geq 1\}.$$

(a) Relational composition

$$R_f \mid R_g$$

Take an arbitrary pair

$$(a_i, c_j) \in R_f \mid R_g.$$

By definition of relational composition, there exists some index  $k$  such that

$$(a_i, b_k) \in R_f \wedge (b_k, c_j) \in R_g.$$

Because

$$R_f = \{(a_i, b_i) \mid i \geq 1\},$$

the only pair whose first component is  $a_i$  is  $(a_i, b_i)$ . Thus

$$b_k = b_i \rightarrow k = i.$$

Similarly, since

$$R_g = \{(b_k, c_k) \mid k \geq 1\},$$

then

$$c_j = c_k \rightarrow j = k.$$

Therefore,

$$j = k = i,$$

which implies

$$R_f \mid R_g = \{(a_i, c_i) \mid i \geq 1\}.$$

(b) Function composition

$$g \circ f$$

For each  $i \geq 1$ ,

$$(g \circ f)(a_i) = g(f(a_i)) = g(b_i) = c_i,$$

so the graph of the composite is

$$R_{g \circ f} = \{(a_i, c_i) \mid i \geq 1\}.$$

Thus,

$$R_f \mid R_g = R_{g \circ f} = \{(a_i, c_i) \mid i \geq 1\}.$$

## 26.2 Restriction and Image

Let  $f : A \rightarrow B$  be a function and let  $C \subseteq A$ . The restriction of  $f$  to  $C$ , denoted  $f \upharpoonright C : C \rightarrow B$ , is defined by

$$(f \upharpoonright C)(x) = f(x), \forall x \in C.$$

Equivalently, in terms of graphs:

$$R_{f \upharpoonright C} = \{(x, y) \in R_f \mid x \in C\}.$$

The image of  $C$  under  $f$  is:

$$f[C] = \{f(x) \mid x \in C\}.$$

### 1. Example 1:

Let  $f : \mathbb{R} \rightarrow \mathbb{R}$  be defined by

$$f(x) = x^2.$$

Let  $C = [0, \infty) \subseteq \mathbb{R}$ . The restriction of  $f$  to  $C$  is the function

$$f \upharpoonright C : C \rightarrow \mathbb{R},$$

defined by

$$(f \upharpoonright C)(x) = x^2 \quad \forall x \in C.$$

The graph of  $f$  is

$$R_f = \{(x, x^2) \mid x \in \mathbb{R}\}.$$

The graph of the restricted function is

$$R_{f|C} = \bigcup_{x \in [0, \infty)} \{(x, x^2)\}.$$

## 2. Example 2:

Let  $f : \mathbb{N} \rightarrow \mathbb{Z}$  be defined by

$$f(n) = (-1)^n \cdot n.$$

Let  $\mathbb{P}$  be the set of prime numbers:

$$\mathbb{P} = \{2, 3, 5, 7, 11, \dots\} \subseteq \mathbb{N}.$$

The restriction of  $f$  to  $\mathbb{P}$  is the function

$$f \upharpoonright \mathbb{P} : \mathbb{P} \rightarrow \mathbb{Z},$$

defined by

$$(f \upharpoonright \mathbb{P})(p) = (-1)^p \cdot p \quad \forall p \in \mathbb{P}.$$

The graph of  $f$  is

$$R_f = \{(n, (-1)^n \cdot n) \mid n \in \mathbb{N}\}.$$

The graph of the restricted function is

$$R_{f|_{\mathbb{P}}} = \bigcup_{p \in \mathbb{P}} \{(p, (-1)^p \cdot p)\}.$$

## 26.3 Composition of Functions

Let  $f : A \rightarrow B$  and  $g : B \rightarrow C$  be functions. The *composition* of  $f$  and  $g$ , denoted  $g \circ f$ , is the function:

$$(g \circ f) : A \rightarrow C$$

defined by:

$$(g \circ f)(x) = g(f(x)), \forall x \in A$$

This operation is only defined when the range of  $f$  is a subset of the domain of  $g$ .

### 1. Example 1:

Consider two functions:

$$f(x) = x + 1, \quad g(x) = 2x$$

To compute  $(g \circ f)(x)$ :

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(x + 1) \\ &= 2(x + 1) \\ &= 2x + 2\end{aligned}$$

So the composed function is:

$$(g \circ f)(x) = 2x + 2$$

## 2. Example 2:

Consider two functions:

$$f : \mathbb{N} \rightarrow \mathbb{Z}, \quad f(n) = 2n - 5$$

$$g : \mathbb{Z} \rightarrow \mathbb{Q}, \quad g(z) = \frac{z + 1}{3}$$

To compute  $(g \circ f)(n)$ :

$$\begin{aligned}(g \circ f)(n) &= g(f(n)) \\ &= g(2n - 5) \\ &= \frac{(2n - 5) + 1}{3} \\ &= \frac{2n - 4}{3}\end{aligned}$$

So the composed function is:

$$(g \circ f) : \mathbb{N} \rightarrow \mathbb{Q}, \quad (g \circ f)(n) = \frac{2n - 4}{3}$$

## 3. Example 3:

Let

$$f(x) = x + 1, \quad g(x) = 2x$$

Then:

$$(g \circ f)(x) = g(f(x)) = 2(x + 1) = 2x + 2$$

$$(f \circ g)(x) = f(g(x)) = (2x) + 1 = 2x + 1$$

## 26.4 Partial Function

A partial function  $f : A \rightharpoonup B$  is a mapping that assigns to every element of  $A$  *at most one* element of  $B$ .

1. If  $f$  assigns a value to  $x \in A$ , we say  $f(x)$  is defined, and write  $f(x) \downarrow$ .
2. Otherwise,  $f(x)$  is undefined, and we write  $f(x) \uparrow$ .
3. The domain of a partial function  $f$  is:

$$\text{dom}(f) = \{x \in A : f(x) \downarrow\}$$

### 1. Example 1:

Every total function  $f : A \rightarrow B$  is also a partial function where  $\text{dom}(f) = A$ .

Let  $A = \{1, 2, 3\}$  and  $B = \{a, b, c\}$ . Define a function  $f : A \rightarrow B$  by:

$$f(1) = a, \quad f(2) = b, \quad f(3) = c$$

This function is total, since every element of  $A$  is assigned an element of  $B$ . We can also view it as a partial function:

$$f : A \rightharpoonup B \quad \text{with } \text{dom}(f) = A$$

This illustrates that a total function is just a special case of a partial function where the function is defined for all inputs.

### 2. Example 2:

Let  $f : \mathbb{R} \rightharpoonup \mathbb{R}$  be defined by:

$$f(x) = \frac{1}{x}$$

Then  $f$  is undefined at  $x = 0$ :

$$f(0) \uparrow \quad \text{but} \quad f(x) \downarrow \quad \text{for } x \in \mathbb{R} \setminus \{0\}$$

The function  $f$  is defined on all real numbers except 0. So the domain of  $f$  is:

$$\text{dom}(f) = \mathbb{R} \setminus \{0\}$$

### 3. Example 3:

Define  $g : \mathbb{N} \rightharpoonup [0, 1]$  by:

$$g(n) = \begin{cases} \frac{1}{2^n} & n \text{ even,} \\ \uparrow & n \text{ odd.} \end{cases}$$

This is a partial function because  $g(n)$  is undefined for all odd natural numbers. Here  $\text{dom}(g) = \{0, 2, 4, 6, \dots\} \subset \mathbb{N}$ .

## 26.5 Graph of a Partial Function

The graph of a partial function  $f : A \rightarrow B$  is the set:

$$R_f = \{(x, y) \in A \times B \mid f(x) = y\}$$

Let  $R \subseteq A \times B$  satisfy:

$$\forall x \in A, \forall y, y' \in B, (x, y) \in R \wedge (x, y') \in R \rightarrow y = y'$$

Then  $R$  is the graph of a partial function  $f : A \rightarrow B$ , defined by:

$$f(x) = \begin{cases} y & \text{if } (x, y) \in R, \exists y \in B \\ \uparrow & \text{otherwise} \end{cases}$$

If in addition,  $R$  is serial, i.e.,  $\forall x \in A, \exists y \in B \mid (x, y) \in R$ , then  $f$  is a total function.

**Example:**

Let  $A = \{1, 2, 3, 4\}$  and  $B = \{a, b\}$ .

Define a relation  $R \subseteq A \times B$  by:

$$R = \{(1, a), (2, a), (4, b)\}$$

This satisfies:

$$\forall x \in A, \forall y, y' \in B, (x, y) \in R \wedge (x, y') \in R \rightarrow y = y'$$

So  $R$  is the graph of a partial function  $f : A \rightarrow B$ , where:

$$f(1) = a, \quad f(2) = a, \quad f(4) = b, \quad f(3) \uparrow$$

## 27 Inverses of Functions

A function  $g : Y \rightarrow X$  is an inverse of a function  $f : X \rightarrow Y$  if

$$f(g(y)) = y \wedge g(f(x)) = x, \quad \forall x, \forall y (x \in X \wedge y \in Y)$$

**Example:**

Let

$$f(x) = ax + b, \quad g(y) = \frac{y - b}{a}.$$

Then we can verify that

$$f(g(y)) = a \left( \frac{y - b}{a} \right) + b = y,$$

and

$$g(f(x)) = \frac{(ax + b) - b}{a} = x.$$

Therefore,  $g$  is the inverse of  $f$ .

## 27.1 Left and Right Inverse

Let  $f : X \rightarrow Y$

1. A function  $g : Y \rightarrow X$  is a left inverse of  $f$  if  $g(f(x)) = x, \forall x \in X$ .

$$X \xrightarrow{f} Y \xrightarrow{g} X$$

The condition is:

$$g(f(x)) = x, \quad \forall x \in X.$$

Logical implication:

$$(\exists g : Y \rightarrow X) [g \circ f = \text{id}_X] \leftrightarrow f \text{ is injective.}$$

**Example:**

Let

$$f : [0, \infty) \rightarrow \mathbb{R}, \quad f(x) = a^x, \quad a > 0, a \neq 1.$$

Define

$$g(y) = \log_a(y).$$

Then

$$g(f(x)) = \log_a(a^x) = x,$$

so  $g$  is a left inverse of  $f$ .

2. A function  $h : Y \rightarrow X$  is a right inverse of  $f$  if  $f(h(y)) = y, \forall y \in Y$ .

$$Y \xrightarrow{h} X \xrightarrow{f} Y$$

The condition is:

$$f(h(y)) = y, \quad \forall y \in Y.$$

Logical implication:

$$(\exists h : Y \rightarrow X) [f \circ h = \text{id}_Y] \leftrightarrow f \text{ is surjective.}$$

**Example:**

Let

$$f : [0, \infty) \rightarrow \mathbb{R}, \quad f(x) = x^2.$$

Define

$$h(y) = \sqrt{y}.$$

Then

$$f(h(y)) = (\sqrt{y})^2 = y,$$

so  $h$  is a right inverse of  $f$ .

### 3. Two-Sided Inverse

$$X \begin{matrix} \xrightarrow{f} \\ \xleftarrow{f^{-1}} \end{matrix} Y$$

The conditions are:

$$f(f^{-1}(y)) = y, \quad f^{-1}(f(x)) = x.$$

Logical implication:

$$f \text{ is bijective, } f^{-1} \text{ is unique.}$$

#### **Example:**

Let

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}, \quad \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Define a bijection  $f : \mathbb{N} \rightarrow \mathbb{Z}$ :

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even} \\ -\frac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

Define its inverse  $f^{-1} : \mathbb{Z} \rightarrow \mathbb{N}$ :

$$f^{-1}(z) = \begin{cases} 2z, & \text{if } z > 0 \\ 1, & \text{if } z = 0 \\ -2z + 1, & \text{if } z < 0 \end{cases}$$

Left inverse condition:

$$f^{-1}(f(n)) = n, \quad \forall n \in \mathbb{N}.$$

Right inverse condition:

$$f(f^{-1}(z)) = z, \quad \forall z \in \mathbb{Z}.$$

Thus,

$f$  is bijective and  $f^{-1}$  is unique.

## 27.2 Injective Case

If  $f : X \rightarrow Y$  is injective, then there exists a left inverse  $g : Y \rightarrow X$  such that  $g(f(x)) = x$ ,  $\forall x \in X$ .

**Example:**

Let  $X = \{1, 2, 3\}$  and  $Y = \{a, b, c, d\}$ .

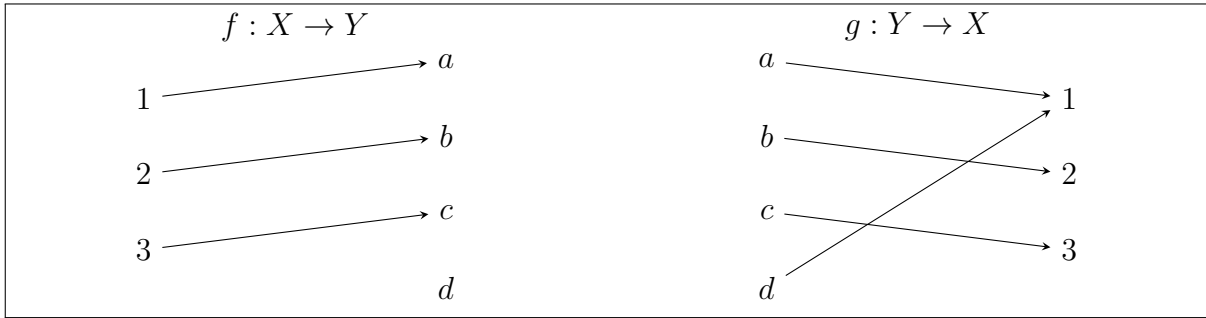
Define  $f : X \rightarrow Y$  by

$$f(1) = a, \quad f(2) = b, \quad f(3) = c$$

Then  $f$  is injective but not surjective (since  $d \notin \text{ran}(f)$ ).

Define a function  $g : Y \rightarrow X$  by

$$g(a) = 1, \quad g(b) = 2, \quad g(c) = 3, \quad g(d) = 1$$



Then  $\forall x \in X$ ,  $g(f(x)) = x$ , so  $g$  is a left inverse of  $f$ .

## 27.3 Surjective Case

If  $f : X \rightarrow Y$  is surjective, then there exists a right inverse  $h : Y \rightarrow X$  such that  $f(h(y)) = y$ ,  $\forall y \in Y$ .

**Example:**

Let  $X = \{1, 2, 3, 4\}$  and  $Y = \{a, b\}$ .

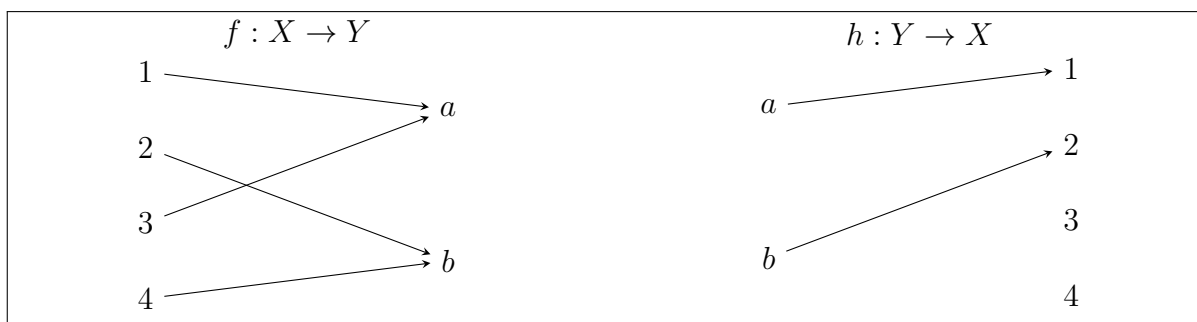
Define  $f : X \rightarrow Y$  by

$$f(1) = a, \quad f(2) = b, \quad f(3) = a, \quad f(4) = b$$

Then  $f$  is surjective but not injective.

A right inverse  $h : Y \rightarrow X$  may be defined as

$$h(a) = 1, \quad h(b) = 2$$



Then  $\forall y \in Y$ ,  $f(h(y)) = y$ , so  $h$  is a right inverse of  $f$ .

## 27.4 Bijective Case

If  $f: X \rightarrow Y$  is bijective, then there exists a function  $f^{-1}: Y \rightarrow X$  such that

$$f^{-1}(f(x)) = x, \forall x \in X \quad \wedge \quad f(f^{-1}(y)) = y, \forall y \in Y$$

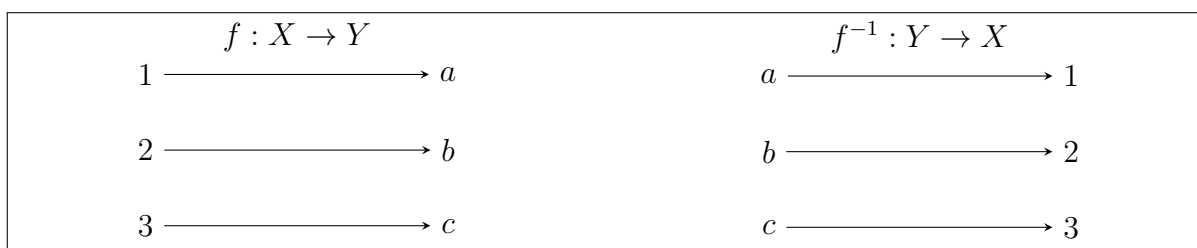
**Example:**

Let  $X = \{1, 2, 3\}$  and  $Y = \{a, b, c\}$  with

$$f(1) = a, \quad f(2) = b, \quad f(3) = c$$

Then  $f$  is bijective. Its inverse  $f^{-1}$  satisfies

$$f^{-1}(a) = 1, \quad f^{-1}(b) = 2, \quad f^{-1}(c) = 3$$



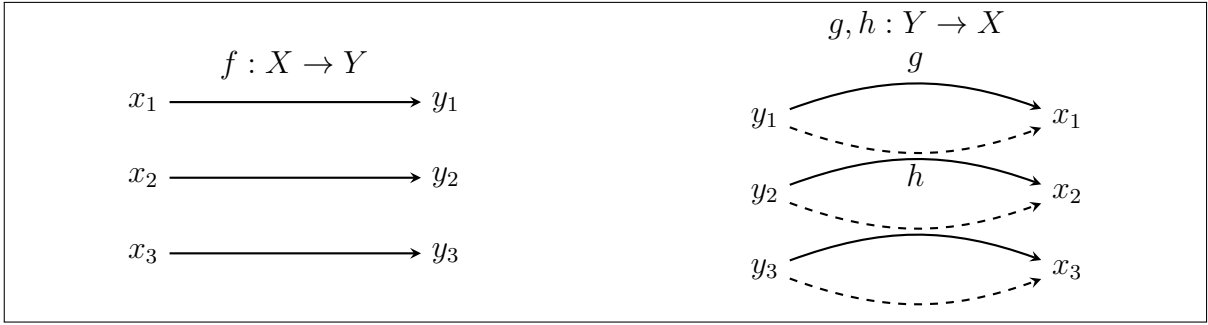
## 27.5 Uniqueness of Inverse

If  $f : X \rightarrow Y$  has a left inverse  $g$  and a right inverse  $h$ , then  $g = h$ . Then, every function has at most one inverse.

Formally:

$$\forall f : X \rightarrow Y, \forall g, h : Y \rightarrow X$$

$$[(g \circ f = \text{id}_X) \wedge (f \circ g = \text{id}_Y) \wedge (h \circ f = \text{id}_X) \wedge (f \circ h = \text{id}_Y)] \rightarrow g = h$$



### 1. Example 1:

Let

$$X = \{1, 2, 3\}, \quad Y = \{a, b, c\}$$

Define

$$f : X \rightarrow Y, \quad f(1) = a, \quad f(2) = b, \quad f(3) = c$$

Then  $f$  is bijective.

Let

$$g : Y \rightarrow X, \quad g(a) = 1, \quad g(b) = 2, \quad g(c) = 3$$

and

$$h : Y \rightarrow X, \quad h(a) = 1, \quad h(b) = 2, \quad h(c) = 3$$

Then

$$g(f(x)) = x \quad \text{and} \quad f(h(y)) = y$$

Thus  $g$  is a left inverse,  $h$  is a right inverse, and

$$g = h = f^{-1}$$

Hence, the inverse of  $f$  is unique.

## 2. Example 2:

Let

$$f : \mathbb{N} \rightarrow \mathbb{Q}, \quad f(n) = n$$

where we regard  $\mathbb{N} \subset \mathbb{Q}$ . Then  $f$  is injective but not surjective, since many rational numbers (e.g.  $\frac{1}{2}, \frac{3}{4}$ ) are not images of any natural number.

Define

$$g : \mathbb{Q} \rightarrow \mathbb{N}, \quad g(q) = \begin{cases} n, & \text{if } q = n \in \mathbb{N} \\ 1, & \text{otherwise} \end{cases}$$

Then  $\forall n \in \mathbb{N}$ ,

$$g(f(n)) = g(n) = n$$

so  $g$  is a left inverse of  $f$ .

However,  $f$  has no right inverse, since it is not surjective, there is no  $h : \mathbb{Q} \rightarrow \mathbb{N}$  such that

$$f(h(q)) = q, \forall q \in \mathbb{Q}.$$

Hence,  $f$  has a left inverse but no right inverse, and therefore no true inverse. If a true inverse existed, it would be unique.

## 28 Enumerations and Countable Sets

### 28.1 Enumeration

Let  $A$  be a non-empty set. An *enumeration* of  $A$  is an ordered list

$$(a_1, a_2, a_3, \dots)$$

of elements of  $A$  such that every element of  $A$  appears at a finite position in the list. Equivalently, an enumeration of a non-empty set  $A$  is a surjective function

$$f : \mathbb{Z}^+ \rightarrow A, \quad \mathbb{Z}^+ = \{1, 2, 3, \dots\},$$

where

$$f(n) = a_n \quad \forall n \in \mathbb{Z}^+.$$

Surjectivity ensures that every element of  $A$  appears at least once:

$$\forall a \in A \exists n \in \mathbb{Z}^+ \text{ such that } f(n) = a.$$

1. **Example 1:**

Let

$$A = \{2k \mid k \in \mathbb{Z}^+\}.$$

Define  $f : \mathbb{Z}^+ \rightarrow A$  by

$$f(n) = 2n.$$

Then the enumeration is

$n$	1	2	3	4	5	6	7	8	9	10	...
$f(n)$	2	4	6	8	10	12	14	16	18	20	...

2. **Example 2:**

Define  $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}$  by

$$f(n) = \begin{cases} 0, & n = 1, \\ \frac{n}{2}, & n \text{ even}, \\ -\frac{n-1}{2}, & n \text{ odd and } n > 1. \end{cases}$$

We show that  $f$  is bijective.

Surjectivity:

For any  $z \in \mathbb{Z}$ :

- (a) If  $z = 0$ , then  $f(1) = 0$ .
- (b) If  $z = k > 0$ , then  $f(2k) = k$ .
- (c) If  $z = -k < 0$ , then  $f(2k+1) = -k$ .

Injectivity:

If  $f(m) = f(n)$ , then  $m = n$ , since:

- (a) even inputs map to positive integers,
- (b) odd inputs greater than 1 map to non-positive integers,
- (c) and within each case the formulas are injective.

Thus,

$$\mathbb{Z} \sim \mathbb{Z}^+, \quad |\mathbb{Z}| = \aleph_0.$$

The enumeration is

$n$	1	2	3	4	5	6	7	8	9	10	...
$f(n)$	0	1	-1	2	-2	3	-3	4	-4	5	...

### 3. Example 3:

Let  $\mathbb{B} = \{0, 1\}$ . An enumeration of  $\mathbb{B}^*$  is a surjective function

$$f : \mathbb{N} \rightarrow \mathbb{B}^*.$$

Define

$$\begin{aligned} f(0) &= \varepsilon, \\ f(1) &= 0, \\ f(2) &= 1, \\ f(3) &= 00, \\ f(4) &= 01, \\ f(5) &= 10, \\ f(6) &= 11, \\ &\vdots \end{aligned}$$

More generally, for each  $n \in \mathbb{N}$ , let  $k$  be the unique integer such that

$$2^k - 1 < n \leq 2^{k+1} - 1.$$

Then  $f(n)$  is the binary representation of  $n - (2^k - 1)$  using exactly  $k$  bits.

Hence  $\mathbb{B}^*$  is countable.

## 28.2 Countable Sets

A set  $A$  is called *countable* if it is either empty or admits an enumeration.

Formally,

$$A \text{ is countable} \leftrightarrow (A = \emptyset) \vee (\exists f : \mathbb{Z}^+ \rightarrow A \text{ surjective}).$$

Equivalently,

$$\forall a \in A \exists n \in \mathbb{Z}^+ \text{ such that } f(n) = a.$$

### Example

Let  $f : \mathbb{Z}^+ \rightarrow \{a, b, c\}$  be defined by

$$f(1) = a, f(2) = b, f(3) = a, f(4) = c, f(5) = b, f(6) = a, \dots$$

Define  $g$  by selecting the first occurrence of each element:

$$\begin{aligned} g(1) &= a, \\ g(2) &= b, \\ g(3) &= c. \end{aligned}$$

Then

$$g : \{1, 2, 3\} \rightarrow \{a, b, c\}$$

is a bijection. Hence every surjection  $f : \mathbb{Z}^+ \rightarrow A$  induces a bijection onto  $A$ , and therefore  $A$  is countable.

## 29 Cantor's Zig-Zag Method

Recall

$$\mathbb{N}^2 = \{\langle n, m \rangle : n, m \in \mathbb{N}\}.$$

Then we can construct Cantor's zig-zag method as follows.

Let  $\mathbb{N} = \{0, 1, 2, \dots\}$ . Define the bijection

$$f : \mathbb{N} \rightarrow \mathbb{N}^2$$

by

$$f(k) = (i, j),$$

where

$$n = \left\lfloor \frac{\sqrt{8k+1}-1}{2} \right\rfloor, \quad t = \frac{n(n+1)}{2},$$

and

$$i = \begin{cases} k - t, & \text{if } n \text{ is even,} \\ n - (k - t), & \text{if } n \text{ is odd,} \end{cases} \quad j = \begin{cases} n - i, & \text{if } n \text{ is even,} \\ k - t, & \text{if } n \text{ is odd.} \end{cases}$$

In detail:

1.  $k = 0$

$$\begin{aligned} n &= \left\lfloor \frac{\sqrt{8 \cdot 0 + 1} - 1}{2} \right\rfloor = 0, & t &= 0, \\ k - t &= 0, \quad n \text{ even} \rightarrow i = 0, \quad j = 0, \\ f(0) &= (0, 0). \end{aligned}$$

2.  $k = 1$

$$\begin{aligned} n &= \left\lfloor \frac{\sqrt{8 \cdot 1 + 1} - 1}{2} \right\rfloor = 1, & t &= 1, \\ k - t &= 0, \quad n \text{ odd} \rightarrow i = 1, \quad j = 0, \\ f(1) &= (1, 0). \end{aligned}$$

3.  $k = 2$

$$\begin{aligned} n &= \left\lfloor \frac{\sqrt{8 \cdot 2 + 1} - 1}{2} \right\rfloor = 1, & t &= \frac{1 \cdot 2}{2} = 1, \\ k - t &= 1, \quad n \text{ odd} \rightarrow i = 0, \quad j = 1, \\ f(2) &= (0, 1). \end{aligned}$$

4.  $k = 4$

$$\begin{aligned} n &= \left\lfloor \frac{\sqrt{8 \cdot 4 + 1} - 1}{2} \right\rfloor = 2, & t &= \frac{2 \cdot 3}{2} = 3, \\ k - t &= 1, \quad n \text{ even} \rightarrow i = 1, \quad j = 1, \\ f(4) &= (1, 1). \end{aligned}$$

5.  $k = 5$

$$n = \left\lfloor \frac{\sqrt{8 \cdot 5 + 1} - 1}{2} \right\rfloor = 2, \quad t = \frac{2 \cdot 3}{2} = 3,$$

$$k - t = 2, \quad n \text{ even} \rightarrow i = 0, \quad j = 2,$$

$$f(5) = (0, 2).$$

We can organize these ordered pairs into an array:

	0	1	2	3	...
0	$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 0, 2 \rangle$	$\langle 0, 3 \rangle$	...
1	$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 1, 2 \rangle$	$\langle 1, 3 \rangle$	...
2	$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 2, 2 \rangle$	$\langle 2, 3 \rangle$	...
3	$\langle 3, 0 \rangle$	$\langle 3, 1 \rangle$	$\langle 3, 2 \rangle$	$\langle 3, 3 \rangle$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Clearly, every ordered pair in  $\mathbb{N}^2$  appears exactly once in the array. In particular,  $\langle n, m \rangle$  appears in the  $n$ th row and  $m$ th column.

To organize these elements into a one-dimensional list, we use the following pattern:

	0	1	2	3	4	...
0	0	1	3	6	10	...
1	2	4	7	11	...	...
2	5	8	12	...	...	...
3	9	13	...	...	...	...
4	14	...	...	...	...	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

This is Cantor's zig-zag method, which enumerates  $\mathbb{N}^2$  as

$$\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 1, 0 \rangle, \langle 0, 2 \rangle, \langle 1, 1 \rangle, \langle 2, 0 \rangle, \langle 0, 3 \rangle, \langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 3, 0 \rangle, \dots$$

Moreover, we can use this method to enumerate ordered triples:

$$\mathbb{N}^3 = \{ \langle n, m, k \rangle : n, m, k \in \mathbb{N} \}.$$

Viewing

$$\mathbb{N}^3 = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} = \{ \langle \langle n, m \rangle, k \rangle : n, m, k \in \mathbb{N} \},$$

we enumerate  $\mathbb{N}^3$  by labeling one axis with  $\mathbb{N}$  and the other with  $\mathbb{N}^2$ :

	0	1	2	3	...
$\langle 0, 0 \rangle$	$\langle 0, 0, 0 \rangle$	$\langle 0, 0, 1 \rangle$	$\langle 0, 0, 2 \rangle$	$\langle 0, 0, 3 \rangle$	...
$\langle 0, 1 \rangle$	$\langle 0, 1, 0 \rangle$	$\langle 0, 1, 1 \rangle$	$\langle 0, 1, 2 \rangle$	$\langle 0, 1, 3 \rangle$	...
$\langle 1, 0 \rangle$	$\langle 1, 0, 0 \rangle$	$\langle 1, 0, 1 \rangle$	$\langle 1, 0, 2 \rangle$	$\langle 1, 0, 3 \rangle$	...
$\langle 0, 2 \rangle$	$\langle 0, 2, 0 \rangle$	$\langle 0, 2, 1 \rangle$	$\langle 0, 2, 2 \rangle$	$\langle 0, 2, 3 \rangle$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Thus, Cantor's zig-zag method yields an enumeration of  $\mathbb{N}^3$ , and similarly of  $\mathbb{N}^n$  for any  $n \in \mathbb{N}$ .

## 30 Pairing Functions and Codes

A function

$$f : A \times B \rightarrow \mathbb{N}$$

is called an *arithmetical pairing function* if it is a bijection. We say that  $f$  encodes  $A \times B$ , and that  $f(x, y)$  is the code for  $\langle x, y \rangle$ .

We define the pairing function  $g : \mathbb{N}^2 \rightarrow \mathbb{N}$  by

$$g(n, m) = \frac{(n + m)(n + m + 1)}{2} + n.$$

This allows us to calculate the exact index of  $\langle n, m \rangle$  in the enumeration of  $\mathbb{N}^2$ .

In fact, we can define  $g$  directly by making two observations about the diagonal enumeration of  $\mathbb{N}^2$ :

1. Along a fixed diagonal  $n + m = k$ , if the entry in the  $n$ -th row and  $m$ -th column has value  $v$ , then the entry in the  $(n + 1)$ -st row and  $(m - 1)$ -st column has value  $v + 1$ .
2. The first row of the enumeration consists of the triangular numbers  $0, 1, 3, 6, \dots$

The  $k$ -th triangular number is

$$T_k = \sum_{i=0}^k i = \frac{k(k + 1)}{2}.$$

Using these observations, we enumerate  $\mathbb{N}^2$  along diagonals of constant sum. Define

$$g(x, y) = T_{x+y} + x = \frac{(x + y)(x + y + 1)}{2} + x,$$

which enumerates pairs by increasing  $x + y$ , and within each diagonal counts from top to bottom (increasing  $x$ ).

**Examples:**

1. **Encoding**  $\langle 1, 2 \rangle$ .

- (a) Diagonal index:

$$1 + 2 = 3.$$

- (b) Triangular number of previous entries:

$$T_3 = \frac{3 \cdot 4}{2} = 6.$$

- (c) Add the row index:

$$g(1, 2) = T_3 + 1 = 6 + 1 = 7.$$

	0	1	2	3	...
0	0	1	3	6	...
1	2	4	<span style="border: 1px solid black;">7</span>	11	...
2	5	8	12	17	...
3	9	13	18	24	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

## 2. Encoding $\langle 2, 3 \rangle$ .

(a) Diagonal index:

$$2 + 3 = 5.$$

(b) Triangular number:

$$T_5 = \frac{5 \cdot 6}{2} = 15.$$

(c) Add the row index:

$$g(2, 3) = T_5 + 2 = 15 + 2 = 17.$$

$g(x, y)$	0	1	2	3	4
0	0	1	3	6	10
1	2	4	7	11	16
2	5	8	12	<span style="border: 1px solid black;">17</span>	23
3	9	13	18	24	31
4	14	19	25	32	40

Since we already know the pattern, it is easy to assign the value for every pair directly without recomputing triangular numbers. For example:

$$g(1, 1) = 4, \quad g(1, 2) = 7, \quad g(1, 3) = 11, \dots$$

Extending the row-offset pairing to  $\mathbb{N}^3$ :

$$G(x, y, z) = g(g(x, y), z),$$

where

$$g(x, y) = T_{x+y} + x = \frac{(x+y)(x+y+1)}{2} + x.$$

Then

$$G(x, y, z) = \frac{\left(\frac{(x+y)(x+y+1)}{2} + x + z\right) \left(\frac{(x+y)(x+y+1)}{2} + x + z + 1\right)}{2} + \frac{(x+y)(x+y+1)}{2} + x.$$

For compactness, set

$$A = \frac{(x+y)(x+y+1)}{2} + x.$$

Then

$$\boxed{G(x, y, z) = \frac{(A+z)(A+z+1)}{2} + A} \quad \text{with} \quad A = \frac{(x+y)(x+y+1)}{2} + x.$$

### 3. **Encoding** $\langle 1, 2, 3 \rangle$ .

First,

$$g(1, 2) = T_3 + 1 = \frac{3 \cdot 4}{2} + 1 = 7.$$

Second,

$$G(1, 2, 3) = g(7, 3) = T_{10} + 7 = \frac{10 \cdot 11}{2} + 7 = 62.$$

Thus,

$$\boxed{G(1, 2, 3) = 62.}$$

$G(x, y, 3)$	0	1	2	3
0	6	11	24	51
1	17	32	<span style="border: 1px solid black;">62</span>	116
2	41	74	132	227
3	87	149	249	402

### 4. **Encoding** $\langle 2, 1, 3 \rangle$ :

Firstly,

$$g(2, 1) = T_{2+1} + 2 = T_3 + 2 = \frac{3 \cdot 4}{2} + 2 = 6 + 2 = 8$$

Secondly,

$$G(2, 1, 3) = g(8, 3) = T_{8+3} + 8 = T_{11} + 8 = \frac{11 \cdot 12}{2} + 8 = 66 + 8 = 74$$

Thus,

$$\boxed{G(2, 1, 3) = 74.}$$

$G(2, 1, 3)$	0	1	2	3
0	6	11	24	51
1	17	32	62	116
2	41	<span style="border: 1px solid black;">74</span>	132	227
3	87	149	249	402

There are other enumerations of  $\mathbb{N}^2$  that make it easier to determine inverse functions. Rather than visualizing the enumeration in a grid, we begin with the natural numbers viewed as initially empty positions, which we then fill successively with ordered pairs  $\langle n, m \rangle$ .

We begin with pairs whose first component is 0, that is, pairs of the form  $\langle 0, m \rangle$ . Place  $\langle 0, 0 \rangle$  in the first position, then skip one position and place  $\langle 0, 1 \rangle$ , skip again and place  $\langle 0, 2 \rangle$ , and so on.

Recall the grid representation of  $\mathbb{N}^2$ :

	0	1	2	3	...
0	$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 0, 2 \rangle$	$\langle 0, 3 \rangle$	...
1	$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 1, 2 \rangle$	$\langle 1, 3 \rangle$	...
2	$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 2, 2 \rangle$	$\langle 2, 3 \rangle$	...
3	$\langle 3, 0 \rangle$	$\langle 3, 1 \rangle$	$\langle 3, 2 \rangle$	$\langle 3, 3 \rangle$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Initially, the enumeration appears as follows:

<b>Position:</b>	1	2	3	4	5	6	7	8	9	...
<b>Pair:</b>	$\langle 0, 0 \rangle$		$\langle 0, 1 \rangle$		$\langle 0, 2 \rangle$		$\langle 0, 3 \rangle$		$\langle 0, 4 \rangle$	

Since  $2^0 = 1$ , the pairs  $\langle 0, m \rangle$  occupy every odd position. Next, insert the pairs  $\langle 1, m \rangle$ . Because  $2^1 = 2$ , these occupy every second remaining empty position:

<b>Position:</b>	1	2	3	4	5	6	7	8	9	10
<b>Pair:</b>	$\langle 0, 0 \rangle$	$\langle 1, 0 \rangle$	$\langle 0, 1 \rangle$		$\langle 0, 2 \rangle$	$\langle 1, 1 \rangle$	$\langle 0, 3 \rangle$		$\langle 0, 4 \rangle$	

Continuing this process for  $\langle 2, m \rangle$ ,  $\langle 3, m \rangle$ , and so on yields the enumeration:

<b>Position:</b>	1	2	3	4	5	6	7	8	9	10
<b>Pair:</b>	$\langle 0, 0 \rangle$	$\langle 1, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 2, 0 \rangle$	$\langle 0, 2 \rangle$	$\langle 1, 1 \rangle$	$\langle 0, 3 \rangle$	$\langle 3, 0 \rangle$	$\langle 0, 4 \rangle$	$\langle 1, 2 \rangle$

Numbering positions according to this scheme gives the following table:

	0	1	2	3	4	5	...
0	1	3	5	7	9	11	...
1	2	6	10	14	18	...	...
2	4	12	20	28	...	...	...
3	8	24	40	...	...	...	...
4	16	48	...	...	...	...	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

For all  $n, m \in \mathbb{N}$ , the position of  $\langle n, m \rangle$  in this enumeration is

$$\langle n, m \rangle \mapsto 2^n(2m + 1).$$

To shift the enumeration so that it begins at 0, define the pairing function  $h : \mathbb{N}^2 \rightarrow \mathbb{N}$  by

$$h(n, m) = 2^n(2m + 1) - 1.$$

$(n, m)$	0	1	2	3	4	5
0	0	2	4	6	8	10
1	1	5	9	13	17	21
2	3	11	19	27	35	43
3	7	23	39	55	71	87
4	15	47	79	111	143	175
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

## 31 Uncountable Sets

It is known that, some sets, such as the set  $\mathbb{Z}^+$  of positive integers, are infinite. So far, we have encountered infinite sets that are all countable. For example, the set of even positive integers  $E = \{2, 4, 6, 8, \dots\}$  is countable. Although  $E$  seems smaller than  $\mathbb{Z}^+$ , we can pair each element of  $E$  with exactly one element of  $\mathbb{Z}^+$  using the function:

$$f(n) = 2n, \quad \text{for } n \in \mathbb{Z}^+$$

Specifically

$\mathbb{Z}^+$	1	2	3	4	5	$\dots$	$n$
$E$	2	4	6	8	10	$\dots$	$2n$

This function is a bijection from  $\mathbb{Z}^+$  to  $E$ , proving that  $E$  is countable. In other words:

$$|E| = |\mathbb{Z}^+|$$

However, there exist infinite sets which do not have this property. Such sets are called uncountable. By definition, a set  $S$  is countable if there exists a surjective function  $f : \mathbb{Z}^+ \rightarrow S$ . Otherwise,  $S$  is uncountable. If a set is uncountable, then no function mapping  $\mathbb{Z}^+$  to  $S$  can cover all elements of  $S$ . Thus, there are more elements in  $S$  than there are in  $\mathbb{Z}^+$ ,

$$|\mathbb{Z}^+| < |S|$$

To prove a set is uncountable, we must show that no such surjective function can exist. Equivalently, the elements of  $S$  cannot be enumerated in a one-way infinite list. A powerful technique for demonstrating this is called \*Cantor's diagonal method\*.

### 1. Example 1

Suppose, for contradiction, that  $\mathbb{B}^\omega$  is countable. Then we could list all its elements:

$$s_1, s_2, s_3, s_4, \dots, s_n$$

This means there exists a surjective function  $f : \mathbb{Z}^+ \rightarrow \mathbb{B}^\omega$  with  $f(i) = s_i$ , so:

$$\mathbb{B}^\omega = \{s_1, s_2, s_3, \dots\}$$

Each  $s_i$  is itself an infinite binary sequence, written as:

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

where

$$s_i(j) \in \{0, 1\}, \forall j \in \mathbb{Z}^+$$

We may organize this list into an infinite array where each row corresponds to a sequence and each column to a digit in the sequence:

	1	2	3	4	5	...
$s_1$	<span style="border: 1px solid black;">0</span>	1	0	1	1	...
$s_2$	1	<span style="border: 1px solid black;">1</span>	0	0	1	...
$s_3$	0	1	<span style="border: 1px solid black;">0</span>	1	0	...
$s_4$	1	0	1	<span style="border: 1px solid black;">1</span>	0	...
$s_5$	0	1	0	1	<span style="border: 1px solid black;">0</span>	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Define the new sequence:

$$\bar{s}(n) = \begin{cases} 1, & \text{if } s_n(n) = 0 \\ 0, & \text{if } s_n(n) = 1 \end{cases}$$

Or equivalently,

$$\forall n \in \mathbb{Z}^+, \quad \bar{s}(n) \neq s_n(n)$$

Flipping the diagonal:

$$\begin{aligned} s_1(1) &= \text{0} \rightarrow \bar{s}(1) = 1 \\ s_2(2) &= \text{1} \rightarrow \bar{s}(2) = 0 \\ s_3(3) &= \text{0} \rightarrow \bar{s}(3) = 1 \\ s_4(4) &= \text{1} \rightarrow \bar{s}(4) = 0 \\ s_5(5) &= \text{0} \rightarrow \bar{s}(5) = 1 \\ &\vdots \end{aligned}$$

Therefore,

$$\bar{s} = (1, 0, 1, 0, 1, \dots)$$

Then:

$$\forall n \in \mathbb{Z}^+, \quad \bar{s}(n) \neq s_n(n)$$

Assume  $\exists k \in \mathbb{Z}^+$  such that  $\bar{s} = s_k$

$$\bar{s}(k) = s_k(k)$$

But by construction:

$$\bar{s}(k) \neq s_k(k)$$

This contradiction shows that  $\bar{s} \notin \{s_1, s_2, \dots\}$ , even though  $\bar{s} \in \mathbb{B}^\omega$ . Therefore,

$$\boxed{\mathbb{B}^\omega \text{ is uncountable}}$$

## 2. Example 2

Suppose, for contradiction, that  $\mathcal{P}(\mathbb{Z}^+)$  is countable. Then there exists a bijection:

$$f : \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$$

Enumerate all subsets of  $\mathbb{Z}^+$  as:

$$\mathcal{P}(\mathbb{Z}^+) = \{Z_1, Z_2, Z_3, \dots\}$$

where  $f(n) = Z_n$ .

Define the diagonal set:

$$\bar{Z} = \{n \in \mathbb{Z}^+ \mid n \notin Z_n\}$$

Equivalently, for each  $n \in \mathbb{Z}^+$ :

$$n \in \bar{Z} \leftrightarrow n \notin Z_n$$

Consider this enumeration:

	1	2	3	4	5
$Z_1$	<span style="border: 1px solid black;">1</span>	2	3	4	5
$Z_2$	—	<span style="border: 1px solid black;">2</span>	—	4	—
$Z_3$	1	2	<span style="border: 1px solid black;">—</span>	—	5
$Z_4$	—	—	3	<span style="border: 1px solid black;">4</span>	5
$Z_5$	—	2	3	—	<span style="border: 1px solid black;">—</span>

Diagonal entries correspond to the membership condition  $n \in Z_n$ .

Constructing  $\bar{Z}$  by flipping diagonal membership:

$$\bar{Z} = \{n \in \mathbb{Z}^+ : n \notin Z_n\}$$

From the diagram:

$$\bar{Z} = \{3, 5\}$$

By construction:

$$\forall k \in \mathbb{Z}^+, \quad k \in \overline{Z} \leftrightarrow k \notin Z_k \quad \rightarrow \quad \overline{Z} \neq Z_k$$

but by definition:

$$(k \in \overline{Z}) \leftrightarrow (k \notin Z_k)$$

Therefore:

$$\forall k \in \mathbb{Z}^+, \quad \overline{Z} \neq Z_k$$

In detail:

- (a)  $\overline{Z} \neq Z_1$  since  $1 \notin \overline{Z}$  but  $1 \in Z_1$ ,
- (b)  $\overline{Z} \neq Z_2$  since  $2 \notin \overline{Z}$  but  $2 \in Z_2$ ,
- (c)  $\overline{Z} \neq Z_3$  since  $3 \in \overline{Z}$  but  $3 \notin Z_3$ .

Thus:

$$\forall k \in \mathbb{Z}^+, \quad \overline{Z} \neq Z_k$$

and hence  $\overline{Z}$  is not in the enumeration  $\{Z_1, Z_2, Z_3, \dots\}$ . Contradiction.

Therefore:

$$|\mathcal{P}(\mathbb{Z}^+)| > |\mathbb{Z}^+|$$

$\mathcal{P}(\mathbb{Z}^+) \text{ is uncountable.}$

Recall that for two sets  $A$  and  $B$ , the Cartesian product is defined as

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

For three sets  $A$ ,  $B$ , and  $C$ :

$$A \times B \times C = \{(a, b, c) \mid a \in A \wedge b \in B \wedge c \in C\}.$$

In fact, we can extend this idea to a finite collection of sets, and then to an infinite one. Suppose we have a finite index set

$$I = \{1, 2, \dots, n\},$$

and a collection of sets

$$\{A_i\}_{i \in I}.$$

Then the Cartesian product is defined as

$$\prod_{i=1}^n A_i = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ for each } i = 1, 2, \dots, n\}.$$

This is the set of all  $n$ -tuples, where the  $i^{\text{th}}$  coordinate comes from  $A_i$ .

Now, let  $I$  be any index set, possibly infinite. We have a family of sets  $\{A_i\}_{i \in I}$ . We can no longer write down a tuple like  $(a_1, a_2, \dots)$ , since there are infinitely many coordinates. Instead, we define elements as functions.

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

Each  $f$  acts like an infinite tuple:

$$f = (f(i))_{i \in I}.$$

Thus, we can think informally of an element of the product as

$$(a_i)_{i \in I} \quad \text{where } a_i \in A_i.$$

### Example:

Let

$$A_i = \{0, 1\}$$

for each

$$i \in \mathbb{N}.$$

Then the infinite Cartesian product is

$$\prod_{i \in \mathbb{N}} A_i = \{f : \mathbb{N} \rightarrow \{0, 1\}\}.$$

Each element  $f$  of this product is a function that assigns to every natural number  $i$  either 0 or 1. Equivalently, each  $f$  corresponds to an infinite binary sequence:

$$f = (f(1), f(2), f(3), \dots) = (0, 1, 1, 0, 0, 1, \dots).$$

Thus, the product can be written more compactly as

$$\{0, 1\}^{\mathbb{N}} = \text{the set of all infinite binary sequences.}$$

Suppose, for the sake of contradiction, that we could list all such sequences:

$$f_1, f_2, f_3, \dots$$

where each

$$f_k : \mathbb{N} \rightarrow \{0, 1\}.$$

Then, define a new sequence

$$\bar{f} : \mathbb{N} \rightarrow \{0, 1\}$$

by flipping the diagonal entries:

$$\bar{f}(n) = \begin{cases} 1, & \text{if } f_n(n) = 0, \\ 0, & \text{if } f_n(n) = 1. \end{cases}$$

Or equivalently,

$$\forall n \in \mathbb{N}, \quad \bar{f}(n) \neq f_n(n).$$

By construction,  $\bar{f}$  differs from each  $f_n$  at least in the  $n$ -th position. Therefore,  $\bar{f}$  cannot appear anywhere in the list  $(f_1, f_2, f_3, \dots)$ .

This contradiction shows that no such enumeration exists, in other words,

$$\{0, 1\}^{\mathbb{N}} \text{ is uncountable or equivalently, } |\{0, 1\}^{\mathbb{N}}| = 2^{\aleph_0}.$$

Specifically:

1. Constant zero function:  $f(n) = 0 \quad \forall n \in \mathbb{N}$ . Sequence:  $(0, 0, 0, 0, \dots)$
2. Constant one function:  $f(n) = 1 \quad \forall n \in \mathbb{N}$ . Sequence:  $(1, 1, 1, 1, \dots)$
3. Alternating sequence:  $f(n) = \begin{cases} 0, & \text{if } n \text{ is odd,} \\ 1, & \text{if } n \text{ is even.} \end{cases}$  Sequence:  $(0, 1, 0, 1, 0, 1, \dots)$
4. Prime indicator function:  $f(n) = \begin{cases} 1, & \text{if } n \text{ is prime,} \\ 0, & \text{otherwise.} \end{cases}$  Sequence:  $(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, \dots)$
5. The diagonal function from Cantor's argument:  $\bar{f}(n) \neq f_n(n)$ .

This set  $\{0, 1\}^{\mathbb{N}}$  has the same cardinality as the real numbers  $\mathbb{R}$ , known as the cardinality of the continuum.

Hence,

$$\prod_{i \in \mathbb{N}} \{0, 1\} \text{ is uncountable.}$$

## 32 Reduction and Equinumerosity

### 32.1 Reduction

A *reduction* from a set  $A$  to a set  $B$  is a surjective function

$$f : A \rightarrow B.$$

If such a surjection exists, we say that the cardinality of  $A$  is greater than or equal to the cardinality of  $B$ , and thus

$$|A| \geq |B|.$$

Equivalently, the existence of a surjective function  $f : A \rightarrow B$  implies the existence of an injective function  $g : B \rightarrow A$ , that is,

$$\exists f : A \rightarrow B \text{ (surjective)} \leftrightarrow \exists g : B \rightarrow A \text{ (injective)}.$$

1. **Example 1**

Let  $\mathbb{N}$  and  $2\mathbb{N} = \{0, 2, 4, 6, \dots\}$ . Define  $f : \mathbb{N} \rightarrow 2\mathbb{N}$  by

$$f(n) = 2n.$$

Then  $f$  is surjective, since for every even number  $2k \in 2\mathbb{N}$ , there exists  $n = k \in \mathbb{N}$  such that  $f(n) = 2k$ . Thus, there exists an injection  $g : 2\mathbb{N} \rightarrow \mathbb{N}$ , for instance

$$g(2k) = k.$$

Hence,

$$|\mathbb{N}| \geq |2\mathbb{N}|.$$

2. **Example 2**

Reduction from  $\mathcal{P}(\mathbb{Z}^+)$  to  $\mathbb{B}^\omega$ . Suppose  $\mathcal{P}(\mathbb{Z}^+)$  is countable with enumeration:

$$Z_1, Z_2, Z_3, \dots$$

Define  $f : \mathcal{P}(\mathbb{Z}^+) \rightarrow \mathbb{B}^\omega$  by:

$$f(Z) = (b_1, b_2, b_3, \dots) \quad \text{where} \quad b_n = \begin{cases} 1 & \text{if } n \in Z \\ 0 & \text{if } n \notin Z \end{cases}$$

According to the definition of  $f$ , each subset  $Z \subseteq \mathbb{Z}^+$  is represented by its characteristic sequence in  $\mathbb{B}^\omega$ . a sequence of 1's and 0's indicating which natural numbers belong to  $Z$ . For example:

$$\begin{aligned} f(\{1, 3, 5, 7, \dots\}) &= (1, 0, 1, 0, 1, 0, 1, \dots), \\ f(\{2, 4, 6, 8, \dots\}) &= (0, 1, 0, 1, 0, 1, 0, \dots), \\ f(\emptyset) &= (0, 0, 0, 0, \dots), \\ f(\mathbb{Z}^+) &= (1, 1, 1, 1, \dots). \end{aligned}$$

We now verify that the function  $f$  defined above is surjective, that is, for every sequence  $s \in \mathbb{B}^\omega$ , there exists some subset  $Z \subseteq \mathbb{Z}^+$  such that  $f(Z) = s$ .

For any  $s = (b_1, b_2, b_3, \dots) \in \mathbb{B}^\omega$ , define

$$Z = \{n \in \mathbb{Z}^+ : s(n) = 1\}.$$

By construction, this subset  $Z$  produces exactly the sequence  $s$  when substituted into the definition of  $f$ ; that is,

$$f(Z) = s.$$

Hence,  $f$  is surjective:

$$f : \mathcal{P}(\mathbb{Z}^+) \rightarrow \mathbb{B}^\omega.$$

Therefore, the enumeration  $f(Z_1), f(Z_2), f(Z_3), \dots$  would list all elements of  $\mathbb{B}^\omega$ , implying that  $\mathbb{B}^\omega$  is countable. However,  $\mathbb{B}^\omega$  is uncountable (by Cantor's diagonal argument). This contradiction shows that  $\mathcal{P}(\mathbb{Z}^+)$  must be uncountable. We conclude that,

$$|\mathcal{P}(\mathbb{Z}^+)| \geq |\mathbb{B}^\omega|.$$

However, the function  $g : \mathbb{B}^\omega \rightarrow \{0, 1\}$  defined by  $g(s) = s(1)$  is also surjective, yet it does not imply that  $\{0, 1\}$  is uncountable, since

$$|\mathbb{B}^\omega| \geq |\{0, 1\}| = 2$$

is trivially true. Thus, the direction of the surjection determines the direction of the inequality in cardinality. To illustrate the importance of surjectivity, define  $h : \mathbb{Z}^+ \rightarrow \mathbb{B}^\omega$  by

$$h(n) = (\underbrace{0, 0, \dots, 0}_n, 1, 0, 0, \dots).$$

Here,  $(1, 1, 1, 1, \dots) \notin \text{Im}(h)$ , so  $h$  is not surjective. Consequently,  $h$  cannot be used to infer any relationship between  $|\mathbb{Z}^+|$  and  $|\mathbb{B}^\omega|$ .

## 32.2 2Equinumerosity

A set  $A$  is *equinumerous* with a set  $B$ , written  $A \approx B$ , if and only if there exists a bijection

$$f : A \rightarrow B.$$

That is,

$$A \approx B \leftrightarrow \exists f : A \rightarrow B \text{ (bijective)}.$$

The relation  $\approx$  is an equivalence relation on the class of all sets, since it satisfies the following properties:

1. Reflexive

$$\text{Id}_A : A \rightarrow A, \quad \text{where } \forall x \in A, \text{Id}_A(x) = x.$$

$$\text{Id}_A \text{ is a bijection} \rightarrow A \approx A.$$

2. Symmetric

Suppose  $A \approx B$ , i.e., there is a bijection  $f : A \rightarrow B$ . Since  $f$  is bijective, its inverse  $f^{-1}$  exists and is also bijective. Hence,  $f^{-1} : B \rightarrow A$  is a bijection, so  $B \approx A$ .

3. Transitive

$$A \approx B \wedge B \approx C \rightarrow \exists f : A \rightarrow B, \exists g : B \rightarrow C \text{ such that } f, g \text{ are bijective.}$$

$$(g \circ f) : A \rightarrow C \text{ is bijective. Therefore } A \approx C.$$

### 1. Example 1:

It is well known that,

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$$

In detail:

- (a)  $\mathbb{N}$  and  $\mathbb{Z}$

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

$\mathbb{N}$	0	1	2	3	4	5	6	7	$\dots$
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	$\dots$

(b)  $\mathbb{N}$  and  $\mathbb{Q}^+$

Using Cantor's diagonal enumeration (pairing method):

$\mathbb{N}$	1	2	3	4	5	6	7	8	...
$\mathbb{Q}^+$	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{3}{2}$	$\frac{2}{3}$	...

Following the diagonal path through the grid of fractions  $\frac{p}{q}$ , skipping duplicates.

## 2. Example 2:

Nonetheless, there is no direct bijection function from  $\mathbb{N}$  into  $[0, 1] \in \mathbb{R}$ , as proven by Cantor's Diagonal Argument. Specifically, suppose we have a function  $f : \mathbb{N} \rightarrow [0, 1]$  that attempts to enumerate all real numbers in the interval  $[0, 1]$ .

$\mathbb{N}$	$[0, 1]$
0	0.1372894651
1	0.4029135702
2	0.7182390045
3	0.5927813409
$\vdots$	$\vdots$

Now, we can construct a new real number  $\bar{r} \in [0, 1]$  by altering the  $n$ -th digit of the  $n$ -th number in the list.

$\mathbb{N}$	$[0, 1]$	$r$
0	0. <u>1</u> 372894651	2
1	0.4 <u>0</u> 29135702	1
2	0.71 <u>8</u> 2390045	9
3	0.592 <u>7</u> 813409	8
$\vdots$	$\vdots$	$\vdots$

Thus, we have constructed a new number  $\bar{r} = 0.2198\dots$  that differs from every number in the list at least at one decimal place, proving that no function  $f : \mathbb{N} \rightarrow [0, 1]$  can be surjective.

With this in mind, we conclude that  $\mathbb{N}$  cannot enumerate  $[0, 1] \subseteq \mathbb{R}$ . Therefore:

$$|\mathbb{N}| = \aleph_0 < |[0, 1]| = |\mathbb{R}| = 2^{\aleph_0}$$

This result is related to the *Continuum Hypothesis (CH)*, which states that there is no set whose cardinality is strictly between  $\aleph_0$  and  $2^{\aleph_0}$ :

$$\nexists S : \aleph_0 < |S| < 2^{\aleph_0}$$

## 33 Sets of Different Sizes

Let  $A, B$  be sets. We define the following relations:

1. No larger than

$$A \preceq B \leftrightarrow \exists f : A \rightarrow B \text{ such that } f \text{ is injective.}$$

2. Smaller than

$$A \prec B \leftrightarrow \exists f : A \rightarrow B \text{ injective, and } \nexists g : A \rightarrow B \text{ bijective.}$$

Equivalently,

$$A \prec B \leftrightarrow A \preceq B \text{ and } A \not\approx B.$$

## 34 Cantor's Theorem

For any set  $A$ ,

$$\forall A, \neg \exists f : A \rightarrow \mathcal{P}(A) \text{ (surjective),}$$

which implies

$$|A| < |\mathcal{P}(A)|.$$

*Proof*

Suppose, for the sake of contradiction, that there exists a surjection

$$f : A \rightarrow \mathcal{P}(A),$$

that is, every subset of  $A$  is the image of some element of  $A$ .

Define the set

$$B = \{x \in A \mid x \notin f(x)\}.$$

Thus,  $B$  consists of all elements of  $A$  that do not belong to their image under  $f$ .

Since  $f$  is assumed to be surjective, there exists some element  $x \in A$  such that

$$f(x) = B.$$

We now consider two cases:

1. Case  $x \in B$  By the definition of  $B$ , this implies  $x \notin f(x)$ . Since  $f(x) = B$ , we conclude  $x \notin B$ , a contradiction.
2. Case  $x \notin B$  By the definition of  $B$ , this implies  $x \in f(x) = B$ , again a contradiction.

In both cases, we reach a contradiction. Therefore, the assumption that  $f$  is surjective must be false. Hence, no surjection exists from  $A$  onto  $\mathcal{P}(A)$ .

Consequently, the power set of any set is strictly larger than the set itself:

$$|A| < |\mathcal{P}(A)|.$$

### 1. Example 1 :

Let

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

Then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

Any function  $f : A \rightarrow \mathcal{P}(A)$  can map at most 2 elements, whereas  $\mathcal{P}(A)$  has 4 elements. Hence,  $f$  cannot be surjective.

Thus,

$$|A| = 2, \quad |\mathcal{P}(A)| = 4,$$

and clearly,

$$|A| < |\mathcal{P}(A)|.$$

## 2. Example 2:

For the set of natural numbers,

$$|\mathbb{N}| = \aleph_0, \quad |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} > \aleph_0.$$

This shows that the set of all subsets of  $\mathbb{N}$  is uncountably infinite.

# 35 Cantor–Schröder–Bernstein

Let  $A, B$  be sets. If  $A \preceq B$  and  $B \preceq A$ , then  $A \approx B$ . Equivalently: if there exist injective functions

$$f : A \rightarrow B, \quad g : B \rightarrow A,$$

then there exists a bijection

$$h : A \rightarrow B.$$

*proof.*

Define the starting layers in  $A$ :

$$A_0 = A \setminus g(B), \quad A_{n+1} = g(f(A_n)), \quad n \geq 0.$$

For  $a_0 \in A$ , consider the alternating chain:

$$\begin{array}{ccccccc} A_0 & \xrightarrow{f} & B & \xrightarrow{g} & A & \xrightarrow{f} & B & \xrightarrow{g} & \dots \\ a_0 \in A_0 & & f(a_0) & & g(f(a_0)) & & f(g(f(a_0))) & & \dots \end{array}$$

Similarly, define the starting layers in  $B$ :

$$B_0 = B \setminus f(A), \quad B_{n+1} = f(g(B_n)), \quad n \geq 0.$$

$$\begin{array}{ccccccc} \dots & \xleftarrow{f} & A & \xleftarrow{g} & B & \xleftarrow{f} & A & \xleftarrow{g} & B_0 \\ \dots & & g(f(g(b_0))) & & f(g(b_0)) & & g(b_0) & & b_0 \in B_0 \end{array}$$

If, after finitely many steps, this chain leaves  $g(B)$ , then  $a_0 \in X$ . Formally,

$$X = \{a \in A \mid \exists n \geq 0 : (g \circ f)^n(a) \notin g(B)\},$$

and equivalently,

$$X = \bigcup_{n=0}^{\infty} A_n.$$

Define

$$Y = A \setminus X = \{a \in A \mid \forall n \geq 0 : (g \circ f)^n(a) \in g(B)\},$$

the set of elements that always remain within the image  $g(B)$  under repeated application of  $f$  and  $g$ , or equivalently,

$$Y = \bigcap_{n=0}^{\infty} (A \setminus A_n).$$

Similarly, define  $Z = f(X)$  and  $W = B \setminus Z$ . We define our bijection  $h : A \rightarrow B$  as:

$$h(a) = \begin{cases} f(a), & a \in X, \\ g^{-1}(a), & a \in Y. \end{cases}$$

1. Injective

- (a) If  $a_1, a_2 \in X$ , then  $h(a_1) = h(a_2) \rightarrow f(a_1) = f(a_2) \rightarrow a_1 = a_2$ .
- (b) If  $a_1, a_2 \in Y$ , then  $h(a_1) = h(a_2) \rightarrow g^{-1}(a_1) = g^{-1}(a_2) \rightarrow a_1 = a_2$ .
- (c) If  $a_1 \in X, a_2 \in Y$ , then  $h(a_1) = h(a_2)$  implies  $f(a_1) = g^{-1}(a_2)$ , which means  $a_2 = g(f(a_1))$ . But  $a_2 \in Y$  (complement of  $X$ ), while  $g(f(a_1)) \in X$ . This contradiction ( $a_2 \in X \cap Y$ ) shows  $h$  is injective.

2. Surjective  $\forall b \in B$ :

- (a) If  $b \in f(X)$ , then  $\exists a \in X$  such that  $b = f(a) = h(a)$ .
- (b) If  $b \notin f(X)$ , then  $g(b) = a$  must be in  $Y$  (if  $a$  were in  $X$ ,  $b$  would be in  $f(X)$ ). Then  $h(a) = g^{-1}(g(b)) = b$ .

Therefore  $h$  is bijective, and  $|A| = |B|$ .

**Example:**

Firstly, define injective functions:

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{N}, & f(x) &= x, \\ g : \mathbb{N} &\rightarrow \mathbb{N}, & g(0) &= 1, & g(y) &= y + 1 \text{ for } y \geq 1. \end{aligned}$$

The forward roots are:

$$X_0 = \mathbb{N} \setminus g(\mathbb{N}) = \{0\} \text{ is false here; actually } \mathbb{N} \setminus \{1, 2, \dots\} = \{0\}.$$

(Note: In this specific example,  $g(\mathbb{N}) = \{1, 2, 3, \dots\}$ , so  $0 \in A_0$ .)

Continuing the chain:

$$0 \xrightarrow{f} 0 \xrightarrow{g} 1 \xrightarrow{f} 1 \xrightarrow{g} 2 \xrightarrow{f} 2 \dots$$

This implies  $X = \{0, 1, 2, \dots\} = \mathbb{N}$ , and  $Y = \emptyset$ .

Then the bijection  $h : \mathbb{N} \rightarrow \mathbb{N}$  is:

$$h(x) = f(x) = x.$$

Alternatively, if we define the chain such that  $Y_0 = \mathbb{N} \setminus f(\mathbb{N}) = \emptyset$ , we follow the construction provided:

$$h : 1 \mapsto 0, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 3, \dots$$

which is the mapping  $h(x) = x - 1$ .