Set Theory

SETS

1 Basic Definitions

Definition of a Set. A set is any collection of objects. These objects are called the elements of the set. Elements can be numbers, points, functions, other sets, or nearly anything we desire.

Elements of Sets. Given a set A, we write $x \in A$ if x is an element of A. If x is not an element of A, we write $x \notin A$.

Describing a Set. Sets can be described using various ways.

1. Certain sets can be describe using special symbols: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{H}, ...$

2. Set can be described with words. For instance, define the set A to be the set of all characters in Breaking Bad.

3. List out directly: $S = \{a\}, K = \{a, b, c, d\}$, $B = \{$Saul Goodman, Mr. White$\}$, etc.

4. Using rules or algorithm:

$$S = \{p \in \mathbb{Z} : p \text{ are Mersenne primes}\}$$

Fundamental Definitions. For any two set A and B,

1. The Union is written $A \cup B$ and is defined by asserting that if $x \in A \cup B$, then $x \in A$ or $x \in B$ (or potentially both).

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

2. The Intersection is written $A \cap B$ and is defined by asserting that if $x \in A \cap B$, then $x \in A$ and $x \in B$.

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

3. Difference Sets. We define $A - B$ or $A \backslash B$ to be the set A with any elements of B removed

$$A \backslash B = \{x \in A : x \notin B\}$$

4. Given $A \subseteq X$, the Complement of A, written A^c, refers to the set of all elements of X not in A. Thus for $A \subseteq X$,

$$A^c = \{x \in X : x \notin A\} = X \backslash A = X - A$$

5. Two sets A and B are equal if they contain exactly the same elements. To assert that $A = B$ means that $A \subseteq B$ and $B \subseteq A$.

6. If A is a set, then the expression $|A|$ is called the cardinality of the set A. For a finite set, cardinality is defined as the number of elements in the set. For example, if $A = \{1, 2, 3\}$, then $|A| = 3$, and if $B = \{4, 5, 6\}$, then $|A| = |B|$. For an infinite set, cardinality is understood as the "size" of the set.

Some Special and Basic Sets.

1. **Singleton Sets, Pair Sets, and Discrete Sets.** Given an object a, we can form the set that has a as its only element. This set is denoted by $\{a\}$, called the singleton set (or a unit set). If a and b are objects, then there exists a set $\{a, b\}$ whose only elements are a and b, called the pair sets. In general, given elements $a, b, c, ..$, we can form the set $\{a, b, c, ...\}$, called discrete sets.

If $a = b$, then $\{a, b\} = \{a\}$. For any a and b, the pair $\{a, b\}$ is the same as $\{b, a\}$ by the definition of equal sets.

2. **The Empty Set.** The set $\varnothing = \{\}$ is called the empty set and is understood to be the set that contains no elements. The empty set is an element of all sets.

3. **Disjoint Sets.** Two sets A and B are disjoint if $A \cap B = \varnothing$.

4. **Finite Set.** Finite sets are sets having a finite/countable number of elements. For example, $S = \{1, 2, 3\}$ is a finite set, and $\mathbb{N} = \{0, 1, 2, ...\}$ is not a finite set.

2 Subsets and Power Sets

Subsets. The inclusion relationship $A \subseteq B$ or $B \supseteq A$ is used to indicate that every element of A is also an element of B. In this case, we say A is a subset of B, or B contains A. We write $A \nsubseteq B$ if A is not a subset of B, that is, there is at least one element of A that is not an element of B.

Properties.

1. A set A is a subset of B if and only if their intersection is equal to A.

$$A \subseteq B \text{ if and only if } A \cap B = A$$

2. A set A is a subset of B if and only if their intersection is equal to B.

$$A \subseteq B \text{ if and only if } A \cup B = A$$

Power Sets. Let A be a set, the power of set of A, denoted $\mathcal{P}(A)$ is defined to be the set of all subsets of A. Symbolically,

$$\mathcal{P}(A) = \{X : X \subseteq A\}$$

3 Indexed Sets. The Great Union and Intersection

Let A and Ω be sets, and suppose that with each element α of A there is an associated $E_\alpha \subseteq \Omega$.

Union. The union of the sets E_α is defined to be the set S such that $x \in S$ if and only if $x \in E_\alpha$ for at least one $\alpha \in A$.

$$S = \bigcup_{\alpha \in A} E_\alpha = \{x : x \in E_\alpha \text{ for at least one set } E_\alpha \text{ with } \alpha \in A\}$$

Intersection. The Intersection of the set E_α is defined to be the set P such that if $x \in P$ if and only if $x \in E_\alpha, \forall \alpha \in A$.

$$P = \bigcap_{\alpha \in A} E_\alpha = \{x : x \in E_\alpha \text{ for every set } E_\alpha \text{ with } \alpha \in A\}]$$

For example, if $A = \{3, 6, 9\}$, then

$$S = \bigcup_{\alpha \in A} E_\alpha = E_3 \cup E_6 \cup E_9$$

If A consists of the integer $1, 2, ..., n$, then we write

$$S = \bigcup_{m=1}^{n} E_m = E_1 \cup E_2 \cup ... \cup E_n$$

If $A = \mathbb{Z}^+$, the set of all positive integers, then

$$S = \bigcup_{m=1}^{\infty} E_m = E_1 \cup E_2 \cup ... \cup E_n \cup ...$$

Similarly, if A consists of finitely or infinitely many integers, then

$$P = \bigcap_{m=1}^{n} E_m \quad \text{or} \quad P = \bigcap_{m=1}^{\infty} E_m$$

4 Major Properties and Laws of Set Operations

De Morgan's Law. Given two set A and B, then

$$(A \cap B)^c = A^c \cup B^c \quad \text{and} \quad (A \cup B)^c = A^c \cap B^c$$

Proof. Part 1: $(A \cap B)^c = A^c \cup B^c$

- Forward ($\Longrightarrow$): Let $x \in (A \cap B)^c$. Then, $x \notin A \cap B$. Because $A \cap B = \{y : y \in A \text{ or } y \in B\}$, therefore it must also be the case that $x \notin A$ or $x \notin B$. If $x \notin A$, then $x \in A^c$, so $x \in A^c \cup B^c$. Similarly, if $x \in B$, then $x \in B^c$, so $x \in A^c \cup B^c$. Thus, for every $x \in (A \cap B)^c$, $x \in (A \cap B)^c$ implies that $x \in A^c \cup B^c$. That is, $(A \cap B)^c \subseteq A^c \cup B^c$.
- Backward ($\Longleftarrow$): Let $x \in A^c \cup B^c$, and for contradiction, assume that $x \notin (A \cap B)^c$. Under that assumption, it must be the case that $x \in A \cap B$, so it follows that $x \in A$ and $x \in B$, and thus $x \notin A^c$ and $x \notin B^c$. However, that means $x \notin A^c \cup B^c$, which is contradicted to the hypothesis that $x \in A^c \cup B^c$, therefore the assumption of $x \notin (A \cap B)^c$ must not be the case, meaning that $x \in (A \cap B)^c$. Hence, for every $x \in (A \cap B)^c$, $x \in A^c \cup B^c$ implies that $x \in (A \cap B)^c$. That is, $A^c \cup B^c \subseteq (A \cap B)^c$.

De Morgan's Law for n Sets Given n sets $A_1, A_2, ..., A_n$, then

$$(A_1 \cap A_2, ..., \cap A_n)^c = A_1^c \cup A_2^c \cup ... \cup A_n^c$$

$$(A_1 \cup A_2, ..., \cup A_n)^c = A_1^c \cap A_2^c \cap ... \cap A_n^c$$

Proof: We can prove this easily using mathematical induction.

De Morgan's Law, Infinite Edition. Given a collection of sets $A_1, A_2, ...$, then

$$\left(\bigcup_{i=1}^{\infty} A_i\right)^c = \bigcap_{i=1}^{\infty} A_i^c \quad \text{and} \quad \left(\bigcap_{i=1}^{\infty} A_i\right)^c = \bigcup_{i=1}^{\infty} A_i^c$$

De Morgan's Law, Generalized Edition. Let $\{E_\alpha\}$ be a finite or infinite collection of sets E_α, and let A be the index set. Then

$$\left(\bigcup_{\alpha \in A} E_\alpha\right)^c = \bigcap_{\alpha \in A} E_\alpha^c \quad \text{and} \quad \left(\bigcap_{\alpha \in A} E_\alpha\right)^c = \bigcup_{\alpha \in A} E_\alpha^c$$

Theorem 4.1. If A, B and C are sets, then they satisfy the following properties

1. Associativity: $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$
2. Commutativity: $A \cup B = B \cup A$ and $A \cap B = B \cap A$
3. Distributivity:

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(b) $A \cap (B \cap C) = (A \cap B) \cup (A \cap C)$

4. Idempotency:

(a) $A \cup A = A$ and $A \cap A = A$

(b) $A \cup \varnothing = A$ and $A \cap \varnothing = \varnothing$

5. Difference Law: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$ and $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$
6. Self-exclusion: $A - A = A \backslash A = \varnothing$
7. If $A \subseteq B$, then $A \cup B = A \cup (B \backslash A) = B$ and $A \cap B = A$.

5 The Cartesian Product

Ordered Pair. If we wish to define the order, then we define the ordered pair (a, b) as the set $\{a, \{a, b\}\}$. Given ordered pairs (a, b) and (c, d). $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. The order is now important, as if $a \neq b$, then $(a, b) \neq (b, a)$.

The Cartesian Product. The Cartesian product $A \times B$ of two sets A and B is defined as the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

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

From the definition of order pairs, one can define order triples (a, b, c) as $(a, (b, c))$, or in general $(a_1, .., a_n)$ as $(a_1, (a_2, ..., a_n))$.

The General Cartesian Product. The Cartesian Product $A_1 \times A_2 \times ... \times A_n$ of the sets $A_1, A_2, ..., A_n$ is the set of all n-tuples $(a_1, a_2, ..., a_n)$ such that $a_i \in A_i, \forall i \in 1, ..., n$.

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, ..., a_n) \mid a_i \in A_i, \forall i \in \{1, ..., n\}\}$$

For $n \geq 2$, the n-times Cartesian product of a set A, denoted by A^n is the set of all $n-$tuples of elements of A.

MAPPING AND FUNCTIONS

6 Basic Definitions

Mapping. Given two sets S and T. If there is some rule f such that for each $x \in S$, there is some equivalent unique $y \in T$, then we say that f is a map from S to T, we write $f : S \to T$. The element y is called the image of x, and we write $y = f(x)$. Mapping is the generalized concept of functions.

Function. Given two sets A and B, a function from A to B is a rule for mapping that take each element $x \in A$ and associates with it a single element of B. In this case, we write.

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

For some element $x \in A$, the expression $f(x)$ is used to represent the element of B associated with x by f.

Mapping and Function, What's the Difference? Well, they are exactly the same. The terms map and function can be used interchangeably. However, in many mathematical texts, the notion of function is often used to associate a number (or a list of numbers) in A with another number in B. The notion of the map, however, is often used in a much broader way.

Other Terminologies. Depending on the context, functions are sometimes called maps or transformations. They are also known as morphisms, albeit a morphism is a more broad class of object that may or may not correspond to actual functions depending on the situation.

Domain and Range. For a function $f : A \to B$, the set A is called the domain of f, and B is called the range, or codomain of f. The range of f is not necessarily equal to B but refers to a subset E of B given by

$$E = \{y \in B : y = f(x) \text{ for some } x \in A\} \subseteq B.$$

Image. The image of f is a concept close to the range of a function, but not necessarily equal to the range of f. It is defined by

$$\operatorname{im} f = f(A) = \{f(x) : x \in A\}$$

Inverse Image. Consider a function $f : A \to B$. For each subset C of B, the set

$$f^{-1}(C) = \{x \in A : f(x) \in C\}$$

consisting of the elements of A mapping into C under f is called the inverse image of C under f.

Composite Function. If $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by

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

Function composition is associative. If $f : A \to B$, $g : B \to C$, and $h : C \to D$, then

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

Equality of Functions. Two functions $f : A \to B$, $g : A \to B$ with the same domain and range are said to be equal if and only if $f(x) = g(x), \forall x \in A$.

7 Injective, Surjective, and Bijective Functions

Injection, Surjection, and Bijection. Given a function (or a mapping) $f : A \to B$.

1. f is said to be injective (or one-to-one) provided that $\forall a, b \in A$, if $f(a) = f(b)$ then $a = b$. Equivalently, if $a \neq b$ then $f(a) \neq f(b)$. Symbolically,

$$\forall a, b \in A,\ f(a) = f(b) \Rightarrow a = b$$

$$\forall a, b \in A,\ a \neq b \Rightarrow f(a) \neq f(b)$$

In other words, f is one-to-one if every element of the set B corresponds to at most one element of the set A.

2. f is said to be surjective (or onto) if, for all $b \in B$, there is some $a \in A$ such that $f(a) = b$, i.e., the image of f is all of B. Symbolically,

$$\text{If } f : A \to B, \text{ then } f \text{ is injective if } \forall b \in B, \exists a \in A \text{ such that } f(a) = b.$$

In other words, a mapping is onto if every element of the set B corresponds to at least one element of the set A. Another analogous to this definition is that f is injective if

$$\operatorname{im} f(A) = B$$

3. f is considered bijective if it is both injective and surjective. Bijective functions are also called invertible functions.

Theorem 7.1 (Cantor-Schröder-Bernstein Theorem). If there exist injective functions $f : A \to B$ and $g : B \to A$ between the sets A and B, then there exists a bijective function $h : A \to B$.

Examples: one-to-one, onto, and bijective functions.

- Strictly monotone functions on its entire domain are one-to-one.
- The functions $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 - 3x$ and $g : [-1, 1] \to [0, 1]$ defined by $g(x) = x^2$ are onto but not one-to-one since $f(-1) = f(0)$ and $g(-1) = g(1)$.
- The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + x$ is both one-to-one and onto, but $f : \mathbb{R} \to \mathbb{C}$ is still one-to-one but fails to be onto since $\mathbb{R}$ is closed under both $+$ and $\times$.
- The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ is neither one-to-one nor onto, but $g : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $g(x) = x^2$ is both one-to-one and onto.
- The exponent function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = e^x$ is one-to-one but not onto. However, $f : \mathbb{R} \to (0, +\infty)$, $f(x) = e^x$ is both one-to-one and onto, and therefore bijective.
- Define A a set of all (legal) American citizens, and S a set of numbers. The mapping "the Social Security Number of" as a mapping from $A \to S$ is one-to-one because no two Americans have the same social security number. However, it is not onto since there exist numbers that are not social security numbers.

Example Exercises.

1. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 4x + 5$. Is f one-to-one? Is f onto? Is f bijective?

Solution. Suppose $f(x_1) = f(x_2)$; that is, $4x_1 + 5 = 4x_2 + 5$, therefore $x_1 = x_2$, and hence f is one-to-one. By definition, a function is onto if for every $y \in Y$, there exists at least one $x \in X$ such that $f(x) = y$. Consider $x = \frac{y-5}{4} \in \mathbb{R}$, we have $f(x) = f\left(\frac{y-5}{4}\right) = y$, therefore f is onto. Since f is both 1-1 and onto, therefore f is bijective.

2. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 5$. Is f one-to-one? Is f onto? Find $f^{-1}(8)$.

Solution. The function f is not one-to-one because $-1 \neq 1$, but $f(1) = f(-1) = 6$. f is also not onto since there does not exist $x \in \mathbb{R}$ satisfying, for instance, $x^2 + 5 = -2 \in \mathbb{R}$. If the range of f is defined by $(5, +\infty)$ on the other hand, then f is onto. Finally, by definition, $f^{-1}(8) = \{x \in \mathbb{R} : x^2 + 5 = 8\} = \{\sqrt{3}, -\sqrt{3}\}$.

3. Define $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x + 8$. Is f one-to-one? Is f onto? What about if $f(x) = x + 3$?

Solution. Suppose $f(x_1) = f(x_2)$, then we have $x_1 = x_2$, therefore f is one-to-one. f is not onto since for $y = 0 \in \mathbb{Z}$, we have a corresponding $x = -8/3 \notin \mathbb{Z}$.

For $f(x) = x + 3$, if $f(x_1) = f(x_2)$, it follows that $x_1 = x_2$ and hence f is one-to-one. f onto since if we pick any $x = y - 3 \in \mathbb{Z}$, it immediately follows that $f(x) = f(y - 3) = f(y)$.

4. Let a, b, c, d be real numbers such that $ad - bc \neq 0$ and $c \neq 0$. Consider the function $f : \mathbb{R}\backslash\{\frac{-d}{c}\} \to \mathbb{R}\backslash\{\frac{a}{c}\}$ defined by $f(x) = \dfrac{ax + b}{cx + d}$.

(a) Prove that f is a bijection.

(b) Find the inverse function of f.

Solution.

Base on the hypothesis, $f(x)$ is a function defined on $\left(-\infty, \dfrac{-d}{c}\right) \cup \left(\dfrac{-d}{c}, +\infty\right)$, and

$$f(x) = \frac{ax + b}{cx + d},\ \forall x \neq \frac{-d}{c}.$$

a) First, we will prove f is one-to-one, and for fun, we prove this by contradiction. Assume that $x_1, x_2 \in \mathbb{R}\backslash\{\frac{-d}{c}\}$ and $x_1 \neq x_2$. We need to prove that $f(x_1) \neq f(x_2)$. Assume on the contrary that if $x_1 \neq x_2$, then $f(x_1) = f(x_2)$. By then,

$$\frac{ax_1 + b}{cx_1 + d} = \frac{ax_2 + b}{cx_2 + d}$$
$$\Leftrightarrow acx_1x_2 + adx_1 + bcx_2 + bd = acx_1x_2 + adx_2 + bcx_1 + bd$$
$$\Leftrightarrow (ad - bc)x_1 = (ad - bc)x_2$$

Since $ad - bc \neq 0$, therefore $x_1 = x_2$, a contradiction. Therefore, $x_1 \neq x_2$ implies $f(x_1) = f(x_2)$, and f is one-to-one. Next, we will prove that f is onto. For every $y \in \mathbb{R}\backslash\{\frac{a}{c}\}$, consider the equation

$$y = \frac{ax + b}{cx + d} \Leftrightarrow cyx + dy = ax + b \Leftrightarrow x = \frac{b - dy}{cy - a}.$$

Note that $x = \frac{b-dy}{cy-a} \neq -\frac{d}{c}$, $\forall y \in \mathbb{R}\backslash\{\frac{a}{c}\}$, because if $\frac{b-dy}{cy-a} = -\frac{d}{c}$, then $cb - cdy = -cdy + ad \Rightarrow ad = bc$, contradiction with hypothesis. In summary, for every $y \in \mathbb{R}\backslash\{\frac{a}{c}\}$, there exists an $x = \frac{b-dy}{cy-a} \in \mathbb{R}\backslash\{-\frac{d}{a}\}$ such that $f(x) = y$. Therefore f is onto, and bijective.

b) Base on a), since f is a bijection, there must exists an inverse function $f^{-1} : \mathbb{R}\backslash\{\frac{a}{c}\} \to \mathbb{R}\backslash\{-\frac{d}{c}\}$, and

$$f^{-1}(x) = \frac{b - dx}{cx - a}.$$

5. Prove that if the function $f : \mathbb{R} \to \mathbb{R}$ satisfies the condition

$$f(f(x)) = ax + b,\ \forall x \in \mathbb{R}\ (a \neq 0),$$

then f is a bijection.

Solution. Suppose that $f(x_1) = f(x_2)$, then obviously, we have $f(f(x_1)) = f(f(x_2))$, or $ax_1 + b = ax_2 + b$, and since $a \neq 0$, this implies $x_1 = x_2$. This proves that f is one-to-one. Now, note that for every $y \in \mathbb{R}$, there exists $x = f\left(\frac{y-b}{a}\right) \in \mathbb{R}$ such that

$$f(x) = f\left(f\left(\frac{y - b}{a}\right)\right) = a \cdot \frac{y - b}{a} + b = y.$$

Therefore, f is onto, and hence f is a bijection.

6. Consider the function $\phi : [0, 1] \to [a, b]$ defined by

$$\phi(t) = (1 - t)a + tb,\ \forall t \in [0, 1],\ a \neq b$$

(a) Prove that $\phi : [0, 1] \to [a, b]$ is a bijection.

(b) Find the inverse function ϕ^{-1} of ϕ.

Solution. Suppose $t_1, t_2 \in [0, 1]$. Consider t_1, t_2 such that $\phi(t_1) = \phi(t_2)$. With the condition that $a \neq b$, we have

$$(1 - t_1)a + t_1b = (1 - t_2)a + t_2b \Leftrightarrow (b - a)t_1 + a = (b - a)t_2 + a \Leftrightarrow t_1 = t_2.$$

This proves the injection of ϕ. Now, we need to show that for every $w \in [a, b]$, there exists a $t \in [a, b]$ such that $\phi(t) = w$. Suppose that $w \in [a, b]$, then $t = \frac{w-a}{b-a} \in [0, 1]$, and

$$\phi(t) = \phi\left(\frac{w - a}{b - a}\right) = w.$$

This proves the surjection of ϕ, and hence ϕ is a bijection.

b) Since ϕ is a bijection, there must exists an inverse function $\phi^{-1} : [a, b] \to [0, 1]$, and

$$\phi^{-1}(t) = \frac{t - a}{b - a}.$$

8 Left and Right Inverse

Identity Function. We say that $f : X \to Y$ is the identity function if $X = Y$ and $f(x) = x, \forall x \in X$. In this case, we write $f = \mathrm{id}_X = x$. Basically, an identity function is a function that doesn't do anything.

Left and Right Inverse. Given a function $f : X \to Y$.

1. f has a left inverse if there is a function $g : Y \to X$ such that $g \circ f : X \to X$ is the identity map on X, i.e., $g(f(x)) = \mathrm{id}_X = x, \forall x \in X$.

2. f has a right inverse if there is a function $h : Y \to X$ such that $f \circ h : Y \to Y$ is the identity map on Y, i.e., $f(g(y)) = \mathrm{id}_Y = y, \forall y \in Y$.

3. f has a two-sided inverse (or simply an inverse) if it has both a left and right inverse.

Proposition 8.1. Let $f : A \to B$ be a function

1. The map f is injective if and only if f has a left inverse.

2. The map f is surjective if and only if f has a right inverse.

3. The map f is bijective if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A, i.e. $f(g(y)) = y, g(f(x)) = x$. Symbolically,

$$\text{If } f : A \to B, \text{ then } f \text{ is said to be bijective if and only if}$$

$$\exists g : B \to A \text{ such that } f \circ g = Id_B \text{ and } g \circ f = Id_A$$

4. If A and B are finite sets with the same number of elements ($|A| = |B|$), then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.

Proposition 8.2. If $f : A \to B$, and $g : B \to C$ are both invertible, then so is $g \circ f$, and its inverse is

$$f^{-1} \circ g^{-1}.$$

Applying this repeatedly, if $f_1, f_2, ..., f_n$ are invertible and the composition $f_1 \circ f_2 \circ \cdots \circ f_n$ makes sense, then it is invertible, and its inverse is $f_n^{-1} \circ f_{n-1}^{-1} \circ \cdots \circ f_1^{-1}$.

Question: Does there exist a function that has a left inverse, but not a right inverse, and vice versa?

- Consider the infinite-dimensional space $\mathbb{R}^\infty$. If we think of $\mathbb{R}^\infty$ as a set of infinite sequences, then the function $f : \mathbb{R}^\infty \to \mathbb{R}^\infty$ defined by the right shift $f(x_1, x_2, x_3, ...) = (x_2, x_3, x_4, ...)$ has a right inverse, but no left inverse. One possible right inverse is $g(x_1, x_2, x_3, ...) = (0, x_1, x_2, x_3, ...)$. That is, $(f \circ g)(x_1, x_2, x_3, ...) = (x_1, x_2, x_3, ...)$, which is the identity map, but there is no left inverse. Similarly, the function $f(x_1, x_2, x_3, ...) = (0, x_1, x_2, x_3, ...)$ has a left inverse, but no right inverse.

- Another example would be the functions $f, g : \mathbb{R} \to \mathbb{R}$,

$$f(x) = \frac{x}{1 + |x|} \quad \text{and} \quad g(x) = \begin{cases} \dfrac{x}{1 - |x|} & \text{if } |x| < 1 \\ 0 & \text{if } |x| \geq 1 \end{cases}.$$

  Then g is a left inverse of f, but $f \circ g$ is not the identity function.

9 Functions on Finite Sets

Theorem 9.1. Let X and Y be finite sets.

1. If $f : X \to Y$ is injective, then $|X| \leq |Y|$.

2. If $f : X \to Y$ is surjective, then $|X| \geq |Y|$.

3. If $f : X \to Y$ is bijective, then $|X| = |Y|$.

Theorem 9.2. Let X be a finite set. A function $f : X \to X$ is injective if and only if it is surjective. This implies that if such an f is injective or surjective, then it is bijective. This isn't true for infinite sets since a function from an infinite set to itself can be injective without being surjective, or surjective without being injective.

10 Functions and Well-definedness

Formal Definition. In mathematics, a well-defined expression or unambiguous expression is an expression whose definition assigns it a unique interpretation or value. Otherwise, the expression is said to be not well-defined, ill-defined, or ambiguous.

Well-defined Functions. Based on the definition of functions, a function $f : A \to B$ is said to be well-defined if for each $a \in A$, there is a unique B with $f(a) = b$. A function can have multiple inputs (multivariate functions), but there can exist one, and only one output.

Examples.

- Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function defined by $f(n) =$ the first digit of the decimal expansion of n after the decimal point. $f(n)$ is not well-defined since $f(1) = 0$ and $f(0.999...) = 9$ even though $0.999... = 1$.
- The Dirichlet function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \mathbf{1}_{\mathbb{Q}}(x) = \begin{cases} 0 & \text{if } x \notin \mathbb{Q} \\ 1 & \text{if } x \in \mathbb{Q} \end{cases}.$$

  Although this is a strange function, it is in fact well-defined.
- Define a function $f : \mathbb{Q} \to \mathbb{N}$ by

$$f(p/q) = p + q.$$

  The problem with this "function" is that $1/2 = 2/4$, but $1 + 2 \neq 2 + 4$. The definition above violates the definition that a function has one and only one output for each input, therefore we say f is not well-defined.

CARDINALITY OF A SET (FORMAL)

Equal Cardinality. Two sets A and B have equal cardinality if and only if there exists a bijective function $f : A \to B$ from A to B.

Remark. Two sets that have equal cardinality do not prevent one set from containing the other. For example, if X is the set of natural numbers, and Y is the set of even natural numbers, then the map $f : X \to Y$ defined by $f(n) = 2n$ is a bijection from X to Y, and so X and Y have the same cardinality, despite Y being a subset of X and seeming intuitive as if it has "half" of the elements of X.

Proposition 10.1. Let A, B, C be sets. Then,

1. $|A| = |A|$.
2. If $|A| = |B|$, then $|B| = |A|$.
3. If $|A| = |B|$, and $|B| = |C|$, then $|A| = |C|$.

Proposition 10.2 (Uniqueness of Cardinality). A set A is said to have cardinality n if and only if it has equal cardinality with the set $S = \{i \in \mathbb{N} : i < n\}$. Let A be a set with cardinality n. Then A cannot have any other cardinality, and $|A|$ is unique.

ORDINALS

Ordinal Numbers and Their Successors. The first ordinal number is $\varnothing$. Given an ordinal α, the next bigger ordinal called the (immediate) successor of α is the set $\alpha \cup \{\alpha\}$. Thus, the successor of α is just the set of α together with one more element, that element is α itself.

Finite Ordinal Numbers. The finite ordinal numbers are those obtained by starting with the set $\varnothing$ and repeatedly taking the successor.

Construction of the Natural Numbers. In set theory, natural numbers can be constructed as finite ordinals:

$$\begin{aligned} 0 &= \{\} = \varnothing \\ 1 &= \varnothing \cup \{\varnothing\} = \{\varnothing\} \\ 2 &= \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} \\ 3 &= \{\varnothing, \{\varnothing\}\} \cup \{\varnothing, \{\varnothing\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\ &\vdots \end{aligned}$$

Notice that $1 = \{0\}, 2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, and in general, $n = \{0, 1, 2, \cdots, n-1\}$. Therefore, every natural number n is the set of its predecessors.

The Set of Finite Ordinals. The set of all finite ordinals is denoted by the letter ω. Thus, ω is just the set $\mathbb{N}$ of natural numbers. ω is also an ordinal, and it's the first infinite ordinal. Notice that ω is not the successor of any ordinal, and so it is called a limit ordinal.

COUNTABILITY OF SETS

Equivalent Sets and Equivalence Relation. If there exists a 1-1 mapping of A onto B, we say that A and B can be put in a 1-1 correspondence, or say that A and B have the same cardinal number, or A and B are equivalent, and we write $A \sim B$. This relation has the following properties:

1. Reflexivity: $A \sim A$,
2. Symmetry: If $A \sim B$, then $B \sim A$,
3. Transitivity: If $A \sim B$ and $B \sim C$, then $A \sim C$.

Major Definitions. Define A to be any set, and consider the finite set $S_n = \{1, 2, ..., n\}$, and $S = \mathbb{Z}^+ = \{1, 2, ...\}$, the set of all positive integers.

1. **Finite Set.** A is finite if $A \sim S_n$ (the set $\varnothing = \{\}$ is also considered to be finite).
2. **Infinite Set.** A is infinite if A is not finite.
3. **Countable Set.** A is countable if $A \sim \mathbb{Z}^+$.
4. **Uncountable Set.** A is uncountable if A is neither finite nor countable.
5. **At most Countable Set.** A is at most countable if A is either finite or countable.

What does it mean for an infinite set to be countable? A set A is considered to be countable if every single element in that set can be mapped with a 1-1 correspondence with the set $\mathbb{Z}^+ = \{1, 2, 3, 4...\}$. We may say that the elements of any countable set can be arranged in a sequence.

Example.

1. Consider $\mathbb{Z}$, the set of all integers, then $\mathbb{Z}$ is countable. Considering the following arrangement of the set $\mathbb{Z}$ and J:

$$\begin{aligned} \mathbb{Z}: &\quad 0, 1, -1, 2, -2, 3, -3, .. \\ \mathbb{Z}^+: &\quad 1, 2, 3, 4, 5, 6, 7, ... \end{aligned}$$

In this example, we can give an explicit formula for $f : J \to A$ which sets up a 1-1 correspondence:

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ -\dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

2. Consider $\mathbb{Q}$, the set of all rationals. The set of rational numbers is countable.

Proof. Set $A_1 = \{0\}$, and for each $n \geq 2$, let A_n be the set given by

$$A_n = \left\{ \pm\frac{p}{q} : \text{ where } p, q \in \mathbb{Z}^+ \text{ are in lowest term with } p + q = n \right\}.$$

The first few of these sets are

$$A_1 = \{0\}, \quad A_2 = \left\{\frac{1}{1}, -\frac{1}{1}\right\}, \quad A_3 = \left\{\frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}\right\},$$

$$A_4 = \left\{\frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}\right\}, \quad \text{and} \quad A_5 = \left\{\frac{1}{4}, -\frac{1}{4}, \frac{2}{3}, -\frac{2}{3}, \frac{3}{2}, -\frac{3}{2}, \frac{4}{1}, -\frac{4}{1}\right\}$$

Our one-to-one correspondence with $\mathbb{Z}^+$ is achieved by consecutively listing the elements in each A_n.

$\mathbb{Z}^+$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
$\mathbb{Q}$	0	$\frac{1}{1}$	$-\frac{1}{1}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{2}{1}$	$-\frac{2}{1}$	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{3}{1}$	$-\frac{3}{1}$	$\cdots$

Since for any given positive integer n, the set A_n is finite, so we know that any rational number $\pm p/q$ must be included in the set A_{p+q}. To verify the relationship between the set $\mathbb{Z}^+$ and $\mathbb{Q}$ is one-to-one, we observe that the sets A_n are constructed to be disjoint so that no rational number appears twice, ending the proof.

Subset of a Countable Set. If $A \subseteq B$ and B is countable, then A is either countable or finite.

Theorem 10.1. Every infinite subset of a countable set A is countable.

Example. Consider $S = \{1, 2, 3, 4, ...\}$, a countable set, then $P = \{2, 3, 5, 7, 11, ...\}$ must also be countable.

Theorem 10.2 (Union of Countable Sets). Let $\{E_n\}$ be a sequence of countable sets

1. If the sequence is finite up to m, then $P = \bigcup_{n=1}^{m} E_n = E_1 \cup E_2 \cup ... \cup E_m$ is countable.
2. If the sequence is infinite, then $S = \bigcup_{n=1}^{\infty} E_n$ is countable

Corollary. Suppose A is at most countable (that is; either finite or countable), and, $\forall \alpha \in A$, B_α is at most countable, then the set

$$T = \bigcup_{\alpha \in A} B_\alpha$$

is also at most countable. For T is equivalent to a subset of S (3.1).

Tuples. In mathematics, a tuple is a finite ordered list of elements. An n-tuple is a sequence of n elements, where n is a non-negative integer.

Theorem 10.3. Let $A = \{a_1, a_2, \cdots\}$ be a countable set, and let B_n be the set of all n-tuples $(a_1, ..., a_n)$, where $a_k \in A, (k = 1, ..., n)$, and the elements $a_1, ..., a_n$ need not be distinct. Then B_n is countable.

Example.

1. A complex number z is said to be algebraic if there are integers $a_o, a_1, \cdots a_n$, where $a_0^2 + \cdots + a_n^2 \neq 0$ such that

$$a_n z^n + a_{n-1} z^{n-1} + \cdots a_1 z + a_0 = 0.$$

Show that the set of all algebraic numbers is countable.

Proof. Let A be the set of all algebraic numbers. Denote $\mathbf{P}$ the set of all polynomials $p(z) = a_0 + a_1 z + ... + a_n z^n$ with integer coefficients, for some non-negative integer n. Notice that each of these polynomials in the set can be uniquely associated with an $n-$tuple $(a_0, \cdots a_n)$. Since the set that contains all elements $a_0, a_1, ...$ is the set of integers, a countable set, therefore the combination of all $n-$tuples $(a_0, \cdots a_n)$ must also be countable by theorem 10.3, making $\mathbf{P}$ countable. Now, define $R_{p(\alpha)}$ a set of all algebraic number $\alpha \in A$ that satisfies the equation $p(\alpha) = 0$, for some collection of arbitrary polynomials $p(z)$ and algebraic number α; that is,

$$R_{p(\alpha)} := \bigcup_{p(z) \in \mathbf{P}} E_{p(z)} = \bigcup_{p(z) \in \mathbf{P}} \{\alpha \in \mathbb{C} : p(\alpha) = 0\}.$$

By the Fundamental Theorem of Algebra, each of the set $E_{p(z)} = \{\alpha \in \mathbb{C} : p(\alpha) = 0\}$ is finite and only has at most n elements, therefore their union $R_{p(\alpha)}$ must also be countable. Thus, the set of all algebraic number

$$A = \bigcup_{\alpha \in A} R_{p(\alpha)}$$

must also be countable.

2. Let A be the set of all sequences whose elements are the digits 0 and 1. For example, a sequence like 1, 0, 0, 1, 0, 1, 1,... is an element of A. Show that this set is uncountable.

Proof. We assume the contrary; that is this set A is countable and therefore can be arranged in a sequence $s_1, s_2, s_3, s_4...$, for example, as below:

$$\begin{aligned}
s_1 &\mapsto \boxed{0}, 1, 0, 0, 1, 0, 1, 1, 0, 0... \\
s_2 &\mapsto 1, \boxed{1}, 0, 0, 1, 0, 1, 1, 1, 0... \\
s_3 &\mapsto 1, 0, \boxed{0}, 0, 1, 0, 1, 0, 1, 1... \\
s_4 &\mapsto 1, 1, 1, \boxed{0}, 1, 1, 0, 1, 0, 0... \\
&\vdots
\end{aligned}$$

We construct a new sequence s as follows: if the nth digit of s_n is 1, we let the nth digit of s be 0, and vice versa. Taking the example above, the new sequence s is constructed as:

$$s \mapsto 1, 0, 1, 1, ...$$

This sequence is different with s_1 by the first digit, with s_2 by the second digit, with s_3 by the third digit, and so on. This sequence is different from all of the elements in A, therefore it clearly cannot be in A, contradicting the fact that all elements of A can be listed by all s_i, therefore A is uncountable.

3. Prove that there exist real numbers which are not algebraic.

Proof. Denote A to be the set of algebraic numbers and A^* to be the set of non-algebraic numbers. Besides dividing the set $\mathbb{R}$ to be the union of the rationals and irrationals, one can also define it to be the union of algebraic (A) and non-algebraic numbers (A^*). We know for certain that A^* must exist and be non-empty, otherwise $\mathbb{R} = A \cup A^* = A \cup \varnothing = A$, which is a contradiction since A is countable, and $\mathbb{R}$ certainly is not.

4. Prove that $(-1, 1) \sim \mathbb{R}$, and then prove that $(a, b) \sim \mathbb{R}$ for any interval (a, b).

Proof. Define $f : (-1, 1) \to \mathbb{R}$ to be $f(x) = \tan\left(\frac{\pi}{2}x\right)$. Taking the derivative of f, we obtain

$$f'(x) = \frac{\pi}{2} \sec^2\left(\frac{\pi}{2}x\right) \geq 0, \ \forall x \in (-1, 1),$$

hence f is a monotonically increasing function on $(-1, 1)$; that is, $x \leq y$ iff $f(x) \leq f(y)$. Ignore the $x < y$ case and take the case $x = y$, we obtain the desired argument. Notice also that

$$\lim_{x \to 1^-} f(x) = +\infty, \quad \text{and} \quad \lim_{x \to -1^+} f(x) = -\infty.$$

Some simple calculus has shown that this function takes the interval $(-1, 1)$ onto $\mathbb{R}$ in a one-to-one manner. Thus, $(-1, 1) \sim \mathbb{R}$.

AXIOM OF CHOICE AND ORDERED SET

Order on a Set. Let S be a set. An order on S is a relation, denoted by $<$ with the following properties:

1. If $x \in S$ and $y \in S$, then one, and only one of the statement $x < y, x = y$ and $y < x$ is true.

2. For $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

Ordered Sets. An ordered set is a set S in which an order is defined. For example, $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ are ordered sets.