Week 1-2

1 Some Warm-up Questions

Abstraction: The process going from specific cases to general problem.

Proof: A sequence of arguments to show certain conclusion to be true.

"If ... then ...": The part after "if" is called the **hypothesis**, the part after "then" is called the **conclusion** of the sentence or statement.

Fact 1: If m, n are integers with $m \le n$, then there are exactly $n - m + 1$ integers i between m and n inclusive, i.e., $m \le i \le n$.

Fact 2: Let k, n be positive integers. Then the number of multiples of k between 1 and n inclusive is $\lfloor n/k \rfloor$.

Proof. The integers we want to count are the integers

$$1k,\ 2k,\ 3k,\ \ldots, mk$$

such that $mk \le n$. Then $m \le n/k$. Since m is an integer, we have $m = \lfloor n/k \rfloor$, the largest integer less than or equal to n/k. □

Theorem 1.1. *Let m, n be integers with $m \le n$, and k a positive integer. Then the number of multiples of k between m and n inclusive is*

$$\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{m-1}{k} \right\rfloor.$$

Proof. The number of multiples of k between m and n inclusive are the integers

$$ak,\ (a+1)k,\ (a+2)k,\ \ldots,\ (b-1)k,\ bk,$$

where $ak \ge m$ and $bk \le n$. It follows that $a \ge m/k$ and $b \le n/k$. We then have $a = \lceil m/k \rceil$ and $b = \lfloor n/k \rfloor$. Thus by Fact 1, the number of multiples between m and n inclusive is

$$b - a + 1 = \left\lfloor \frac{n}{k} \right\rfloor - \left\lceil \frac{m}{k} \right\rceil + 1.$$

Now by definition of the ceiling function, m can be written as $m = ak - r$, where $0 \le r < k$. Then

$$m - 1 = (a-1)k + (k - r - 1).$$

Let $s = k - r - 1$. Since $k > r$, i.e., $k - 1 \ge r$, then $s \ge 0$. Since $r \ge 0$, then $s \le k - 1$, i.e., $s < k$. So we have

$$m - 1 = (a-1)k + s,\ 0 \le s < k.$$

By definition of the floor function, this means that

$$\left\lceil \frac{m}{k} \right\rceil - 1 = a - 1 = \left\lfloor \frac{m-1}{k} \right\rfloor.$$

□

2 Factors and Multiples

A **prime** is an integer that is greater than 1 and is not a product of any two smaller positive integers.

Given two integers m and n. If there is an integer k such that $n = km$, we say that n is a **multiple** of m or say that m is a **factor** or **divisor** of n; we also say that m **divides** n or n is **divisible** by m, denoted

$$\boldsymbol{m \mid n}.$$

If m does not divide n, we write $\boldsymbol{m \nmid n}$.

Proposition 2.1. *An integer $p \ge 2$ is a prime if and only if its only positive divisors are 1 and p.*

Theorem 2.2 (Unique Prime Factorization)**.** *Every positive integer n can be written as a product of primes. Moreover, there is only one way to write n in this form except for rearranging the order of the terms.*

Let m, n, q be positive integers. If $m \mid n$, then $m \le n$. If $m \mid n$ and $n \mid q$, then $m \mid q$.

A **common factor** or **common divisor** of two positive integers m and n is any integer that divides both m and n. The integer 1 is always a common divisor of m and n. There are only finite number of common divisors for any two positive integers m and n. The very largest one among all common factors of m, n is called the **greatest common divisor** of m and n, denoted

$$\gcd(m, n).$$

Two positive integers m, n are said to be **relatively prime** if 1 is the only common factor of m and n, i.e., $\gcd(m, n) = 1$.

Proposition 2.3. *Let m, n be positive integers. A positive integer d is the greatest common divisor of m, n, i.e., $d = \gcd(a, b)$, if and only if*

(i) $d \mid m$, $d \mid n$, and

(ii) if c is a positive integer such that $c \mid m$, $c \mid n$, then $c \mid d$.

Theorem 2.4 (Division Algorithm)**.** *Let m be a positive integer. Then for each integer n there exist unique integers q, r such that*

$$n = qm + r \quad \text{with} \quad 0 \leq r < m.$$

Proposition 2.5. *Let m, n be positive integers. If $n = qm + r$ with integers $q \geq 0$ and $r > 0$, then $\gcd(n, m) = \gcd(m, r)$.*

Theorem 2.6 (Euclidean Algorithm)**.** *For arbitrary integers m and n, there exist integers s, t such that*

$$\gcd(m, n) = sm + tn.$$

Example 2.1. For the greatest common divisor of integers 231 and 525 is 21, that is, $\gcd(231, 525) = 21$. In fact,

$$525 = 2 \times 231 + 63; \quad 231 = 3 \times 63 + 42; \quad 63 = 1 \times 42 + 21.$$

Then

$$\begin{aligned} 21 &= 63 - 42 = 63 - (231 - 3 \times 63) \\ &= 4 \times 63 - 231 = 4 \times (525 - 2 \times 231) - 231 \\ &= 4 \times 525 - 9 \times 231. \end{aligned}$$

A **common multiple** of two positive integers m and n is any integer that is a multiple of both m and n. The product mn is one such common multiple. There are infinite number of common multiples of m and n. The smallest among all positive common multiples of m and n is called the **least common multiple** of m and n, denoted

$$\operatorname{lcm}(m,n).$$

Let a, b be integers. The minimum and maximum of a and b are denoted by $\min\{a,b\}$ and $\max\{a,b\}$ respectively. We have

$$\min\{a,b\}+\max\{a,b\}=a+b.$$

Theorem 2.7. *For positive integers m and n, we have*

$$\gcd(m,n)\operatorname{lcm}(m,n)=mn.$$

Proof. (Bases on the Unique Prime Factorization) Let us write

$$m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},\quad n=q_1^{f_1}q_2^{f_2}\cdots q_l^{f_l},$$

where p_i, q_j are primes and e_i, f_j are nonnegative integers with $1\le i\le k$, $1\le j\le l$, and

$$p_1<p_2<\cdots<p_k,\quad q_1<q_2<\cdots<q_l.$$

We may put the primes p_i, q_j together and order them as $t_1<t_2<\cdots<t_r$. Then

$$m=t_1^{a_1}t_2^{a_2}\cdots t_r^{a_r},\quad n=t_1^{b_1}t_2^{b_2}\cdots t_r^{b_r},$$

where a_i are nonnegative integers with $1\le i\le r$. Thus

$$\gcd(m,n)=t_1^{\min\{a_1,b_1\}}t_2^{\min\{a_2,b_2\}}\cdots t_r^{\min\{a_r,b_r\}}=\prod_{i=1}^{r}t_i^{\min\{a_i,b_i\}},$$

$$\gcd(m,n)=t_1^{\max\{a_1,b_1\}}t_2^{\max\{a_2,b_2\}}\cdots t_r^{\max\{a_r,b_r\}}=\prod_{i=1}^{r}t_i^{\max\{a_i,b_i\}},$$

$$mn=t_1^{a_1+b_1}t_2^{a_2+b_2}\cdots t_r^{a_r+b_r}=\prod_{i=1}^{r}t_i^{a_i+b_i}.$$

Since $\min\{a_i, b_i\} + \max\{a_i, b_i\} = a_i + b_i$ for all $1 \le i \le r$, we have

$$\begin{aligned} \gcd(m,n)\mathrm{lcm}(m,n) &= \prod_{i=1}^{r} t_i^{\min\{a_i,b_i\}+\max\{a_i,b_i\}} \\ &= \prod_{i=1}^{r} t_i^{a_i+b_i} \\ &= mn. \end{aligned}$$

□

Theorem 2.8. *Let m and n be positive integers.*

(a) If a divides both m and n, then a divides $\gcd(m, n)$.

(b) If b is a multiple of both m and n, then b is a multiple of $\mathrm{lcm}(m, n)$.

Proof. (a) Let us write $m = ka$ and $n = la$. By the Euclidean Algorithm, we have $\gcd(m, n) = sm + tn$ for some integers s, t. Then

$$\gcd(m, n) = ska + tla = (sk + tl)a.$$

This means that a is a factor of $\gcd(m, n)$.

(b) Let b be a common multiple of m and n. By the Division Algorithm, $b = q\mathrm{lcm}(m, n) + r$ for some integer q and r with $0 \le r < \mathrm{lcm}(m, n)$. Now both b and $\mathrm{lcm}(m, n)$ are common multiples of m and n. It follows that $r = b - q\mathrm{lcm}(m, n)$ is a common multiple of m and n. Since $0 \le r < \mathrm{lcm}(m, n)$, we must have $r = 0$. This means that $\mathrm{lcm}(m, n)$ divides b. □

3 Sets and Subsets

A **set** is a collection of distinct objects, called **elements** or **members**, satisfying certain properties. A set is considered to be a whole entity and is different from its elements. Sets are usually denoted by uppercase letters, while elements of a set are usually denoted by lowercase letters.

Given a set A. We write "$x \in A$" to say that x *is an element of* A or x *belongs to* A. We write "$x \notin A$" to say that x *is not an element of* A or x *does not belong to* A.

The collection of all integers forms a set, called the **set of integers**, denoted

$$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

The collection of all nonnegative integers is a set, called the **set of natural numbers**, denoted

$$\mathbb{N} := \{0, 1, 2, \ldots\}.$$

The set of positive integers is denoted by

$$\mathbb{P} := \{1, 2, \ldots\}.$$

We have

$$\begin{aligned} \mathbb{Q}: &\quad \text{set of rational numbers;} \\ \mathbb{R}: &\quad \text{set of real numbers;} \\ \mathbb{C}: &\quad \text{set of complex numbers.} \end{aligned}$$

There are two ways to express a set. One is to list all elements of the set; the other one is to point out the attributes of the elements of the set. For instance, let A be the set of integers whose absolute values are less than or equal to 2. The set A can be described in two ways:

$$A = \{-2, -1, 0, 1, 2\} \quad \text{and}$$

$$\begin{aligned} A &= \{a : a \in \mathbb{Z}, |a| \leq 2\} \\ &= \{a \in \mathbb{Z} : |a| \leq 2\} \\ &= \big\{a \in \mathbb{Z} \,\big|\, |a| \leq 2\big\}. \end{aligned}$$

Two sets A and B are said to be **equal**, written $A = B$, if every element of A is an element of B and every element of B is also an element of A. As usual, we write "$A \neq B$" to say that the sets A and B are not equal. In other words, there is at least one element of A which is not an element of B, or, there is at least one element of B which is not an element of A.

A set A is called a **subset** of a set B, written $A \subseteq B$, if every element of A is an element of B; if so, we say that A is **contained** in B or B **contains** A. If A is not a subset of B, written $A \not\subseteq B$, it means that there exists an element $x \in A$ such that $x \notin B$.

Given two sets A and B. If $A \subseteq B$, it is common to say that B is a **superset** of A, written $B \supseteq A$. If $A \subseteq B$ and $A \neq B$, we abbreviate it as $A \subsetneq B$. The equality $A = B$ is equivalent to $A \subseteq B$ and $B \subseteq A$.

A set is called **finite** if it has only finite number of elements; otherwise, it is called **infinite**. For a finite set A, we denote by $|A|$ the number of elements of A, called an **cardinality** of A. The sets $\mathbb{P}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all infinite sets and

$$\mathbb{P} \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}.$$

Let a, b be real numbers with $a \leq b$. We define **intervals**:

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\},$$
$$(a, b) = \{x \in \mathbb{R} : a < x < b\},$$
$$(a, b] = \{x \in \mathbb{R} : a < x \leq b\},$$
$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}.$$

We define **infinite intervals**:

$$[a, \infty) = \{x \in \mathbb{R} : a \leq x\},$$
$$(a, \infty) = \{x \in \mathbb{R} : a < x\},$$
$$(-\infty, a] = \{x \in \mathbb{R} : x \leq a\},$$
$$(-\infty, a) = \{x \in \mathbb{R} : x < a\}.$$

Consider the set A of real numbers satisfying the equation $x^2 + 1 = 0$. We see that the set contains no elements at all; we call it empty. The set without elements is called the **empty set**. There is one and only one empty set, and is denoted by the symbol

$$\varnothing.$$

The empty set $\varnothing$ is a subset of every set, and its cardinality $|\varnothing|$ is 0.

The collection of everything is *not* a set. Is $\{x : x \notin x\}$ a set?

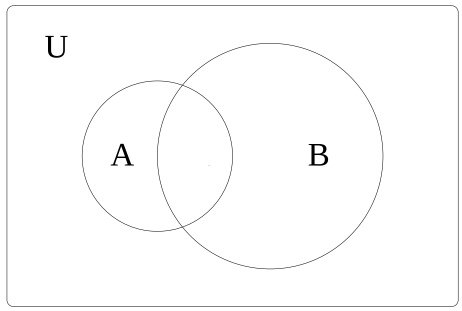
Exercise 1. Let $A = \{1, 2, 3, 4, a, b, c, d\}$. Identify each of the following as true or false:

$$2 \in A; \quad 3 \notin A; \quad c \in A; \quad d \notin A; \quad 6 \in A; \quad e \in A;$$
$$8 \notin A; \quad f \notin A; \quad \varnothing \in A; \quad A \in A; \quad \} \in A; \quad , \in A.$$

Exercise 2. List all subsets of a set A with

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

A convenient way to visualize sets in a universal set U is the **Venn diagram**. We usually use a rectangle to represent the universal set U, and use circles or ovals to represent its subsets as follows:



Exercise 3. Draw the Venn diagram that represents the following relationships.

1. $A \subseteq B$, $A \subseteq C$, $B \not\subseteq C$, and $C \not\subseteq B$.
2. $x \in A$, $x \in B$, $x \notin C$, $y \in B$, $y \in C$, and $y \notin A$.
3. $A \subseteq B$, $x \notin A$, $x \in B$, $A \not\subseteq C$, $y \in B$, $y \in C$.

The **power set** of a set A, written $\mathcal{P}(A)$, is the set of all subsets of A. Note that the empty set $\varnothing$ and the set A itself are two elements of $\mathcal{P}(A)$. For instance, the power set of the set $A = \{a, b, c\}$ is the set

$$\mathcal{P}(A) = \Big\{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\Big\}.$$

Let Σ be finite nonempty set, called **alphabet**, whose elements are called **letters**. A **word** of length n over Σ is a string

$$a_1 a_2 \cdots a_n$$

with the letters $a_1, a_2, \ldots, a_n$ from Σ. When $n = 0$, the word has no letters, called the **empty word** (or **null word**), denoted λ. We denote by $\Sigma^{(n)}$ the set of words of length n and by Σ^* the set of all words of finite length over Σ. Then

$$\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^{(n)}.$$

A subset of Σ^* is called a **language** over Σ.

If $\Sigma = \{a, b\}$, then $\Sigma^{(0)} = \{\lambda\}$, $\Sigma^{(1)} = \Sigma$, $\Sigma^{(2)} = \{aa, ab, ba, bb\}$, and

$$\Sigma^{(3)} = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}, \quad \ldots.$$

If $\Sigma = \{a\}$, then

$$\Sigma^* = \{\lambda, a, aa, aaa, aaaa, aaaaa, aaaaaa, \ldots\}.$$

4 Set Operations

Let A and B be two sets. The **intersection** of A and B, written $A \cap B$, is the set of all elements common to the both sets A and B. In set notation,

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

The **union** of A and B, written $A \cup B$, is the set consisting of the elements belonging to either the set A or the set B, i.e.,

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

The **relative complement** of A in B is the set consisting of the elements of B that is not in A, i.e.,

$$B \smallsetminus A = \{x \mid x \in B, x \notin A\}.$$

When we only consider subsets of a fixed set U, this fixed set U is sometimes called a **universal set**. Note that a universal set is *not universal*; it does not mean that it contains everything. For a universal set U and a subset $A \subseteq U$, the relative complement $U \smallsetminus A$ is just called the **complement** of A, written

$$\overline{A} = U \smallsetminus A.$$

Since we always consider the elements in U, so, when $x \in \overline{A}$, it is equivalent to saying $x \in U$ and $x \notin A$ (in practice no need to mention $x \in U$). Similarly, $x \in A$ is equivalent to $x \notin \overline{A}$. Another way to say about "equivalence" is the phrase "if and only if." For instance, $x \in \overline{A}$ if and only if $x \notin A$. To save space in writing or to make writing succinct, we sometimes use the symbol "$\Longleftrightarrow$"

instead of writing "is (are) equivalent to" and "if and only if." For example, we may write "$x \in \overline{A}$ if and only $x \notin A$" as "$x \in \overline{A} \iff x \notin A$."

Let $A_1, A_2, \ldots, A_n$ be a family of sets. The **intersection** of $A_1, A_2, \ldots, A_n$ is the set consisting of elements common to all $A_1, A_2, \ldots, A_n$, i.e.,

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \Big\{x : x \in A_1, x \in A_2, \ldots, x \in A_n\Big\}.$$

Similarly, the **union** of $A_1, A_2, \ldots, A_n$ is the set, each of its element is contained in at least one A_i, i.e.,

$$\begin{aligned}\bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup \cdots \cup A_n \\ &= \Big\{x : \text{there exists at least one } A_i \text{ such that } x \in A_i\Big\}.\end{aligned}$$

We define the **intersection** and **union** of infinitely many set $A_1, A_2, \ldots$ as follows:

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots = \Big\{x : x \in A_i, i = 1, 2, \ldots\Big\};$$

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots = \Big\{x : \text{there exists one } i \text{ such that } x \in A_i\Big\}.$$

In general, let A_i with $i \in I$ be a family of sets. We can also define the **intersection** and **union**

$$\bigcap_{i \in I} A_i \;=\; \Big\{x : x \in A_i \text{ for all } i \in I\Big\}$$

$$\bigcup_{i \in I} A_i \;=\; \Big\{x : x \in A_i \text{ for at least one } i \in I\Big\}.$$

Theorem 4.1 (DeMorgan Law)**.** *Let A and B be subsets of a universal set U. Then*

$$(1)\quad \overline{\overline{A}} = A, \qquad (2)\quad \overline{A \cap B} = \overline{A} \cup \overline{B}, \qquad (3)\quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Proof. (1) By definition of complement, $x \in \overline{\overline{A}}$ is equivalent to $x \notin \overline{A}$. Again by definition of complement, $x \notin \overline{A}$ is equivalent to $x \in A$.

(2) By definition of complement, $x \in \overline{A \cap B}$ is equivalent to $x \notin A \cap B$. By definition of intersection, $x \notin A \cap B$ is equivalent to either $x \notin A$ or $x \notin B$. Again by definition of complement, $x \notin A$ or $x \notin B$ can be written as $x \in \overline{A}$ or $x \in \overline{B}$. Now by definition of union, this is equivalent to $x \in \overline{A} \cup \overline{B}$.

(3) To show that $\overline{A \cup B} = \overline{A} \cap \overline{B}$, it suffices to show that their complements are the same. In fact, applying parts (1) and (2) we have

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

Their complements are indeed the same. □

The **Cartesian product** (or **product**) of two sets A and B, written $A \times B$, is the set consisting of all ordered pairs (a, b), where $a \in A$ and $b \in B$, i.e.,

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

The **product** of a finite family of sets $A_1, A_2, \ldots, A_n$ is the set

$$\begin{aligned} \prod_{i=1}^{n} A_i &= A_1 \times A_2 \times \cdots \times A_n \\ &= \Big\{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\Big\}, \end{aligned}$$

the element $(a_1, a_2, \ldots, a_n)$ is called an **ordered n-tuple**. The product of an infinite family $A_1, A_2, \ldots$ of sets is the set

$$\prod_{i=1}^{\infty} A_i = A_1 \times A_2 \times \cdots = \Big\{(a_1, a_2, \ldots) : a_1 \in A_1, a_2 \in A_2, \ldots\Big\}.$$

Each element of $\prod_{i=1}^{\infty} A_i$ can be considered as an infinite sequence. If $A = A_1 = A_2 = \cdots$, we write

$$\begin{aligned} A^n &= \underbrace{A \times \cdots \times A}_{n}, \\ A^\infty &= \underbrace{A \times A \times \cdots}_{\infty}. \end{aligned}$$

Example 4.1. For sets $A = \{0, 1\}$, $B = \{a, b, c\}$, the product A and B is the set

$$A \times B = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\};$$

and the product $A^3 = A \times A \times A$ is the set

$$A^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}.$$

For the set $\mathbb{R}$ of real numbers, the product $\mathbb{R}^2$ is the 2-dimensional coordinate plane, and $\mathbb{R}^3$ is the 3-dimensional coordinate space.

A **sequence** of a nonempty set A is a list (elements can repeat) of finite or infinite number of objects of A in order:

$$\begin{array}{ll} a_1, a_2, \ldots, a_n & \text{(finite sequence)} \\ a_1, a_2, a_3, \ldots & \text{(infinite sequence)} \end{array}$$

where $a_i \in A$. The sequence is called **finite** in the former case and **infinite** in the latter case.

Exercise 4. Let A be a set, and let A_i, $i \in I$, be a family of sets. Show that

$$\begin{aligned} \overline{\bigcup_{i \in I} A_i} &= \bigcap_{i \in I} \overline{A_i}; \\ \overline{\bigcap_{i \in I} A_i} &= \bigcup_{i \in I} \overline{A_i}; \\ A \cap \bigcup_{i \in I} A_i &= \bigcup_{i \in I} (A \cap A_i); \\ A \cup \bigcap_{i \in I} A_i &= \bigcap_{i \in I} (A \cup A_i). \end{aligned}$$

Exercise 5. Let A, B, C be finite sets. Use Venn diagram to show that

$$\begin{aligned} |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & -|A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \end{aligned}$$

5 Functions

The elements of any set are distinct. For instance, the collection

$$A = \{a, d, c, d, 1, 2, 3, 4, 5, 6\}$$

is a set. However, the collection

$$B = \{a, b, c, c, d, d, d, 1, 2, 2, 2\}$$

is *not* a set.

Definition 5.1. Let X and Y be nonempty sets. A **function** f of (from) X to Y is a rule such that every element x of X is assigned (or sent to) a *unique* element y in Y. The function f is denoted by

$$f : X \to Y.$$

If an element x of X is sent to an element y in Y, we write

$$y = f(x);$$

we call y the **image** (or **value**) of x under f, and x the **inverse image** of y. The set X is called the **domain** and Y the **codomain** of f. The **image** of f is the set

$$\mathrm{Im}(f) = f(X) = \{f(x) : x \in X\}.$$

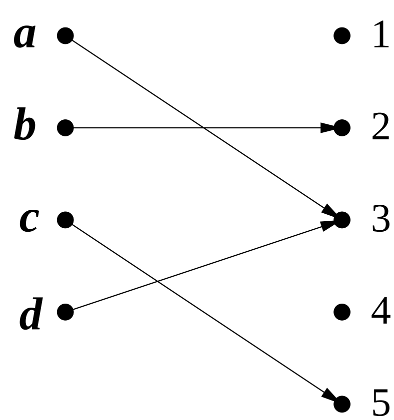
Two functions $f : X \to Y$ and $g : X \to Y$ are said to be **equal**, written as $f = g$, if

$$f(x) = g(x) \quad \text{for all} \quad x \in X.$$

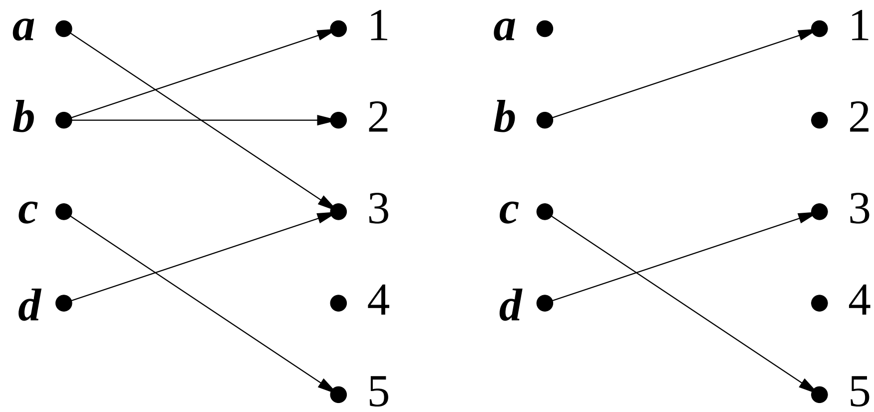
Example 5.1. Let $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$. Let

$$f(a) = 3, \quad f(b) = 2, \quad f(c) = 5, \quad f(d) = 3.$$

Then the function $f : X \to Y$ can be demonstrated by the figure



However, the following assignments are not functions



In calculus, for a function $y = f(x)$, the variable x is usually called an **independent variable** and y the **dependent variable** of f.

Example 5.2. Some ordinary functions.

1. The usual function $y = x^2$ is considered as the function
$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2.$$
Its domain and codomain are $\mathbb{R}$. The function $y = x^2$ can be also considered as a function
$$g : \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad g(x) = x^2.$$
2. The exponential function $y = e^x$ is considered as the function
$$f : \mathbb{R} \to \mathbb{R}_+, \quad f(x) = e^x.$$
The domain of f is $\mathbb{R}$ and the codomain of f is $\mathbb{R}_+$. The function $y = e^x$ can be also considered as a function
$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = e^x.$$
3. The logarithmic function $y = \log x$ is the function
$$\log : \mathbb{R}_+ \to \mathbb{R}, \quad \log(x) = \log x.$$
Its domain is $\mathbb{R}_+$ and codomain is $\mathbb{R}$.
4. The formal rule
$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sqrt{x},$$
is *not* a function from $\mathbb{R}$ to $\mathbb{R}$. However,
$$g : \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad g(x) = \sqrt{x}$$
is a function from $\mathbb{R}_{\geq 0}$ to $\mathbb{R}$.

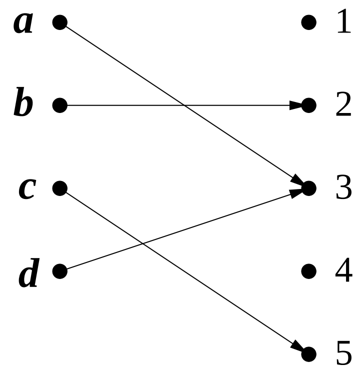
5. The following rule
$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \tfrac{1}{x-1},$$
is *not* a function from $\mathbb{R}$ to $\mathbb{R}$. However,
$$g : \mathbb{R} \setminus \{1\} \to \mathbb{R}, \quad g(x) = \tfrac{1}{x-1}$$
is a function from the set $\mathbb{R} \setminus \{1\} = \{x \in \mathbb{R} : x \neq 1\}$ to $\mathbb{R}$.

6. The absolute value function $y = |x|$ is a function from $\mathbb{R}$ to $\mathbb{R}_{\geq 0}$. It can be also considered as a function from $\mathbb{R}$ to $\mathbb{R}$.

7. The sine function $y = \sin x$ is a function $\sin : \mathbb{R} \to [-1, 1]$. It can be also considered as a function from $\mathbb{R}$ to $\mathbb{R}$.

Let $f : X \to Y$ be a function. For each subset $A \subseteq X$, the set
$$f(A) = \{f(a) \in Y : a \in A\},$$
is called the **image** of A. For each subset $B \subseteq Y$, the set
$$f^{-1}(B) = \{x \in X : f(x) \in B\}$$
is called the **inverse image** (or **pre-image**) of B under f. For each $y \in Y$, the set of all inverse images of y under f is the set
$$f^{-1}(y) := \{x \in X : f(x) = y\}.$$
Clearly,
$$f^{-1}(B) = \bigcup_{y \in B} f^{-1}(y).$$
The **graph** of a function $f : X \to Y$ is the set
$$G(f) = \mathrm{Graph}(f) := \{(x, y) \in X \times Y \mid f(x) = y\}.$$

Example 5.3. Let $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$. Let $f : X \to Y$ be a function given by the figure



Then

$$\begin{array}{lcl} f(\{b,d\}) & = & \{2,3\}, \\ f(\{a,b,c\} & = & \{2,3,5\}, \\ f(\{a,b,c,d\}) & = & \{2,3,5\}; \\ f^{-1}(\{1,2\}) & = & \{b\}, \\ f^{-1}(\{2,3,4\}) & = & \{a,b,d\}, \\ f^{-1}(\{1,4\}) & = & \varnothing, \\ f^{-1}(\{2,3,5\}) & = & \{a,b,c,d\}. \end{array}$$

The graph of the function f is the product set

$$G(f) = \{(a,3),(b,2),(c,5),(d,3)\}.$$

Example 5.4. Some functions to appear in the coming lectures.

1. A finite sequence

   $$s_1, s_2, \ldots, s_n$$

   of a set A can be viewed as a function

   $$s : \{1,2,\ldots,n\} \to A,$$

   defined by

   $$s(k) = s_k, \quad k = 1,2,\ldots,n.$$

2. An infinite sequence $s_1, s_2, \ldots$ of A can be viewed as a function

   $$s : \mathbb{P} \to A, \quad s(k) = s_k, \quad k \in \mathbb{P}.$$

3. The **factorial** is a function $f : \mathbb{N} \to \mathbb{P}$ defined by

   $$\begin{array}{lcl} f(0) & = & 0! = 1, \\ f(n) & = & n! = n(n-1)\cdots 3\cdot 2\cdot 1, \quad n \geq 1. \end{array}$$

4. The **floor function** is the function $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$, defined by

$$\lfloor x \rfloor = \text{greatest integer} \leq x.$$

5. The **ceiling function** is the function $\lceil\ \rceil : \mathbb{R} \to \mathbb{Z}$, defined by

$$\lceil x \rceil = \text{smallest integer} \geq x.$$

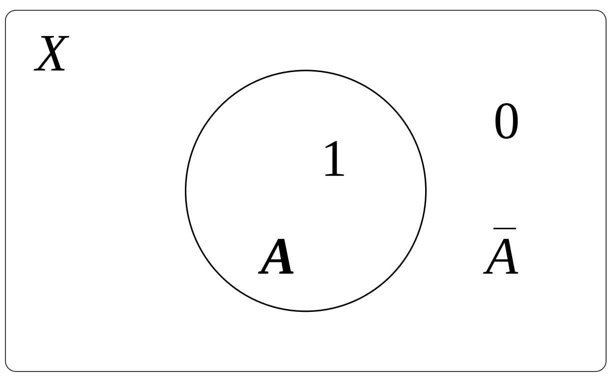
6. Given a universal set X. The **characteristic function** of a subset $A \subseteq X$ is the function

$$1_A : X \to \{0, 1\}$$

defined by

$$1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

The function 1_A can be also viewed as a function from X to $\mathbb{Z}$, and from X to $\mathbb{R}$.



If $X = \{1, 2, \ldots, n\}$, then the subsets can be identified as sequences of 0 and 1 of length n. For instance, let

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

The characteristic function of A corresponds to the sequence

0	1	0	1	1	0	1	1
1	2	3	4	5	6	7	8

7. Let a be a positive integer. Then for each integer b there exist unique integers q and r such that

$$b = qa + r, \quad 0 \leq r < a.$$

We then have the function $\mathsf{Quo}_a : \mathbb{Z} \to \mathbb{Z}$, defined by

$$\mathsf{Quo}_a(b) = q, \quad b \in \mathbb{Z};$$

and the function $\mathsf{Rem}_a : \mathbb{Z} \to \{0, 1, 2, \ldots, a-1\}$, defined by

$$\mathsf{Rem}_a(b) = r, \quad b \in \mathbb{Z}.$$

8. Let a be a positive real number. Then for each real number x there exist unique integers q and r such that

$$x = qa + r, \quad 0 \le r < a.$$

We then have the function $\mathsf{Quo}_a : \mathbb{R} \to \mathbb{Z}$, defined by

$$\mathsf{Quo}_a(x) = q, \quad x \in \mathbb{R};$$

and the function $\mathsf{Rem}_a : \mathbb{R} \to [0, a)$, defined by

$$\mathsf{Rem}_a(x) = r, \quad x \in \mathbb{R}.$$

Let $f : X \to \mathbb{R}$ and $g : X \to \mathbb{R}$ be two functions. The **addition** of f and g is a function $f + g : X \to \mathbb{R}$ defined by

$$(f + g)(x) = f(x) + g(x), \quad x \in X.$$

The **subtraction** of f and g is a function $f - g : X \to \mathbb{R}$ defined by

$$(f - g)(x) = f(x) - g(x), \quad x \in X.$$

The **scalar multiplication** of f by a constant c is a function $cf : X \to \mathbb{R}$ defined by

$$(cf)(x) = cf(x), \quad x \in X.$$

The **multiplication** of f and g is a function $f \cdot g : X \to \mathbb{R}$ defined by

$$(f \cdot g)(x) = f(x)g(x), \quad x \in X.$$

Usually, we simply write $f \cdot g$ as fg.

Example 5.5. Given a universal set X and subsets $A \subseteq X$, $B \subseteq X$. Find the characteristic function $1_{\overline{A}}$ of $\overline{A}$ in terms of 1_A and the characteristic function $1_{A \cup B}$ in terms of 1_A, 1_B, and $1_{A \cap B}$.

By definition of characteristic function, we have

$$1_{\overline{A}}(x) = \begin{cases} 1 & \text{if} \quad x \in \overline{A} \\ 0 & \text{if} \quad x \notin \overline{A} \end{cases} = \begin{cases} 1 & \text{if} \quad x \notin A \\ 0 & \text{if} \quad x \in A \end{cases}.$$

Note that

$$\begin{aligned} (1_X - 1_A)(x) &= 1_X(x) - 1_A(x) \\ &= \begin{cases} 1-0 & \text{if} \quad x \notin A \\ 1-1 & \text{if} \quad x \in A \end{cases} \\ &= \begin{cases} 1 & \text{if} \quad x \notin A \\ 0 & \text{if} \quad x \in A. \end{cases} \end{aligned}$$

Then

$$(1_X - 1_A)(x) = 1_{\overline{A}}(x) \quad \text{for all} \quad x \in X.$$

This means that

$$1_{\overline{A}} = 1_X - 1_A.$$

$$\begin{aligned} (1_A \cdot 1_B)(x) &= 1_A(x) \cdot 1_B(x) \\ &= \begin{cases} 1 \cdot 1 & \text{if} \quad x \in A \cap B \\ 1 \cdot 0 & \text{if} \quad x \in A \setminus B \\ 0 \cdot 1 & \text{if} \quad x \in B \setminus A \end{cases} \\ &= \begin{cases} 1 & \text{if} \quad x \in A \cap B \\ 0 & \text{if} \quad x \notin A \cap B \end{cases} \\ &= 1_{A \cap B}(x) \quad \text{for all} \quad x \in X. \end{aligned}$$

Thus

$$1_A \cdot 1_B = 1_{A \cap B}.$$

6 Injection, Surjection, and Bijection

Definition 6.1. A function $f : X \to Y$ is said to be

1. **injective** (or **one-to-one**) if distinct elements of X are mapped to distinct elements in Y. That is, for $x_1, x_2 \in X$,

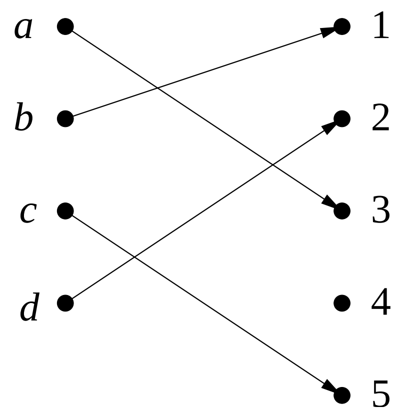
$$\text{if} \quad x_1 \neq x_2, \quad \text{then} \quad f(x_1) \neq f(x_2).$$

An injective function is also called an **injection** (or **one-to-one mapping**).

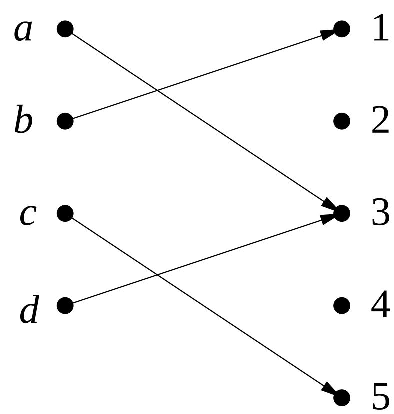
2. **surjective** (or **onto**) if every element in Y is an image of some elements of X; that is, for each $y \in Y$, there exist $x \in X$ such that $f(x) = y$. In other words, $f(X) = Y$. A surjective function is also called a **surjection** (or **onto mapping**).

3. **bijective** if it is both injective and surjective. A bijective function is also called a **bijection** (or **one-to-one correspondence**).

Example 6.1. Let $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$. The function given by the figure

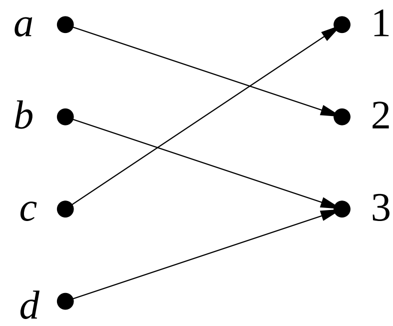


is injective, but not surjective. The function given by the figure



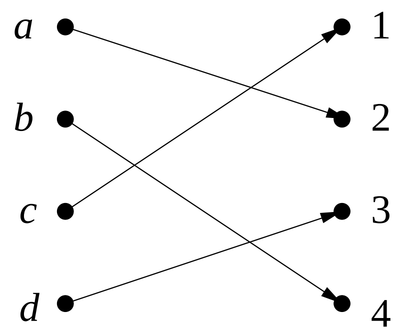
is neither injective nor surjective.

Example 6.2. Let $X = \{a, b, c, d\}$, $Y = \{1, 2, 3\}$. The function given by the figure



is surjective, but not injective.

Example 6.3. Let $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4\}$. The function given by the figure



is bijective.

Example 6.4. 1. The function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = e^x$, is injective, but not surjective.

2. The function $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = x^2$ is surjective, but not injective.

3. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is bijective.

4. The function $f : \mathbb{R}_+ \to \mathbb{R}$ defined by $f(x) = \log x$ is bijective.

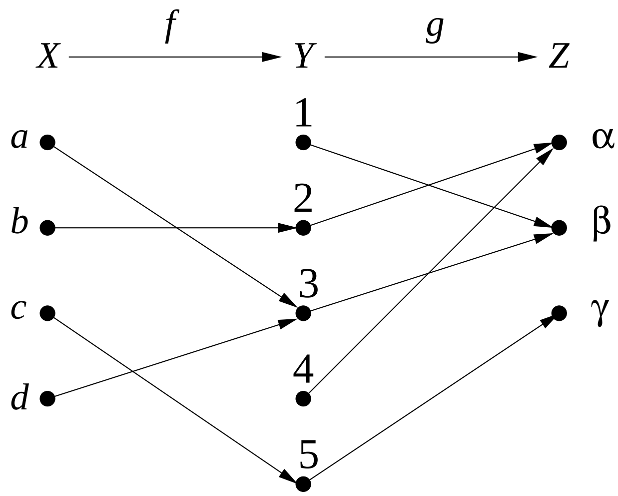
Definition 6.2. The **composition** of functions

$$f : X \to Y \quad \text{and} \quad g : Y \to Z$$

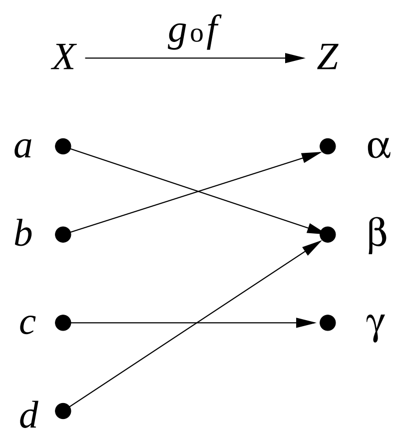
is a function $g \circ f : X \to Z$, defined by

$$(g \circ f)(x) = g(f(x)), \quad x \in X.$$

Example 6.5. Let $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$, $Z = \{\alpha, \beta, \gamma\}$. Let $f : X \to Y$ and $g : Y \to Z$ be given by



The composition $g \circ f : X \to Z$ is given by



Theorem 6.3 (Associativity of Composition)**.** *Given functions*

$$f : X \to Y, \quad g : Y \to Z, \quad h : Z \to W.$$

Then

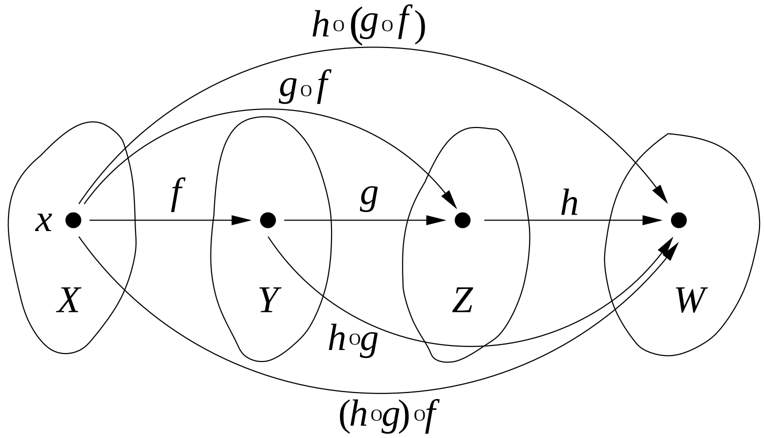
$$h \circ (g \circ f) = (h \circ g) \circ f,$$

as functions from X to W. We write

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

Proof. For any $x \in X$, we have

$$\begin{aligned}
\big(h \circ (g \circ f)\big)(x) &= h\big((g \circ f)(x)\big) \\
&= h\Big(\big(g(f(x))\big)\Big) \\
&= (h \circ g)\big(f(x)\big) \\
&= \big((h \circ g) \circ f\big)(x).
\end{aligned}$$



□

Example 6.6. Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$ and $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \frac{x}{x^2+2}$. Then both $g \circ f$ and $f \circ g$ are functions from $\mathbb{R}$ to $\mathbb{R}$, and for $x \in \mathbb{R}$,

$$\begin{aligned}
(g \circ f)(x) &= g(f(x)) = g(2x + 1) \\
&= \frac{2x + 1}{(2x + 1)^2 + 2} \\
&= \frac{2x + 1}{4x^2 + 4x + 3}; \\
(f \circ g)(x) &= f(g(x)) = f\left(\frac{x}{x^2 + 2}\right) \\
&= \frac{2x}{x^2 + 2} + 1 \\
&= \frac{x^2 + 2x + 2}{x^2 + 2}.
\end{aligned}$$

Obviously,

$$f \circ g \neq g \circ f.$$

The **identity function** of a set X is the function

$$\mathrm{id}_X : X \to X, \quad \mathrm{id}_X(x) = x \quad \text{for all} \quad x \in X.$$

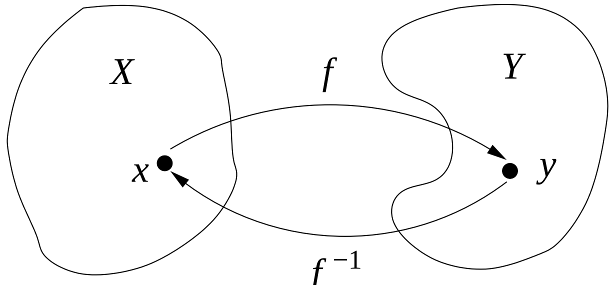
Definition 6.4. A function $f : X \to Y$ is said to be **invertible** if there exists a function $g : Y \to X$ such that

$$\begin{aligned}
g(f(x)) &= x \quad \text{for} \quad x \in X, \\
f(g(y)) &= y \quad \text{for} \quad y \in Y.
\end{aligned}$$

In other words,

$$g \circ f = \mathrm{id}_X, \quad f \circ g = \mathrm{id}_Y.$$

The function g is called the **inverse** of f, written as $g = f^{-1}$.



Remark. Given a function $f : X \to Y$. For each element $y \in Y$ and each subset $B \subseteq Y$, we define their inverse images

$$\begin{aligned} f^{-1}(y) &= \{x \in X : f(x) = y\} \\ f^{-1}(B) &= \{x \in X : f(x) \in B\}. \end{aligned}$$

Here $f^{-1}(y)$ and $f^{-1}(B)$ are just notations for the above sets; it does not mean that f is invertible. So $f^{-1}(y)$ and $f^{-1}(B)$ are meaningful for every function f. However, f^{-1} alone is meaningful only if f is invertible.

If $f : X \to Y$ is invertible, then the inverse of f is **unique**. In fact, let g and h be inverse functions of f, i.e.,

$$\begin{aligned} g(f(x)) &= h(f(x)) = x \quad \text{for} \quad x \in X; \\ f(g(y)) &= f(h(y)) = y \quad \text{for} \quad y \in Y. \end{aligned}$$

For each fixed $y \in Y$, write $x_1 = g(y)$, $x_2 = h(y)$. Apply f to x_1, x_2, we have

$$f(x_1) = f(g(y)) = y = f(h(y)) = f(x_2).$$

Apply g to $f(x_1), f(x_2)$, we obtain

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2.$$

This means that $g(y) = h(y)$ for all $y \in Y$. Hence, $g = h$.

The inverse function f^{-1} of any invertible function f is invertible, and the inverse of f^{-1} is the function f, i.e., $(f^{-1})^{-1} = f$.

Theorem 6.5. *A function $f : X \to Y$ is invertible if and only if f is one-to-one and onto.*

Proof. Necessity (" $\Rightarrow$ "): Since f is invertible, there is a function $g : Y \to X$ such that

$$g \circ f = \mathrm{id}_X, \quad f \circ g = \mathrm{id}_Y.$$

For any $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2.$$

This means that f is one-to-one. On the other hand, for each $y \in Y$ we have $g(y) \in X$ and $f(g(y)) = y$. This means that f is onto.

Sufficiency (" $\Leftarrow$ "): Since f is one-to-one and onto, then for each $y \in Y$ there is one and only one element $x \in X$ such that $f(x) = y$. We define a function

$$g : Y \to X, \quad g(y) = x,$$

where x is the unique element in X such that $f(x) = y$. Then

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g(y) = x, \quad x \in X, \\ (f \circ g)(y) &= f(g(y)) = f(x) = y, \quad y \in Y. \end{aligned}$$

By definition, f is invertible, and $g = f^{-1}$. $\square$

Example 6.7. Let $2\mathbb{Z}$ denote the set of even integers. The function

$$f : \mathbb{Z} \to 2\mathbb{Z}, \quad f(n) = 2n,$$

is invertible. Its inverse is the function

$$f^{-1} : 2\mathbb{Z} \to \mathbb{Z}, \quad f^{-1}(n) = \tfrac{n}{2}.$$

Check: For each $n \in \mathbb{Z}$,

$$(f^{-1} \circ f)(n) = f^{-1}(f(n)) = f^{-1}(2n) = \tfrac{2n}{2} = n.$$

For each $m = 2k \in 2\mathbb{Z}$,

$$(f \circ f^{-1})(m) = f\left(\tfrac{m}{2}\right) = 2 \cdot \tfrac{m}{2} = m.$$

However, the function

$$f_1 : \mathbb{Z} \to \mathbb{Z}, \quad f_1(n) = 2n$$

is not invertible; and the function

$$f_2 : \mathbb{Z} \to 2\mathbb{Z}, \quad f_2(n) = n(n-1)$$

is also not invertible.

Example 6.8. The function

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^3$$

is invertible. Its inverse is the function

$$f^{-1} : \mathbb{R} \to \mathbb{R}, \quad f^{-1}(x) = \sqrt[3]{x}.$$

Check: For each $x \in \mathbb{R}$,

$$\begin{array}{rclclclcl} (f^{-1} \circ f)(x) &=& f^{-1}(f(x)) &=& f^{-1}(x^3) &=& \sqrt[3]{x^3} &=& x, \\ (f \circ f^{-1})(x) &=& f(f^{-1}(x)) &=& f(\sqrt[3]{x}) &=& (\sqrt[3]{x})^3 &=& x. \end{array}$$

Example 6.9. The function

$$f : \mathbb{R} \to \mathbb{R}_+, \quad g(x) = e^x$$

is invertible. Its inverse is the function

$$g : \mathbb{R}_+ \to \mathbb{R}, \quad g^{-1}(x) = \log x.$$

Check:

$$\begin{array}{rclclcll} g \circ f(x) &=& g(e^x) &=& \log(e^x) &=& x, & x \in \mathbb{R}; \\ f \circ g(y) &=& f(\log y) &=& e^{\log y} &=& y, & y \in \mathbb{R}_+. \end{array}$$

Example 6.10.

The function

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2,$$

is *not* invertible. However, the function

$$f_1 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad f_1(x) = x^2,$$

is invertible; its inverse is the function

$$f_1^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad f_1^{-1}(x) = \sqrt{x}.$$

Likewise the function

$$f_2 : \mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0}, \quad f_2(x) = x^2,$$

is invertible; its inverse is the function

$$f_2^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\leq 0}, \quad f_2^{-1}(x) = -\sqrt{x}.$$

The function $f : \mathbb{R} \to [-1,1]$, $f(x) = \sin x$, is not invertible. However, the function

$$f_1 : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1,1], \quad f_1(x) = \sin x,$$

is invertible (which is the restriction of f to $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$) and has the inverse

$$f_1^{-1} : [-1,1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right], \quad f_1^{-1}(x) = \arcsin x.$$

Exercise 6. Let $f : X \to Y$ be a function.

1. For subsets $A_1, A_2 \subseteq X$, show that

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2),$$
$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2);$$

2. For subsets $B_1, B_2 \subseteq Y$, show that

$$f^{-1}(B_1 \cap B_2) = f^{-1}\big(B_1) \cap f^{-1}(B_2\big),$$
$$f^{-1}(B_1 \cup B_2) = f^{-1}\big(B_1) \cup f^{-1}(B_2\big).$$

Example 6.11. Let $f : X \to X$ be a function. If X is a finite set, then the following statements are equivalent.

(1) f is bijective.

(2) f is one-to-one.

(3) f is onto.

Exercise 7. Let $f : X \to X$ be a function. Let

$$\begin{aligned} f^0 &= \mathrm{id}_X, \\ f^n &= \underbrace{f \circ \cdots \circ f}_{n} = f^{n-1} \circ f, \quad n \in \mathbb{Z}_+. \end{aligned}$$

It is easy to see that for nonnegative integers $m, n \in \mathbb{N}$,

$$f^m \circ f^n = f^{m+n}.$$

Exercise 8. Let $f : X \to X$ be an invertible function. Let $f^{-n} = (f^{-1})^n$ for $n \in \mathbb{Z}_+$. Then

$$f^m \circ f^n = f^{m+n} \quad \text{for all} \quad m, n \in \mathbb{Z}.$$

Proof. Note that f^0 is the identity function id_X. We see that for each function $g : X \to X$,

$$f^0 \circ g = g \circ f^0 = g.$$

For each positive integer k,

$$\begin{aligned}
f^k \circ f^{-k} &= \underbrace{f \circ \cdots \circ f}_{k} \circ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k} \\
&= \underbrace{f \circ \cdots \circ f}_{k-1} \circ (f \circ f^{-1}) \circ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k-1} \\
&= \underbrace{f \circ \cdots \circ f}_{k-1} \circ f^0 \circ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k-1} \\
&= \underbrace{f \circ \cdots \circ f}_{k-1} \circ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k-1} \\
&= \cdots = f \circ f^{-1} = f^0.
\end{aligned}$$

Likewise, $f^{-k} \circ f^k = \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k} \circ \underbrace{f \circ \cdots \circ f}_{k} = f^0$. Thus for all $k \in \mathbb{Z}$,

$$f^k \circ f^{-k} = f^0 = \mathrm{id}_X, \quad \text{i.e.,} \quad (f^k)^{-1} = (f^{-1})^k.$$

Now we divide the situation into four cases: (i) $m \geq 0, n \geq 0$; (ii) $m \leq 0, n \leq 0$; (iii) $m > 0, n < 0$; and (iv) $m < 0, n > 0$. The cases (i) and (ii) are trivial.

Case (iii). We have two subcases: (a) $m \geq -n$, and (b) $m \leq -n$. For the subcase (a), we write $k = -n$ and $m = k + a$, where a is a nonnegative integer. Then $a = m + n$, and

$$f^m \circ f^n = f^a \circ f^k \circ f^{-k} = f^a \circ f^0 = f^a = f^{m+n}.$$

For the subcase (b), we write $n = -m - a$, where a is a nonnegative integer. Then $-a = m + n$, and

$$f^m \circ f^n = f^m \circ f^{-m} \circ f^{-a} = f^0 \circ f^{-a} = f^{-a} = f^{m+n}.$$

Case (iv). There are also two subcases: (a) $-m \geq n$, and (b) $-m \leq n$. For the subcase (a), let $m = -n - a$. Then

$$f^m \circ f^n = f^{-a} \circ f^{-n} \circ f^n = f^{-a} \circ f^0 = f^{-a} = f^{m+n}$$

For the subcase (b), let $k = -m$ and write $n = k + a$. Then

$$f^m \circ f^n = f^{-k} \circ f^k \circ f^a = f^0 \circ f^a = f^a = f^{m+n}.$$

□

Example 6.12. Let $f : X \to X$ be an invertible function. For each $x \in X$, the **orbit** of x under f is the set

$$\mathrm{Orb}(f, x) = \{f^n(x) : n \in \mathbb{Z}\}.$$

Show that if $\mathrm{Orb}(f, x_1) \cap \mathrm{Orb}(f, x_2) \neq \varnothing$ then $\mathrm{Orb}(f, x_1) = \mathrm{Orb}(f, x_2)$.

Proof. Let $x_0 \in \mathrm{Orb}(f, x_1) \cap \mathrm{Orb}(f, x_2)$. There exist integers m and n such that $x_0 = f^m(x_1)$ and $x_0 = f^n(x_2)$, that is, $f^m(x_1) = f^n(x_2)$. Applying the function f^{-m} to both sides, we have

$$\begin{aligned} x_1 &= f^0(x_1) = (f^{-m} \circ f^m)(x_1) = f^{-m}(f^m(x_1)) \\ &= f^{-m}(f^n(x_2)) = (f^{-m} \circ f^n)(x_2) = f^{n-m}(x_2). \end{aligned}$$

Thus for each $f^k(x_1) \in \mathrm{Orb}(f, x_1)$ with $k \in \mathbb{Z}$, we have

$$f^k(x_1) = f^k(f^{n-m}(x_2)) = f^{k+n-m}(x_2) \in \mathrm{Orb}(f, x_2).$$

This means that $\mathrm{Orb}(f, x_1) \subset \mathrm{Orb}(f, x_2)$. Likewise, $\mathrm{Orb}(f, x_2) \subset \mathrm{Orb}(f, x_1)$. Hence $\mathrm{Orb}(f, x_1) = \mathrm{Orb}(f, x_2)$. □

Example 6.13. Let X be a finite set. A bijection $f : X \to X$ is called a **permutation** of X. A permutation f of $X = \{1, 2, \ldots, 8\}$ can be stated as follows:

$$\begin{pmatrix} 1 & 2 & \cdots & 8 \\ f(1) & f(2) & \cdots & f(8) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 5 & 4 & 3 & 8 & 2 & 1 \end{pmatrix}.$$

Then

$$\mathrm{Orb}(f, 1) = \mathrm{Orb}(f, 6) = \mathrm{Orb}(f, 8) = \{1, 6, 8\};$$

$$\mathrm{Orb}(f,2) = \mathrm{Orb}(f,7) = \{2,7\};$$
$$\mathrm{Orb}(f,3) = \mathrm{Orb}(f,5) = \{3,5\};$$
$$\mathrm{Orb}(f,4) = \{4\}.$$

Exercise 9. Let $f : \mathbb{R} \smallsetminus \mathbb{Q} \to \mathbb{R} \smallsetminus \mathbb{Q}$ be defined by

$$f(x) = \tfrac{1}{x-1}, \quad x \in \mathbb{R} \smallsetminus \mathbb{Q}.$$

(a) Show that f is invertible.

(b) List all elements of the set $\{f^k : k \in \mathbb{Z}\}$.

7 Infinite Sets

Let A be a finite set of m elements. When we count the elements of A, we have the 1st element a_1, the 2nd element a_2, the 3rd element a_3, and so on. The result is to have listed the elements of A as follows

$$a_1, a_2, \ldots, a_m.$$

Then a bijection $f : \{1, 2, \ldots, m\} \to A$ is automatically given by

$$f(i) = a_i, \quad i = 1, 2, \ldots, m.$$

To compare the number of elements of A with another finite B of n elements. We do the same thing by listing the elements of B as follows

$$b_1, b_2, \ldots, b_n.$$

If $m = n$, we automatically have a bijection $g : A \to B$, given by

$$g(a_i) = b_i, \quad i = 1, 2, \ldots, m.$$

If $m \neq n$, there is no bijection from A to B.

Theorem 7.1. *Two finite sets A and B have the same number of elements if and only if there is a bijection $f : A \to B$, i.e., they are in one-to-one correspondent.*

Definition 7.2. A set A is said to be **equivalent** to a set B, written as $A \sim B$, if there is a bijection $f : A \to B$.

If $A \sim B$, i.e., there is a bijection $f : A \to B$, then f has the inverse function $f^{-1} : B \to A$. Of course, f^{-1} is a bijection. Thus B is equivalent to A, i.e., $B \sim A$.

If $A \sim B$ and $B \sim C$, there are bijections $f : A \to B$ and $g : B \to C$. Obviously, the composition $g \circ f : A \to C$ is a bijection. Thus $A \sim C$.

For infinite sets, to compare the "number" of elements of one set with another, the right method is to use one-to-one correspondence. We say that two sets A and B have the same **cardinality** if $A \sim B$, written as

$$|A| = |B|.$$

The symbol $|A|$ is called the **cardinality** of A, meaning the size of A. If A is finite, we have

$$|A| = \text{number of elements of } A.$$

Example 7.1. The set $\mathbb{Z}$ of integers is equivalent to the set $\mathbb{N}$ of nonnegative integers, i.e., $\mathbb{Z} \sim \mathbb{N}$.

The function $f : \mathbb{Z} \to \mathbb{N}$, defined by

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

is a bijection. Its inverse function $f^{-1} : \mathbb{N} \to \mathbb{Z}$ is given by

$$f^{-1}(n) = \begin{cases} n/2 & \text{if} \quad n = \text{even} \\ -(n+1)/2 & \text{if} \quad n = \text{odd}. \end{cases}$$

We can say that $\mathbb{Z}$ and $\mathbb{N}$ have the same cardinality, i.e.,

$$|\mathbb{Z}| = |\mathbb{N}|.$$

Example 7.2. For any real numbers $a < b$, the closed interval $[a, b]$ is the set

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}.$$

Then $[a, b]$ is equivalent to $[0, 1]$, i.e., $[a, b] \sim [0, 1]$.

The function $f : [a, b] \to [0, 1]$, defined by

$$f(x) = \frac{x - a}{b - a},$$

is a bijection. Its inverse $f^{-1} : [0, 1] \to [a, b]$ is given by

$$f^{-1}(x) = (b - a)x + a, \quad x \in [0, 1].$$

Definition 7.3. A set A is called **countable** if,

- A is either finite, or
- there is bijection from A to the set $\mathbb{P}$ of positive integers.

In other words, the elements of A can be listed as either a finite sequence

$$a_1, a_2, \ldots, a_n;$$

or an infinite sequence

$$a_1, a_2, a_3, \ldots .$$

Sets that are not countable are said to be **uncountable**.

Proposition 7.4. *Every infinite set contains an infinite countable subset.*

Proof. Let A be an infinite set. Select an element a_1 from A. Since A is infinite, the set $A_1 = A \smallsetminus \{a_1\}$ is still infinite. One can select an element a_2 from A_1. Similarly, the set

$$A_2 = A_1 \smallsetminus \{a_2\} = A \smallsetminus \{a_1, a_2\}$$

is infinite, one can select an element a_3 from A_2, and the set

$$A_3 = A_2 \smallsetminus \{a_3\} = A \smallsetminus \{a_1, a_2, a_3\}$$

is infinite. Continue this procedure, we obtain an infinite sequence

$$a_1, a_2, a_3, \ldots$$

of distinct elements from A. The set $\{a_1, a_2, a_3, \ldots\}$ is an infinite countable subset of A. $\square$

Theorem 7.5. *If A and B are countable subsets, then $A \cup B$ is countable.*

Proof. It is obviously true if one of A and B is finite. Let

$$A = \{a_1, a_2, \ldots\}, \quad B = \{b_1, b_2, \ldots\}$$

be countably infinite. If $A \cap B = \varnothing$, then

$$A \cup B = \{a_1, b_1, a_2, b_2, \ldots\}$$

is countable as demonstrated. If $A \cap B \neq \varnothing$, we just need to delete the elements that appeared more than once in the sequence $a_1, b_1, a_2, b_2, \ldots$. Then the leftover is the set $A \cup B$. ☐

Theorem 7.6. *Let A_i, $i = 1, 2, \cdots$, be countable sets. If $A_i \cap A_j = \varnothing$ for any $i \neq j$, then $\bigcup_{i=1}^{\infty} A_i$ is countable.*

Proof. We assume that each A_i is countably infinite. Write

$$A_i = \{a_{i1}, a_{i2}, a_{i3}, \cdots\}, \quad i = 1, 2, \ldots$$

The countability of $\bigcup_{i=1}^{\infty} A_i$ can be demonstrated as

$$\begin{array}{cccccccc}
a_{11} & \rightarrow & a_{12} & & a_{13} & \rightarrow & a_{14} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \\
a_{21} & & a_{22} & & a_{23} & & a_{24} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \\
a_{31} & & a_{32} & & a_{23} & & a_{34} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \\
a_{41} & & a_{42} & & a_{23} & & a_{44} & \cdots \\
\vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

$$\begin{array}{cccccccc}
a_{11} & \rightarrow & a_{12} & & a_{13} & \rightarrow & a_{14} & \cdots \\
 & & \downarrow & & \uparrow & & \downarrow & \\
a_{21} & \leftarrow & a_{22} & & a_{23} & & a_{24} & \cdots \\
\downarrow & & & & \uparrow & & \downarrow & \\
a_{31} & \rightarrow & a_{32} & \rightarrow & a_{23} & & a_{34} & \cdots \\
 & & & & & & \downarrow & \\
a_{41} & \leftarrow & a_{42} & \leftarrow & a_{23} & \leftarrow & a_{44} & \cdots \\
\downarrow & & & & & & & \\
\vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

□

The condition of disjointness in Theorem 7.6 can be omitted.

Theorem 7.7. *The closed interval* $[0, 1]$ *of real numbers is uncountable.*

Proof. Suppose the set $[0, 1]$ is countable. Then the numbers in $[0, 1]$ can be listed as an infinite sequence $\{\alpha_i\}_{i=1}^{\infty}$. Write all real numbers α_i in infinite decimal forms, say in base 10, as follows:

$$\begin{aligned}
\alpha_1 &= 0.a_1a_2a_3a_4\cdots \\
\alpha_2 &= 0.b_1b_2b_3b_4\cdots \\
\alpha_3 &= 0.c_1c_2c_3c_4\cdots \\
&\cdots
\end{aligned}$$

We construct a number $x = 0.x_1x_2x_3x_4\cdots$, where x_i are given as follows:

$$\begin{aligned}
x_1 &= \begin{cases} 1 & \text{if } a_1 = 2 \\ 2 & \text{if } a_1 \neq 2, \end{cases} \\
x_2 &= \begin{cases} 1 & \text{if } b_2 = 2 \\ 2 & \text{if } b_2 \neq 2, \end{cases} \\
x_3 &= \begin{cases} 1 & \text{if } c_3 = 2 \\ 2 & \text{if } c_3 \neq 2, \end{cases} \\
&\cdots
\end{aligned}$$

Obviously, x is an infinite decimal number between 0 and 1, i.e., $x \in [0, 1]$. Note that

$$x_1 \neq a_1, \quad x_2 \neq a_2, \quad x_3 \neq a_3, \quad \ldots.$$

This means that

$$x \neq \alpha_1, \quad x \neq \alpha_2, \quad x \neq \alpha_3, \quad \ldots.$$

Thus x is not in the list $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$. Since all real numbers of $[0, 1]$ are already in the list, in particular, x must be in the list. This is a contradiction.

□

Example 7.3. For any set Σ, either finite or infinite, recall that $\Sigma^{(n)}$ is the set of words of length n over Σ, and Σ^n is the product of n copies of Σ. Then the function $f : \Sigma^{(n)} \to \Sigma^n$, defined by

$$f(a_1 a_2 \cdots a_n) = (a_1, a_2, \ldots, a_n), \quad a_1, a_2, \ldots, a_n \in \Sigma,$$

is a bijection. Thus $\Sigma^{(n)} \sim \Sigma^n$.

Theorem 7.8 (Cantor-Bernstein-Schroeder Theorem)**.** *Given sets A and B. If there are injections $f : A \to B$ and $g : B \to A$, then there exists a bijection $h : A \to B$.*

Proof. First Proof (non-constructive). Note that $f : A \to f(A)$ and $g : B \to g(B)$ are bijections. Our aim is to find a subset $S \subseteq A$ such that $g(\overline{f(S)}) = \overline{S}$. If so, the bijections $f : S \to f(S)$ and $g : \overline{f(S)} \to \overline{S}$ give rise to a bijection between A and B.

For each subset $E \subseteq A$, clearly, $f(E) \subseteq B$ and $g(\overline{f(E)}) \subseteq A$; we have

$$\hat{E} := \overline{g(\overline{f(E)})} \subseteq A.$$

If there exists a subset $S \subseteq A$ such that $\hat{S} = S$, i.e., $S = \overline{g(\overline{f(S)})}$, then $\overline{S} = g(\overline{f(S)})$. We claim that such subset S with $\hat{S} = S$ does exist.

We say that a subset $E \subseteq A$ **expandable** if $E \subseteq \hat{E}$. Expandable subsets of A do exist, since the empty set $\varnothing$ is expandable. Let S be the union of all expandable subsets of A. We claim that $\hat{S} = S$.

We first show that $E_1 \subseteq E_2$ implies $\hat{E}_1 \subseteq \hat{E}_2$ for subsets E_1, E_2 of A. In fact, if $E_1 \subseteq E_2$, then $f(E_1) \subseteq f(E_2)$; consequently, $\overline{f(E_1)} \supseteq \overline{f(E_2)}$ by taking complement; hence $g(\overline{f(E_1)}) \supseteq g(\overline{f(E_2)})$ by applying the injective map g; now we see that $\overline{g(\overline{f(E_1)})} \subseteq \overline{g(\overline{f(E_2)})}$ by taking complement again, i.e., $\hat{E}_1 \subseteq \hat{E}_2$.

Let D be an expandable subset of A, i.e., $D \subseteq \hat{D}$. Clearly, $D \subseteq S$ by definition of S; then $\hat{D} \subseteq \hat{S}$ by the previous argument; thus $D \subseteq \hat{S}$ as $D \subseteq \hat{D}$. Since D is an arbitrary expandable subset, we see that $S \subseteq \hat{S}$. Again, the previous argument implies that $\hat{S} \subseteq \hat{\hat{S}}$; this means that $\hat{S}$ is an expandable subset; hence $\hat{S} \subseteq S$ by definition of S. Therefore $\hat{S} = S$.

Second Proof (constructive). Since $A \sim f(A)$, it suffices to show that $B \sim f(A)$. To this end, we define sets

$$A_1 = g(f(A)), \quad B_1 = f(g(B)).$$

Then $gf : A \to A_1$ and $fg : B \to B_1$ are bijections, and

$$A_1 \subseteq g(f(A)) \subseteq g(B), \quad B_1 = f(g(B)) \subseteq f(A).$$

Set $A_0 := A$, $B_0 := B$, and introduce subsets

$$A_i := g(B_{i-1}), \quad B_i := f(A_{i-1}), \quad i \geq 2.$$

We claim the following chains of inclusion

$$A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots, \quad B = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots.$$

In fact,

$$A_2 = g(B_1) = g(f(g(B))) \subseteq gf(A) = A_1,$$
$$B_2 = f(A_1) = f(g(f(A))) \subseteq fg(B) = B_1.$$

By induction, for $i \geq 2$, we have

$$A_{i+1} = g(B_i) \subseteq g(B_{i-1}) = A_i \quad (\because B_i \subseteq B_{i-1});$$

$$B_{i+1} = f(A_i) \subseteq f(A_{i-1}) = B_i \quad (\because A_i \subseteq A_{i-1}).$$

Now we set $D := \bigcap_{i=1}^{\infty} B_i$. Recall $B_1 \subseteq f(A) \subseteq B$. We have disjoint unions

$$\begin{aligned} B &= (B - f(A)) \cup (f(A) - B_1) \cup (B_1 - D) \cup D \\ &= D \cup (f(A) - B_1) \cup (B - f(A)) \cup \bigcup_{i=1}^{\infty} (B_i - B_{i+1}); \\ f(A) &= D \cup (f(A) - B_1) \cup \bigcup_{i=1}^{\infty} (B_i - B_{i+1}). \end{aligned}$$

Note that $fg : B \to B_1$ is a bijection. By definition of A_i and B_i, we have

$$fg(B - f(A)) = fg(B) - fgf(A) = B_1 - B_2,$$

$$\begin{aligned} fg(B_i - B_{i+1}) &= fg(B_i) - fg(B_{i+1}) \\ &= f(A_{i+1}) - f(A_{i+2}) \\ &= B_{i+2} - B_{i+3}, \quad i \geq 1. \end{aligned}$$

We see that fg sends $(B-f(A))\cup\bigcup_{i=0}^{\infty}(B_{2i+1}-B_{2i+2})$ to $\bigcup_{i=0}^{\infty}(B_{2i+1}-B_{2i+2})$ bijectively. Note that both B and $f(A)$ contain the subset

$$D\cup(f(A)-B_1)\cup\bigcup_{i=1}^{\infty}(B_{2i}-B_{2i+1}),$$

whose complement in the sets B, $f(A)$ are respectively the subsets

$$(B-f(A))\cup\bigcup_{i=0}^{\infty}(B_{2i+1}-B_{2i+2}),\quad \bigcup_{i=0}^{\infty}(B_{2i+1}-B_{2i+2}).$$

It follows that the function $\phi : B \to f(A)$, defined by

$$\phi(x)=\begin{cases} x & \text{if } x\in D\cup(f(A)-B_1)\cup\bigcup_{i=1}^{\infty}(B_{2i}-B_{2i+1}) \\ fg(x) & \text{if } x\in (B-f(A))\cup\bigcup_{i=0}^{\infty}(B_{2i+1}-B_{2i+2}) \end{cases},$$

is a bijection. □