1 Countable sets

The purpose of this chapter is to talk about countable sets. We will start with basic notions and operations on functions as a warm up, then we will define the notion of finite sets, coutable sets and uncountable sets along with several examples. In the end of the chapter, we will also describe operatioins to construct countably infinite sets.

1.1 Functions

Let us start with elementary notions, such as injective, surjective, and bijective functions.

Definition 1.1.1 : Given two sets S and T, and a function $f : S \to T$. We say that f is

- injective (**單射**), or an injection, if for any $x, y \in S$, $x \neq y$ implies $f(x) \neq f(y)$;
- surjective (**滿射**), or a surjection, if for any $z \in T$, there exists $x \in S$ such that $f(x) = z$;
- bijective (**雙射**), or a bijection, if it is injective and surjective.

Remark 1.1.2 : In the language of set theory, a function $f : S \to T$ may also be seen as an element $f \in T^S$.

Example 1.1.3 : Below are a few examples.

(1) The map $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ is a bijection.

(2) The map $x \mapsto x^2$ defines an injection from $\mathbb{R}_+$ to $\mathbb{R}$, a surjection from $\mathbb{R}$ to $\mathbb{R}_+$, and also a bijection between $\mathbb{R}_+$ and $\mathbb{R}_+$.

(3) Let $\sigma \in S_N$ be an element in the symmetric group. Then σ is a bijection.

(4) Let $M \in \mathcal{M}_{n\times n}(\mathbb{R})$ with $\det M \neq 0$. Then, the map $X \mapsto MX$ is a bijection on $\mathbb{R}^n$.

We recall the following classical results on composition of injective (resp. surjective and bijective) maps. You should be able to reproduce the proofs by yourself.

Proposition 1.1.4 : *Let $f : S \to T$ and $g : T \to U$.*

- *If f and g are both injective, then $g \circ f$ is also injective.*
- *If f and g are both surjective, then $g \circ f$ is also surjective.*
- *If f and g are both bijective, then $g \circ f$ is also bijective.*

Proposition 1.1.5 : *Let A, B, C, D be sets, and $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions.*

(1) If $g \circ f$ is injective, then f is injective.

(2) If $g \circ f$ is surjective, then g is surjective.

(3) If $g \circ f$ and $h \circ g$ are bijective, then f, g and h are all bijective.

Definition 1.1.6 : Given a bijection $f : S \to T$, we may define $f^{-1} : T \to S$ as follows. For any $y \in T$, we may find a unique $x \in S$ such that $y = f(x)$, called preimage or inverse image (像原), of y, and we define $f^{-1}(y) = x$. Such a function f^{-1} is unique, and is called the inverse function (反函數) of f.

Definition 1.1.7 : Given a function $f : S \to T$ which is not necessarily a bijection. For $A \subseteq S$ and $B \subseteq T$, let us define

$$f(A) = \{f(x) : x \in A\} \quad \text{and} \quad f^{-1}(B) = \{x \in S : f(x) \in B\}.$$

This generalizes the notion of image and preimage to subsets.

Remark 1.1.8 : We note that if $f : S \to T$ is a bijection, then $f(x) = y$ can be rewritten as

$$f^{-1}(y) = x \quad \text{and} \quad f^{-1}(\{y\}) = \{x\}.$$

Proposition 1.1.9 : *If $f : S \to T$ is a bijection, then*

$$f^{-1} \circ f = \mathrm{Id}_S \quad \textit{and} \quad f \circ f^{-1} = \mathrm{Id}_T.$$

Given a function $f : S \to T$, how to check that it is a bijection? The following proposition gives us a possible way to do this.

Proposition 1.1.10 : *Let $f : S \to T$ and $g : T \to S$ satisfying $f \circ g = \mathrm{Id}_T$ and $g \circ f = \mathrm{Id}_S$. Then, f and g are bijective and are inverse one of the other.*

Proof : By symmetry, it is enough to show that f is bijective and g is the inverse of f.

Given $y \in T$, we want to look for $x \in S$ such that $f(x) = y$. Assume that such x exists, leading to $x = g \circ f(x) = g(y)$. Let $x = g(y)$. We can easily check that $f(g(y)) = f \circ g(y) = y$. This allows us to say that $x = g(y)$ is the unique preimage of y by f.

Thus, f is a bijection and g is its inverse. □

1.2 Equinumerous sets

Definition 1.2.1 : Two sets S and T are said to be equinumerous (等勢), denoted by $S \sim T$, if there exists a bijective function (or bijection) f from S to T.

Remark 1.2.2 : It is not hard to check the following properties.

(1) For any set S, we have $S \sim S$.

(2) For any sets S and T, we have $S \sim T$ if and only if $T \sim S$.

(3) For any sets S, T, and U, if we have $S \sim T$ and $T \sim U$, then $S \sim U$.

Proposition 1.2.3 : *For any set S, write $\mathcal{P}(S)$ for its power set (冪集合), that is*

$$\mathcal{P}(S) := \{T \subseteq S\}.$$

Then, S is not equinumerous to $\mathcal{P}(S)$.

Proof : We prove by contradiction. Let us assume that S and $\mathcal{P}(S)$ are equinumerous, and we want to reach at a contradiction.

Let $f : S \to \mathcal{P}(S)$ be a bijection. Consider the following subset of S,

$$T := \{x \in S : x \notin f(x)\} \in \mathcal{P}(S).$$

Then, T has a preimage via f, that we may denote by x, i.e. $f(x) = T$. We have two possible cases to discuss:

- If $x \in T = f(x)$, then by the definition of T, we find $x \notin f(x) = T$.
- If $x \notin T = f(x)$, then again by the definition of T, we find $x \in f(x) = T$.

We have found a contradiction. □

Question 1.2.4: What is the difference between a proof by contradiction (反證法) and a proof by contraposition (對位證明法)?

In general, how to know whether two given sets are equinumerous? By definition, we need to explicit a bijection between them, but it is not always obvious. The following theorem gives a criterion and also an algorithm on how to build such a bijection. We will not discuss its proof here, which is a little bit technical. You may follow the steps in Exercise 1.7 for details.

Theorem 1.2.5 (Cantor–Schröder–Bernstein Theorem) **:** *Given two sets S and T. Suppose that there exists an injection from S to T and an injection from T to S. Then, there exists a bijection between S and T.*

1.3 Finite sets

Definition 1.3.1 : Given a set S. If there exists a non-negative integer n such that

$$S \sim \{1, \dots, n\} =: [n],$$

then we say that S is finite and contains n elements, denoted $n = |S| = \mathrm{Card}(S)$. We also say that the cardinal number, or cardinality (基数) of S is n.

Proposition 1.3.2 : *For a finite set S, its cardinality is uniquely defined.*

Proof : Let us proceed by contradiction. Suppose that there exists a finite set S with two different cardinals n and m, that is, there exist bijections $f : S \to [n]$ and $g : S \to [m]$. Then, the function $h := f \circ g^{-1} : [m] \to [n]$ is also a bijection by composition. However, by the pigeonhole principle (鴿籠原理), it is not possible. More precisely, if $m > n$, the pigeonhole principle implies that there exists $x, y \in [m]$ with $x \neq y$ such that $h(m) = h(n)$. If $m < n$, we conclude in the same way by looking at $h^{-1} : [n] \to [m]$. □

Example 1.3.3 : We give a few examples below.

(1) Fix a positive integer $n \geqslant 1$, the symmetric group S_n has cardinality $n!$. One may establish a bijection between S_n and $[n] \times S_{n-1}$ and proceed by induction.

(2) Given two finite sets E and F, then the set of functions from E to F has cardinality $|F|^{|E|}$.

(3) Let p be a prime number. The general linear group on the finite field $\mathbb{F}_p$ of order n, denoted by

$$GL(n, p) = GL_n(\mathbb{F}_p) = \{M \in \mathcal{M}_{n\times n}(\mathbb{F}_p) : \det(M) \neq 0\}$$

has cardinality

$$\mathrm{Card}\, GL(n, p) = \prod_{k=0}^{n-1} (p^n - p^k).$$

1.4 Countable sets

Below, we follow the Anglo-Saxon notations to denote the set of natural numbers. We write $\mathbb{N} := \{1, 2, \dots\}$ for the set of positive integers, and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ for the set of non-negative integers. Note that in the French or German notations, $\mathbb{N}$ stands for the set of non-negative integers, whereas $\mathbb{N}^*$ stands for the set of positive integers.

Definition 1.4.1 : Given a set S. We say that S is coutably infinite (無窮可數) if $S \sim \mathbb{N}$.

Remark 1.4.2 : Let S be a countably infinite set. By Definition 1.2.1, there is a bijection from $\mathbb{N}$ to S, that we may denote by f. In this case, we can enumerate the elements of S as follows,

$$S = \{f(1), f(2), \dots\} = \{a_1, a_2, \dots\},$$

where we write $a_k = f(k)$ for all $k \geqslant 1$.

Definition 1.4.3 : If S is a countably infinite set, then we write $\aleph_0$ for its cardinality. In other words, $\aleph_0 := |\mathbb{N}| = \mathrm{Card}(\mathbb{N})$.

Example 1.4.4 : The set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ of integers is countably infinite. To see this, we may define the functions $f : \mathbb{N} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{N}$ as below,

$$f(n) = \begin{cases} -\frac{n}{2} & \text{if } n \text{ is even,} \\ \frac{n-1}{2} & \text{if } n \text{ is odd,} \end{cases} \qquad \text{and} \qquad g(n) = \begin{cases} 2n+1 & \text{if } n \geqslant 0, \\ -2n & \text{if } n < 0. \end{cases}$$

It is easy to check that $f \circ g = \mathrm{id}_{\mathbb{Z}}$ and $g \circ f = \mathrm{id}_{\mathbb{N}}$, so from Proposition 1.1.10, we know that $f = g^{-1}$ and that both f and g are bijective.

The above construction is equivalent to enumerating the elements of $\mathbb{Z}$ as follows,

$$0, -1, 1, -2, 2, -3, 3, \dots$$

Example 1.4.5 : The set $\mathbb{N}^2$ is countably infinite. We may enumerate its elements as shown in the following figure.

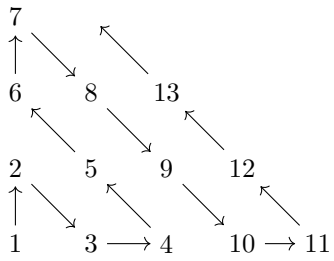

Figure 1.1: A possible enumeration of the elements in $\mathbb{N}^2$.

Question 1.4.6: Construct an explicit bijection between $\mathbb{N}$ and $\mathbb{N}^2$ using the enumeration shown in Figure 1.1.

Definition 1.4.7 : Given a set S. We say that S is countable (可数) if S is either a finite set or a coutably infinite set. Otherwise, we say that S is uncountable (不可数).

Proposition 1.4.8 : *Any subset of a countable set is countable.*

Proof : Let S be a countable set and $A \subseteq S$ be a subset. If A is finite, the statement holds clearly, so we may assume that A is infinite, and so is S a fortiori. According to Remark 1.4.2, we may enumerate the elements of S as

$$S = \{s_1, s_2, \dots\}.$$

We may define a strictly increasing function $\varphi : \mathbb{N} \to \mathbb{N}$ by induction,

$$\begin{aligned} \varphi(1) &= \min\{n \geqslant 1 : s_n \in A\}, \\ \varphi(k+1) &= \min\{n > \varphi(k) : s_n \in A\}, \quad k \geqslant 1. \end{aligned}$$

It is easy to see that φ is well defined on $\mathbb{N}$ due to the fact that A is infinite. Therefore, the function

$$\begin{array}{rccc} f: & \mathbb{N} & \to & A \\ & n & \mapsto & s_{\varphi(n)} \end{array}$$

is a bijection between $\mathbb{N}$ and A, so A is countably infinite. □

Corollary 1.4.9 : *Given a set S.*

(1) It is countable if and only if there exists a bijection between S and a subset of $\mathbb{N}$.

(2) It is countable if and only if there exists an injection from S into $\mathbb{N}$.

(3) It is countable if and only if there exists a surjection from $\mathbb{N}$ onto S.

(4) it is countably infinite if and only if one of the previous points holds and S is infinite.

Proof : Given a set S.

(1) Suppose that S is countable. If S is finite, then it is in bijection with $\{1, \dots, n\}$ for some finite $n \geqslant 0$. If S is infinite, then it is countably infinite, and by definition, it is in bijection with $\mathbb{N}$. For the converse, assume that S is in bijection with a subset $I \subseteq \mathbb{N}$. Proposition 1.4.8 implies that I is countable, so is S.

(2) Suppose that S is countable. By (1), we can find a bijection $f : S \to I \subseteq \mathbb{N}$. Let $i : I \hookrightarrow \mathbb{N}$ be the canonical injection (包含映射) $x \mapsto x$. Then, $i \circ f$ is an injection from S to $\mathbb{N}$.

For the converse, assume that $i : S \hookrightarrow \mathbb{N}$ is an injection, then i is a bijection between S and $i(S)$, which is a subset of the countable set $\mathbb{N}$. Therefore, Proposition 1.4.8 implies that S is also countable.

(3) We may proceed in a similar way as (2).

(4) It was already implicitly proven in the previous points.

□

Example 1.4.10 : The set $\mathbb{N}^2$ is countably infinite. We may consider the map $(p, q) \mapsto 2^p 3^q$ which is an injection from $\mathbb{N}^2$ into $\mathbb{N}$ due to the uniqueness of integer factorization.

Remark 1.4.11 : In practice, to show that an infinite set S is countably infinite, we may

(1) construct a bijection between S and $\mathbb{N}$;

(2) construct an injection from S into $\mathbb{N}$, or any other countably infinite set;

(3) construct a surjection from $\mathbb{N}$, or any other countably infinite set, onto S.

1.5 Operations on countable sets

1.5.1 Cartesian product

Proposition 1.5.1 : *If S and T are countably infinite sets, then their Cartesian product* (笛卡爾積) *$S \times T$ is also countably infinite.*

Proof : Given two countably infinite sets S and T. Let $f : S \to \mathbb{N}$ and $g : T \to \mathbb{N}$ be bijective maps. Then, the map $h := (f, g) = S \times T \to \mathbb{N}^2$ defined by $h(x, y) = (f(x), g(y))$ is also a bijection. Since $\mathbb{N}^2$ is countably infinite (Example 1.4.5), Corollary 1.4.9 implies that so is $S \times T$. □

Example 1.5.2 : The above proposition gives us a simpler criterion to show that some infinite sets are countably infinite.

(1) We saw in Example 1.4.4 that $\mathbb{Z}$ in countably infinite, so $\mathbb{Z}^2$ is also countably infinite.

(2) The set $\mathbb{Q}$ of rational numbers is countably infinite. Actually, we first know that $\mathbb{Z} \times \mathbb{N}$ is countably infinite, and we may construct a surjective map from $\mathbb{Z} \times \mathbb{N}$ onto $\mathbb{Q}$ by $(p, q) \mapsto \frac{p}{q}$. And we conclude by Corollary 1.4.9 (3).

Corollary 1.5.3 : *Any non-empty finite product of countably infinite sets is still coutably infinite.*

Proof : We want to prove this by induction on the cardinality of the product. For any positive integer n, we define the property $\mathcal{P}_n$ to be "for any finite set I with $|I| = n$, and countably infinite sets $(S_i)_{i \in I}$, the product $\prod_{i \in I} S_i$ is countably infinite."

If $|I| = 1$, the statement clearly holds. Let $n \geqslant 1$ be an integer and assume that $\mathcal{P}_n$ holds. Given a finite family I with $|I| = n + 1$ and a sequence of countably infinite sets $(S_i)_{i \in I}$ indexed by elements of I. Fix an arbitrary element $i_0 \in I$ and define $I' = I \backslash \{i_0\}$, then I can be rewritten as the disjoint union $I = I' \sqcup \{i_0\}$. Let $S = \prod_{i \in I} S_i = \left(\prod_{i \in I'} S_i\right) \times S_{i_0}$. By the induction hypothesis $\mathcal{P}_n$, we know

that $S' := \prod_{i \in I'} S_i$ is countably infinite. Then, Proposition 1.5.1 implies that $S' \times S_{i_0} = S$ is countably infinite. Therefore, the property $\mathcal{P}_{n+1}$ holds. □

Example 1.5.4 : For any positive integer $n \geqslant 1$, the sets $\mathbb{N}^n$ and $\mathbb{Z}^n$ are countably infinite.

1.5.2 Union

Proposition 1.5.5 : *Any countable union of coutable sets is still countable.*

Proof : Let I be a countable set and $(S_i)_{i \in I}$ be a family of countable sets indexed by I. By Corollary 1.4.9, we may be given a surjection $f_i : \mathbb{N} \to S_i$ for each $i \in I$. Then, the map defined by

$$\begin{array}{rccc} f : & I \times \mathbb{N} & \to & \bigcup_{i \in I} S_i \\ & (i, x) & \mapsto & f_i(x) \end{array}$$

is clearly a surjection. Since $I \times \mathbb{N}$ is countable, using Corollary 1.4.9 again, we deduce that $\bigcup_{i \in I} S_i$ is also countable. □

Example 1.5.6 : Let S and T be two countable subsets of $\mathbb{R}$. Then, the set

$$S + T := \{s + t : s \in S, t \in T\}$$

is also countable. Actually, we can see this by rewriting

$$S + T = \bigcup_{s \in S} (s + T)$$

which is a countable union of countable sets.

1.5.3 Examples of uncountable sets

Proposition 1.5.7 : *The set $\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof : By Proposition 1.2.3, there is no bijection between $\mathcal{P}(\mathbb{N})$ and $\mathbb{N}$. Therefore, Corollary 1.4.9 implies that $\mathcal{P}(\mathbb{N})$ is not countable. □

Proposition 1.5.8 : *The set $\{0, 1\}^{\mathbb{N}}$ is uncountable.*

Proof : We have at least two ways to see this.

- First approach is to notice that, $\{0,1\}^{\mathbb{N}}$ is in bijection with $\mathcal{P}(\mathbb{N})$. Actually, the map

$$\begin{array}{rccc} f: & \{0,1\}^{\mathbb{N}} & \to & \mathcal{P}(\mathbb{N}) \\ & (x_n)_{n\in\mathbb{N}} & \mapsto & \{n\in\mathbb{N} : x_n = 1\} \end{array}$$

  defines a bijection. Therefore, we may conclude by applying directly Proposition 1.5.7.

- Second approach is to apply the so-called *Cantor's diagonal argument.* Suppose that the set $\{0,1\}^{\mathbb{N}}$ is countably infinite, that is it is in bijection with $\mathbb{N}$. Let us enumerate its elements as follows, $\{0,1\}^{\mathbb{N}} = \{s_1, s_2, \dots\}$. For each $n \geqslant 1$, s_n is a sequence consisting of 0's and 1's, given by

$$s_n = (s_{n,1}, s_{n,2}, s_{n,3}, \dots),$$

  where $s_{n,k} \in \{0,1\}$ for all $k \geqslant 1$.

  Let us consider another 0, 1 sequence y as follows,

$$y = (y_1, y_2, \dots),$$

  where $y_k = 1 - s_{k,k}$. Since $y \in \{0,1\}^{\mathbb{N}}$, there exists n such that $y = s_n$. However, if we look at the n-th digit in y and s_n, we note that they are not the same. We find a contradiction.

□

Proposition 1.5.9 : *The set $\mathbb{R}$ of real numbers is uncountable.*

Remark 1.5.10 : There are several different proofs to this proposition. Here, we present a proof using the result from Proposition 1.5.8. In Exercise 1.17, we will see an alternative proof using sequences.

Proof : We only need to show that the interval $(0,1)$ is uncountable. Since otherwise, if the interval $(0,1)$ were countable, then $(0,1]$ would also be countable, and

$$\mathbb{R} = \bigcup_{x\in\mathbb{Z}} (x, x+1] = \bigcup_{x\in\mathbb{Z}} (x + (0,1])$$

would also be countable by Proposition 1.5.5.

For any $x \in (0,1)$, we may write its binary expansion,

$$x = 0.x_1x_2x_3\cdots = \sum_{k\geqslant 1} x_k 2^{-k},$$

where $x_k = 0$ or 1 for all $k \geqslant 1$. Note that this binary expansion may not be unique.

It is not hard to show that the numbers in $(0,1)$ which do not have a unique binary expansion are exactly those in the dyadic set

$$\mathcal{D} := \{\tfrac{m}{2^n} : n \in \mathbb{N}, 1 \leqslant m \leqslant 2^n - 1, m \in \mathbb{N}\}.$$

Additionally, every such point $x \in \mathcal{D}$ can be written in exactly two ways, one with infinitely many 0's

in the end, the other with infinitely many 1's in the end. Let us write

$$\mathcal{S}_0 := \{s = (s_n)_{n\geqslant 1} : \exists N \geqslant 1\ \forall n \geqslant N, s_n = 0\},$$
$$\mathcal{S}_1 := \{s = (s_n)_{n\geqslant 1} : \exists N \geqslant 1\ \forall n \geqslant N, s_n = 1\}.$$

Then, the binary expansion defines a bijection between $(0,1)\backslash\mathcal{D}$ and $\mathcal{S} := \{0,1\}^{\mathbb{N}}\backslash(\mathcal{S}_0 \cup \mathcal{S}_1)$.

The set $\mathcal{S}_0$ is countable, since it can be seen as the following countable union of finite sets,

$$\mathcal{S}_0 = \bigcup_{N\geqslant 1} (\{0,1\}^{N-1} \times \{0\}^{\mathbb{N}}).$$

Similary, we can also deduce that $\mathcal{S}_1$ is countable. Therefore, $\mathcal{S}$ is still uncountable (Proposition 1.5.8), so $(0,1)\backslash\mathcal{D}$ is uncountable. Since $\mathcal{D}$ is countable, we conclude that $(0,1)$ is uncountable. □

Remark 1.5.11 : The cardinality of $\mathbb{N}$ is denoted by $\aleph_0$ (Definition 1.4.3), and Proposition 1.5.7 tells us that $\mathcal{P}(\mathbb{N})$ is not equinumerous to $\mathbb{N}$. A natural question would be: is there any set S in between, in the sense that $\mathbb{N} \hookrightarrow S \hookrightarrow \mathcal{P}(\mathbb{N})$ such that S is not in bijection with $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$? If the answer is negative, it means that $|\mathcal{P}(\mathbb{N})|$ is the *successor cardinal* of $\aleph_0$, in the sense that $\aleph_1 = 2^{\aleph_0} = |\mathcal{P}(\mathbb{N})|$. Otherwise, we would have $\aleph_0 < \aleph_1 < |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$.

The question that whether $\aleph_1 = 2^{\aleph_0}$ is true or false was first formulated by Georg Cantor in 1878, and was the first of Hilbert's 23 problems presented in 1900. In 1963, Paul Cohen established that this is independent of Zermelo–Fraenkel set theory with axiom of choice (ZFC), meaning that the property $\aleph_1 = 2^{\aleph_0}$ (called continuum hypothesis) *or its negation* can be added as one of the axioms to the ZFC set theory.