Contents

1	Definition of cardinality	2
2	Countable infinities	2
3	Power sets	7
4	Uncountable infinities	8
5	Schröder-Bernstein theorem	Ć

Remark. $\mathbb{N} = \{1, 2, 3, \ldots\}.$

The following is mostly paraphrased from Chapter 2 of [PMA] and Sections 1.5 and 1.6 of [UA].

1 Definition of cardinality

Definition 1. Let A and B be sets. Define a relation \sim by declaring that $A \sim B$ if there exists a bijection between A and B; it is clear that \sim is an equivalence relation. We say that A and B have the same **cardinality** if and only if $A \sim B$.

- (i) If $A \sim \{1, ..., n\}$ for some $n \in \mathbb{N}$, then we say that A is **finite**. In this case, the cardinality or "size" of A is simply the number of elements belonging to A and we write |A| = n. We also take the empty set to be finite and consider it to contain zero elements.
- (ii) If A is not finite, then we say that A is **infinite**.
- (iii) If $A \sim \mathbb{N}$, then we say that A is **countably infinite**, **countable**, **denumerable**, or **enumerable**.
- (iv) If A is finite or countably infinite, we say that A is at most countable.
- (v) If A is infinite but not countably infinite, we say that A is **uncountably infinite** or **uncountable**.

2 Countable infinities

Proposition 2. \mathbb{Z} is countably infinite.

Proof. Define functions $f: \mathbb{N} \to \mathbb{Z}$ and $g: \mathbb{Z} \to \mathbb{N}$ as follows:

It is straightforward to verify that f and g are mutual inverses.

Proposition 3. Suppose A is countably infinite and $B \subseteq A$ is infinite. Then B is countably infinite.

Proof. Since A is countably infinite, there exists a bijection $f: \mathbb{N} \to A$. We will inductively construct a bijection $g: \mathbb{N} \to B$ as follows. Since B is non-empty, $f^{-1}(B)$ is also non-empty, so we may set $n_1 = \min(f^{-1}(B))$. Suppose that after k steps we have chosen positive integers $n_1 < \cdots < n_k$ such that

$$n_1 = \min(f^{-1}(B)), \quad n_i = \min(f^{-1}(B) \setminus \{n_1, \dots, n_{i-1}\}) \text{ for } 2 \le i \le k.$$

We claim that the set $E := f^{-1}(B) \setminus \{n_1, \dots, n_k\}$ is non-empty; indeed, E must be infinite. Since f is a bijection, we have

$$B = f(f^{-1}(B)) = f(E \cup \{n_1, \dots, n_k\}) = f(E) \cup f(\{n_1, \dots, n_k\}).$$

Evidently: $f(\{n_1, \ldots, n_k\})$ is a finite set; the union of two finite sets is again a finite set; and $E \sim f(E)$ via f. Hence E being finite implies that E is finite; by the contrapositive we see that E must be infinite. We are then justified in setting $n_{k+1} = \min(f^{-1}(B) \setminus \{n_1, \ldots, n_k\})$. In this way we obtain a sequence $n_1 < \cdots < n_k < \cdots$ of positive integers such that

$$n_1 = \min(f^{-1}(B)), \quad n_k = \min(f^{-1}(B) \setminus \{n_1, \dots, n_{k-1}\}) \text{ for } 2 \le k.$$

We define q by setting $q(k) = f(n_k) \in B$. Observe that since f is injective we have

$$g(k) = g(l) \iff f(n_k) = f(n_l) \iff n_k = n_l.$$

Suppose that k < l. Then $n_k < n_l$; it follows that g is injective. To see that g is surjective, let $b \in B$ be given. Since f is surjective, there is a positive integer N such that f(N) = b. Suppose that for all $k \in \mathbb{N}$ we have $N \neq n_k$. It cannot be the case that $N < n_1$, else n_1 would not be the minimum of $f^{-1}(B)$, so we must have $n_1 < N$. Then the set $\{k \in \mathbb{N} : n_k < N\}$ is non-empty and finite (it contains at most N - 1 elements), so $l := \max\{k \in \mathbb{N} : n_k < N\}$ exists and we have $n_l < N < n_{l+1}$; but this contradicts n_{l+1} being the minimum of the set $f^{-1}(B) \setminus \{n_1, \ldots, n_l\}$. So in fact there must exist a $k \in \mathbb{N}$ such that $n_k = N$ and it follows that $g(k) = f(n_k) = f(N) = b$. \square

Proposition 4. A set A is countably infinite if and only if A is infinite and there exists a surjection $f: \mathbb{N} \to A$.

Proof. A bijection is in particular a surjection, so the forward implication is clear. For the converse implication, suppose there exists a surjection $f: \mathbb{N} \to A$. Then $f^{-1}\{a\}$ is non-empty for any $a \in A$, so the function $g: A \to \mathbb{N}$ given by $g(a) = \min(f^{-1}\{a\})$ is well-defined. This function is injective since

$$g(a_1) = g(a_2) \implies f(g(a_1)) = f(g(a_2)) \iff a_1 = a_2.$$

Hence we see that $A \sim g(A)$ via g. Since A is infinite, g(A) must also be infinite. Then by Proposition 3, $g(A) \sim \mathbb{N}$. It follows that $A \sim \mathbb{N}$, i.e. A is countably infinite.

Proposition 5. Suppose for each $n \in \mathbb{N}$ we have a countably infinite set A_n . Then the union $\bigcup_{n=1}^{\infty} A_n$ is countably infinite.

Proof. By Proposition 4, it will suffice to construct a surjection $g: \mathbb{N} \to \bigcup_{n=1}^{\infty} A_n$. For each $n \in \mathbb{N}$ we have a bijection $f_n: \mathbb{N} \to A_n$. For $m, n \in \mathbb{N}$, let $a_{mn} = f_n(m)$. As a sketch of our construction, arrange these terms in an "infinite grid" like so:

We define g by working our way through the grid along the diagonals as shown in the infinite grid, setting $g(1) = a_{11}$, $g(2) = a_{12}$, $g(3) = a_{21}$, $g(4) = a_{13}$, $g(5) = a_{22}$, $g(6) = a_{31}$, and so on. Since each f_n is in particular a surjection, each element of $\bigcup_{n=1}^{\infty} A_n$ appears somewhere in this grid, lying on some diagonal. It follows that g is a surjection. To give an explicit construction of g is tedious and not particularly illuminating, but nonetheless we will do so.

To be explicit then, for $n \in \mathbb{N}$, let $t_n = \frac{n(n-1)}{2}$, so that $t_1 = 0, t_2 = 1, t_3 = 3, t_4 = 6$, and so on. Let $k \in \mathbb{N}$ be given. The set $T_k = \{m \in \mathbb{N} : t_m < k\}$ is non-empty $(t_1 \in T_k)$ and finite (it could contain at most k-1 elements), so $n := \max T_k$ exists; it follows that $t_n < k \le t_{n+1}$. Conversely, if $t_n < k \le t_{n+1}$ for some $n \in \mathbb{N}$, then $n = \max T_k$. Given this, setting

$$g(k) = a_{k-t_n, t_{n+1}+1-k} = f_{t_{n+1}+1-k}(k-t_n)$$

gives us a well-defined function $g: \mathbb{N} \to \bigcup_{n=1}^{\infty} A_n$. To see that g is surjective, let $a \in \bigcup_{n=1}^{\infty} A_n$ be given. Then $a \in A_n$ for some $n \in \mathbb{N}$. Since f_n is a surjection, there exists $m \in \mathbb{N}$ such that $a = f_n(m) = a_{mn}$. Let $k = t_{m+n-1} + m$. Observe that

$$k \le t_{m+n} \iff \frac{(m+n-1)(m+n-2)}{2} + m \le \frac{(m+n)(m+n-1)}{2} \iff m \le m+n-1.$$

The statement $m \le m+n-1$ is certainly true, so we see that $t_{m+n-1} < k \le t_{m+n}$. It follows that $\max T_k = m+n-1$. Then $k-t_{m+n-1} = m$ and

$$t_{m+n} + 1 - k = t_{m+n} - t_{m+n-1} - m + 1$$

$$= \frac{(m+n)(m+n-1)}{2} - \frac{(m+n-1)(m+n-2)}{2} - m + 1$$

$$= m + n - 1 - m + 1$$

$$= n.$$

Hence
$$g(k) = a_{mn} = a$$
.

Corollary 6. Suppose we have an at most countable set A and a countably infinite set B. Then $A \cup B$ is countably infinite.

Proof. (i) If A is empty then the result is clear. Suppose that A is non-empty and finite, say $A = \{a_1, \ldots, a_k\}$ for some $k \in \mathbb{N}$. By Proposition 4, there is a surjection $f : \mathbb{N} \to B$. Define a function $g : \mathbb{N} \to A \cup B$ by

$$g(1) = a_1, \dots, g(k) = a_k$$
, and $g(n) = f(n-k)$ for $n > k$.

Then g is a surjection and we may invoke Proposition 4 to conclude that $A \cup B$ is countably infinite.

(ii) Suppose that A is countably infinite. This is then a special case of Proposition 5. Indeed, take $E_1 = A$ and $E_n = B$ for $n \ge 2$; then each E_n is countably infinite and

$$A \cup B = \bigcup_{n=1}^{\infty} E_n.$$

Proposition 5 then implies that $A \cup B$ is countably infinite.

Proposition 7. Suppose we have some at most countable indexing set I and, for each $i \in I$, an at most countable set A_i .

- (i) If I is finite and each A_i is finite, then $\bigcup_{i \in I} A_i$ is finite.
- (ii) If I is countably infinite and there is a finite subset $J \subseteq I$ such that A_i is finite for $i \in J$ and A_i is empty for $i \notin J$, then $\bigcup_{i \in I} A_i$ is finite. (This includes the possibility that each A_i is empty.)
- (iii) If at least one A_i is countably infinite, then $\bigcup_{i\in I} A_i$ is countably infinite.
- (iv) If I is countably infinite and there is an infinite subset $J \subseteq I$ such that A_i is finite and non-empty for $i \in J$ and A_i is empty for $i \notin J$, then $\bigcup_{i \in I} A_i$ is at most countable.

These cases are exclusive and exhaustive. In any case, $\bigcup_{i\in I} A_i$ is at most countable; we can never obtain an uncountably infinite set by taking at most countable unions of at most countable sets.

- *Proof.* (i) $\bigcup_{i \in I} A_i$ contains at most $\sum_{i \in I} |A_i|$ elements; less if the A_i 's have elements in common. (The exact number of elements in the union is given by the inclusion-exclusion principle.)
 - (ii) We have $\bigcup_{i \in I} A_i = \bigcup_{i \in J} A_i$; now apply part (i).

(iii) Suppose A_j is countably infinite for some $j \in I$. If I is finite, say $\{1, \ldots, k\} \sim I$ via some bijection f, let $E_n = A_{f(n)} \cup A_j$ for $1 \le n \le k$ and $E_n = A_j$ for n > k. If I is countably infinite, let $f : \mathbb{N} \to I$ be a bijection, and define $E_n = A_{f(n)} \cup A_j$ for $n \in \mathbb{N}$. In either case, by Corollary 6, each E_n is countably infinite. Furthermore,

$$\bigcup_{i \in I} A_i = \bigcup_{n=1}^{\infty} E_n.$$

The result now follows from Proposition 5.

(iv) For $i \in J$, let $E_i = A_i \cup \mathbb{N}$. Then each E_i is countably infinite by Corollary 6 and

$$\bigcup_{i \in I} A_i = \bigcup_{i \in J} A_i \subseteq \bigcup_{i \in J} E_i.$$

J is countably infinite by Proposition 3, so we may apply part (iii) to see that $\bigcup_{i \in J} E_i$ is countably infinite. If $\bigcup_{i \in J} A_i$ is finite, we are done. If it is infinite, then the desired result follows from Proposition 3.

Remark. In part (iv) of Proposition 7, it may be the case that $\bigcup_{i \in J} A_i$ is finite or countably infinite. For two examples, consider $A_i = \{0\}$ for each $i \in \mathbb{N}$. Then $\bigcup_{i=1}^{\infty} A_i = \{0\}$, a finite set. Now consider $A_i = \{i\}$ for each $i \in \mathbb{N}$. Then $\bigcup_{i=1}^{\infty} A_i = \mathbb{N}$, a countably infinite set.

Corollary 8. Suppose we have finitely many at most countable sets A_1, \ldots, A_n .

- (i) If each A_i is finite, then $\prod_{i=1}^n A_i$ is finite (where $\prod_{i=1}^n A_i$ is the Cartesian product $A_1 \times \cdots \times A_n$).
- (ii) If each A_i is non-empty and at least one A_i is countably infinite, then $\prod_{i=1}^n A_i$ is countably infinite.

Proof. (i) $\prod_{i=1}^n A_i$ has exactly $\prod_{i=1}^n |A_i|$ elements.

(ii) First, let us prove the special case where each A_i is countably infinite. For the base case, suppose we have countably infinite sets A_1 and A_2 . Let $f: \mathbb{N} \to A_2$ be a bijection. For any fixed $a \in A_1$, we have $\mathbb{N} \sim (\{a\} \times A_2)$ via the map $n \mapsto (a, f(n))$. Observe that

$$A_1 \times A_2 = \bigcup_{a \in A_1} (\{a\} \times A_2).$$

Hence $A_1 \times A_2$ is countably infinite by Proposition 7 (iii). The special case now follows by induction. For the general case, suppose A_j is countably infinite for some $1 \le j \le n$. Let

 $E_i = A_i \cup A_j$ for $1 \le i \le n$. Then each E_i is countably infinite by Corollary 6 and so the product $\prod_{i=1}^n E_i$ is also countably infinite by the special case we just proved. Furthermore,

$$\prod_{i=1}^{n} A_i \subseteq \prod_{i=1}^{n} E_i.$$

Since each A_i is non-empty, there exists $a_i \in A_i$ for each $1 \le i \le n$. Then the infinite set $\{a_1\} \times \cdots \times A_j \times \cdots \times \{a_n\}$ is contained in $\prod_{i=1}^n A_i$. It follows that $\prod_{i=1}^n A_i$ is infinite and so by Proposition 3 we may conclude that $\prod_{i=1}^n A_i$ is countably infinite.

Remark. Corollary 8 cannot be generalised to the product of infinitely many sets, i.e. the product of infinitely many at most countable sets need not be at most countable – even if the factors are finite! We shall give a counterexample in Proposition 12.

Corollary 9. \mathbb{Q} is countably infinite.

Proof. Let us take as our construction of \mathbb{Q} the set of equivalence classes of elements in $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ where we declare (a,b) and (c,d) equivalent if and only if ad = bc. Let $\pi : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ be the canonical map, which is always a surjection. By Proposition 2, \mathbb{Z} is countably infinite; it is straightforward to modify the proof of that proposition to see that $\mathbb{Z} \setminus \{0\}$ is also countably infinite. Then by Corollary 8, $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is countably infinite. Let $f : \mathbb{N} \to \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ be a bijection. Then the composition $\pi \circ f : \mathbb{N} \to \mathbb{Q}$ is a surjection and hence by Proposition 4 we see that \mathbb{Q} is countably infinite.

3 Power sets

For a set A, we will write $\mathcal{P}(A)$ for the power set of A.

Proposition 10. Suppose we have sets A and B such that $A \sim B$. Then $\mathscr{P}(A) \sim \mathscr{P}(B)$.

Proof. Let $f:A\to B$ be a bijection. We define two functions $F:\mathscr{P}(A)\to\mathscr{P}(B)$ and $G:\mathscr{P}(B)\to\mathscr{P}(A)$ by

$$F(X) = \{ f(x) : x \in X \}$$
 and $G(Y) = \{ f^{-1}(y) : y \in Y \}.$

It is straightforward to verify that F and G are mutual inverses.

Proposition 11 (Cantor's theorem). Let A be a set and $f: A \to \mathcal{P}(A)$ a function. Then f is not a surjection.

Proof. Let $B = \{x \in A : x \notin f(x)\} \in \mathcal{P}(A)$ (this set is sometimes called the Cantor diagonal set of f). Suppose f is a surjection, so that there exists some $x \in A$ such that f(x) = B. Then $x \in B \iff x \notin f(x) = B$, a contradiction. It follows that f cannot be a surjection.

4 Uncountable infinities

Proposition 12. Let T be the set of all binary sequences, i.e.

$$T = \prod_{n=1}^{\infty} \{0, 1\} = \{(x_1, x_2, x_3, \dots) : x_n \in \{0, 1\}\},\$$

and let $f: \mathbb{N} \to T$ be a function. Then f is not a surjection.

Proof. For each $n \in \mathbb{N}$, let $x_n = 0$ if f(n) = 1 and let $x_n = 1$ if f(n) = 0. Then the sequence $\mathbf{x} = (x_1, x_2, x_3, \ldots)$ cannot possibly belong to the image $f(\mathbb{N})$ since it differs from each f(n) in the *n*th position. It follows that $f(\mathbb{N}) \neq T$, i.e. that f is not a surjection.

Proposition 12 implies that the set of all binary sequences T cannot be put in bijection with \mathbb{N} ; since T is evidently infinite, it follows that T is uncountably infinite.

Proposition 13. $\mathscr{P}(\mathbb{N})$ has the same cardinality as T.

Proof. Define a function $f: \mathscr{P}(\mathbb{N}) \to T$ by mapping a subset $E \subseteq \mathbb{N}$ to the binary sequence (a_1, a_2, a_3, \ldots) , where $a_n = 1$ if $n \in E$ and $a_n = 0$ if $n \notin E$, and define a function $g: T \to \mathscr{P}(\mathbb{N})$ by mapping a sequence (a_1, a_2, a_3, \ldots) to the subset $E = \{n \in \mathbb{N} : a_n = 1\}$. It is straightforward to verify that f and g are mutual inverses.

Remark. We could have proved Proposition 12 by combining Proposition 11 (Cantor's theorem) with Proposition 13.

Let us now consider the cardinality of \mathbb{R} . Using the binary representation of real numbers, one can construct a bijection between \mathbb{R} and the set of all binary sequences T. Proposition 12 then implies that \mathbb{R} is uncountably infinite. However, we will take a different approach, using the nested interval property of \mathbb{R} , which is much closer to Cantor's original 1874 proof of the uncountability of \mathbb{R} .

Proposition 14. Let $f: \mathbb{N} \to \mathbb{R}$ be a function. Then f is not a surjection.

Proof. Let $I_1 = [a_1, b_1]$ be any closed bounded interval which does not contain f(1); taking $I_1 = [f(1) + 1, f(1) + 2]$ will do. Let $m = \frac{2}{3}a_1 + \frac{1}{3}b_1$ and $M = \frac{1}{3}a_1 + \frac{2}{3}b_1$.



If $f(2) \notin [a_1, m]$, then let $a_2 = a_1, b_2 = m$, and set $I_2 = [a_2, b_2]$. If $f(2) \in [a_1, m]$, then $f(2) \notin [M, b_1]$, so let $a_2 = M, b_2 = b_1$, and set $I_2 = [a_2, b_2]$. In either case, $f(1) \notin I_1, f(2) \notin I_2$,

and $|I_2| = b_2 - a_2 = 3^{-1}(b_1 - a_1)$. Now repeat this argument with I_2 , and then with I_3 , and so on; inductively, we obtain a sequence of shrinking nested intervals $(I_n)_{n \in \mathbb{N}}$ such that $f(n) \notin I_n$ for each $n \in \mathbb{N}$. By the nested interval property of \mathbb{R} , there exists an $x \in \mathbb{R}$ such that $\bigcap_{n=1}^{\infty} I_n = \{x\}$. It follows that x does not belong to the image of f, since x = f(n) implies that $f(n) \in I_n$. Hence f is not a surjection.

Evidently, \mathbb{R} is infinite; Proposition 14 then implies that \mathbb{R} is uncountably infinite. In light of Corollary 6, which implies that the union of two countably infinite sets is countably infinite, and Corollary 9, which says that \mathbb{Q} is countably infinite, we see that the set of irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ must be uncountably infinite.

5 Schröder-Bernstein theorem

Remark. In what follows, we will write A^{c} for the complement of a set A, i.e. A^{c} is the set of those x which do not belong to A.

Proposition 15 (Schröder-Bernstein theorem). Let X and Y be sets and suppose we have injective functions $f: X \to Y$ and $g: Y \to X$. Then there exists a bijection $h: X \to Y$.

Proof. Let $A_1 = [g(Y)]^c$, $A_n = g(f(A_{n-1}))$ for $n \geq 2$, $A = \bigcup_{n=1}^{\infty} A_n$, and $B = \bigcup_{n=1}^{\infty} f(A_n)$. Consider the restriction $f|_A : A \to B$; we will abuse notation slightly and write this restriction simply as $f : A \to B$. From the definitions of A and B, it is clear that f indeed maps A into B and in fact is surjective. Since $f : X \to Y$ is injective, $f : A \to B$ is also injective and hence bijective. Now consider the restriction $g|_{B^c} : B^c \to A^c$; again, we will write $g : B^c \to A^c$ for this restriction. This maps into A^c since

$$b \in B^{c} \iff \forall n \in \mathbb{N}, \ b \notin f(A_{n})$$

 $\iff \forall n \in \mathbb{N}, \ g(b) \notin g(f(A_{n}))$
 $\iff \forall n \in \mathbb{N}, \ g(b) \notin A_{n+1}$
 $\iff \forall n \geq 2, \ g(b) \notin A_{n}.$

Since A_1 is the complement of the image of Y under g, it follows that $g(y) \notin A_1$ for any $y \in Y$. Hence

$$b \in B^{\mathsf{c}} \iff \forall n \in \mathbb{N}, \ g(b) \not\in A_n \iff g(b) \in A^{\mathsf{c}}.$$

Furthermore, $g: B^c \to A^c$ is surjective since for any $a \in A^c$ we have $a \notin A_1 \iff a \in g(Y)$, so that a = g(y) for some $y \in Y$. The chain of biconditionals above then shows that $y \in B^c$.

Since $g: Y \to X$ is injective, $g: B^c \to A^c$ is also injective and hence bijective. Given this, the functions $h_1: X \to Y$ and $h_2: Y \to X$ given by

$$h_1(x) = \begin{cases} f(x) & \text{if } x \in A, \\ g^{-1}(x) & \text{if } x \in A^{\mathsf{c}}, \end{cases} \qquad h_2(y) = \begin{cases} f^{-1}(y) & \text{if } y \in B, \\ g(y) & \text{if } y \in B^{\mathsf{c}} \end{cases}$$

are well-defined and mutual inverses.

For an application of the Schröder-Bernstein theorem, let us show that $[0,1] \sim (0,1)$. Consider the injections $f:[0,1] \to (0,1)$ and $g:(0,1) \to [0,1]$ given by $f(x) = \frac{1}{2}x + \frac{1}{4}$ and g(x) = x. The Schröder-Bernstein theorem then guarantees the existence of a bijection between [0,1] and (0,1), but furthermore shows us how to find an explicit bijection. Following the procedure detailed in the proof of the theorem, we have $A_1 = \{0,1\}, A_2 = \{\frac{1}{4}, \frac{3}{4}\}, A_3 = \{\frac{3}{8}, \frac{5}{8}\}$, and in general $A_n = \{\frac{1}{2} - 2^{-n}, \frac{1}{2} + 2^{-n}\}$, which gives $f(A_n) = \{\frac{1}{2} - 2^{-n-1}, \frac{1}{2} + 2^{-n-1}\}$. Then if we define $h: X \to Y$ by

$$h(x) = \begin{cases} \frac{1}{2}x + \frac{1}{4} & \text{if } x \in \bigcup_{n=1}^{\infty} \left\{ \frac{1}{2} - 2^{-n}, \frac{1}{2} + 2^{-n} \right\}, \\ x & \text{otherwise,} \end{cases}$$

we can be sure that h is a bijection with inverse

$$h^{-1}(y) = \begin{cases} 2y - \frac{1}{2} & \text{if } y \in \bigcup_{n=1}^{\infty} \left\{ \frac{1}{2} - 2^{-n-1}, \frac{1}{2} + 2^{-n-1} \right\}, \\ y & \text{otherwise.} \end{cases}$$

[PMA] Rudin, W. (1976) Principles of Mathematical Analysis. 3rd edn. [UA] Abbott, S. (2015) Understanding Analysis. 2nd edn.