Lecture 5
Part II

CARDINALITY
(NON-EXAMINABLE)

Informally, the **cardinality** of a set A, denoted $|A|$, is the size of A.

For a finite set A, its cardinality is the number of distinct elements in A, so that the notation $|A|$ agrees with what we defined earlier.

Let $f : A \to B$ be a function. Intuitively,

- If f is injective, then B has at least as many elements as A, i.e. $|A| \leq |B|$.
- If f is surjective, then A has at least as many elements as B, i.e. $|A| \geq |B|$.
- If f is bijective, then A has as many elements as B, i.e. $|A| = |B|$.

Definition

Let A and B be sets.

- We write $|A| \leq |B|$ if and only if there exists an injective function $f : A \to B$.
- We write $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$.
- We further write $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$.

Note

- By Cantor-Bernstein Theorem, $|A| = |B|$ if and only if there exists a bijective function $f : A \to B$.
- For a finite set A, we have $|B| < |A|$ if B is a proper subset of A.
- For an infinite set A, it is possible for a proper subset B of A to have $|B| = |A|$. Eg. $|\mathbb{Z}^+| = |\mathbb{Z}|$.

Note

- Let A be a set. Then $|A| = |A|$ and $|A| \leq |A|$.
- Because composition of functions preserves injectivity and surjectivity, we have

$$\begin{aligned}
|A| = |B| \wedge |B| = |C| \quad &\Rightarrow \quad |A| = |C|; \\
|A| \leq |B| \wedge |B| \leq |C| \quad &\Rightarrow \quad |A| \leq |C|; \\
|A| = |B| \wedge |B| \leq |C| \quad &\Rightarrow \quad |A| \leq |C|; \\
|A| \leq |B| \wedge |B| = |C| \quad &\Rightarrow \quad |A| \leq |C|.
\end{aligned}$$

  We summarise these as:

$$\begin{aligned}
|A| = |B| = |C| \quad &\Rightarrow \quad |A| = |C|; \\
|A| \leq |B| \leq |C| \quad &\Rightarrow \quad |A| \leq |C|; \\
|A| = |B| \leq |C| \quad &\Rightarrow \quad |A| \leq |C|; \\
|A| \leq |B| = |C| \quad &\Rightarrow \quad |A| \leq |C|.
\end{aligned}$$

Lemma

Let A be a set. Then $|A| < |\mathscr{P}(A)|$.

Proof.

The function $f : A \to \mathscr{P}(A)$ defined by $a \mapsto \{a\}$ for all $a \in A$ is injective, so that $|A| \leq |\mathscr{P}(A)|$.

Suppose, for the sake of contradiction, that $|A| = |\mathscr{P}(A)|$.

1. Then there exists a bijective function $g : A \to \mathscr{P}(A)$.
2. Let $X = \{a \in A \mid a \notin g(a)\}$.
3. Then $X \in \mathscr{P}(A)$.
4. By (1) and (3), there exists $x \in A$ such that $g(x) = X$.
    1. Case 1: $x \in X$.
        1. By (2) and (4.1), $x \notin g(x)$.
        2. By (4) and (4.1.1), $x \notin X$, contradicting (4.1).
    2. Case 2: $x \notin X$.
        1. By (2) and (4.2), $x \in g(x)$.
        2. By (4) and (4.2.1), $x \in X$, contradicting (4.2).
5. Thus, there does not exist $x \in A$ such that $g(x) = X$.
6. Thus g is not surjective, a contradiction.

$\square$

$\mathbb{Z}^+$ has the smallest cardinality among infinite sets:

Lemma

Let A be an infinite set. Then $|\mathbb{Z}^+| \leq |A|$.

Sketch of proof.

1. We pick distinct $a_1, a_2, \ldots \in A$ as follows:
   1. Let a_1 be any element of A.
   2. Having chosen $a_1, \ldots, a_n$, we have $\{a_1, \ldots, a_n\} \subsetneq A$.
   3. Thus $A \setminus \{a_1, \ldots, a_n\} \neq \varnothing$, and we may pick $a_{n+1} \in A \setminus \{a_1, \ldots, a_n\}$.
2. Define $f : \mathbb{Z}^+ \to A$ by $f(n) = a_n$ for all $n \in \mathbb{Z}^+$. Then f is injective by construction.

$\square$

Countable Sets

Definition

A set A is **countable** if and only if $|A| \leq |\mathbb{Z}^+|$.

Example

1. All finite sets are countable.
2. If $|B| \leq |A|$ and A is countable, then B is countable. In particular, all subsets of a countable set are countable.

Note

The last lemma tells us that:

- If A is infinite, then A is countable if and only if $|A| = |\mathbb{Z}^+|$.
- Every infinite set has a subset that is infinite and countable.

Proposition

Let A and B be countable sets. Then $A \times B$ is countable.

Proof.

1. There exist injective functions $f : A \to \mathbb{Z}^+$ and $g : B \to \mathbb{Z}^+$.
2. Define $h : A \times B \to \mathbb{Z}^+$ by $h(a, b) = 2^{f(a)} 3^{g(b)}$ for all $(a, b) \in A \times B$.
3. Take $(a_1, b_1), (a_2, b_2) \in A \times B$, and assume that $h(a_1, b_1) = h(a_2, b_2)$.
4. Then $2^{f(a_1)} 3^{g(b_1)} = 2^{f(a_2)} 3^{g(b_2)}$.
5. By uniqueness of prime factorisation of positive integers, we have $f(a_1) = f(a_2)$ and $g(b_1) = g(b_2)$.
6. Thus $a_1 = a_2$ and $b_1 = b_2$ by injectivity of f and g.
7. Hence $(a_1, b_1) = (a_2, b_2)$.
8. Consequently, h is injective, and $A \times B$ is countable.

$\square$

Note

The last proposition may be generalised to the following:
Let $n \in \mathbb{Z}^+$. If $A_1, A_2, \ldots, A_n$ are countable, then $A_1 \times A_2 \times \ldots \times A_n$ is countable.
In other words: A finite product of countable sets is countable.

Corollary

$\mathbb{Q}$ is countable.

Sketch of proof.

1. Every rational number has a unique expression in the form $\frac{a}{b}$ with $\gcd(a, b) = 1$ and $b \in \mathbb{Z}^+$.
2. Thus we have an injective function $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}^+$; $\frac{a}{b} \mapsto (a, b)$.
3. Thus, $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}^+|$.
4. But $\mathbb{Z}$ and $\mathbb{Z}^+$ are both countable, so that $\mathbb{Z} \times \mathbb{Z}^+$ is countable. Thus $|\mathbb{Z} \times \mathbb{Z}^+| \leq |\mathbb{Z}^+|$.
5. Hence $|\mathbb{Q}| \leq |\mathbb{Z}^+|$, i.e. $\mathbb{Q}$ is countable.

$\square$

Proposition

A countable union of countable sets is countable: Let I be a countable set, and for each $i \in I$, let A_i be a countable set. Then $\bigcup_{i \in I} A_i$ is countable.

Sketch of proof.

1. We may assume that $I \subseteq \mathbb{Z}^+$.
2. There exist injective functions $f_i : A_i \to \mathbb{Z}^+$ for each $i \in I$.
3. For each $a \in \bigcup_{i \in I} A_i$, let $n_a := \min\{i \in I \mid a \in A_i\}$.
4. Define $h : \bigcup_{i \in I} A_i \to \mathbb{Z}^+ \times \mathbb{Z}^+$ by $h(a) = (n_a, f_{n_a}(a))$.
5. Take $a, a' \in \bigcup_{i \in I} A_i$, and assume that $h(a) = h(a')$.
6. Then $n_a = n_{a'}$ and $f_{n_a}(a) = f_{n_{a'}}(a')$.
7. Thus $f_{n_a}(a) = f_{n_a}(a')$, so that $a = a'$ since f_{n_a} is injective.
8. Hence h is injective, so that $|\bigcup_{i \in I} A_i| \leq |\mathbb{Z}^+ \times \mathbb{Z}^+|$.
9. But $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable, so that $|\mathbb{Z}^+ \times \mathbb{Z}^+| \leq |\mathbb{Z}^+|$.
10. Thus $|\bigcup_{i \in I} A_i| \leq |\mathbb{Z}^+|$, and $\bigcup_{i \in I} A_i$ is countable.

$\square$

Uncountable Sets

Definition

A set is **uncountable** if and only if it is not countable.

Note

- All uncountable sets are infinite.
- Let A be a set. Then A is uncountable if and only if $|\mathbb{Z}^+| < |A|$.
- $\mathscr{P}(\mathbb{Z}^+)$ is uncountable.

Lemma

Let A and B be sets. If B is uncountable and $|B| \leq |A|$, then A is uncountable.

Proof by contradiction.

1. Suppose that A is countable, i.e. $|A| \leq |\mathbb{Z}^+|$.
2. Since $|B| \leq |A|$, we have $|B| \leq |\mathbb{Z}^+|$, i.e. B is countable, a contradiction.

$\square$

In particular, if $B \subseteq A$ and B is uncountable, then A is uncountable.

Proposition

Let $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$. Then S is uncountable.

Sketch of proof using Cantor's diagonal argument.

1. Every real number has a unique decimal expansion with no trailing 9's.
2. Suppose that S is countable.
3. Since S is infinite, $|S| = |\mathbb{Z}^+|$, so there exists a bijective function $f : \mathbb{Z}^+ \to S$.
4. For each $n \in \mathbb{Z}^+$, let the decimal expansion of $f(n)$ be $0.d_{1n}d_{2n}\cdots$.
5. Let a be the real number whose decimal expansion is $0.a_1a_2\cdots$, where

$$a_i = \begin{cases} 4, & \text{if } d_{ii} = 5; \\ 5, & \text{if } d_{ii} \neq 5. \end{cases}$$

6. Then $a \in S$, but $a \neq f(i)$, since they differ at the i-th decimal place, for all $i \in \mathbb{Z}^+$.
7. Thus f is not surjective, a contradiction.

$\square$

Corollary

$\mathbb{R}$ *is uncountable.*

Proof.

$S \subseteq \mathbb{R}$ and S is uncountable, so $\mathbb{Q}$ is uncountable. □

Corollary

The set $\mathbb{R} - \mathbb{Q}$ *of irrational numbers is uncountable, and* $|\mathbb{Q}| < |\mathbb{R} - \mathbb{Q}|$.

Proof.

1. $\mathbb{Q}$ is infinite and countable, so that $|\mathbb{Q}| = |\mathbb{Z}^+|$.
2. If $\mathbb{R} - \mathbb{Q}$ is countable, then $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$ is the union of two countable sets, and hence countable, a contradiction.
3. Thus $\mathbb{R} - \mathbb{Q}$ is uncountable, and $|\mathbb{Q}| = |\mathbb{Z}^+| < |\mathbb{R} - \mathbb{Q}|$.

□