§ 1 Preliminaries

1.1 Functions

Definition :

Let A, B be two sets. A **function** from A to B is a subset of $f \subseteq A \times B$ such that for all $a \in A$, there exists unique $b \in B$ such that $(a,b) \in f$.

We usually denote it by $f : A \to B$. If $(a,b) \in f$, then we write $f(a) = b$.

Domain of f $= D(f) = A$

Range of f $= R(f) = \{ b \in B : (a,b) \in f \text{ for some } a \in A \} \subseteq B$

If $E \subseteq A$, **image of E under f**

$= f(E) = \{ f(x) \in B : x \in E \}$

If $H \subseteq B$, **preimage of H under f**

$= f^{-1}(H) = \{ a \in A : f(a) \in H \}$

Exercise :

1) Let $f : A \to B$, and let $G, H \subseteq B$. Show that

   a) $f^{-1}(G \cap H) = f^{-1}(G) \cap f^{-1}(H)$

   b) $f^{-1}(G \cup H) = f^{-1}(G) \cup f^{-1}(H)$

2) Let $f : A \to B$. Show that

   a) $f(A) \subseteq B$

   b) For all $x \in A$, $\{x\} \subseteq f^{-1}(\{f(x)\})$

   When do the equalities in (a) and (b) hold ?

Definition :

Let $f : A \to B$.

- f is said to be **injective** if

  for all $x_1, x_2 \in A$ with $f(x_1) = f(x_2)$, we have $x_1 = x_2$.

  (Equivalently : $\{x\} = f^{-1}(\{f(x)\})$ for all $x \in A$)

- f is said to be **surjective** if

  for all $y \in B$, there exists $x \in A$ such that $f(x) = y$.

  (Equivalently: $f(A) = B$)

- f is said to be **bijective** if

  f is both injective and surjective.

Exercise:

1) Prove that $f: \mathbb{N} \to \mathbb{N}$ defined by $f(n) = 2n$ is injective but NOT surjective.

   (Remark: In this course, $\mathbb{N} = \{1, 2, 3, \cdots\}$)

2) Prove that $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is injective.

If $f: A \to B$ is bijective, we can define $f^{-1}: B \to A$ such that $f \circ f^{-1}: B \to B$ and $f^{-1} \circ f: A \to A$ are identity maps on B and A respectively. (Think: $(a, b) \in f$ if and only if $(b, a) \in f^{-1}$.)

1.2 Natural Numbers and Mathematical Induction

Set-theoretic Definition of Natural Numbers

Regard $0 = \phi$ empty set

$1 = \{0\} = \{\phi\}$

$2 = \{0, 1\} = \{\phi, \{\phi\}\}$

$3 = \{0, 1, 2\} = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$

$\vdots$

$n = \{0, 1, 2, \cdots, n-1\}$

With this definition, $m \leq n$ if m is a subset of n.

(Remark: In this course, $\mathbb{N} = \{1, 2, 3, \cdots\}$)

FACT: "$\leq$" gives a partial order of $\mathbb{N}$.

Well-Ordering Property of $\mathbb{N}$:

Every nonempty subset of $\mathbb{N}$ has a least element.

(For details, refer to axiomatic set theory.)

Addition (Additional axioms)

Theorem: (Mathematical Induction)

Let $S \subseteq \mathbb{N}$ such that

1) $1 \in S$

2) For every $k \in S$, we have $k+1 \in S$.

Then $S = \mathbb{N}$.

proof:

Suppose $S \neq \mathbb{N}$, i.e. $\mathbb{N} \setminus S$ is nonempty.

Well-ordering principle, there exists $m \in \mathbb{N} \setminus S$ such that $m \leq x$ for all $x \in \mathbb{N} \setminus S$

Since $1 \in S$ and $m \in \mathbb{N} \setminus S$, m cannot be 1.

Therefore $m-1$ (NOT really subtraction, but the previous one) $\in \mathbb{N}$

$m-1 \leq m$, so $m-1 \in S$.

By assumption, $m = (m-1)+1 \in S$ (Contradiction!)

$\therefore S = \mathbb{N}$.

Variation:

Let $S \subseteq \mathbb{N}$ such that

1) $k_0 \in S$

2) For every $k \in S$, we have $k+1 \in S$.

Then $S = \{k_0, k_0+1, k_0+2, \cdots\}$

$= \mathbb{N} \setminus \{1, 2, \cdots, k_0-1\}$

Theorem: (Strong Induction)

Let $S \subseteq \mathbb{N}$ such that

1) $1 \in S$

2) For every $k \in \mathbb{N}$, if $\{1, 2, \cdots, k\} \subseteq S$, then $k+1 \in S$.

Then $S = \mathbb{N}$.

1.3 Finite and Infinite Sets

Definition:

- The empty set is said to have 0 element.
- A set S is said to have n elements if there exists a bijection from $\mathbb{N}_n = \{1, 2, \cdots, n\}$ onto S (denoted by $|S| = n$).
- A set S is said to be finite if it is either empty or it has n elements for some $n \in \mathbb{N}$.
- A set S is said to be infinite if it is NOT finite.

Lemma:

Let $m, n \in \mathbb{N}$ with $m > n$. Then there does not exist an injection from $\mathbb{N}_m$ into $\mathbb{N}_n$.

proof:

Induction on n. (Refer to Theorem B.1 in [1])

Uniqueness Theorem:

If S is a finite set, then the number of elements of S is unique.

proof:

Claim: If $|S| = m$ and $|S| = n$, then $m = n$.

Suppose $|S| = m$ and $|S| = n$.

There exist bijections $f: \mathbb{N}_m \to S$ and $g: \mathbb{N}_n \to S$.

Then $g^{-1} \circ f: \mathbb{N}_m \to \mathbb{N}_n$ is a bijection. by the above lemma $m \leq n$.

Similarly, $f^{-1} \circ g: \mathbb{N}_n \to \mathbb{N}_m$ is a bijection and so $m \geq n$.

$\therefore m = n$.

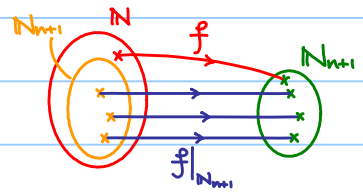
Lemma :

If $n \in \mathbb{N}$, there does not exist an injection from $\mathbb{N}$ to $\mathbb{N}_n$.

proof :

Note $\mathbb{N}_{n+1} \subseteq \mathbb{N}$, if there exists an injection $f : \mathbb{N} \to \mathbb{N}_n$,

then the restriction $f|_{\mathbb{N}_{n+1}}$ is also an injection from $\mathbb{N}_{n+1}$ into $\mathbb{N}_n$ (Contradiction).



Direct consequence of the above lemma :

Theorem :

$\mathbb{N}$ is an infinite set.

Theorem :

- $|A| = m$, $|B| = n$ and $A \cap B = \phi \Rightarrow |A \cup B| = m+n$
- $|A| = m$, $|C| = 1$ and $C \subseteq A \Rightarrow |A \setminus C| = m-1$
- C is infinite and B is finite $\Rightarrow C \setminus B$ is infinite

proof : (Exercise)

Theorem :

Suppose $T \subseteq S$.

- S is finite $\Rightarrow$ T is finite
- T is infinite $\Rightarrow$ S is infinite

proof :

Hints : • Induction

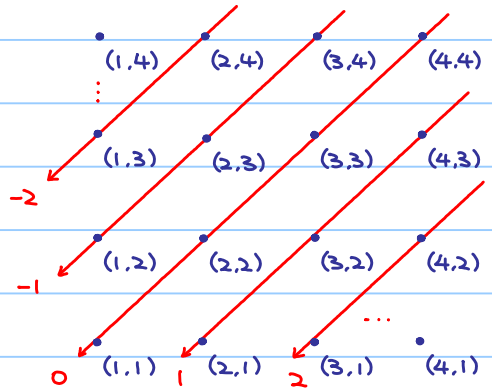
• Contrapositive of the first statement.

Integers $\mathbb{Z}$:

$\mathbb{Z}$ can be defined as $\mathbb{N} \times \mathbb{N} / \sim$ where $(a,b) \sim (c,d)$ if $a+d = c+b$

(Idea : $a-b = c-d$, but we do NOT have subtraction so far !)

Rough idea :



Identifying points on the same red line to be a single point.

Think : How to define subtraction on $\mathbb{Z}$?

Rational Numbers $\mathbb{Q}$:

$\mathbb{Z}$ (with standard + and x) is a ring , $\mathbb{Q}$ is defined to be the field of fraction of $\mathbb{Z}$.

(Refer to any standard Algebra textbook)

Countable Sets :

Definition :

- A set S is said to be countably infinite if there exists a bijection of $\mathbb{N}$ onto S.
- A set S is said to be countable if it is either finite or countably infinite.
- A set S is said to be uncountable if it is NOT countable.

Examples :

1) E = the set of all positive even number is countably infinite.

(Consider $f : \mathbb{N} \to E$ defined by $f(n) = 2n$.)

2) $\mathbb{Z}$ is countably infinite.

How to construct a bijection from $\mathbb{N}$ onto $\mathbb{Z}$?

Hint : $1 \longmapsto 0$

$2 \longmapsto 1$

$3 \longmapsto -1$

$4 \longmapsto 2$

$5 \longmapsto -2$

$\vdots$

Idea : Construction an algorithm to go through all elements in $\mathbb{Z}$ one by one.

(Exercise · Write down the function explicitly .)

Exercise :

Prove that

a) If A and B are both countably infinite and $A \cap B = \phi$, then $A \cup B$ is also countably infinite.

b) If A and B are both countably infinite, then $A \cup B$ is also countably infinite.

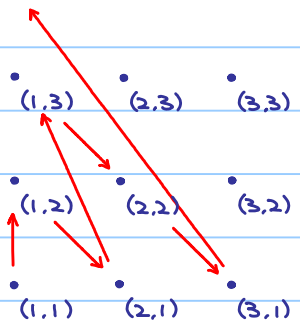
(Using (a), $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$)

Theorem :

$\mathbb{N} \times \mathbb{N}$ is countably infinite.

proof :

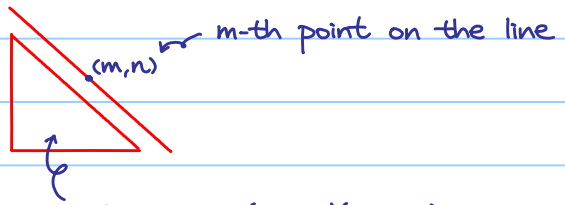
Rough idea :



Go through every element in $\mathbb{N} \times \mathbb{N}$ one by one.

Define $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ by

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



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

Exercise : Show that f is bijective.

(and so $f^{-1} : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ is bijective.)

Theorem:

Suppose $T \subseteq S$.

- S is countable $\Rightarrow$ T is countable
- T is uncountable $\Rightarrow$ S is uncountable

proof:

(Refer to Theorem B.3 and B.4 in [1])

Theorem B.3

If $A \subseteq \mathbb{N}$ and A is infinite, there exists a function $\varphi: \mathbb{N} \to A$ such that $\varphi(n+1) > \varphi(n) \geq n$ for all $n \in \mathbb{N}$. Moreover φ is a bijection of $\mathbb{N}$ onto A.

(Rough idea: φ arranges elements in A in ascending order.)

Theorem B.4

If $A \subseteq \mathbb{N}$, then A is countable.

The result is just a consequence of theorem B.4

Theorem:

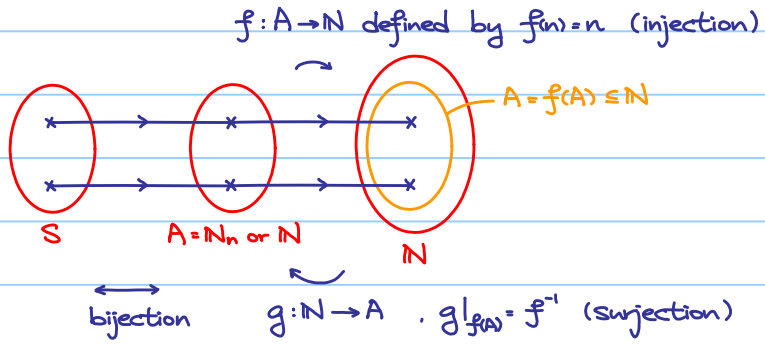
The followings are equivalent (TFAE):

(a) S is countable.

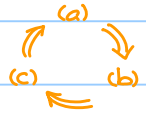
(b) There exists a surjection of $\mathbb{N}$ onto S.

(c) There exists an injection of S onto $\mathbb{N}$.

Idea:



How to prove? Show that



Theorem :

$\mathbb{Q}^+$ is countably infinite.

Idea of proof :

- $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q}^+$ defined by $f(m,n) = \frac{m}{n}$ is a surjection.
- $\mathbb{N} \times \mathbb{N}$ is countably infinite, i.e. there exists a bijection $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

$\therefore f \circ g : \mathbb{N} \to \mathbb{Q}^+$ is a surjection.

$\mathbb{Q}^+$ is countable (by the previous theorem)

Furthermore, $\mathbb{N} \subseteq \mathbb{Q}^+$ (By regarding $n = \frac{n}{1}$) which is infinite

$\therefore \mathbb{Q}^+$ is infinite and so it can only be countably infinite.

$\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$, hence $\mathbb{Q}$ is also countably infinite.

Theorem :

If A_m is a countable set for each $m \in \mathbb{N}$, then $A := \bigcup_{m=1}^{\infty} A_m$ is countable.

Troubles :

1) Some A_i's are finite while some A_j's are infinite

2) $A_i \cap A_j$ may NOT be empty.

proof :

For each $m \in \mathbb{N}$, let $\varphi_m : \mathbb{N} \longrightarrow A_m$ be a surjection.

Then, define $f : \mathbb{N} \times \mathbb{N} \longrightarrow A$ by $f(m,n) = \varphi_m(n)$.

Check f is a surjection.

Furthermore, $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Then, there exists a bijection $g : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$.

$\therefore f \circ g : \mathbb{N} \to A$ is a surjection and the result follows.

Theorem : (Cantor's Theorem)

If A is any set, then there exists no surjection of A onto $\mathcal{P}(A)$,

where $\mathcal{P}(A)$ is the set of all subsets of A.

Think : If $A = \{1,2\}$, then $\mathcal{P}(A) = \{\phi, \{1\}, \{2\}, \{1,2\}\}$

Sort of clear if A is finite

proof :

If $A = \phi$, the statement is trivial (If $A = \phi$, then $\mathcal{P}(A) = \{\phi\}$)

Assume A is nonempty.

Suppose $\psi : A \to \mathcal{P}(A)$ is a surjection

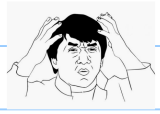
Then pick an element $a \in A$, $\psi(A)$ is a subset of A, we either have $a \in \psi(a)$ or $a \notin \psi(a)$.

Let $D = \{a \in A : a \notin \psi(a)\}$ which is again a subset of A.

By surjectivity of ψ, $D = \psi(a_0)$ for some a_0

Now, $a_0 \in D$ or $a_0 \notin D$?

However, both cases give contraction !



Consequences :

1) $A \underset{\text{inj}}{\hookrightarrow} \mathcal{P}(A) \underset{\text{inj}}{\hookrightarrow} \mathcal{P}(\mathcal{P}(A)) \hookrightarrow \cdots$ larger and larger

2) There exist no surjection from $\mathbb{N}$ onto $\mathcal{P}(\mathbb{N})$

$\therefore \mathcal{P}(\mathbb{N})$ is uncountable (Existence of uncountable set)