Basic Structures

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

July 19, 2021

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Outline

1. Set Theory
   - Cartesian Product & Binary Relation
   - Partition
   - Function
   - Countable & Uncountable Sets

Outline

Set

Set theory is that mathematical discipline which today occupies an outstanding role in our science and radiates its powerful influence into all branches of mathematics

– David Hilbert

Set

Set theory is that mathematical discipline which today occupies an outstanding role in our science and radiates its powerful influence into all branches of mathematics

– David Hilbert

Definition

A set is any collection of definite, distinguishable objects of our intuition or of our intellect to be conceived as a whole.

– Georg Cantor

Set

Set theory is that mathematical discipline which today occupies an outstanding role in our science and radiates its powerful influence into all branches of mathematics

– David Hilbert

Definition

A set is any collection of definite, distinguishable objects of our intuition or of our intellect to be conceived as a whole.

– Georg Cantor

Definition

*A set is a **well defined** collection of objects.*

Set

Exercise

Which of the following collections is a set:

- (i) *Collection of some integers.*
- (ii) *Collection of small primes.*
- (iii) *Collection of positive integer ≥ 300 digits.*
- (iv) *Collection of all English alphabet.*
- (v) *Collection of all employee of IIIT.*
- (vi) *Collection of all rich people in Lucknow.*
- (vii) $\{x \ : \ x \text{ is an integer } s/t \ x^2 = 2\}$
- (viii) *Collection of all functions* $f : \mathbb{N} \to \mathbb{N}$
- (ix) *Collection of all one-to-one functions* $f : \{0, 1\}^n \to \{0, 1\}^n$, *where* n *is a positive integer.*

Set

Exercise

Which of the following collections is a set:

(x) *Collection of all possible plaintexts*

(xi) *Collections of all possible encryption functions*

(xii) *Collection of all decision problems*

(xiii) *Collection of all computable functions*

Set

Exercise

Which of the following collections is a set:

(x) *Collection of all possible plaintexts*

(xi) *Collections of all possible encryption functions*

(xii) *Collection of all decision problems*

(xiii) *Collection of all computable functions*

The term '**well defined**' specifies that it can be determined whether or not certain objects belong to the set in question.

Definition

Definition

*A set is said to be **empty** (or **null**) set if it does not contain any element. It is denoted by* ϕ

Definition

If X *and* Y *are two sets such that every element of* X *is also an element of* Y *, then* X *is called **subset** of* Y *and is denoted by* $X \subseteq Y$ *(or simply by* $X \subset Y$*).*

Notations

$\mathbb{N}$ (or $\mathbb{Z}_{>0}$)	the set of all positive integers
$\mathbb{Z}_{\geq 0}$	the set of all non-negative integers
$\mathbb{Z}$	the set of all integers (positive, negative, and zero)
$\mathbb{Q}$	the set of all rational numbers
$\mathbb{Q}_{>0}$	the set of all positive rational numbers
$\mathbb{R}$	the set of all real numbers
$\mathbb{R}_{>0}$	the set of all positive real numbers
$\mathbb{C}$	the set of all complex numbers
$\exists$	'there exists'
$\forall$	'for all'
$!$	'uniqueness'
$P \Rightarrow Q$	P implies Q (or if P, then Q)
$P \Leftrightarrow Q$	P implies Q & Q implies P (or if and only if, i.e., iff)

Examples

Example

(i) $\mathbb{N} \subset \mathbb{Z}$

(ii) $\mathbb{Z} \subset \mathbb{Q}$

(iii) $\mathbb{Q} \subset \mathbb{R}$

(iv) $\mathbb{R} \subset \mathbb{C}$

(v) $B = \{b : b \in \{0, 1\}^8\} \subset W = \{w : w \in \{0, 1\}^{32}\}$

Definition & Properties

Definition

*Two sets X and Y are said to be **equal**, denoted by $X = Y$ iff they have the same elements.*

Proposition

1. $X = Y$ *iff* $X \subseteq Y$ *and* $Y \subseteq X$;
2. *All null subsets are equal.*

Proposition

A set X of n elements has 2^n subsets.

Definition

Definition

*The **union** (or **join**) of two sets A and B, written as $A \cup B$, is the set $A \cup B = \{x : x \in A \; or \; x \in B\}$.*

Definition

*The **intersection** (or **meet**) of two sets A and B, written as $A \cap B$, is the set $A \cap B = \{x : x \in A \; and \; x \in B\}$.*

Definition

*Two non-empty sets A and B are said to be **disjoint** iff $A \cap B = \phi$.*

Definition

Definition

The ***difference*** *of a set A w.r.t. a set B, denoted by $B \setminus A$ is the set of exactly all elements which belong to B but not to A, i.e.,*

$$B \setminus A = \{x \in B \ : \ x \notin A\}.$$

Definition

The ***symmetric difference*** *of two given sets A and B, denoted by $A \Delta B$, is defined by*

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Properties

Theorem

Each of the operations $\cup$ *and* $\cap$ *is*

1. (i) ***idempotent:*** $A \cup A = A = A \cap A$, *for every set* A;
2. (ii) ***associative:*** $A \cup (B \cup C) = (A \cup B) \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C$ *for any three sets* A, B, C;
3. (iii) ***commutative:*** $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$ *for any two sets* A, B;
4. (iv) ***distributive:*** $\cap$ *distributes over* $\cup$ *and* $\cup$ *distributes over* $\cap$:
   - (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
   - (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *for any three sets* A, B, C.

Definition

Definition

Let X and Y be two sets. Then the ***Cartesian product*** *of X and Y in this order to be denoted by $X \times Y$, is defined by*

$$\begin{aligned} X \times Y &:= \{(x, y) \; : \; x \in X, \; y \in Y\} \\ &:= \phi \text{ if either } X \text{ or } Y = \phi, \end{aligned}$$

where (x, y) denotes the ordered pairs with x as the 1^{st} coordinate and y as the 2^{nd} coordinate.

Definition

A ***binary relation*** *ρ from X to Y is by definition a subset of $X \times Y$.*

If $(x, y) \in \rho$ we sometimes write $x \rho y$ holds.

Definition & Example

Definition

Let $\rho : X \to Y$ *and* $\sigma : Y \to Z$ *binary relation. Then the* **composite** $\sigma \circ \rho$ *in this order is defined by*

$$\sigma \circ \rho := \{(x,z) \ : \ for\ some\ y \in Y\ such\ that\ (x,y) \in \rho\ \&\ (y,z) \in \sigma\}.$$

Example

Let $X = \{1,2,3,4,5\},\ Y = \{3,4,5,6\}$ *and* $Z = \{3,9,7,4\}$*.*

Let $\rho = \{(1,3),(2,4),(3,3),(4,6)\}$ *and* $\sigma = \{(3,3),(3,9),(4,4),(5,9)\}$*.*

Then $\sigma \circ \rho = \{(1,3),(1,9),(2,4),(3,3),(3,9)\}$*.*

From this construction it is clear that $\sigma \circ \rho$ *may be* ϕ *even if* $\rho \neq \phi$ *and* $\sigma \neq \phi$*.*

Note: rho is said to be **null relation** if $\rho = \phi$ and ρ is said to be **Cartesian product relation** if $\rho = X \times Y$.

Definition & Properties

Definition

Let ρ be a binary relation from $X \to Y$, then ρ^{-1} is a relation from $Y \to X$, defined by

$$\rho^{-1} = \{(y, x) \ : \ (x, y) \in \rho\}.$$

Proposition

Let $\rho : X \to Y$, $\sigma : Y \to Z$ and $\delta : Z \to W$ be binary relations. Then

(i) $\delta \circ (\sigma \circ \rho) = (\delta \circ \sigma) \circ \rho$;.

(ii) $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

If $X = Y$ and ρ is a binary relation from X to X, then we say that ρ is a binary relation on X.

Type of Relations

Definition

(i) *Let* ρ *be a binary relation on* $X\ (\neq \phi)$ *then* ρ *is said to be* ***reflexive*** *iff for each* $x \in X,\ (x, x) \in \rho$ *i.e. iff* $\Delta x = \{(x, x)\ :\ x \in X\} \subset \rho$.

(ii) ρ *is said to be* ***symmetric*** *iff for each* $(x, y) \in \rho \Rightarrow (y, x) \in \rho$ *i.e. iff* $\rho = \rho^{-1}$.

(iii) ρ *is said to be* ***asymmetric*** *iff* ρ *is not symmetric i.e.* $\exists\ x,\ y \in X$ *such that* $(x, y) \in \rho$ *but* $(y, x) \notin \rho$.

(iv) ρ *is said to be* ***transitive*** *iff for each triplet* $x, y, z \in X,\ (x, y) \in \rho$ *and* $(y, z) \in \rho \Rightarrow (x, z) \in \rho$ *i.e. iff* $\rho \circ \rho \subset \rho$.

(v) ρ *is said to be* ***antisymmetric****, iff* $(x, y) \in \rho$ *and* $(y, x) \in \rho \Rightarrow x = y$ *i.e. if* $x \neq y$ *at most one of* (x, y) *or* (y, x) *can belong to* ρ.

Type of Relations

Definition

(vi) ρ *is said to be* ***complete*** *iff for each* $x, y \in X$ *either* $(x, y) \in \rho$ *or* $(y, x) \in \rho$.

(vii) *A binary relation* ρ *on a non-void set* X *is said to be an* ***equivalence relation*** *iff* ρ *is reflexive, symmetric and transitive.*

(viii) *A binary relation* ρ *on* X $(\neq \phi)$ *is said to be a* ***pre-order*** *iff* ρ *is reflexive and transitive.*

(ix) ρ *is said to be* ***partial order*** *on* X *(and we say that* (X, ρ) *is a* ***poset****) iff* ρ *is reflexive, antisymmetric and transitive.*

(x) ρ *is said to be a* ***linear order*** *(or* ***total order*** *or* ***chain****) on* X *(and* (X, ρ) *is said to be a* ***linear ordered set****) iff* ρ *is a partial order and complete.*

Examples

Equivalence relation

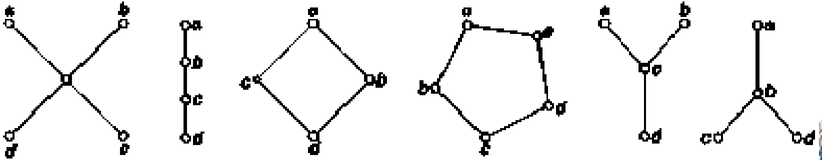
Let $\mathbb{Z}$ be the set of integers and n be a positive integer. Define a relation ρ on $\mathbb{Z}$ by $(x, y) \in \rho$ iff $y - x$ is divisible by n, i.e., $y - x = k.n$ for some $k \in \mathbb{Z}$. Then ρ is an equivalence relation.

Examples

Equivalence relation

Let $\mathbb{Z}$ be the set of integers and n be a positive integer. Define a relation ρ on $\mathbb{Z}$ by $(x, y) \in \rho$ iff $y - x$ is divisible by n, i.e., $y - x = k.n$ for some $k \in \mathbb{Z}$. Then ρ is an equivalence relation.

Different partial order relations



Exercise

Exercise

Give an example of binary relation ρ on a set X such that

1. (i) ρ is *symmetric and reflexive but not transitive.*
2. (ii) ρ is *reflexive and transitive but not symmetric.*
3. (iii) ρ is *symmetric and transitive but not reflexive.*
4. (iv) ρ is *pre-order but not partial order.*
5. (v) ρ is *partial order but not linear order.*

Definition

Definition

1. *Let $(X, \leq)$ be a poset and S be a subset of X. Then an element $x_0 \in X$ is called an* ***upper bound*** *(**lower bound**) of S iff for each $x \in S, \; x \leq x_0 \; (x_0 \leq x)$.*
2. *x_0 will be said to be a lub (least upper bound) [glb (greatest lower bound)] of S iff*
   1. *x_0 is an upper bound of S*
   2. *if y be any upper bound of S then $x_0 \leq y$.*

   or

   1. *x_0 is a lower bound of S*
   2. *if y be any lower bound of S then $y \leq x_0$.*

Definition and Example

Definition

An element x_0 is called the greatest or maximum element of a subset S iff

- (i) x_0 *is an upper bound of* S &
- (ii) $x_0 \in S$.

Example

- (i) *Consider* $\mathbb{R}$ *with usual linear order* $\leq$, *i.e.,* $x \leq y$ *iff* $x - y \leq 0$. *Let* $T = (0, 1) \subset \mathbb{R}$. *Then* $glb\ T = 0$ & $lub\ T = 1$. *But* T *does not have greatest or least element.*
- (ii) *Let* $T = \{x : x > 0\} \subset \mathbb{R}$. *Then* T *does not have a* lub *but it has a* $glb = 0$. *But it does not have a least element.*

Definition and Example

Definition

Let $(X, \leq)$ be a poset and $S \subseteq X$ be a non-empty subset. An element $x_0 \in S$ is said to be a maximal element of S iff for any $y \in S$ & $x_0 \leq y \Rightarrow x_0 = y$, i.e., if $y \in S$, then $y \nless x_0$.

Dually, one can define minimal element in a set S.

If S has a greatest or least element then they are rsp $!$ maximal or minimal element of S.

Example

Let $X = \mathbb{N}$ and $X_0 \subseteq \mathcal{P}(\mathbb{N})$ be the set of all non-void subset of $\mathbb{N}$ which contains at most n elements, where $n > 1$. Let the partial order relation on X be defined by $\leq$, i.e., for any $A, B \in X_0,\ A \leq B$ iff $A \subseteq B$. This is a partial order on X_0 (induced on $\mathcal{P}(\mathbb{N})$). The maximal element in X_0 are all the set which contains n elements. So there are infinite number of maximal element. And all the singleton set are the minimal element and the minimal element are also infinite.

Well-ordered Set

Definition

A poset in which each pair of elements

- (i) *has the lub is called an upper semi-lattice;*
- (ii) *has the glb is called a lower semi-lattice; and*
- (iii) *has both the lub and the glb are called a lattice.*

The question arises when can we say that a partially ordered set $(X, \leq)$ has a maximal element?

Well-ordered Set

Definition

A poset in which each pair of elements

(i) *has the lub is called an upper semi-lattice;*
(ii) *has the glb is called a lower semi-lattice; and*
(iii) *has both the lub and the glb are called a lattice.*

The question arises when can we say that a partially ordered set $(X, \leq)$ has a maximal element?

Lemma

(Zorn's Lemma) *Let $(X, \leq)$ be a poset such that each linearly ordered subset has a lub. Then X has a maximal element.*

Well-ordered Set

Definition

*Let $(X, \leq)$ be a poset. Then X is said to be **well-ordered set** (and $\leq$ an well ordering of X) iff each non-void subset of X has a least element.*

Note: any well-ordered set is a linearly ordered. Real line $\mathbb{R}$ or set of integers $\mathbb{Z}$ with usual linear ordering $\leq$ is not well-ordered. The set $\mathbb{Z}_{\geq 0}$ of all non-negative integers is well-ordered.

Theorem

Zermelo's Theorem: *Every non-void set can be well-ordered.*

Well-ordering theorem (above) $\iff$ Zorn's lemma.

Partition

Definition

Let X be a non-void set. Then a family $\mathcal{P}$ of subset of X is called a partition of X iff

1. *for each $A, B \in \mathcal{P}$ either $A = B$ or $A \cap B = \phi$*
2. $\bigcup\{A : A \in \mathcal{P}\} = X$.

Theorem

Let X be a non-void set and ρ be an equivalence relation on X. Let $(x) = \{y \in X : (x, y) \in \rho\}$. Then

1. *for each $x \in X$, $x \in (x)$*
2. *for each $x, y \in X$ either $(x) = (y)$ or $(x) \cap (y) = \phi$*
3. *if $\mathcal{P}(\rho) = \{(x) : x \in X\}$, then $\mathcal{P}(\rho)$ is a partition of X induced by ρ.*

Conversely, let $\mathcal{P}$ be a partition of X, then $\mathcal{P}$ generates an equivalence relation.

Example

Example

Let $X = \mathbb{Z}$ and n be a positive integer > 1.
Define ρ on $\mathbb{Z}$ by $(x, y) \in \rho$ iff $x - y = k.n$ i.e. $x - y$ is divisible by n.
Clearly, ρ is an equivalence relation. $(x, y) \in \rho$ iff x, y when divisible by n leaves the same remainder.

Division Algorithm: Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Then $\exists\,!$ integer $q\ ;\&\ r$ with $r \geq 0$ such that $a = b.q + r$, where $0 \leq r < |b|$.
Since there are exactly n possible remainders $0, 1, 2, \cdots, n-1$, so there are n equivalence classes, viz., $(0), (1), (2), \cdots, (n-1)$.
If $m \in \mathbb{Z},\ (m)$ must be one of the above classes.

Note: Let X be a non-void set and ρ be an equivalence relation on X. Then $\mathcal{P}(\rho)$ is usually denoted by X/ρ is called **qutioned set** of X by ρ.

Functions

Definition

*A **function** f on X to Y is a binary relation from X to Y s/t for each $x \in X,\ (x, y_1)\ \&\ (x, y_2) \in f\ \Rightarrow y_1 = y_2$.*

$$Domain\ of\ f := \{x \in X\ :\ (x, y) \in f\ for\ some\ y \in Y\}.$$

$$Range\ of\ f := \{y \in Y\ :\ (x, y) \in f\ for\ some\ x \in X\}.\}$$

If $(x, y) \in f$, then we write $y = f(x)$ and call y the image of x under f. Thus a function f is a correspondence which associates with each point of $x \in Domain\ f$ a ! element $y(= f(x)) \in Y$.

Our definition of function identifies a function with its graph, i.e.

$$f \equiv \{(x, y) \in X \times Y\ :\ y = f(x)\}.$$

If domain of $f = X$, we use the symbol $f : X \to Y$.

Functions

Definition

Let $f : X \to Y$ *and* $A \subseteq X,\ B \subseteq Y$*, then the direct image of* A *under* f *to be denoted by* $f(A)$ *is defined by*

$$\begin{aligned} f(A) &:= \{y \in Y \ :\ (x,y) \in f \ \ for\ some\ x \in A\} \\ &:= \{y \in Y \ :\ y = f(x)\ for\ some\ x \in A\} \end{aligned}$$

Inverse image of B *under* f *to be denoted by* $f^{-1}(B)$ *is defined by*

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

Functions

Definition

Let $f : X \to Y$ *and* $A \subseteq X,\ B \subseteq Y$*, then the direct image of* A *under* f *to be denoted by* $f(A)$ *is defined by*

$$\begin{aligned} f(A) &:= \{y \in Y : (x,y) \in f \text{ for some } x \in A\} \\ &:= \{y \in Y : y = f(x) \text{ for some } x \in A\} \end{aligned}$$

Inverse image of B *under* f *to be denoted by* $f^{-1}(B)$ *is defined by*

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

Example

Let $f : \mathbb{R} \to \mathbb{R},\ s/t,\ x \mapsto x^2$ *and* $A = (-2,4),\ B = (-1,4)$*. Therefore,* $f(A) = (0,16),\ f^{-1}(B) = (-2,2)$*. If* $C = (-2,-1),\ f^{-1}(C) = \phi$*.*

Functions

Theorem

Let $f : X \to Y$ be a function and let $A, B \subseteq X$ and $C, D \subseteq Y$. Then

1. (i) $f(A \cup B) = f(A) \cup f(B)$
2. (ii) $f(A \cap B) \subseteq f(A) \cap f(B)$
3. (iii) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$
4. (iv) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
5. (v) $f^{-1}(Y \setminus D) = X \setminus f^{-1}(D)$

Functions

Theorem

Let $f : X \to Y$ *be a function and let* $A,\ B \subseteq X$ *and* $C,\ D \subseteq Y$. *Then*

(i) $f(A \cup B) = f(A) \cup f(B)$

(ii) $f(A \cap B) \subseteq f(A) \cap f(B)$

(iii) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$

(iv) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

(v) $f^{-1}(Y \setminus D) = X \setminus f^{-1}(D)$

Example

Let $f : X \to Y$ *be not one-one. Then* $\exists\ x_1,\ x_2 \in X$ *s/t* $f(x_1) = f(x_2) = y$. *Let* $A = \{x_1\},\ B = \{x_2\}$. *Then* $A \cap B = \phi$ *and* $f(A) \cap f(B) = \{y\}$.

This gives us $f(A \cap B)(= \phi) \subset f(A) \cap f(B)(= \{y\})$.

Functions

Definition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. Then the composition $g \circ f$ is defined by

$$\begin{aligned} g \circ f &= \{(x,z) \in X \times Z \;:\; for\ some\ y \in Y\ s/t\ (x,y) \in f\ \&\ (y,z) \in g\} \\ &= \{(x,z) \in X \times Z \;:\; \exists\, y \in Y\ s/t\ y = f(x)\ \&\ z = g(y)\} \end{aligned}$$

Proposition

Let $f : X \to Y,\ g : Y \to Z,\ h : Z \to W$ be functions. Then $(h \circ g) \circ f = h \circ (g \circ f)$.

Functions

Definition

A function $f : X \to Y$ is said to be one-one or injective iff $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, i.e., iff image of distinct elements are distinct.

Definition

A function $f : X \to Y$ is said to be onto or surjective iff $f(X) = Y$, i.e., iff for each $y \in Y$ $\exists$ $x \in X$ s/t $f(x) = y$.

Note: Let $f : X \to Y$ be an injective function. Then f^{-1} is defined as a function on Y to X with $domain\ f^{-1} = range\ f$ and $range\ f^{-1} = domain\ f$.
Note: If $f : X \to Y$ is injective, $f^{-1} : range\ f \to X$ is also injective.

Exercise

If $f : X \to Y$ is injective and $A,\ B \subseteq X$, then $f(A \cap B) = f(A) \cap f(B)$.

Functions

Definition

A function $f : X \to Y$ is said to be bijective iff it is injective and surjective.

Proposition

Let $f : X \to Y$ and $g : Y \to Z$ be functions, then

- (i) $g \circ f$ *is injective if* $f,\ g$ *are injective,*
- (ii) $g \circ f$ *is surjective if* $g,\ f$ *are surjective,*
- (iii) $g \circ f$ *is bijective if* $g,\ f$ *are bijective,*
- (iv) *if* $f : X \to Y$ *be bijective, then* $f^{-1} : Y \to X$ *is bijective.*

Functions

Definition

Let X be a non-void set and let $T = \mathcal{P}(X) \setminus \phi$ be the collection of all non-void subset of X. Then a choice function on X is a function $c : T \to X$ s/t for each $A \in T,\ c(A) \in A$.

Functions

Definition

Let X be a non-void set and let $T = \mathcal{P}(X) \setminus \phi$ be the collection of all non-void subset of X. Then a choice function on X is a function $c : T \to X$ s/t for each $A \in T,\ c(A) \in A$.

Axiom

Axiom of Choice: *Every non-void set X admits a choice function.*

$$Zorn's\ lemma \Leftrightarrow Well\ ordering\ theorem \Leftrightarrow Axiom\ of\ choice$$

Countable Sets

Definition

(i) *Let* $J_n = \{1, 2, 3, \cdots, n\}$. *A set* X *is said to be* *finite* *iff either* $X = \phi$ *or* $\exists$ *for some* $n \in \mathbb{N}$ *and* $f : J_n \to X$ *s/t* f *is bijective. In the latter case,* $\#X = n$.

(ii) *A set* X *is said to be* *infinite* *if it is not finite.*

(iii) *A set* X *is said to be* *countable* (*enumerable*) *iff either* X *is finite or* $\exists$ *a bijection* $f : \mathbb{N} \xrightarrow{onto} X$.

Proposition

(i) *If* X *is countable and* $A \subseteq X$, *then* A *is countable.*

(ii) *A set* X $(\neq \phi)$ *is countable iff the elements of* X *can be arranged in infinite sequence* $\{x_1, x_2, x_3, \cdots\}$.

(iii) *If* X & Y *are countable, then* $X \times Y$ *is countable.*
More generally, if $X_1, X_2, \cdots, X_k$ *are finitely many countable sets then* $X_1 \times X_2 \times \cdots \times X_k$ *is also countable.*

Countable Sets

Proposition

(iv) *If* $\{X_n \ : \ n \in \mathbb{N}\}$ *is a countable collection of countable set then* $\bigcup_{n=1}^{\infty} X_n$ *is countable, i.e. countable union of countable sets is countable.*

(v) *The set of all rationals,* $\mathbb{Q}$*, is countable.*

Countable Sets

Theorem

The set of all integers Z, is a countably infinite set.

Countable Sets

Theorem

The set of all integers Z, is a countably infinite set.

Proof.

Define a function $f : \mathbb{N} \to \mathbb{Z}$ as follows:

$$f(n) = \begin{cases} 0, & when \quad n = 1, \\ \frac{n}{2}, & when \quad n \text{ is even} \\ -\frac{n-1}{2}, & when \quad n \text{ is odd } \& \; n > 1 \end{cases}$$

□

Countable Sets

Theorem

Prove that $\mathbb{N} \times \mathbb{N}$ *is countable.*

Countable Sets

Theorem

Prove that $\mathbb{N} \times \mathbb{N}$ is countable.

Proof.

$$\begin{array}{ccccc}
(0,0) & (1,0) & (2,0) & (3,0) & \cdots \\
(0,1) & (1,1) & (2,1) & (3,1) & \cdots \\
(0,2) & (1,2) & (2,2) & (3,2) & \cdots \\
(0,3) & (1,3) & (2,3) & (3,3) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

$\square$

Countable Sets

Theorem

Prove that $\mathbb{N} \times \mathbb{N}$ is countable.

Proof.

$$\begin{array}{ccccc}
(0,0) & (1,0) & (2,0) & (3,0) & \cdots \\
(0,1) & (1,1) & (2,1) & (3,1) & \cdots \\
(0,2) & (1,2) & (2,2) & (3,2) & \cdots \\
(0,3) & (1,3) & (2,3) & (3,3) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

$\square$

$$\{(0,0),(0,1),(1,0),(0,2),(1,1),(2,0),\ldots\}$$

Prove that set of positive rational numbers is countable.

Countable & Uncountable Sets

Theorem

$[0,1]$ *is uncountable and hence* $\mathbb{R}$ *is uncountable.*

Countable & Uncountable Sets

Theorem

$[0, 1]$ *is uncountable and hence* $\mathbb{R}$ *is uncountable.*

Theorem

Let X *be any countable set and* $f : X \to Y$ *be a surjection. Then* Y *is also countable.*

Exercise

Let X $(\neq \phi)$ *be a countable set. Then the collection of all finite sequence of elements of* X *is also countable. The collection of all finite subset of* X *is also countable.*

Countable & Uncountable Sets

Definition

An element $x \in \mathbb{C}$ is said to be algebraic number (or algebraic integer) iff it satisfies a polynomial equations

$$a_0 + a_1 x + \cdots + a_n x^n = 0$$

with rational (or integer) coefficient ($a_n \neq 0$).

Exercise

Show that the set of all algebraic numbers is countable and contains $\mathbb{Q}$.

Exercise

Let X be any infinite set. Then $\exists$ a countably infinite subset T of X s/t there is a bijection from $X \setminus T$ onto X.

Countable & Uncountable Sets

Exercise

If X be a finite set and $f : X \to X$ is surjective (or injective) then f is bijective.

Countable & Uncountable Sets

Exercise

If X be a finite set and $f : X \to X$ is surjective (or injective) then f is bijective.

Exercise

Construct counter examples to prove that the above is not true for both the cases if X is a infinite set.

Countable & Uncountable Sets

Example

(i) *Consider the function* $f : \mathbb{N} \to \mathbb{N}$ *defined by*

$$\begin{aligned} f(1) &= 1 && = f(2) \\ f(n) &= n - 1 && \forall\, n \geq 3 \end{aligned}$$

Then f *is surjective but not injective.*

(ii) *Consider the function* $g : \mathbb{N} \to \mathbb{N}$ *defined by*

$$g(n) = n + 1$$

Then g *is injective but not surjective.*

Countable & Uncountable Sets

Theorem

Schröder-Bernstine *If* A, B *be non-void sets,* $f : A \to B$ *be an injective and* $g : B \to A$ *be an injective functions then* $\exists$ *a bijection* $h : A \xrightarrow{onto} B$.

Countable & Uncountable Sets

Example

Show that there is a bijection $f : [0, 1] \overset{onto}{\rightarrow} (0, 1)$.

Countable & Uncountable Sets

Example

Show that there is a bijection $f : [0,1] \xrightarrow{onto} (0,1)$.

Solution

Consider the mapping $h : (0,1) \to [0,1]$ *given by* $x \mapsto x$. *Then* h *is injection.*

Define $g : [0,1] \to (0,1)$ *given by* $x \mapsto \frac{1}{2}x + \frac{1}{4}$.

Then g *is injection.*

So by Schröder-Bernstine theorem $\exists$ *a bijection* $f : [0,1] \xrightarrow{onto} (0,1)$.

Countable & Uncountable Sets

Exercise

Show that there is a bijection $f : \mathbb{R} \to (-1, 1)$

Exercise

Show that if I *be any non-degenerate interval of* $\mathbb{R}$ *then there is a bijection of* $\mathbb{R}$ *onto* I.

Countable & Uncountable Sets

- Let X is a finite set of n elements then $|X| = n$. The concept of countability accommodates more infinite sets for determination of their cardinality; e.g., $|\mathbb{N}| = |\mathbb{Q}| = \aleph_0$. The cardinal number $\aleph_0$ or c of an infinite set X asserts that the set is countable or uncountable, respectively.
- The cardinal number of an infinite set is called a transfinite cardinal number.

Proposition

$\aleph_0$ *is the smallest transfinite cardinal number.*

Countable & Uncountable Sets

Continuum Hypothesis

We have shown the existence of three distinct transfinite cardinal numbers $\aleph_0, c$ and 2^c s/t $\aleph_0 < c < 2^c$. We now state the following natural questions which are still unsolved:

Unsolved Problem 1 Does there exist any cardinal number α such that $\aleph_0 < \alpha < c$?

Unsolved Problem 2 Does there exist any cardinal number β such that $c < \beta < 2^c$?

The End

Thanks a lot for your attention!