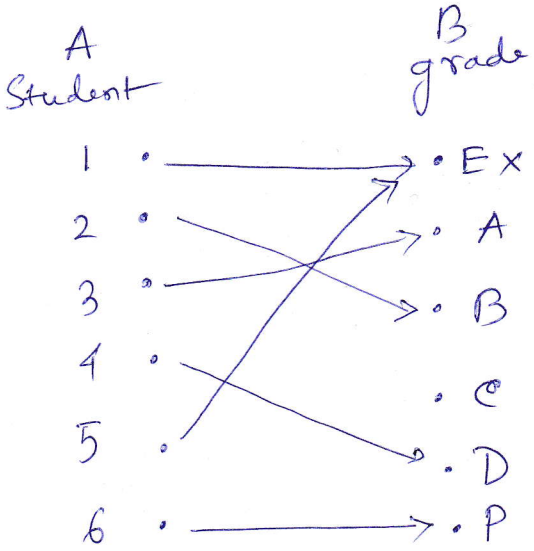
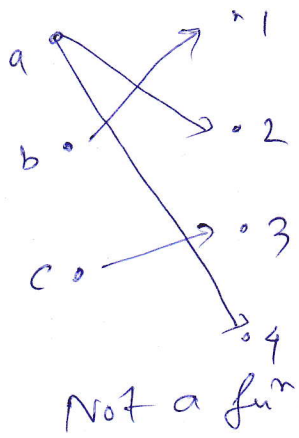
Functions

- Let A & B be nonempty sets.
- $f: A \to B$ is a fun. which is an assignment of exactly one element of B to each element of A.

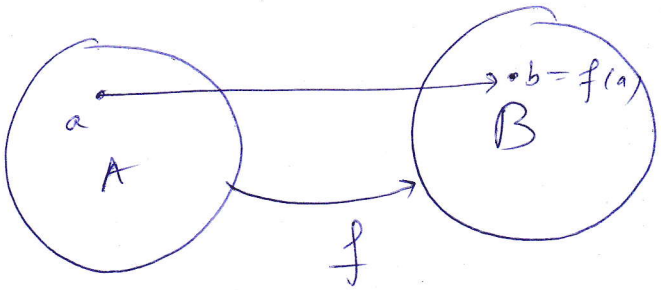




Not a fun.

each Student is assigned exactly one grade.

- function or mapping or ~~treaf~~ transformation.



$f(a) = b$.

- b is the image of a
- a is a preimage of b.

f maps A to B.

↓ domain ↓ co-domain.

- domain
- Codomain
- range → Set of all images of elements of A. $(f(A))$

- $f: A \to B$, $S \subseteq A$

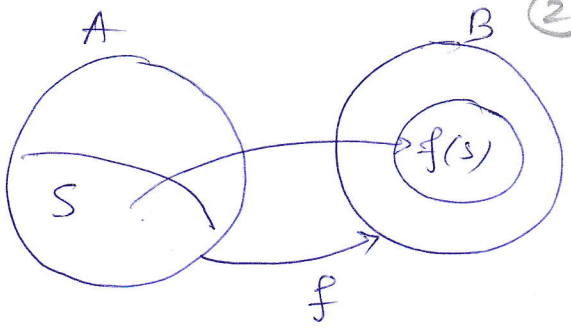


image of S under f

$f(S) \subseteq B$

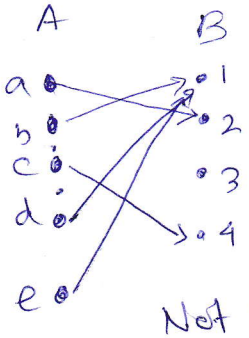
↙ Consisting of images of the elements of S.

$$f(S) = \{ t \in B \mid t = f(s) \text{ for some } s \in S \}.$$

↙ notation, not the value of f for the set S.

$$= \{ f(s) \mid s \in S \}.$$

Example:



$S = \{b, c, d\}$

$f(S) = \{1, 4\}$

Not one-to-one

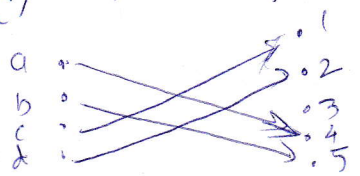
injective or **One-to-one fn.**

- f is injective iff $[f(a) = f(b) \Rightarrow a = b \quad \forall a, b \text{ in the domain of } f]$
- f injective if it is one-to-one.

Example: $f(x) = x^2$ $f: \mathbb{Z} \to \mathbb{Z}$ not one-to-one as

$f(1) = 1^2 = f(-1)$ but $1 \neq -1$.

Example:



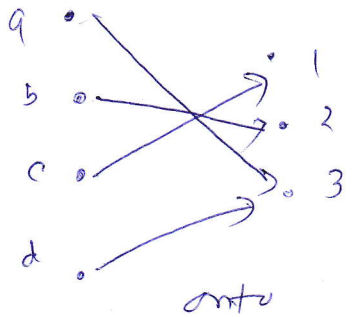
one-to-one

- A fun. that is strictly increasing or strictly decreasing must be one-to-one.
  $\forall x \forall y\ (x < y \rightarrow f(x) < f(y))$
- A fun. that is increasing, but not strictly increasing or decreasing, but no strictly decreasing, is not necessarily one-to-one.

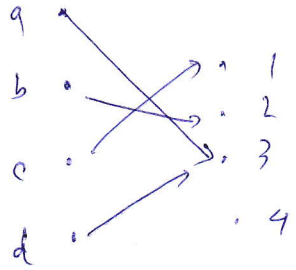
Surjection or onto fun. (the range & the codomain equal)

- $f: A \rightarrow B$ is onto or surjective, iff for every element $b \in B$, there is an element $a \in A$ with $f(a) = b$.
- f surjection if it is onto.

Example:



onto



not onto.

Example: $f(x) = x^2$ not onto as no integer x with $x^2 = -1$.

$f: \mathbb{Z} \rightarrow \mathbb{Z}$

Bijection or one-to-one correspondence

f is bijection iff it is both one-to-one & onto

Example: $f(x) = x + 1$.

one-to-one as

$f(x) = f(y)$ i.e. $x+1 = y+1$

$\Rightarrow x = y$.

or

$x \neq y \Rightarrow x+1 \neq y+1$

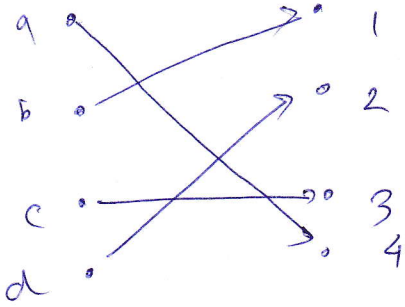
$\Rightarrow f(x) \neq f(y)$

onto as

$f(x) = y$ iff $x+1 = y$

i.e. iff $x = y-1$.

Example:

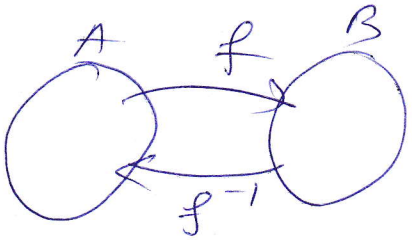


one-to-one & onto.

Example identity fun. on A $f: A \to A$

$f(x) = x$

bijection.



Inverse fun.

- f is a bijection from A to B
- $f^{-1}: B \to A$ defined as

  $f^{-1}(b) = a$ when $f(a) = b$.

  assigns $b \in B$ to the unique elem $a \in A$ s.t. $f(a) = b$.

Example: $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x+1$ invertible $f^{-1}(y) = y-1$.

Example: $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$

not invertible as not one-to-one

$f(2) = 4 = f(-2)$ but $2 \neq -2$

Example: $f: \mathbb{R}^+ \to \mathbb{R}^+$ defined by $f(x) = x^2$

- one-to-one as $x^2 = y^2 \Rightarrow (x+y)(x-y) = 0$

$\Rightarrow x = y$ as x, y non-negative

- onto as each non-negative real no. has a square root.

$f(x) = x^2 = y \Rightarrow x = \sqrt{y}$

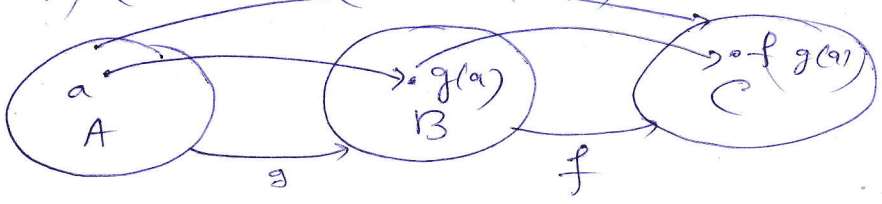
So f is a bijection.

Compositions of functions

- $g: A \to B$, $f: B \to C$ two functions.

The composition of f & g, denoted by $f \circ g$, is defined by

$$(f \circ g)(a) = f(g(a))$$



Example: $f(x) = 2x+3, \quad g(x) = 3x+2$

$(f \circ g)(x) = ?$ $\quad (g \circ f)(x) = ?$

$f : Z \to Z, \; g : Z \to Z$.

$(f \circ g)(x) = f(g(x)) = f(3x+2) = 2(3x+2)+3 = 6x+7$

$(g \circ f)(x) = g(f(x)) = g(2x+3) = 3(2x+3)+2 = 6x+11$

Example $\quad (f^{-1} \circ f)(a) = a \qquad f : A \to B$

$f^{-1} : B \to A$.

$(f \circ f^{-1})(a) = a$.

$f^{-1} \circ f$ = identity fun: on the set A

$f \circ f^{-1}$ = identity fun: on the set B.

Russell's paradox

let S be the set of all sets that do not include themselves.
Does S contain itself ?

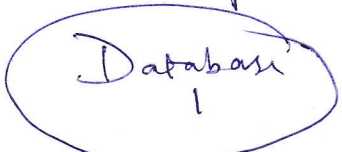
$$S = \{x \mid x \notin x\}$$, domain be the set of all sets.

- Suppose S is not a member of itself.
  Then S satisfies the predicate in the definition & hence S is a member of itself, contradiction

- Suppose S is a member of itself.
  Then the predicate in the difinition is not satisfied & hence S is not a member of itself ; contradiction

Illustration of Russell's paradox

- Suppose every library in the US is preparing a database of all its collections.
- from around the country, all the databases are submitted to the library of Congress.
- Now the national librarian starts to sort through the database and found some of the databases include themselves in the listing, while others do not.
- She compiles two master databases



that include themselves

that do not include themselves.

- However, the national librarian is doomed with the database that does not list itself.
  - Cannot make a database that dont include themselves.
- Where to put database 2 ?
  - if it is listed, then the resulting database would include itself & belongs to database 1 that do include themselves., a contradiction as database 2 dont include themselves
  - if it is not listed, then the database is incomplete.
  - Either way it can never be a true database that do not list themselves.
- $S = \{x \mid x \notin x\}$ Such a set is not well defined.
- Russell's paradox showed inconcistencies in set theory.
- Resolved by having levels of sets.
- Sets exist in hierarchy.

Cardinality of an infinite set (Dedekind, 1888)

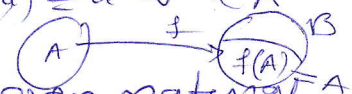
- if A & B are infinite sets, and $A \subset B$, then $|A| = |B|$.

For finite sets, $A \subset B \Rightarrow |A| < |B|$

True??

$f : A \to B$

$f(a) = a \quad \forall a \in A$



Example: Show that there is as many even natural numbers as there are natural numbers.

1-1 cor

$$N = \{1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots, n, \ldots\}$$
$$E = \{2, 4, 6, 8, 10, 12, 14, 16, 18, \ldots, 2n, \ldots\}$$

- But this seems rather odd.

Q) Does not the set E have exactly half the number of elements of N?

Galileo's Th

One can think this way:

if we take all of the even natural nos. & we divide them all by 2, then we would get the set of natural nos.

Hence their cardinality must be the same.

- infinity is a strange concept.
  - a part may be equal to the whole world.
- infinity (∞) — An unbounded quantity or a quantity that is not finite.

S ⊂ T
|S| = |T|
S ⊊ T
S ⊊ P(S)

Example: (finite coffee beans)

- dark & light-roasted coffee beans.
- Without counting them explicitly, is there an equal # of dark roast & light-roast coffee beans?
- match each dark roast bean with a light roast bean
  - → match found; answer YES
  - → unable to match, answer NO
    (cardinality of the dark & light roast coffee beans not the same)

1-1 cor.

Example (1-to-1 correspondence)

Squared nos, which is a proper subset of $\mathbb{N}$, can be paired with every natural nos.

$$\mathbb{N} = \{ 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad \cdots \quad n \quad \cdots \}$$
$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$
$$S = \{ 1 \quad 4 \quad 9 \quad 16 \quad 15 \quad 36 \quad 49 \quad \cdots \quad n^2 \quad \cdots \}$$

- pair the nos. of the two sets so that
  - each no. in S is paired with another no. in $\mathbb{N}$
  - no no. in either set — are left along or are paired to multiple nos.
- if we can do this, then $|S| = |\mathbb{N}|$.
- The idea of pairing in mathematics is called establishing a 1-to-1 correspondence.

Example:

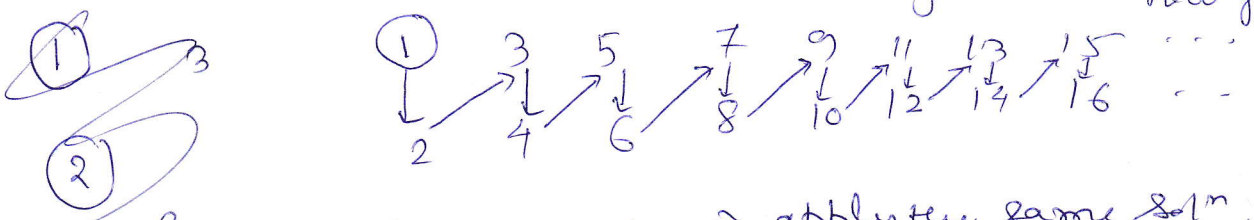
Hilbert's Hotel

- At Hilbert hotel, there is an infinite no. of rooms numbered $1, 2, 3, 4, 5, \ldots$, in each of which a guest is staying.
- if a new traveller arrives at the hotel & would like a room, would the innkeeper still be able to accommodate him?

Finite Hotel

- an innkeeper has a finite # of rooms, say 100, all occupied, each room has a single guest.
- new traveler arrives → cannot accommodate him.

Making room available for new guest



- Any finite no. of new guests → apply the same soln.
- No room shortage in the world of infinite no. of rooms & guests.
- if you were a guest at Hilbert's Hotel, it is unlikely you will get much sleep on account of you moving at any time to make more room for another guest.

- Mathematics with transfinite nos. behave strangly.

Rules of addition

$$\aleph_0 + 1 = \aleph_0$$

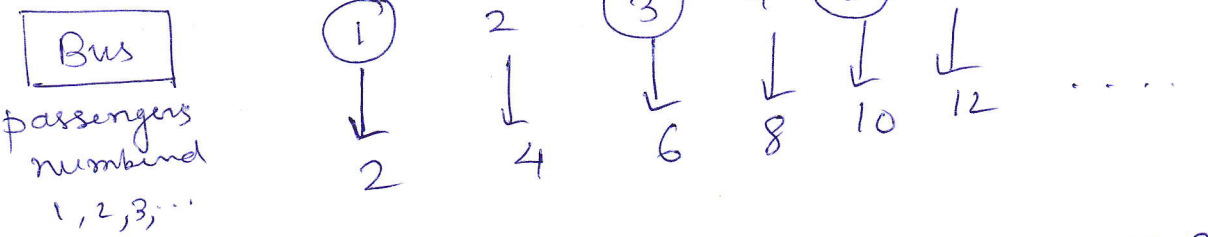
$$\aleph_0 + 2 = \aleph_0$$

$$\aleph_0 + \aleph_0 = \aleph_0$$

Example: (An infinite bus arrives at Hilbert's Hotel)

At Hilbert's Hotel with an infinite no. of rooms, a bus arrives carrying an infinite number of people who each require a room.
Would the inkeeper still be able to accommodate all of these infinitely many guests?

Make odd numbered rooms available.



- guest already in room n is asked to move to room $2n$
- passenger n will receive room $2n-1$.

Rules of multiplication

$$\aleph_0 \times 1 = \aleph_0$$

$$\aleph_0 \times 2 = \aleph_0$$

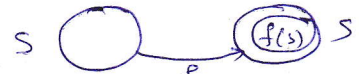
$$\vdots$$

$$\aleph_0 \times \aleph_0 = \aleph_0$$

Def^n A set S is finite with cardinality $n \in \mathbb{N}$ if there is a bijection from the set $\{0, 1, \ldots, n-1\}$ to S.

- infinite set → when the set is not finite.

Def^n A set S is infinite if there exists an injection $f : S \to S$ such that $f(S)$ is a proper subset of S.



Theorem The set $\mathbb{N}$ of natural numbers is an infinite set

Proof Consider an injection $f : \mathbb{N} \to \mathbb{N}$ defined as

$$f(x) = 3x.$$

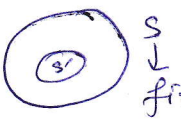
Then $f(\mathbb{N}) = \{3, 6, 9, 12, \ldots\} \subset \mathbb{N} = \{1, 2, 3, \ldots\}$

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

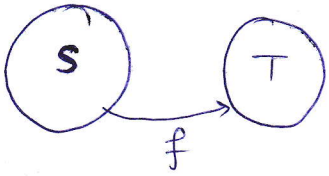
Facts:

- if S' is infinite and is a subset of S, then S is infinite

- every subset of a finite set is finite.



- if $f : S \to T$ is an injection and S is infinite, then T is infinite.



- if S is infinite set, then $P(S)$ is infinite.

- if S and T are infinite set, then $S \cup T$ is infinite
- if S is infinite and $T \neq \emptyset$, then $S \times T$ is infinite
- if S is infinite and $T \neq \emptyset$, then the set of fns from T to S is infinite.

How to compare infinite sets?

- Cantor developed a technique for measuring the size or cardinality of infinite as well as finite sets.
- infinite sets (2 groups) → having the same cardinality as the set of natural nos. (Countable)
  → having different cardinality (uncountable)

Defn

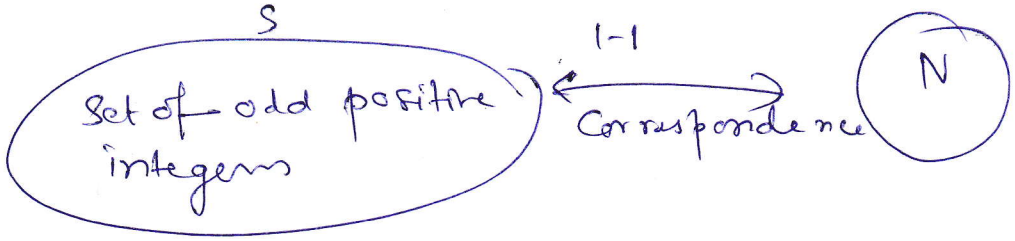
- A set that is either finite or has the same cardinality as the set of positive integers is called countable.
- A set that is not countable is called uncountable.
- When a set is countable, we denote its cardinality by $\aleph_0$ (aleph null)

(Countable sets)

Example Set of odd integer is countable
Set of integer is countable.
Set of the rational nos. Q is countable.

Example: Show that the set of odd positive integers is a countable set.

Soln:



Consider the fn, $f(n) = 2n - 1$.

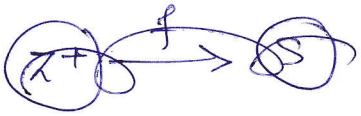
$$f : Z^+ \longrightarrow S$$

- **f one-to-one**

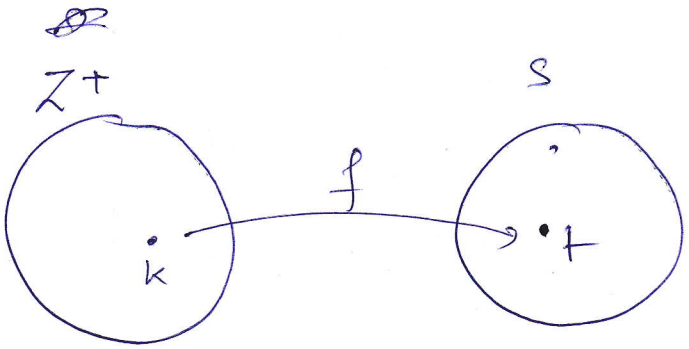
Suppose $f(n) = f(m)$

Then $2n - 1 = 2m - 1$

$\Rightarrow n = m$. $\Rightarrow$ f is injective



- **f onto**



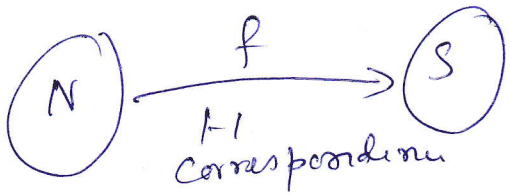
$t \in S \Rightarrow t = 2k - 1$ for some natural no. k.

i.e. t is an odd +ve integer.

$\Rightarrow t = f(k)$

$\Rightarrow$ f is Surjective.

FACT | An infinite set is countable iff it is possible to list the elements of the set in a sequence (indexed by +ve integers).



can be expressed as a sequence $a_1, a_2, \ldots, a_n, \ldots$ where

$a_1 = f(1)$
$a_2 = f(2)$
$a_3 = f(3)$
$\vdots$
$a_n = f(n)$
$\vdots$

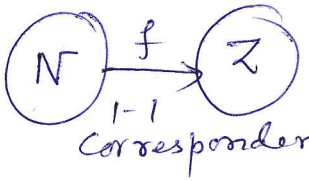
1	2	3	4	5	6	7 ...
↕	↕	↕	↕	↕	↕	↕
1	3	5	7	9	11	13 ...

- Example: Set of odd integers can be listed in a sequence $\{a_n\}$ where $a_n = 2n-1$.

Example: Show that the set of all integers is countable.

Soln:

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ -\frac{(n-1)}{2} & \text{if } n \text{ is odd} \end{cases}$$



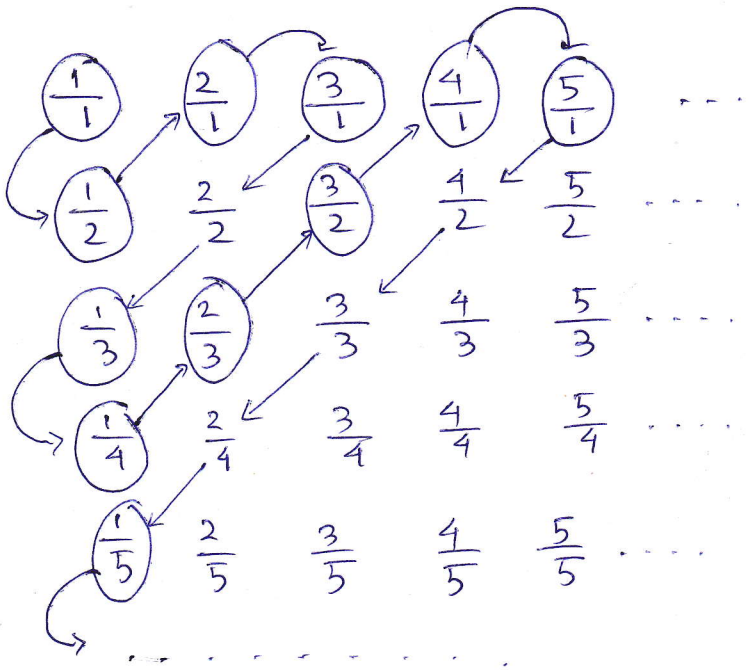
1 2 3 4 5 6 7

$0, 1, -1, 2, -2, 3, -3, \ldots \rightarrow$ list of all integers in a sequence

Example: Show that the set of positive rational nos. is countable.

Soln: $\frac{p}{q}$, p, q positive integer.

- arrange all the +ve rational nos. by listing
  - those with $q = 1$ in the 1st. row,
  - those with $q = 2$ in the 2nd. row,
  - and so on.



- now list all the rational nos. in a sequence as follows.
  - first list +ve rational nos. $\frac{p}{q}$ with $p+q=2$,
  - followed by those with $p+q=3$,
  - followed by those with $p+q=4$,
  - and so on.
- Whenever we encounter a no. $\frac{p}{q}$ that is already listed, we do not list it again.

Example (Uncountable)

Show that the set of real numbers is an uncountable set.

Proof: (by contradiction)

Let the set of real numbers is countable.

Then the subset of all real nos. in $[0,1]$ is also countable.

Therefore, the real nos. in $[0,1]$ can be listed in some order, say $r_1, r_2, r_3 \ldots$

Let the decimal representation of these real nos. be

$r_1 = .d_{11} d_{12} d_{13} d_{14} \ldots$

$r_2 = .d_{21} d_{22} d_{23} d_{24} \ldots$

$r_3 = .d_{31} d_{32} d_{33} d_{34} \ldots$

$r_4 = .d_{41} d_{42} d_{43} d_{44} \ldots$

$\vdots$

where $d_{ij} \in \{0,1,2,\ldots,9\}$.

If you draw the diagonal through the 1-1 correspondence as indicated, then we can construct a decimal no. as follows:

Claim Any subset of a countable set is also countable.

Claim B is countable

A countable

$B \subseteq A$

- if not, [illegible] no listing of elements of B in a seq.
- Also elements of A

So no listing of elements of A in a seq. ($\rightarrow\leftarrow$) as A is countable

if B infinite

$A = \{a_1, a_2, \ldots\}$

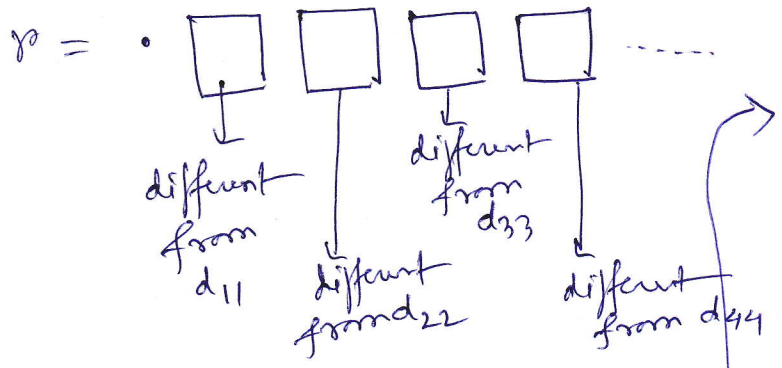
↓

Take the subseq. consisting of elements of B

↓

$B = \{a_{i_1}, a_{i_2}, \ldots, a_{i_k}, \ldots\}$ → countable.

if B finite → countable



This new decimal no. r is different from any decimal no. listed in the 1-1 correspondence since it differs in at least one decimal place.

Thus r is not in the list.

Since we found (or constructed) a no. that is not in the correspondence between the reals & the natural nos., we have arrived at our contradiction.

Hence the set of real nos. in $[0,1]$ is uncountable.

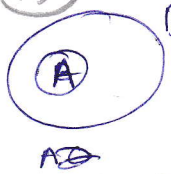
Hence the set of real nos. is uncountable.

claim Any set with an uncountable subset is uncountable. → i.e. any superset of an uncountable set is uncountable

(19)

$A \subseteq B$

↙ uncountable

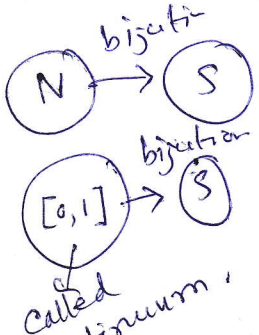


Claim: B uncountable

- if not, then ∃ a seq. $\{b_n\}$ listing all elements of B. ~~$\{b_n\}$ gives a listing~~
- A subsequence of $\{b_n\}$ consisting of elements of A gives a listing of A (→←) as A is uncountable

- Cantor Diagonalization argument. $\aleph$ → first letter of the Hebrew alphabet

Cardinality of $\mathbb{N}$ → $\aleph_0$ (aleph null)



Cardinality of a countable set S = cardinality of $\mathbb{N} = \aleph_0$

Cardinality of an uncountable set S = $\mathfrak{c}$ (continuum)

$\aleph_0 < \aleph_1 < \aleph_2 < \cdots$

$|\mathbb{N}| = \aleph_0$

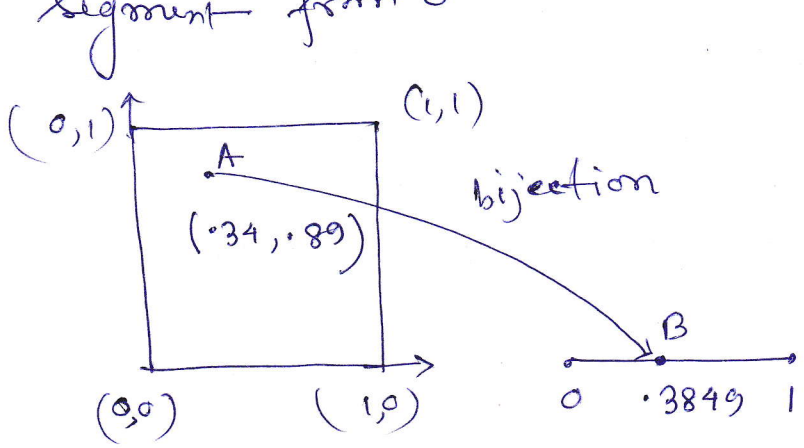
$|P(\mathbb{N})| = \aleph_1 = 2^{\aleph_0}$

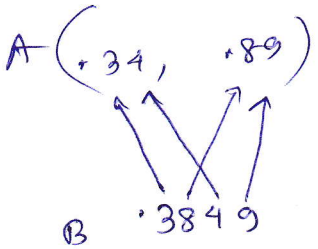
$|P(P(\mathbb{N}))| = \aleph_2 = 2^{\aleph_1}$

} transfinite nos. (invented by Cantor).

Other consequences

We can set up a 1-1 correspondence of all the pts. in the interior of a square & the set of pts. in a line segment from 0 to 1





mapping a pt. in a square to a line segment.

This means $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ has the same cardinality as $\mathbb{R}$.

$\Rightarrow |\mathbb{R}^2| = |\mathbb{R}|$.

Discrete mathematics → the study of finite & countable objects & sets.

Cardinal numbers → used to measure the size of a set.

Defn (Enumeration)
Let S be a set. An enumeration of S is a surjective fun. f from initial line segment of $\mathbb{N}$ to S.
- if f is injective also, then f is an enumeration without repetitions.

- if f is not injective, then f is an enumeration with repetitions.

Fact | A set S is countable iff there exists an enumeration of S.

Example: S = the set of natural nos. of the form $3n$, $n \in N$.

- $\langle 0, 3, 6, 9, \ldots \rangle$ is an enumeration of S defined by $f(n) = 3n$
- $\langle \overbrace{6, 3, 0}^{k=0}, \overbrace{15, 12, 9}^{k=1}, \ldots \rangle$ is also an enumeration of S defined by

$$f(n) = \begin{cases} 3n+6 & \text{if } n = 3k \text{ for some } k \in N \\ 3n & \text{if } n = 3k+1 \text{ for some } k \in N \\ 3n-6 & \text{if } n = 3k+2 \text{ for some } k \in N \end{cases}$$

$k=2 \rightarrow$ 24, 21, 18

$k=3 \rightarrow$ 33, 30, 27.

Example: Let $\Sigma = \{a, b\}$.

The set of strings Σ^* over $\Sigma = \{a, b\}$ is a countably infinite set.

An enumeration τ of Σ^*

$\tau(0) = \varepsilon$
$\tau(1) = a$
$\tau(2) = b$
$\tau(3) = aa$
$\tau(4) = ab$
$\tau(5) = ba$
$\tau(6) = ba$

Theorem

~~Example:~~ Every infinite set contains a countably infinite subset.

proof Let S be an infinite set.

Select a sequence of elements $\{a_n\}_{n=0}^{\infty}$ from S as follows:

Select a_0 from S
Select a_1 from $S - \{a_0\}$
Select a_2 from $S - \{a_0, a_1\}$
Select a_3 from $S - \{a_0, a_1, a_2\}$
& so on.

a_{i+1} is selected from $S - \{a_0, a_1, \cdots, a_i\}$.

each $S - \{a_0, a_1, \cdots, a_i\}$ is infinite, otherwise $\left(S - \{a_0, a_1, \cdots, a_i\}\right) \cup \{a_0, a_1, \cdots, a_i\} = S$ will be finite.

This set $\{a_0, a_1, \cdots\}$ is a countable infinite subset of S

* **Example** The set of all +ve rational nos. is countable.

$\frac{p}{q}$, p, q prime to each other.

- Q^+ → the set of all +ve rational nos.
- $A = \{(p,q) \mid (p,q) \in N \times N, p, q \text{ prime to each other}\}$
- 1-1 Correspondence between Q^+ & A $\Rightarrow$ Q^+ countable iff A countable

As A is a subset of countable set $N \times N$, A is countable $\Rightarrow$ Q^+ is countable

direct proof
Let $A_n = \{\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots\}$ each is countable
$\bigcup_{n=1}^{\infty} A_n$ countable $\Rightarrow Q$.

* **Example:** Q^- countable as it can be put in 1-1 correspondence with Q^+

Example: Q is countable as $Q = Q^+ \cup Q^- \cup \{0\}$.
(each countable)

Theorem The union of a countable collection of countable sets is countable.

Proof Let $S_0, S_1, S_2, \ldots$ be a countable collection of countable sets and

$$S_i = \langle a_{i0}, a_{i1}, a_{i2}, \ldots \rangle .$$

$$\begin{aligned} S_0 &: (a_{00} \quad a_{01} \quad a_{02} \quad a_{03} \cdots) \\ S_1 &: (a_{10} \quad a_{11} \quad a_{12} \quad a_{13} \cdots) \\ S_2 &: (a_{20} \quad a_{21} \quad a_{22} \quad a_{23} \cdots) \\ S_3 &: (a_{30} \quad a_{31} \quad a_{32} \quad a_{33} \cdots) \end{aligned}$$

~~Enumeration~~

Enumerate the elements as shown in the diagram.

Let $b_0, b_1, b_2, \ldots$ be the sequence of elements.

arranged according to height $i+j$

$$\begin{aligned} b_0 &= a_{00} \\ b_1 &= a_{01} \\ b_2 &= a_{10} \\ b_3 &= a_{02} \\ b_4 &= a_{11} \\ b_5 &= a_{20} \\ &\text{and so on.} \end{aligned}$$

$a_{ij} \rightarrow$ having height $i+j$

$(2,3) \rightarrow \frac{1}{2} \times 4^2 \times 3 + 2 = 8$

$(1,1) \rightarrow \frac{1}{2} \times 0 + 1 = 1$

$(1,3) \rightarrow \frac{1}{2} \times 3^2 + 1 = 4$

$(1,2) \rightarrow \frac{1}{2} \times 2^2 + 1 = 3$

This is an enumeration of the elements of $\bigcup_{i=0}^{\infty} S_i$ & hence $\bigcup_{i=0}^{\infty} S_i$ is countable

Let $A_n = \{(1,1), (1,2), (1,3), \ldots, (n,n)\}$

$\Rightarrow N \times N = \bigcup A_n$ countable. → countable

$n=1$

$(i,j) \rightarrow \frac{1}{2}(i+j-1)(i+j-2) + i$

$(1,1) \quad (1,2) \quad (1,3) \quad (1,4) \cdots$

$1 \quad 2 \quad 4 \quad 7$

* **Example** $N \times N$ is countable.

Theorem Let Σ be a finite alphabet and Σ^* the set of all strings over Σ. Then $P(\Sigma^*)$ is uncountable.

Proof (by contradiction).

As Σ^* is countable, let $\langle x_0, x_1, x_2, \ldots \rangle$ be an enumeration of strings in Σ^*.

If possible, let $\langle A_0, A_1, A_2, \ldots \rangle$ be an enumeration of the sets in $P(\Sigma^*)$.

Construct a binary matrix M as follows:

enumeration of $P(\Sigma^*)$ \ x_i	x_0	x_1	x_2	...
A_0	a_{00}	a_{01}	a_{02}	...
A_1	a_{10}	a_{11}	a_{12}	...
A_2	a_{20}	a_{21}	a_{22}	...
⋮	⋮	⋮	⋮	

$$a_{ij} = \begin{cases} 1 & \text{if } x_j \in A_i \\ 0 & \text{o.w.} \end{cases}$$

$a_{ii} = 1 \Rightarrow x_i \in A_i, x_i \notin A$

$a_{ii} = 0 \Rightarrow x_i \in A, x_i \notin A_i$

x_i either $\in A$ or $\in A_i$, $\neq i$

Now construct a set A as follows:

$x_i \in A$ if $a_{ii} = 0$

i.e. if $x_i \notin A_i$

$$A = \{ x_i \mid x_i \notin A_i, i \in N \}.$$

Then A cannot be any A_j & hence cannot appear in the enumeration $\langle A_0, A_1, \ldots \rangle$ even though $A \in P(\Sigma^*)$.

A consists of strings x_i s.t. $a_{ii} = 0$
So $x_i \in A \Rightarrow a_{ii} = 0 \Rightarrow x_i \notin A_i$

Hence we cannot have an enumeration of the sets in $P(\Sigma^*)$ & so $P(\Sigma^*)$ is an uncountable set.

$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph_0$; $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}| \overset{?}{=} \aleph_0$ ($\aleph_0$)

Q> Can we compare cardinality of uncountable sets?

- $[0,1]$ uncountable
- $P(\Sigma^*)$ uncountable.

- $[a,b)$ uncountable
  $c = |[0,1]| \overset{?}{=} |[a,b]|$ (YES)
  $f(x) = \frac{x-a}{b-a}$; $a \le x \le b \Rightarrow 0 \le f(x) \le 1$

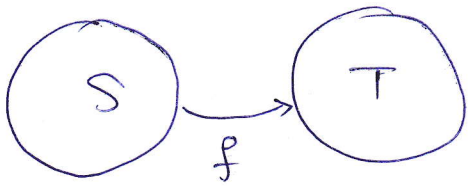
Are there uncountable sets X_1 & X_2 s.t. $|X_1| \le |X_2|$?

$|\Sigma^*| = \aleph_0$ (countable) ; $|P(\Sigma^*)| = \aleph_1$

Defn $[0,1]$ is often called continuum.

- if there is a bijection from $[0,1]$ to a set S, then S is said to have cardinality c.

Defn Let S & T be two sets.
Then S & T are equipotent or have the same cardinality denoted by $|S| = |T|$, if there is a bijection from S to T.



bijection

$|S| = |T|$.

Theorem Equipotence is an equivalence relation over any collection of sets.

Defn
- $|S| \le |T|$ if there is an injection from S to T
- $|S| < |T|$ if there is an injection from S to T, but no bijection from S to T

- either $|S| < |T|$ or $|S| = |T|$ or $|S| > |T|$
- $|S| \le |T|$ & $|T| \le |S| \Rightarrow |S| = |T|$.

Theorem. Let S be a finite set.

Then $|S| < \aleph_0 < c$.

Proof. Let $|S| = n$, $\boxed{Z_n = \{0, 1, \ldots, n-1\}}$.

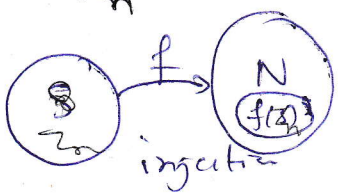
$|S| = |Z_n|$.

Then there is an injection $f : Z_n \to N$ defined by $f(x) = x + 1$

(so an injection from $S \to N$)

But we cannot have a bijection from $N \to Z_n$ as Z_n is finite set

Hence $|S| = |Z_n| < |N| = \aleph_0$



Also there is no bijection from $[0,1]$ to N

as $[0,1]$ is uncountable.

But we can have an injection from N to $[0,1]$

defined as $f(n) = \frac{1}{n+2}$

$\boxed{\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} \end{array}}$

Hence $|N| < |[0,1]| = c$

or $\aleph_0 < c$

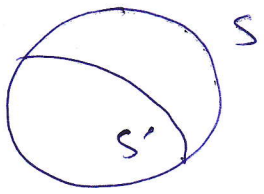
Theorem

If S is an infinite set, then $\aleph_0 \leq |S|$.

proof: if S is infinite, then S contains a countably infinite subset S'.

Consider the mapping $f: S' \to S$ defined as

$$f(x) = x \quad \forall x \in S'$$



f is an injection from S' to S

$f(S') = S' \subseteq S$

Hence, $|S'| \leq |S|$

As S' is countable, $|S'| = \aleph_0$

Hence $|S| \geq \aleph_0$

Theorem. Let S be a set.

Then $|S| < |P(S)|$.

proof: Consider the injection $f: S \to P(S)$ defined as

$$f(a) = \{a\} \text{ for all } a \in S.$$

As we have an injection from $S \to P(S)$, we ha

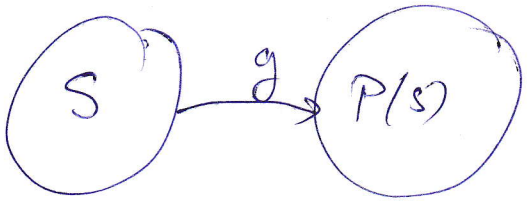
$$|S| \leq |P(S)|$$

Claim $|S| \neq |P(S)|$.

Let g be an arbitrary fun^n from S to $P(S)$.

→ Claim: To show that g is not surjective & hence not bijective.

$$g : S \to P(S)$$



for $x \in S$, $g(x) \in P(S)$

$\therefore g(x) \subseteq S$.

x may or may not be in $g(x)$.

Define a subset A of S as follows:

$$A = \{x \mid x \notin g(x)\}$$

As $A \subseteq S$, we have $A \in P(S)$.

→ Claim: We show that for no $a \in S$, $g(a) = A$.

Suppose for some $a \in S$, $g(a) = A$

Then $a \in A \iff a \in \{x \mid x \notin g(x)\}$

$\iff a \notin g(a) = A$

we arrive at a contradiction

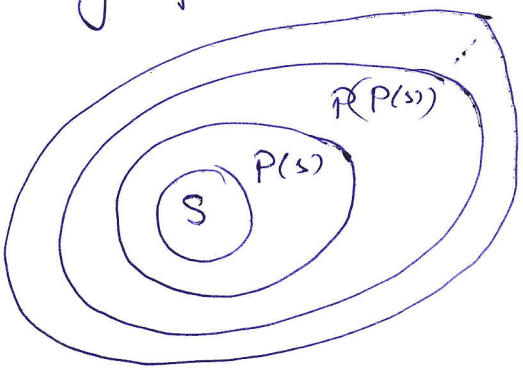
Hence no $a \in S$ for which $g(a) = A$

Hence g is not surjective & hence not bijection

- We have chosen g arbitrarily $\therefore$ hence we can conclude that no bijection exist from S to $P(S)$ $\therefore$ therefore, $|S| \neq |P(S)|$.

  Hence $|S| \leq |P(S)|$.

- We have an infinite ~~trig~~ hierarchy of uncountable sets. i.e. infinite sequence of cardinal nos., each of which is smaller than the next in the sequence.



$\aleph_0 = |\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| < \cdots$ ($\aleph_1$, $\aleph_2$)

$|P(\mathbb{N})|$, $|P(P(\mathbb{N}))|$, ... uncountable

$|\mathbb{N}|$ countable; $|P(\mathbb{N})|$ uncountable; transfinite nos.

- Countable sequence of power sets of power sets.

Note. $|S| = |T|$ if $\exists$ a bijection from S to T.

$|S| \leq |P(S)|$ as $\exists$ no bijection from S to $P(S)$ but $\exists$ injection from S to $P(S)$

S may be finite ~~or infinite~~ (countable)

~~S may be countable (finite)~~

S may be ~~uncountable~~ infinite (uncountable).

S may be infinite (countable)

$\frac{1}{1}$ $\quad$ $\frac{1}{2}, \frac{2}{1}$ $\quad$ $\frac{1}{3}, \frac{2}{2}, \frac{3}{1}$ $\quad$ $\frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}$ $\quad$ $\frac{1}{5}, \frac{2}{4}, \frac{3}{3}, \frac{4}{2}, \frac{5}{1}$

$p+q=2$ $\quad$ $p+q=3$ $\quad$ $p+q=4$ $\quad$ $p+q=5$ $\quad$ $p+q=6.$

φ^+ : $\frac{1}{1}$ $\quad$ $\frac{1}{2}$ $\quad$ $\frac{2}{1}$ $\quad$ $\frac{1}{3}$ $\quad$ $\frac{3}{1}$ $\quad$ $\frac{1}{4}$ $\quad$ $\frac{2}{3}$ $\quad$ $\frac{3}{2}$ $\quad$ $\frac{4}{1}$ $\quad$ ...

N : 1 $\quad$ 2 $\quad$ 3 $\quad$ 4 $\quad$ 5 $\quad$ 6 $\quad$ 7 $\quad$ 8 $\quad$ 9 ...

φ : 0 $\quad$ $\frac{1}{1}$ $\quad$ $\frac{-1}{1}$ $\quad$ $\frac{1}{2}$ $\quad$ $\frac{-1}{2}$ $\quad$ $\frac{2}{1}$ $\quad$ $\frac{-2}{1}$ $\quad$ $\frac{1}{3}$ $\quad$ $\frac{-1}{3}$ $\quad$ $\frac{3}{1}$ $\quad$ $\frac{-3}{1}$ ...

N: 1 $\quad$ 2 $\quad$ 3 $\quad$ 4 $\quad$ 5 $\quad$ 6 $\quad$ 7 $\quad$ 8 $\quad$ 9 $\quad$ 10 $\quad$ 11 ...

Density property of real nos.

Theorem. If x and y are two real numbers such that $x < y$, then $\exists$ a rational no. r, where $x < r < y$.

Proof.

Case 1 Suppose $x > 0$ and $0 < x < y$.

By the Archimedean property, $\exists$ a +ve integer n s.t. $n(y-x) > 1$

$$\text{or } \frac{1}{n} < (y-x) \quad -(1)$$

Let $A = \{ m \in \mathbb{N} \mid \frac{m}{n} > x \}$ → subset of natural nos. $\mathbb{N}$ (m: +ve integer)

Then $A \neq \phi$ as by the Archimedean property,

as $\frac{1}{n}, x \in \mathbb{R}$ and $\frac{1}{n} > 0$, $\exists$ a +ve integer m

s.t. $m\left(\frac{1}{n}\right) > x$

$\therefore$ By the well-ordering principle of natural nos., every non-empty subset of natural nos. has a least element.

$\therefore$ A has a least element, say $p > 1$ (p +ve integer)

$\therefore \frac{p}{n} > x$, but $\frac{p-1}{n} \leq x$.

$$\therefore \frac{p}{n} \leq x + \frac{1}{n} < x + (y-x) \text{ by } (1)$$
$$= y$$

Hence $x < \frac{p}{n} < y$ (p: +ve int., n: +ve int.).

$\therefore$ There exists a rational no. $r = \frac{p}{n}$ contained in $0 < x < y$.

Case 1 $x > 0$

Case 2 $x \leq 0 < y$

Case 3 $x < y < 0$

Archimedean property

If $x, y \in \mathbb{R}$ & $x > 0$, then $\exists$ a +ve integer n s.t. $nx > y$.

Case 2 If $x \leq 0 < y$, then by the Archimedean property $\exists$ a +ve integer n s.t. $x.y > 1$ i.e. $\frac{1}{n} < y$.

Clearly, $\frac{1}{n}$ is a rational no. contained in the interval $x \leq 0 < y$.

Case 3 If $x < y \leq 0$, then $0 \leq -y < -x$ & by the previous cases, there is a rational no. $r \in (-y, -x)$ & so the rational no. $-r \in (x, y)$.

Important consequence

The existence of one rational no. between x & y imply the existence of infinitely many rational nos. between x and y.

Theorem If x, y are two real nos. such that $x < y$, then $\exists$ an irrational no. a s.t. $x < a < y$.

proof-

$$x < y \Rightarrow \frac{x}{\sqrt{2}} < \frac{y}{\sqrt{2}}$$

$\frac{x}{\sqrt{2}}, \frac{y}{\sqrt{2}}$ are two real nos. with $\frac{x}{\sqrt{2}} < \frac{y}{\sqrt{2}}$.

$\therefore$ By the previous theorem, $\exists$ a rational no. r s.t.

$$\frac{x}{\sqrt{2}} < r < \frac{y}{\sqrt{2}}$$

$$\Rightarrow x < r\sqrt{2} < y$$

Clearly, $r\sqrt{2}$ is an irrational no. between two real nos. x & y.

Consequence Every interval I of real nos. contains infinitely many irrational nos.

Final conclusion In between two real nos. x & y, $\exists$ infinitely many real nos., rational as well as irrational.

→ **$\mathbb{R}$ is dense**

Theorem For any positive real no. x, $\exists$ a +ve integer n s.t. $n-1 \leq x < n$.

proof $x > 0$, $1 > 0$

By the Archimedean property, $\exists$ a +ve integer k s.t.

$k \cdot 1 > x$.

Let $A = \{p \in \mathbb{N} \mid p > x\}$.

Then $A \neq \emptyset$ as $k \in A$ -x)

$\therefore$ By the well ordering principle, A must have a least element, say n

$\therefore n > x$ but ~~$n-1 \leq x$~~. $n-1 \notin A$

i.e. $n-1 \leq x$.

$\therefore n-1 \leq x < n$.

Archimedean property for R

If $x, y \in R$ & $x > 0$, then $\exists$ a +ve integer n s.t. $nx > y$.

proof Trivial case: if $y < 0$ or if $0 \leq y < x$, then $x > y$ & the Archimedean property holds for $n = 1$.

Modified form If $x, y \in R$ ~~and $x \neq 0$~~ $x, y > 0$ and $x < y$, then $\exists$ a +ve integer n s.t. $nx > y$.

proof Let $A = \{nx : n = 1, 2, 3, \cdots\}$

If the Archimedean property were not true, then $nx \leq y \; \forall \; n = 1, 2, 3, \cdots$ & so y becomes an upper bound of the set A.

Thus
~~Therefore~~, A is a non-empty subset of real nos. & is bounded above.

Therefore, the least upper bound (supremum) of A exists; $\in R$

i.e. $\sup A = M$

Thus $M \in A = \{ nx : n = 1, 2, \dots \}$ with $nx \le y$, $\forall$ +ve int. n

~~all $nx \le M$~~

~~$M \ge$~~

Since $x > 0$, we have

$M - x < M$ & $M - x$ is not an upper bound of A.

$\Rightarrow$ $\exists$ some element, say $mx \in A$ s.t.

$$mx \nleq M - x$$

i.e. $M - x < mx$

$\Rightarrow M < (m+1)x$.

$(m+1)x \le mx + y$ ~~$\le y + x$~~

but $(m+1)x \in A$.

$\Rightarrow M$ is not $\sup A$. $\Leftarrow\!\Rightarrow (\rightarrow\leftarrow)$

$\therefore R$ is Archimedean.

Theorem. The set Q of all rational nos. in Archimede

- Q countable
- Q dense
- Q Archimedean

- R uncountable
- R dense
- R Archimedean.

$r_1, r_2 \in Q$, $r_1 \neq r_2$

Then $r_3 = \frac{1}{2}(r_1 + r_2) \in Q$

$r_1 < r_3 < r_2$

$r_1 + r_1 < r_1 + r_2 < r_2 + r_2$

$2r_1 < r_1 + r_2 < 2r_2$

$r_1 < \frac{r_1 + r_2}{2} < r_2$

$\frac{\quad}{r_3}$

Theorem The set $\mathbb{Q}$ is Archimedean.

If a is any +ve rational no. & b is any rational no., then $\exists$ a +ve integer n s.t. $na > b$.

proof **Case 1** $(b < 0)$ then clearly $a > b$.

Archimedean property holds for $n = 1$

Case 2 $(b > 0$, but $b < a)$

Then clearly $a > b$

Archimedean property holds for $n = 1$

Case 3 $(b > 0$ & $b > a)$

we wish to show that $\exists$ a +ve integer n s.t. $na > b$

(proof by contradiction)

If possible, let $\mathbb{Q}$ is not Archimedean.

i.e. $\nexists$ +ve integer n, $na \leq b$.

$na \leq b \quad \forall\, n \in \mathbb{N}$

$\Rightarrow (na)\, b^{-1} \leq 1 <$ any natural no. m other than 1

$\Rightarrow n \cdot m^{-1} \leq b a^{-1}$

$\Rightarrow (na)\, b^{-1} \leq m \quad \forall\, m \in \mathbb{N}$

$\Rightarrow n m^{-1} \leq b a^{-1} \quad \forall\, m \in \mathbb{N}$

i.e. for any +ve rational x, we have $x \leq b a^{-1}$ (a fixed +ve rational no.)

$\Rightarrow$ which is not true

Hence $\mathbb{Q}$ cannot be non-Archimedean.

Theorem. Let P_n be the set of all polynomials fns. f of deg. n defined by $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$, where n is any fixed positive integer or $n=0$, the coefficients $a_0, a_1, \dots, a_n$ are taken to be all integers and $a_0 \neq 0$. The set P_n is countable.

Proof. The result is true for $n=0$ as the set of all polynomials of degree 0 is in 1-1 correspondence with the set of all non-zero integers, and is countable.

Let us now assume that P_k is countable for some fixed positive integer k.

For each +ve integer m, let

$$S_m = \{f : f = mx^{k+1} + g,\ g \in P_k\}$$

& $$S_{-m} = \{f : f = -mx^{k+1} + g,\ g \notin P_k\}$$

The sets S_m & S_{-m} are both countable, each being in 1-1 correspondence with the countable set P_k.

$\therefore T_m = S_m \cup S_{-m}$ is countable as union of two countable sets is countable.

$\Rightarrow \bigcup_{m=1}^{\infty} T_m$ is countable as union of countable family of countable sets is countable.

Since $P_{k+1} = \bigcup_{m=1}^{\infty} T_m$, P_{k+1} is countable.

Hence the theorem follows by induction.

- Similarly, one can prove that the set Q_n (n is a fixed non-negative integer) of polynomials $a_0x^n + a_1x^{n-1} + \dots + a_n$, where $a_0, a_1, \dots, a_n$ are rational nos. & $a_0 \neq 0$, is countable, & consequently $\bigcup_{n=1}^{\infty} Q_n$ is countable.

Def^n: A real no. is called algebraic if it is the root of some polynomial eqn. with rational co-efficients.
If it is transcendental if it is not algebraic.

Example: The set of algebraic numbers is countable.

Sol^n: Let n be a given +ve integer. The set Q_n of polynomials

$$a_0x^n + a_1x^{n-1} + \cdots + a_n,$$

where $a_0, a_1, \cdots, a_n$ are rational nos. $(a_0 \neq 0)$ is countable.

∴ ~~We may~~ Let $\{f_{n_1}, f_{n_2}, f_{n_3}, \cdots\}$ be an enumeration of Q_n where f_{n_k} is a polynomial of deg n with rational co-efficients.

Let $A_{n_k} =$ the set of all roots of $f_{n_k} = 0$.

A_{n_k} is countable as it contains at most n numbers.

Let $A_n = \bigcup_{k=1}^{\infty} A_{n_k}$.

Then A_n is the set of all these algebraic numbers which are roots of a poly. of deg. n with rational co-eff

∴ A_n is countable as union of countable family of countable sets is countable.

Let $A = \bigcup_{n=1}^{\infty} A_n$.

Then A is the set of all algebraic numbers & is countable as it is union of countable family of countable sets.

i.e. the set of algebraic numbers is countable.

- Set of transcendental nos. T is uncountable, otherwise $R = A \cup T$ is countable $(\rightarrow\leftarrow)$

Example: The set of transcendental numbers is uncountable

Sol^n: Let T be the set

Example: The set S of all infinite binary sequences is uncountable

Sol^n: (by contradiction)

Suppose S is countable. Clearly it is not a finite set.

$\therefore \exists$ an infinite seq. $f_1, f_2, \ldots$ that contains every element of S at least once.

Let

$$\textcircled{1} \quad \begin{cases} f_1 = b_{1,1}, b_{1,2}, b_{1,3}, \ldots \\ f_2 = b_{2,1}, b_{2,2}, b_{2,3}, \ldots \\ \ldots\ldots \\ f_k = b_{k,1}, b_{k,2}, b_{k,3}, \ldots \\ \ldots\ldots \end{cases}$$

Let $\tau = t_1 t_2 t_3 \ldots$ where $t_i = 1 - b_{ii}$ for $i = 1, 2, \ldots$

Then $\tau \in S$

Claim τ cannot be f_k for any +ve integer k.

Proof: for every positive integer k, the k-th element of the sequence τ is different from $b_{k,k}$, the k-th element of f_k.

So τ is not in the list ①, contradicting S is countable

$\therefore$ S must be uncountable.

- The set of irrational nos. is uncountable, otherwise $\mathbb{R}$ would be countable ($\rightarrow\leftarrow$).
- It is unknown whether there is a set whose cardinality lies between $|\mathbb{N}|$ and $|\mathbb{R}|$. (Continuum hypothesis)
  $\rightarrow$ known to be beyond proof in our system of logic.