SETS

equivalent

$\{2, 4, 18, 19\} \equiv \{4, 19, 18, 2\}$

$\subseteq$ subset

$A \subset B$ A is a strict subset of B, proper subset iff $A \subseteq B$ and $A \neq B$

$\in$ membership

$\notin$ no membership

$A \cup B$

$A \cap B$

$A \setminus B$ — $\{x : x \in A \text{ and } x \notin B\}$

Nine Zulu Queens Ruled China

cardinality – size of a set, denoted as $|A|$

power set of A: $\wp A$

$\mathbb{N}$ – natural numbers (non-negative integers) $\{0, 1, 2, 3, 4, 5 \ldots\}$

set builder notation

$$\mathbb{N}^+ = \{x : \underbrace{x \in \mathbb{N} \text{ and } x > 0}_{\text{condition to be satisfied by } x}\}$$

$\mathbb{Z}$ – integers $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ — German word Zahl

$$\mathbb{Z} = \{x : x \in \mathbb{N} \text{ or } -x \in \mathbb{N}\}$$

$\mathbb{Q}$ – rational numbers: $\left\{x = \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\right\}$

$\mathbb{R}$ – real numbers:

1) ordered field
- field: closure under + and ×
  - + and × are associative, commutative
  - × is distributive over +
  - existence of identities +, ×
  - existence of inverses
- order: we can establish relation $\leq$ between elements
  - $a \leq b$ and $b \leq a$ then $b = a$ (antisymmetry)
  - $a \leq b$ and $b \leq c$ then $a \leq c$ (transitivity)
  - $a \leq b$ or $b \leq a$ completeness

$\mathbb{C}$ – complex numbers: $\{x = a + bi : a \in \mathbb{R}, b \in \mathbb{R}\}$

(a, b)

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \times (c, d) = (ac - bd, ad + bc)$$

Order — separates from rationals, eg. $\sqrt{2}$

* 2) Dedekind-Complete: every non-empty subset S in $\mathbb{R}$ with an upperbound in $\mathbb{R}$ has a "least upper bound" (supremum) also in $\mathbb{R}$

Countable

A set is countable if it has the same cardinality as ~~the~~ some subset of the natural numbers (Georg Cantor)

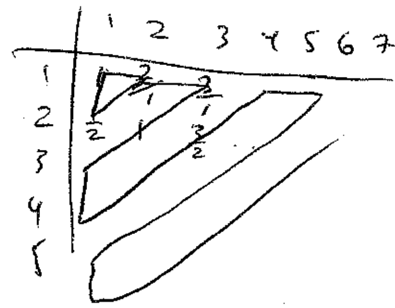
i.e. can be mapped one to one to $\mathbb{N}$ or $\mathbb{N}^+$

for example:

$\mathbb{Z}$ set of integers is countable:

$\mathbb{N}$	1	2	3	4	5	6	7
$\mathbb{Z}$	0	1	−1	2	−2	3	−3 ...

Set of $\mathbb{Q}$



$\mathbb{R}$? uncountable!

Proofs

QED - quod erat demonstratum
"which was to be demonstrated"

Forwards - Backwards

if $n \in \mathbb{Z}_{even}$ then $n^2 \in \mathbb{Z}_{even}$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$n = 2q$, for $q \in \mathbb{Z}$ $\qquad$ $n^2 = 2k$, for $k \in \mathbb{Z}$

$$n^2 = 4q^2$$
$$= 2 \cdot \underbrace{2q^2}_{\mathbb{Z}}$$
$$= 2k$$

Constructive Proof

AKA demonstrative proof

Ex: $\exists x$ st $k^2 = x$ and $k \in \mathbb{Z}$ and x is $\mathbb{Z}_{odd}$

let $x = 9$, $3^2 = 9$, 9 is odd

Induction Principle

suppose the following hold for a set $A \subseteq \mathbb{N}^+$

- $1 \in A$
- if $k \in A$ then $k+1 \in A$

then all positive integers are in A, $A = \mathbb{N}^+$

EX: prove for $n \in \mathbb{Z}^+$

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

BASE: $n=1$, $\frac{1 \cdot 2}{2} = 1$ TRUE

assume k : $1+2+\dots+k = \frac{k(k+1)}{2}$

show $k+1$ $1+2+\dots+k+(k+1) = \frac{k(k+1)}{2} + (k+1)$

$$= \frac{k(k+1)+2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

Weak induction

Strong induction P not only holds for k but for $1 \dots k$

Given $A \subseteq \mathbb{Z}^+$, suppose

- $1 \in A$
- if $\{1,2,\dots,k\} \subseteq A$, then $k+1 \in A$
- then $A = \mathbb{Z}^+$

Eg. Prove every positive integer greater than 1 can be expressed as a product of primes

base case: 2 is prime

Assume: strong induction: claim holds for all integers between 2 and k

: $k+1$ is prime (trivial)

$k+1$ not prime then $k+1 = a \cdot b$, $a, b \neq 1, k+1$

So $2 \le a, b \le k$ but all integers between 2 and k can be written as primes.

induction principle: it's an axiom, not inherently true!

<u>Contradiction</u>

$$A \Rightarrow B$$
$$\downarrow$$
$$A \Rightarrow \neg B$$

Ex: $\sqrt{2}$ is irrational

Proof by contradiction.

Assume $\sqrt{2}$ is rational

$$\sqrt{2} = \frac{p}{q}, \quad \text{where } p, q \in \mathbb{Z}, \ q \neq 0$$

and p, q no common divisor

$\Downarrow$

p, q cannot both be even

$$2 = \frac{p^2}{q^2}$$

$$2q^2 = p^2$$ ← p is even $p \in \mathbb{Z}_{even}$

$$2q^2 = (2k)^2 \quad k \in \mathbb{Z}$$

$$2q^2 = 4k^2$$

$$q^2 = 2k^2$$

so q^2 is even $\Rightarrow$ q is even

<u>contradiction!</u>

Contrapositive

$A \Rightarrow B \qquad \neg B \Rightarrow \neg A$

Ex: if $\underbrace{x, y \in \mathbb{Z} \text{ and } x+y \in \mathbb{Z}_{\text{even}}}_{A}$ then $\underbrace{x, y \text{ have the same parity}}_{B}$

Assume x, y do not have the same parity $\quad \neg B$

without loss of generality

x is even $= 2k$, $k \in \mathbb{Z}$

y is odd $= 2q+1$, $q \in \mathbb{Z}$

$$x+y = 2k + 2q + 1 = 2\underbrace{(k+q)}_{\mathbb{Z}} + 1$$

$$= 2m + 1 \in \mathbb{Z}_{\text{odd}}$$

$\neg A$