

PROOF WRITING & MATHEMATICAL REASONING

2023-07-21

⑥ SET THEORY

① Introduction to Sets

- Any well-defined collection of elements is called a set.

(NEW)

Any object defining an "inclusion" operation ($\in$) is a set.

$\{\text{cat, dog, fish}\} \leftarrow \text{SET} \checkmark$

$\{x \in \mathbb{N} \mid x \text{ is divisible by } 2\} \leftarrow \text{SET} \checkmark$

- A set need not describe a finite collection of elements. It just needs to define a notion of "inclusion", but this notion needs to be well-defined.

- From now on, we will just consider sets to be a check on inclusion, i.e. whether $x \in A$, or not.

$\in$



inclusion /

"belongs to"

$\exists$



there exists

$\notin$



"not in"

$\nexists$



"doesn't exist"

$\exists!$



there exists unique.

$\forall$



for all

$\exists x \in A \mid \mathcal{B}$

$(A \cap B) \neq \emptyset$

$\hookrightarrow \{x \mid \mathcal{B}\}$

$|A \cap B| = 1$

$A \subseteq \{x \mid \mathcal{B}\}$

$A \ni x$

$\Leftrightarrow x \in A$

"contains"

- $A = \{1, 2, 3, 4, 5\}$ $2 \in A, 6 \notin A$ ✓
 $A \ni 2, A \not\ni 6$ ✓

$\exists x \in A \mid x \text{ is even}$ ✓
 $\exists! y \in A \mid y \text{ is composite}$ ✓

$\nexists z \in A \mid z \leq 0$ ✓
 $\Leftrightarrow \forall z \in A \mid z > 0$ ✓ } **Imp!**

$\left\{ \begin{array}{l} \nexists z \in A \mid P \\ \Leftrightarrow \forall z \in A \mid \neg P \end{array} \right\}$ } **proof by contradiction!**

② Subsets & Supersets

- $A \subseteq B \rightarrow \text{if } x \in A \text{ then } x \in B.$



$$\Downarrow$$

$$B \supseteq A$$

$$A \subseteq B, A \neq B.$$

- $A \subset B \equiv \boxed{A \subsetneq B}$ $\rightarrow A \subseteq B, \exists x \in B \mid x \notin A$
 $\hookrightarrow$ "proper subset".

③ Unions, Intersections, Set minus, Symmetric

HW: Check this stuff via Venn Diagram $\Downarrow$

- $A \cup B \equiv \{x \in A \text{ OR } x \in B\}$

- $A \cap B \equiv \{x \in A \text{ AND } x \in B\}$ Common elements.

- $A \setminus B \equiv A \setminus (A \cap B) \equiv A \cap (B^c) \equiv \{x \in A \text{ BUT NOT } x \in B\}$ $\hookrightarrow$ complement.

- $A \Delta B \equiv (A \setminus B) \cup (B \setminus A) \equiv (A \cup B) \setminus (A \cap B)$

n can be ∞ as well! (countable union)

$$\bigcup_{i=1}^n A_i \equiv A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n \rightarrow \text{finite union}$$

$$\bigcap_{j=1}^n B_j \equiv B_1 \cap B_2 \cap B_3 \cap \dots \cap B_n$$

$$\bigcup_{\alpha \in A} S_\alpha \equiv \{x \mid (\exists \alpha \in A \mid x \in S_\alpha)\}$$

$\rightarrow$ indexing set (finite, infinite)
(same holds for intersections) countable uncountable

Commutative: $A \cup B \equiv B \cup A, A \cap B \equiv B \cap A$
($\cup, \cap, A$)

Associative: $(A \cup B) \cup C \equiv A \cup (B \cup C) \equiv A \cup B \cup C$

($\cup, \cap$) Distributive Law:

$(A \cup B) \cap C$ $\parallel$ $(A \cap C) \cup (B \cap C)$	$(A \cap B) \cup C$ $\parallel$ $(A \cup C) \cap (B \cup C)$
--	--

De-Morgan's Law

$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
-------------------------------	-------------------------------

Example: $A = \{1, 2, 3, 4, 5\}$
 $B = \{4, 5, 6, 7, 8\}$
 $C = \{2, 3, 5, 6, 7, 9, 10\}$

$$(A \cup B) \cap C = \{1, 2, 3, 4, 5, 6, 7, 8\} \cap \{2, 3, 5, 6, 7, 9, 10\} = \{2, 3, 5, 6, 7\}$$

$$(A \cap C) = \{2, 3, 5\} \quad (B \cap C) = \{5, 6, 7\}$$

whole numbers $\mathbb{N}_0$ | $\mathbb{N} \rightarrow$ naturals
 $\mathbb{Z} \rightarrow$ integers
 $\mathbb{Q} \rightarrow$ rationals
 $\mathbb{R} \rightarrow$ reals
 $\mathbb{C} \rightarrow$ complex

⑥ Cardinality of a Set

$$N_n = \{i \in \mathbb{N} \mid 1 \leq i \leq n\}$$

$$= \{1, 2, 3, \dots, n\}$$

⑦ $\rightarrow A \cong B$ if there is a bijection between them
 "A is bijective to B"
 one-one correspondence

Example: $\{a, b, c, d\}$

$\{apple, ball, cat, dog\}$

$\cong N_4$

$$|A| = k, A \cong N_k \text{ (Defn.)}$$

number of members of A (finite)
 $\#A = k$
 if elements of A can be labelled by $\{1, 2, 3, \dots, k\}$ then $|A| = k$

$$|A| = 0 \Leftrightarrow A = \emptyset$$

$$\emptyset = \{\} \text{ empty set. } |\emptyset| = 0$$

A is said to be infinite if $\forall n \in \mathbb{N}_0, A \not\cong N_n$

"elements of A cannot be labelled by $1, 2, 3, \dots, n$ regardless of how large we make n ."

{shelves analogy}

- A is said to be countable if $A \cong \mathbb{N}$.

Example: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{A}, \{\text{all even numbers}\}$
 $\downarrow$
 algebraic numbers $\mathbb{C}$

i) $\{1, 2, 3, 4, 5, 6, \dots\} = \mathbb{N}$
 $\downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow$
 $\{2, 4, 6, 8, 10, 12, \dots\} = 2\mathbb{N}$

$$2|\mathbb{N}| \not\leq |\mathbb{N}|, \quad |2\mathbb{N}| = |\mathbb{N}|$$

smallest infinite cardinal $\leftarrow$ "aleph-null" $\aleph_0$

ii) $\mathbb{Z}_7 =$

$(\cdot) \in \mathbb{N}$

$$\begin{aligned} \{ & \downarrow, \downarrow, \downarrow, \downarrow, \dots \} = \mathbb{N} \\ \{ & 0, 1, -1, 2, -2, \dots \} = \mathbb{Z} \end{aligned}$$

$$\hookrightarrow 2n \mapsto n, \quad 2n+1 \mapsto -n \quad (n \in \mathbb{N}_0)$$

$$\tilde{m}) N_0 \cong N_1$$

($\cong$ is an equivalence relation on the ^{of} $\mathcal{P}(S)$ of all sets)

Unrelated, but fun:
Russel's Paradox

Unrelated, but fun:
Russel's Paradox

iv) Countability of Rationals

	...	-4	-3	-2	-1	1	2	3	4	5	...
...	.../...	.../-4	.../-3	.../-2	.../-1	.../1	.../2	.../3	.../4	.../5	.../...
-4	-4/...	-4/-4	-4/-3	-4/-2	-4/-1	-4/1	-4/2	-4/3	-4/4	-4/5	-4/...
-3	-3/...	-3/-4	-3/-3	-3/-2	-3/-1	-3/1	-3/2	-3/3	-3/4	-3/5	-3/...
-2	-2/...	-2/-4	-2/-3	-2/-2	-2/-1	-2/1	-2/2	-2/3	-2/4	-2/5	-2/...
-1	-1/...	-1/-4	-1/-3	-1/-2	-1/-1	-1/1	-1/2	-1/3	-1/4	-1/5	-1/...
0	0/...	0/-4	0/-3	0/-2	0/-1	0/1	0/2	0/3	0/4	0/5	0/...
1	1/...	1/-4	1/-3	1/-2	1/-1	1/1	1/2	1/3	1/4	1/5	1/...
2	2/...	2/-4	2/-3	2/-2	2/-1	2/1	2/2	2/3	2/4	2/5	2/...
3	3/...	3/-4	3/-3	3/-2	3/-1	3/1	3/2	3/3	3/4	3/5	3/...
4	4/...	4/-4	4/-3	4/-2	4/-1	4/1	4/2	4/3	4/4	4/5	4/...
...	.../...	.../-4	.../-3	.../-2	.../-1	.../1	.../2	.../3	.../4	.../5	.../...

If we find something we have already seen, skip it.

Hence, $\mathbb{Q}$ is countable

- Infinite sets, which are not countable, are said 'uncountable'.

Example: $\mathbb{R}$ real numbers (why?)

The Real Numbers are Uncountable

Example:

Show that the set of real numbers is uncountable.

Solution:

This method is called the Cantor diagonalization argument, and is a proof by contradiction.

1. Suppose $\mathbb{R}$ is countable.
Then the real numbers between 0 and 1 are also countable (any subset of a countable set is countable).
2. The real numbers between 0 and 1 can be listed in order $r_1, r_2, r_3, \dots$.
3. Let the decimal representation of this listing be

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}\dots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}\dots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}\dots \end{aligned}$$

4. Form a new real number with the decimal expansion:
where $r_i = 3$ if $d_{ii} \neq 3$ and $r_i = 4$ if $d_{ii} = 3$. $r = .r_1r_2r_3r_4\dots$
5. r is not equal to any of the $r_1, r_2, r_3, \dots$ because it differs from r_i in its i th position after the decimal point.

Therefore there is a real number between 0 and 1 that is not on the list since every real number has a unique decimal expansion.

Hence, all the real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable.

6. Since a set with an uncountable subset is uncountable (an exercise), the set of real numbers is uncountable.

Take $A = [0, 1]$. Suppose it is countable.

$$A = \{r_1, r_2, r_3, \dots, r_n, \dots\}$$

$$r_k = 0.\overset{\text{digits!}}{d_{k1}}d_{k2}d_{k3}d_{k4}d_{k5}d_{k6}d_{k7}d_{k8}\dots$$

$$e_j = \begin{cases} \boxed{d_{jj}+1}, & 0 \leq d_{jj} < 9 \\ 0, & d_{jj} = 9 \end{cases} \quad \Bigg| \quad |e_j - d_{jj}| = 1$$

diagonal elements

$$e = 0.\underset{10^{-1}}{e_1}\underset{10^{-2}}{e_2}\underset{10^{-3}}{e_3}\underset{10^{-4}}{e_4}e_5e_6e_7\dots$$

$$|r_k - e| \geq 10^{-k} \Rightarrow r_k \neq e \quad \forall k \in \mathbb{N}$$

$$\text{But } e \in [0, 1] \Rightarrow e \notin A$$

$\Rightarrow \Leftarrow$

CONTRADICTION

$\therefore [0, 1]$ is uncountable $\Rightarrow \mathbb{R}$ is also uncountable.

Partial Ordering of Sets & Sup-Inf (Increasing & Decreasing Sets)

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq A_4 \subseteq \dots$$

$$A_n \uparrow A, \quad A = \bigcup_{i=1}^{\infty} A_i$$

$$B_1 \supseteq B_2 \supseteq B_3 \supseteq B_4 \supseteq \dots$$

$$B_n \downarrow B, \quad B = \bigcap_{j=1}^{\infty} B_j$$

Examples:

$$[0, n] \uparrow [0, \infty) \quad \checkmark$$

$$[\frac{1}{n}, 1] \uparrow [0, 1] \quad \checkmark$$

Why "increasing" / "decreasing"?

$$(A \subseteq B \iff A \subseteq B) \quad \text{so how?}$$

$$A \supseteq B : A \supseteq B \quad \text{Check this works as expected as "}>!"$$

This is called a "partial order".

$\hookrightarrow =, >, <, \sim$
 $\hookrightarrow$ no order.

But: $A_1 \subseteq A_2 \subseteq A_3 \subseteq A_4 \subseteq \dots$

$$A_n \uparrow A = \sup \text{ ("max", "limit")}$$

(similarly $B_1 \supseteq B_2 \supseteq B_3 \supseteq \dots$
 $B_n \downarrow B = \inf \text{ (min, limit)} \text{ of all these sets!}$)

More Examples:

$$\left[\frac{1}{n}, 2 - \frac{1}{n} \right] \uparrow (0, 2)$$

$$\{1, 2, 3, \dots, n\} \uparrow \mathbb{N}$$

$$\left[n, \infty \right) \downarrow \phi \quad \left\{ \begin{array}{l} \text{HW:} \\ \text{why?} \end{array} \right.$$

Power Set: $\mathcal{P}(A), 2^A$

Set of all subsets of A (including ϕ, A)

(for the day) FIN $\Rightarrow$

2023-07-22

Recap & Doubts

$$A_n \uparrow A : A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots, A = \bigcup_{i=1}^{\infty} A_i \quad \text{sup}$$

$$B_n \downarrow B : B_1 \supseteq B_2 \supseteq B_3 \supseteq \dots, B = \bigcap_{j=1}^{\infty} B_j \quad \text{inf}$$

Countability: Intuitive but true!

$$\begin{aligned} |\mathbb{N}| &\in \mathbb{Q}, & |\mathbb{N}| &= |\mathbb{Q}| \\ & & &= |\mathbb{Z}| \\ & & &= \dots \end{aligned}$$

⑥ RELATIONS & FUNCTIONS

⑦ Cartesian Product

- $A \times B$, the cartesian product of 2 sets, A, B is defined as:

$$A \times B = \{ (a, b) \mid a \in A, b \in B \}$$

2-tuple / ordered pair

- Eg: $\{1, 2, 3\} \times \{10, 11\}$

$$= \{(1, 10), (2, 10), (3, 10), (1, 11), (2, 11), (3, 11)\}$$

$$\{10, 11\} \times \{1, 2, 3\} \quad \neq$$

$$= \{(10, 1), (10, 2), (10, 3), (11, 1), (11, 2), (11, 3)\}$$

⑧ Relations

- A relation from A to B , is any subset of $A \times B$.
A relation on A , is any subset of $A \times A$.

Often denoted by " R ".

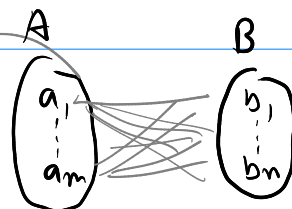
- We say xRy when $(x, y) \in R$

⑨ How many relations are possible from A to B , where A, B are finite sets w/ $|A|=m, |B|=n$?

Ans: 2^{mn}

2 choices for each

mn lines



bipartite graph of a relation.

(we will mostly talk about relations on sets)

- Reflexive Relation:

$\mathcal{R} \subseteq A \times A$ is reflexive iff $\forall a \in A, a \mathcal{R} a$.

- Symmetric Relation

$\mathcal{R} \subseteq A \times A$ is symmetric iff $a \mathcal{R} b \Rightarrow b \mathcal{R} a$

- Transitive Relation

$\mathcal{R} \subseteq A \times A$ is transitive iff $a \mathcal{R} b, b \mathcal{R} c \Rightarrow a \mathcal{R} c$

- $A = \{1, 2, 3\}$

$\mathcal{R}$	R	S	T
i) $\{(1,1), (1,2)\}$	$\otimes$	$\otimes$	$\checkmark$
ii) $\{(1,1), (2,2), (3,3), (1,3)\}$	$\checkmark$	$\otimes$	$\checkmark$
iii) $\emptyset$	$\otimes$	$\checkmark$	$\checkmark$
iv) $\{(1,1), (1,2), (2,3)\}$	$\otimes$	$\otimes$	$\otimes$
v) $\{(1,1), (2,2), (3,3), (1,3), (3,1)\}$	$\checkmark$	$\checkmark$	$\checkmark$

Bonus, $\emptyset$ is reflexive on A , what is A ? — $\emptyset$

- Equivalence Relation

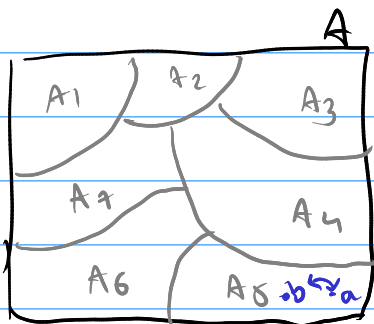
$R \subseteq A \times A$ is an equivalence relation on A , ~~if~~ it is reflexive, symmetric & transitive.

Eg: (v) from prev page

- Equivalence Classes / Partitions

→ An equivalence relation partitioning a set

$A, A = \biguplus_{1 \leq i \leq n} A_i \rightarrow \{A_1, \dots, A_n\}$ is a partition of A
 $\rightarrow$ disjoint union



✓ exclusive (disjoint)
 ✓ exhaustive

Why?? / How??

The partitions are subsets in which all elements are related to each other.

Suppose $a \in A_5$

$a R b, b R a, b \in A_5$
 $b R c, c R a, c \in A_5$
 $(R b)$

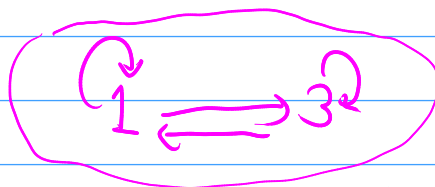
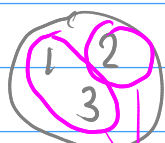
How: Think about it & convince yourself.

If there is a relation between classes: $c_1 R c_2$
 ~~c_1 and c_2~~ fully related

• Example 1

$$A = \{1, 2, 3\}$$

$$R = \{ (1,1), (2,2), (3,3), (1,3), (3,1) \}$$



equivalence classes: $\{1, 3\}, \{2\}$

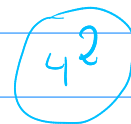
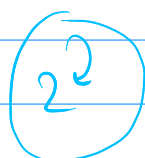
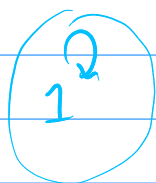
• Example 2

$\mathbb{N}_0$, $a R b$ if $5 \mid a - b \iff a \equiv b \pmod{5}$
What are the partitions?

$$\begin{aligned} C_0 &= \{0, 5, 10, 15, \dots\} = \{5n : n \in \mathbb{N}_0\} \\ C_1 &= \{1, 6, 11, 16, \dots\} = \{5n+1 : n \in \mathbb{N}_0\} \\ C_2 &= \{2, 7, 12, 17, \dots\} = \{5n+2 : n \in \mathbb{N}_0\} \\ C_3 &= \{3, 8, 13, 18, \dots\} = \{5n+3 : n \in \mathbb{N}_0\} \\ C_4 &= \{4, 9, 14, 19, \dots\} = \{5n+4 : n \in \mathbb{N}_0\} \end{aligned}$$

• Example 3

$\mathbb{N}$, $R = \{ (n, n) \mid n \in \mathbb{N} \}$
What are the partitions?



$\{1\}, \{2\}, \{3\}, \{4\}, \dots$

① Functions

"maps"

$a \xrightarrow{f} b$

$$f(a) = b$$

$$f: a \mapsto b$$

"maps to"

- Defn: $f: A \rightarrow B$, f is a relation from A to B ($f \subseteq A \times B$)
w/ the following additional conditions.

$$\forall a \in A, \exists! b \in B \mid f(a) = b$$

everything gets mapped, & no one-many mapping

- $f: \overset{\text{domain}}{A} \rightarrow \overset{\text{codomain}}{B}$
 $\overset{\text{pre-image (of } b)}{a} \mapsto \overset{\text{f-image / image (of } a)}{b}$

Suppose, $A' \subseteq A$, $f(A') = \{f(a) \mid a \in A'\} \subseteq B$.

Range of f : $f(A) \leftarrow$ all possible images.

- Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = |x|$.

domain $\rightarrow \mathbb{Z}$, codomain $\rightarrow \mathbb{Z}$

$$f(-2) = 2, f(\{-5, 3, 6, -3, 0\})$$

$$\text{Range} \rightarrow \mathbb{N} \cup \{0\} = \{0, 3, 5, 6\}$$

images & pre-images make sense for sets too.

- Inverses $f: A \rightarrow B \ni b$ $\rightarrow$ can define $f^{-1}(B')$, $B' \subseteq B$
 $f^{-1}(b) = \{a \in A \mid f(a) = b\} = \{f^{-1}(b) \mid b \in B'\}$

$f^{-1}(\{3\}) = \emptyset$
allowed!

⑥: $f^{-1}(2)$ in the above example? $\{-2, 2\}$

- Injective / One-one Functions

$f: A \rightarrow B$. f is injective $\iff \forall b \in B$

$$\# f^{-1}(b) \leq 1.$$

No many-one mappings.

- Surjective / Onto Functions

$f: A \rightarrow B$. f is surjective $\iff \forall b \in B$

$$\# f^{-1}(b) \geq 1$$

Codomain = Range

i.e. everything in the codomain is an image of (might be multiple things!) $\leftarrow$ something

- Bijective / Invertible Functions

$f: A \rightarrow B$. f is bijective ("a bijection") $\iff$
 f is injective & surjective.

$$\hookrightarrow \forall b \in B, \# f^{-1}(b) = 1$$

$$\Leftrightarrow \forall b \in B, \exists! a \in A \mid f(a) = b$$

one-one

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

correspondence b/w the elements of the two sets!

(refer back to Cardinality!)

• Examples, $f: \mathbb{R} \rightarrow \mathbb{R}$

	f	I	S
i)	$x^2 + 3$	⊗	⊗
ii)	$x^3 - 3x + 1$	⊗	⊙
iii)	$ x $	⊗	⊗
iv)	e^x	⊙	⊗
v)	$\ln x$	⊗ not a valid f^n $\mathbb{R} \rightarrow \mathbb{R}$	

$f: \mathbb{R}^+ \rightarrow \mathbb{R}, f(x) = \ln x$

⊙

⊙

FIN
(for me das) =

Recap & Doubts

2023-07-23

① Doubt #1 by Nishi:

Claim:

$[n, \infty) \downarrow \phi, \text{ as } n \rightarrow \infty$

Counter:

$[n, \infty) \downarrow \phi$
 $n=0 \Rightarrow [0, \infty) \cap [1, \infty) = [1, \infty)$
 $n=2 \Rightarrow [1, \infty) \cap [2, \infty) = [2, \infty)$
 $n=3 \Rightarrow [2, \infty) \cap [3, \infty) = [3, \infty)$
 $\vdots$
 $n=k \Rightarrow [k-1, \infty) \cap [k, \infty) = [k, \infty)$

Hello Sir

I have a doubt

You told us ki decreasing sets me n ki values 1 to infinity rakh ke uska intersection lenge

But if you put 0,1 as n and take there intersection, it would be $[1, \infty)$ and even if be reach a really really big number there would always be a bigger number than that so how can

their intersection be phi

I'm sorry I'm not able to get this

Resolution: $[1, \infty) \supseteq [2, \infty) \supseteq [3, \infty) \supseteq \dots$

$$[n, \infty) \downarrow \mathcal{B} \quad (\text{let})$$

$$\mathcal{B} = \bigcap_{n=1}^{\infty} [n, \infty)$$

Claim was $\mathcal{B} = \emptyset$

Suppose $\mathcal{B} \neq \emptyset$. $\therefore \exists x \in \mathcal{B} \subseteq [0, \infty)$

But, $\exists n_0 \in \mathbb{N} \mid x < n_0 \Rightarrow x \notin [n_0, \infty)$

$$\text{But } \mathcal{B} = [1, \infty) \cap [2, \infty) \cap \dots \cap [n_0, \infty) \cap \dots$$

$$\Rightarrow \mathcal{B} \subseteq [n_0, \infty) \not\ni x \quad \Rightarrow \Leftarrow \text{CONTRADICTION!}$$

Thus, we have a contradiction, showing that our initial assumption " $\mathcal{B} \neq \emptyset$ " was incorrect.

$$\therefore \mathcal{B} = \emptyset.$$

② Doubt #2 by Anuvindam

Let A be a set. Then a partition $\mathcal{P} \in \mathcal{P}(A)$

$$\text{i) } \left\{ \forall A_1, A_2 \in \mathcal{P} \quad A_1 \cap A_2 = \emptyset. \right.$$

pairwise disjoint.

$$\text{ii) } \left\{ \bigcup_{A \in \mathcal{P}} A = A. \right.$$

exhaustive

$\mathcal{P}$ is a set of subsets of A .

$A_* \rightarrow$ subset of A .

eg: $A = \{1, 2, 3, 4, 5, 6, 7\}$

valid partitioning

$$\mathcal{P} = \{ \{1\}, \{2, 3, 5, 7\}, \{4, 6\} \}$$

partitioning

$\mathcal{A}$ unitary

$\mathcal{A}$ prime

$\mathcal{A}$ composite

partitions / parts

In context of equivalence classes, $A \rightarrow$ set

$\mathcal{R} \subseteq A \times A$ relation

$\mathcal{P} \subseteq \mathcal{P}(A)$ partitioning

$$\hookrightarrow \mathcal{P} = \{ \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \dots \}$$

$\mathcal{A}_* \subseteq A$ partitions / parts

"on equivalence relation partitions (splits) a set into non-overlapping parts."
pairwise disjoint.

⑤ An equivalence relation defines a partitioning (in a part, all elements are related to each other). Conversely, every partitioning defines an equivalence relation.

$\hookrightarrow$ elements are said to be related if they are in the same partition. HW: Check that this is an equivalence relation.

MATHEMATICAL REASONING

⑥ PROPOSITIONAL LOGIC & BOOLEAN ALGEBRA

① Statements & Propositions

boolean variable

- $P \rightarrow$ A statement / proposition, which is either true or false
- $T / 1 \rightarrow$ Universal truth / tautology
- $F / 0 \rightarrow$ Universal falsehood / fallacy / falsum

② Logical Operators

- AND
OR
NOT

$\wedge$
 $\vee$
 $\neg$

common
(we will use)

$\cdot$
 $+$
 $\sim$

Theoretical CS

$\&\&$
 $||$
 $!$

programming

"exclusive or"
XOR

truth table!

<u>X</u>	<u>Y</u>	<u>$X \wedge Y$</u>	<u>$X \vee Y$</u>	<u>$\neg X$</u>	<u>$X \oplus Y$</u>
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	0	0

there are also non (NOT) NAND (NOT AND) ops

$$\neg (X \wedge Y) = (\neg X) \vee (\neg Y)$$

$$\neg (X \vee Y) = (\neg X) \wedge (\neg Y)$$

$$X \oplus Y = (X \vee Y) \wedge (\neg (X \wedge Y))$$

All these ops are commutative & associative.

FFD: logic gates



all these are im- via logic gates

- $\Rightarrow$ implies
 $\Leftarrow$ is implied by (rarely used)
 $\Leftrightarrow / \equiv$ is equivalent to
 used for objects: functions / sets / etc
 for statements / booleans.

$$\begin{aligned}
 X \Rightarrow Y &\rightarrow \text{"Y if X"} \\
 Y \Leftarrow X &\rightarrow \text{"X if Y"} \\
 X \Leftrightarrow Y &\rightarrow \text{"Y iff X"} / \text{"X iff Y"} \\
 &\rightarrow \neg(X \oplus Y) \quad \text{better meaning} \rightarrow \text{N XOR (X NOR)}
 \end{aligned}$$

-

<u>X</u>	<u>X</u>	<u>$X \Rightarrow Y$</u>	<u>$X \Leftarrow Y$</u>	<u>$X \Leftrightarrow Y$</u>
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

$$\begin{aligned}
 (X \Rightarrow Y) &\Leftrightarrow (\neg X) \vee (X \wedge Y) \\
 &\quad \updownarrow \\
 (Y \Leftarrow X) &\quad \text{vacuously true}
 \end{aligned}$$

$$\begin{aligned}
 (X \Leftrightarrow Y) &\Leftrightarrow (X \Rightarrow Y) \wedge (X \Leftarrow Y) \\
 &\Leftrightarrow \neg (X \oplus Y) \\
 &\Leftrightarrow (X \wedge Y) \vee (\neg X \wedge \neg Y)
 \end{aligned}$$

• Examples:

i) $C = A \cap B \Rightarrow C \subseteq B$ ✓

ii) $\exists x, y, z \in \mathbb{N} \mid x^n + y^n = z^n \Leftrightarrow n=2$ ✓
 ← easy
 Fermat's Last Theorem ← $\Rightarrow$ HARD!!!

iii) $n \in \mathbb{N}, n > 2, \underbrace{2 \mid n}_{2 \text{ factors } n} \Rightarrow n \text{ is a sum of } 2 \text{ primes} \text{ (?)}$
 ↪ Goldbach Conjecture, probably true?
 No proof till date.

• $\neg (\exists x \in A \mid P(x))$

$\Leftrightarrow \nexists x \in A \mid P(x)$

$\Leftrightarrow \forall x \in A \mid (\neg P)(x)$

The above forms a basis of "proof by contradiction".

• $\neg (x \Rightarrow y) \Leftrightarrow \neg (\neg x \vee (x \wedge y))$

$\Leftrightarrow (\neg(\neg x)) \wedge \neg(x \wedge y)$

$\Leftrightarrow x \wedge ((\neg x) \vee (\neg y))$

$\Leftrightarrow (x \wedge (\neg x)) \vee (x \wedge (\neg y))$

$\Leftrightarrow x \wedge (\neg y)$

$A \wedge (B \vee C)$

$= (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C)$

$= (A \vee B) \wedge (A \vee C)$

$\neg (x \Leftrightarrow y) \equiv x \oplus y$

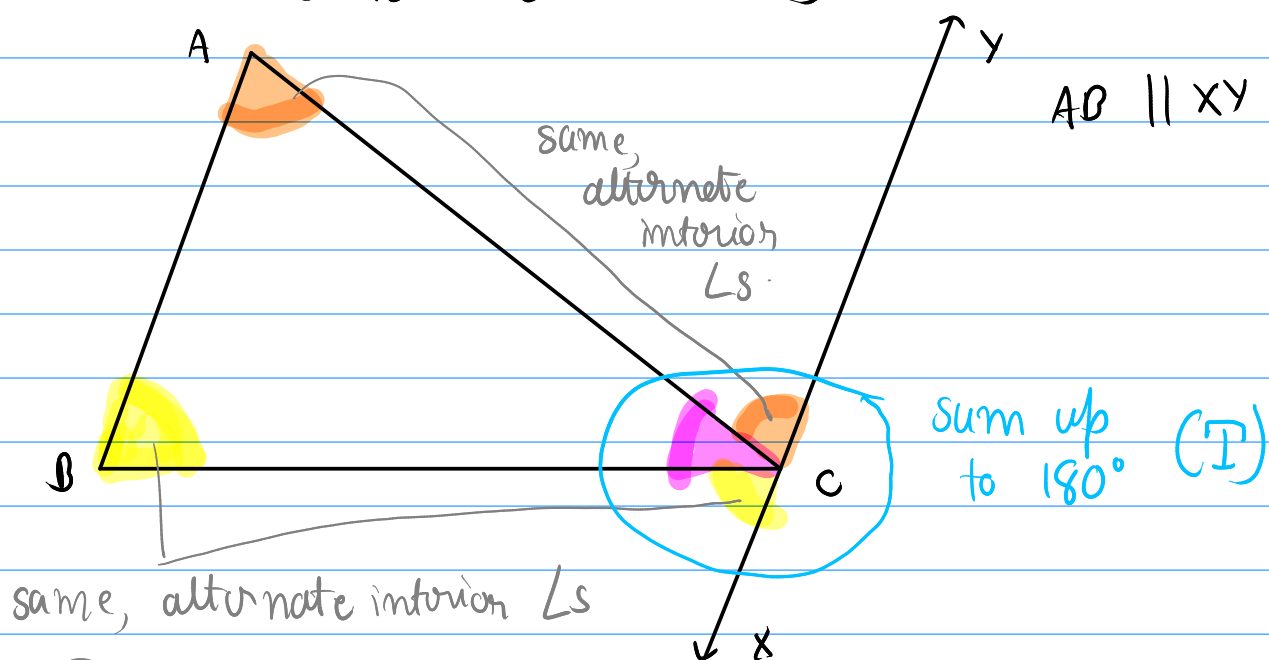
⑥ PROOF WRITING

① What is a proof?

- A proof is a sequence of logical steps from something known to be true, to some unknown proposition

$\boxed{T \Rightarrow P}$ is a proof of P (Why? $(T \Leftrightarrow P) \equiv P$ Check!)

- An 'axiom' is a statement taken to be true, without proof. Eg: ZF(c) in set theory, Euclid's postulates, etc.
- Example Prove that in Euclidean geometry, the sum of interior angles of a triangle is 180° (or π radians)



Proof: (T) $\angle BCX + \angle BCA + \angle ACY = 180^\circ$

$\Rightarrow \angle ABC + \angle BCA + \angle CAB = 180^\circ$

(P)

(Q.E.D.) $\rightarrow \blacksquare$

($\because \angle ABC = \angle BCX$,
 $\angle CAB = \angle ACY$)
cuz alternate interior $\angle$ s

RIN
(for the
day)

⑥ ABSTRACT ALGEBRA

⑦ Motivation

- What is "abstract algebra"?

It is a collection of frameworks describing the properties of mathematical structures which obey certain conditions.

It is a collection of frameworks that help us ^{reason about} mathematical structures based on certain characterising features, regardless of what they are.

Structure over identity $\leftarrow$ Ⓢ "abstract"

- Goal: Understand ordering, sup, inf in general.

⑧ Group

↖ binary operations.

- Let G be a set, $\underline{*} : G \times G \rightarrow G$ closure

$(G, *)$ is said to be a group if.

- associativity i) $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$
 identity elem ii) $\exists e \in G \mid \forall a \in G \quad a * e = a$
 inverse iii) $\forall a \in G \quad \exists a^{-1} \in G \mid a * a^{-1} = e$

$(G, *)$ is called a commutative / Abelian group if $\forall a, b \in G, \quad a * b = b * a$

• Example:

i) $(\mathbb{Z}, +)$ is a Abelian group

$$\forall a, b, c \in \mathbb{Z}, (a+b)+c = a+(b+c) \quad \checkmark$$

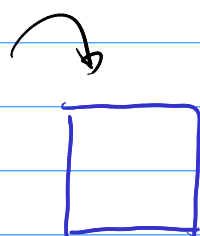
$$\forall a \in \mathbb{Z} \quad a + 0 = a \quad \checkmark$$

$$\forall a \in \mathbb{Z} \quad a + \underbrace{(-a)}_{\in \mathbb{Z}} = 0 \quad \checkmark$$

Also, $\forall a, b \in \mathbb{Z},$
 $a+b = b+a \quad \checkmark$

in
geometry
notation

ii) Dih_4 : ^{regular} dihedral group of the 4-gon



→ symmetries of a square.

→ opⁿ: consecutive application.

same thing!

$$G = \left\{ \begin{array}{c} \text{90}^\circ, \text{180}^\circ, \text{270}^\circ, \text{360}^\circ, \cancel{\text{90}^\circ} \\ \text{[diagram of 90}^\circ \text{ rotation]}, \text{[diagram of 180}^\circ \text{ rotation]}, \text{[diagram of 270}^\circ \text{ rotation]}, \text{[diagram of 360}^\circ \text{ rotation]}, \text{[diagram of 90}^\circ \text{ rotation]} \end{array} \right\}$$

Check: $(G, *)$ is a non-Abelian group
 (HW)

• Moral: The above two examples are completely unrelated. But, any general inference about groups, will be true for both of them!

// skipping "Rings"

○ Fields

• $(\mathbb{F}, +, \cdot)$ is called a field iff:

i) $(\mathbb{F}, +)$ is an Abelian group.

Let the identity be 0.

ii) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an Abelian group.

Let the identity be 1.

iii) Distributive Law!

$$\forall a, b, c \in \mathbb{F} \quad a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

• Example: $(\mathbb{Q}, +, \cdot)$ is a field.

with usual meanings.

• Example: Let p be a prime

← ~~⊗~~

$\mathbb{F}_p =$ the set of residues modulo p .
 $= \{0, 1, \dots, p-1\}$

the set of remainders when stuff is divided by p .

$\mathbb{F}_p$ forms a field under addition & multiplication (modulo p)

we keep the remainder

$-a \rightarrow$ additive inverse
 $a^{-1} \rightarrow$ multiplicative inverse

$$5 + 3 \equiv 1 \pmod{7}$$

$$2 \times 6 \equiv 5 \pmod{7}$$

$$3 \times 4 \equiv 2 \pmod{5}$$

$\mathbb{F}_5 \quad \{0, 1, 2, 3, 4\}$

$$3 \times 4 \equiv 2 \pmod{5}$$

3^{-1} both sides (left)

$$\therefore 3^{-1} \cdot 2 = 4 \pmod{5}$$

$$\left. \begin{array}{l} 3 \times 1 \equiv 3 \\ 3 \times 2 \equiv 1 \\ 3 \times 3 \equiv 4 \\ 3 \times 4 \equiv 2 \\ 3 \times 0 \equiv 0 \end{array} \right\} \pmod{5}$$

unique! ($\because 5$ is prime)

more during Finite Fields.

FFT
 the Janglands
 programme

◉ Ordering (Partial Orders / Total Orders)

- A partial order is a relation ($\leq$) on a set (P) which has the following properties:

- i) Reflexivity: $\forall a \in P, a \leq a$.
- ii) Antisymmetry: $a \leq b, b \leq a \Rightarrow a = b$
- iii) Transitivity: $a \leq b, b \leq c \Rightarrow a \leq c$.

Why partial? Because there is a possibility of having incomparable elements as there is a possibility that $a \not\leq b$ & $b \not\leq a$.

- Total order: Partial order + $a \not\leq b \Rightarrow b \leq a$.
(Strongly connected rel.)

- Example: Let A, B be arbitrary sets.

$$A \leq B \quad \text{iff} \quad A \subseteq B.$$

$$\{1, 2\} \leq \{1, 2, 3\} \leq \{1, 2, 3, 4\} \leq \mathbb{N}.$$

$$\{0, 1\} \not\leq 2 \rightarrow \text{Not comparable.}$$

- Another example would be to use functions on a common domain instead of sets

$$\hookrightarrow [0, 1]$$

↓
weak ordering possible!

starts from a digression---

Supremum & Infimum

- A set $A \subseteq \mathbb{R}$ is said to have an upper bound if $\exists M \in \mathbb{R} \mid \forall a \in A, a \leq M$.
- A set $A \subseteq \mathbb{R}$ is said to have a lower bound if $\exists m \in \mathbb{R} \mid \forall a \in A, m \leq a$.
- But, we want the tightest bounds we can get!
- Let $A \subseteq \mathbb{R}$ be a set having an upper bound.
 $M \in \mathbb{R}$ is said to be the "lowest upper bound" (l.u.b) or "Supremum" (sup) iff:
 - i) $\forall a \in A, a \leq M$
 - ii) $\forall M' \leq M, M' \neq M, \exists a \in A \mid a \not\leq M'$
 $M' < M$
- (Similar for "greatest lower bound" (g.l.b) or "Infimum" (inf))
- NOTE: $\mathbb{Q}$ doesn't have sup property.
 $\mathbb{R}$ is the "extension" of $\mathbb{Q}$ which has sup property.
sup property $\Rightarrow$ every upper bounded ^{sub} set has a Supremum.
 $\Updownarrow$
(inf property) same holds for inf.

<https://math.stackexchange.com/questions/2339136/>

$\mathbb{R}$ is constructed from $\mathbb{Q}$ using the sup property!

• Example: $\sup (0,1) = 1$
 $\inf (0,1) = 0$

Similar but distinct from "max", "min".
 $\max (0,1)$ is undefined.

• Connecting back to ordering of sets...

Suppose $A_1, A_2, A_3, \dots$ are sets

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq A_4 \subseteq \dots \subseteq U$$

Define: $A \leq B$ iff $A \subseteq B$.

upper bound.

Then: $A_1 \leq A_2 \leq A_3 \leq \dots \leq U$

Turns out, you can define a supremum!

$$\sup \{ \underbrace{A_1, A_2, \dots}_{\text{"A"}} \} = \bigcup_{i=1}^{\infty} A_i \quad \leftarrow \text{like we said earlier!}$$

Proof:

I: $\forall i, A_i \subseteq A$ $\Rightarrow A_i \leq A$ $\checkmark$ ($\because A$ is union of all)

II: Say $A' \leq A, A' \neq A \therefore A' \subsetneq A$.

$\Rightarrow \exists x \in A, x \notin A'$

$\exists i \mid x \in A_i$ ($\because A$ is union).

$\therefore x \in A_i, x \notin A' \Rightarrow A_i \not\subseteq A' \checkmark$
 $\Rightarrow A_i \not\leq A'$

FIN
 (for the day)

⑥ PROOF WRITING (continued)

○ Commonly Used Proving Techniques

• Direct Proof:

The most basic way. Start with something you know to be true, do manipulations & get the result.

Eg.: (See the Δ proof given earlier)

$$I \Rightarrow \dots \Rightarrow \dots \Rightarrow \dots \Rightarrow P$$

$$(I \Rightarrow P) \equiv P$$

• Proof by Equivalence

Suppose, you want to prove P .

What you can do is first show $P \Leftrightarrow Q$,
or at least $P \Leftarrow Q$.

Then prove Q . (in some way)

A lot of results are known to be equivalent to the Riemann Hypothesis. Proving one of them is enough to prove all of them.

More relevant to researchers than students.

- Proof by Contradiction

First check: $(\neg P) \Rightarrow P) \equiv (T \Rightarrow P)$
 using truth table proof by contradiction normal, direct proof

Suppose you want to prove P .

Equivalently, you can prove that if P were not true, we would get a logical fallacy.

Eg.: $[0, 1]$ is uncountable. $\Rightarrow$ Using Cantor's diagonal method.

Suppose $[0, 1]$ is countable.

Let $[0, 1] =: A = \{a_1, a_2, a_3, \dots, a_n, \dots\} \cong \mathbb{N}$

Write the decimal representation of a_k as:

$$a_k =: 0.d_{k1}d_{k2}d_{k3}d_{k4}d_{k5}d_{k6}d_{k7}\dots$$

$$= \sum_{i=1}^{\infty} d_{ki} \times 10^{-i}$$

Define: $e_j = \begin{cases} d_{jj} + 1, & \text{if } 0 \leq d_{jj} < 9 \\ 0, & \text{if } d_{jj} = 9 \end{cases}$

Notice: $\forall j \in \mathbb{N}, |e_j - d_{jj}| = 1$.

Define: $e := 0.e_1e_2e_3e_4e_5e_6e_7\dots$

$$= \sum_{j=1}^{\infty} e_j \times 10^{-j}$$

Clearly, $0 \leq e \leq 1$

Now, fix $k \in \mathbb{N}$.

$$\begin{aligned} |e - a_k| &= \left| \sum_{j=1}^{\infty} e_j 10^{-j} - \sum_{i=1}^{\infty} d_{ki} 10^{-i} \right| \\ &= \sum_{i=1}^{\infty} \underbrace{|e_i - d_{ki}|}_{=1} \cdot 10^{-i} > 0 \\ &\geq \underbrace{|e_k - d_{kk}|}_{=1} \cdot 10^{-k} > 0. \end{aligned}$$

$$\Rightarrow e \neq a_n \quad \forall n \in \mathbb{N}$$

$$\Rightarrow e \notin \{a_1, a_2, a_3, \dots\} = A \subset [0, 1]$$

Hence, $[0, 1]$ must be uncountable. $(\Rightarrow \Leftarrow)$ 

• Proof by Contrapositive

Suppose you want to prove $(X \Rightarrow Y)$.

Then, equivalently, prove $(\neg Y \Rightarrow \neg X)$

How: Show these two are equivalent. (the "contrapositive")

Common Use: In proving $X \Leftrightarrow Y$.

i) First show: $X \Rightarrow Y$. ↖ "if" part

ii) Then instead of trying to show $X \Leftarrow Y$,
show: $\neg X \Rightarrow \neg Y$ ↖ "only if" part

Extra: " $\Rightarrow$ " is a partial order on statements.

Try proving this yourself! $\hookrightarrow$ so is " $\Leftarrow$ ".

• Converses: The converse of " $X \Rightarrow Y$ " is " $X \Leftarrow Y$ ".

However, the two are not equivalent, unlike contrapositives.

• Proof by Induction (in 1 dimension)

1 dimensional induction can be performed on totally ordered, countable sets.

Without loss of generality, we will perform induction on $\mathbb{N}_0$ or $\mathbb{N}$ or $\{n \in \mathbb{N} \mid n \geq k\}$ for some k .
 $\hookrightarrow k + \mathbb{N}_0$

Suppose we want to prove $P: \forall n \in \mathbb{N} \quad P(n)$.

Ex! $P: \forall n \geq 3, n \in \mathbb{N}$, (the sum of interior angles of a polygon w/ n sides is $180^\circ \times (n-2)$) $\hookrightarrow P(n)$

The idea is:

$\hookrightarrow P(1), P(2), \dots, P(L)$

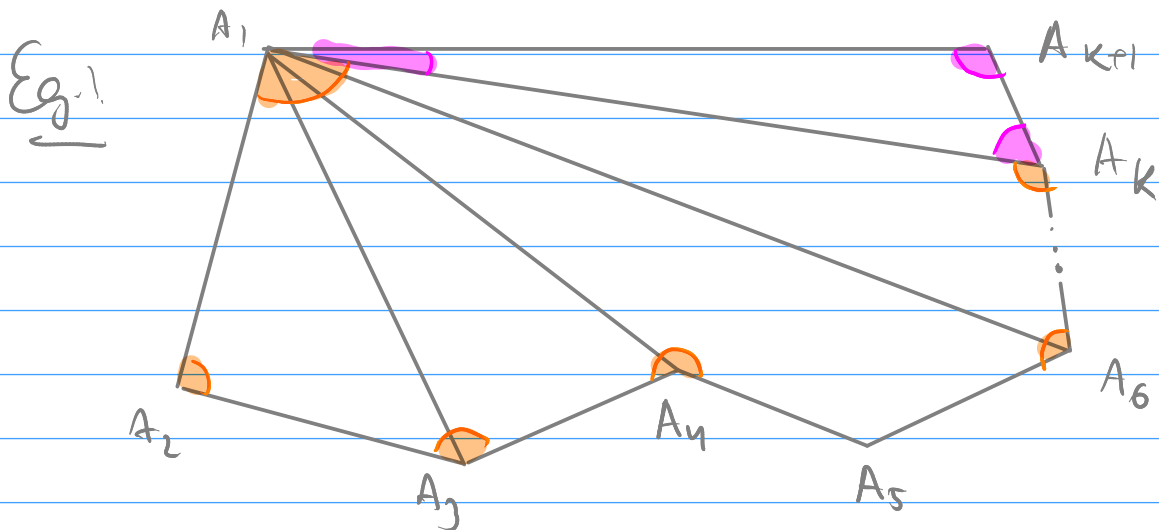
i) Prove a finite number of "base cases" (usually $\{1, \dots, L\}$)

ii) Show, $\exists L \in \mathbb{N} \mid \forall e \geq L, e \in \mathbb{N}, P(e) \Rightarrow P(e+1)$

$\hookrightarrow$ weak induction. $\rightarrow P(e+1)$ comes from $P(e)$ only
strong induction $\checkmark$

ii) Show, $\exists L \in \mathbb{N} \mid \forall e \geq L, e \in \mathbb{N}$,

$P(e+1)$ uses $P(1), P(2), \dots, P(e)$ $\leftarrow$ $\left(\bigwedge_{i=1}^e P(i) \right) \Rightarrow P(e+1)$
 $\downarrow$
 $P(1) \overset{\text{AND}}{\wedge} P(2) \overset{\text{AND}}{\wedge} P(3) \overset{\text{AND}}{\wedge} \dots \overset{\text{AND}}{\wedge} P(e)$



Base Case: $(n=3)$ $\triangle$ case, already done ✓

Induction Hypothesis: Suppose $\forall n \leq k$, sum of int. $\angle$ s of an n -gon is $180^\circ \times (n-2)$

Induction Step: Observe $A_1 A_2 \dots A_k$ is an k -gon
 $\Rightarrow \sum \angle = 180^\circ \times (k-2)$

Now, sum of interior $\angle$ s of $A_1 A_2 \dots A_k A_{k+1}$ is:

$$\sum_{i=1}^{k+1} \angle A_i = \underbrace{\sum \angle}_{180^\circ + (k-2)} + \underbrace{\sum \angle}_{180^\circ} \quad \begin{array}{l} \text{from IH} \\ \text{(induction hypothesis)} \end{array} \quad \begin{array}{l} \text{from} \\ \triangle \text{ case} \end{array}$$

$$= 180^\circ \times (k+1) - 2$$

$\therefore P(k+1)$ holds.

Hence, by the ~~principle of mathematical induction~~ ^{induction} the statement holds $\forall n \geq 3, n \in \mathbb{N}$.

Essentially what happened:

$$P(3), P(k) \Rightarrow P(k+1)$$

$$P(3) \Rightarrow P(4) \Rightarrow P(5) \Rightarrow P(6) \Rightarrow \dots$$

$$\underline{P} \uparrow \mathcal{P}: \forall n \geq 3, n \in \mathbb{N} \quad \underline{P}(n) \leftarrow \text{"sub" of the probs.}$$

https://www.youtube.com/watch?v=6O1s3_GsSHo

↳ more examples (try to solve yourself as well)

⑥

1. The sequence $a_0, a_1, a_2, \dots$ is defined by letting $a_0 = 0$, $a_1 = 1$ and $a_n = 3a_{n-1} - 2a_{n-2}$ for all integers $n \geq 2$. Prove by strong induction on n that $a_n = 2^n - 1$ for all integers $n \geq 0$.
Solution:

Base Case: $(n=0, 1)$ $a_0 = 0 = 2^0 - 1$
 $a_1 = 1 = 2^1 - 1$ } ✓

Induction Hypothesis:

Suppose $\forall n \leq k, n \in \mathbb{N}_0$,
 $a_n = 2^n - 1$.

Induction Step:

$$\begin{aligned} a_{k+1} &= 3a_k - 2a_{k-1} \\ &= 3(2^k - 1) - 2(2^{k-1} - 1) \\ &= 3 \cdot 2^k - 3 - 2^k + 2 \\ &= 2 \cdot 2^k - 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

|| The proof follows
by induction

• Multidimensional Induction

(we will do this in 2 dimensions)

Suppose you want to prove:

$$P: \quad \forall m, n \in \mathbb{N} \quad P(m, n)$$

Split the statement like this:

$$\text{Define } P(m) = \bigwedge_{n \in \mathbb{N}} P(m, n)$$

sub of
propositions

$$\therefore P \equiv \forall m \in \mathbb{N} \quad P(m)$$

Now, for any fixed m , $P(m)$ can be proved
using 1D induction on n

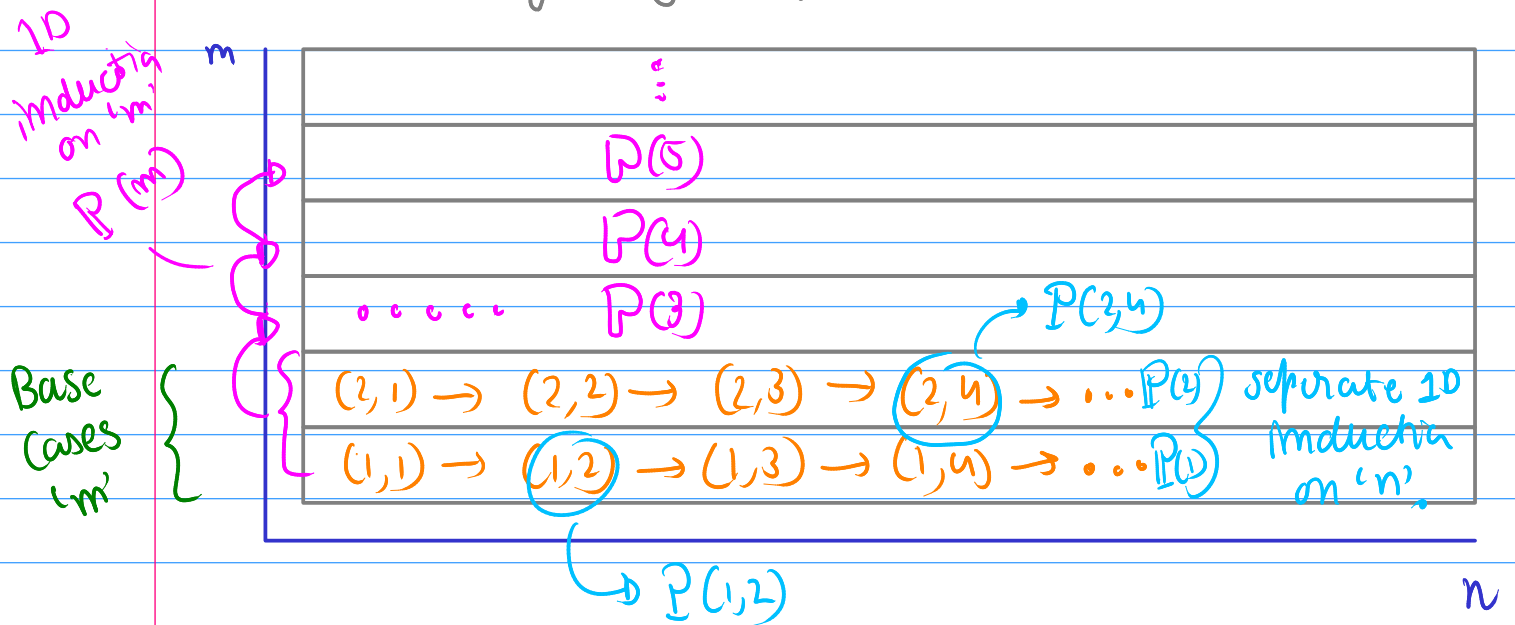
$$(\because P(m) \equiv \forall n \in \mathbb{N} \quad P(m, n))$$

Base case w/ nested induction. { So, identify base cases for m :
 $m_1, m_2, \dots, m_k$
then, prove $P(m_1), P(m_2), \dots, P(m_k)$
using separate 1D inductions on n .

Normal induction on m . { Formulate IH on m as follows:
 $\forall m \in \mathbb{N}, m \leq c \quad P(m)$
Then proceed w/ IS: $P(m) \Rightarrow P(m+1)$

aka : Nested Induction.

What is going on?



$P \rightarrow$ cell (2 arguments) $P(m, n)$
 $P \rightarrow$ row (1 argument) $P(m)$
 $P \rightarrow$ overall (0 arguments)

$$P = \forall m \in \mathbb{N} \quad \underbrace{P(m)}_{\forall n \in \mathbb{N} \quad P(m, n)}$$

Very rarely used.

Disproving a Statement:

- i) Explicit counterexample
- $\rightarrow$ "All primes are odd"
- $\rightarrow$ 2. 

iii) $P \Rightarrow F$
shows P
cannot be
true

- ii) Analytically showing the existence of a counterexample, through constructions, bijections, etc.

Q

A Common Mistake in Induction

induct on $n = \text{cardinality of set.}$

P : All cows are the same colour.

Base Case: $(n=1)$: $\{\text{cow}\}$, obviously  same colour as itself

Induction Hypothesis: $\forall$ sets of cows A , $|A| = n \leq k$ they are of same colour.

Induction Step: Let $A = \{C_1, \dots, C_{k+1}\}$ ^{cows.}

Construct $A' = \{C_1, \dots, C_k\} \subseteq A$
 $A'' = \{C_2, \dots, C_{k+1}\} \subseteq A$

Now, $|A'| = |A''| = k \leq k$.

$\therefore$ By IH: A' , A'' have one colour in them.

$\therefore$ They share elements, A also has only 1 colour of cows. (IS )

By induction, all cows have the same colour. 

HW: Find the mistake in this proof.

FIN
 (for the day) =

② The Cow Conundrum Continued

...

Now, $|A'| = |A''| = k \leq k$.

$\therefore$ By IH: A' , A'' have one colour in them

$\therefore$ They share elements, A also has only
1 colour of cows. (IS $\bullet$)

By induction, all cows have the same colour.

PROBLEM

$P(k)$ $\Rightarrow P(k+1)$ $\cdot \{C_1, \underbrace{[C_2, C_3, \dots, C_k]}_{k \text{ elements}}, \underbrace{C_{k+1}}_{k-1 \text{ common}}\}$
 $\underbrace{\hspace{10em}}_{k \text{ elements}}$

But what if $k=1$? $P(1) \Rightarrow P(2) \quad ??$
 $\underbrace{\hspace{1em}}_{\text{base case (1 cow)}}$
No common elements!

$A = \{ \text{cow 1}, \text{cow 2} \} \begin{cases} \nearrow A' = \{ \text{cow 1} \} \\ \searrow A'' = \{ \text{cow 2} \} \end{cases}$
 They can be diff colours!

$\therefore$ $P(1)$ $\nRightarrow P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow \dots$

Moral:

Appropriate choice of base case!

the first fails

Q

9. If $a_{n+2} = a_{n+1} + a_n$ and $a_1 = 1, a_2 = 1$ then prove using induction that $a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$

Proof:

Base Case: $(n=1)$ $a_1 = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right) \right]$

$$= \frac{1}{\sqrt{5}} \cdot \frac{2\sqrt{5}}{2} = 1$$

$(n=2)$ $a_2 = \frac{1}{\sqrt{5}} \left[\frac{3+\sqrt{5}}{2} - \frac{3-\sqrt{5}}{2} \right]$

$$= \frac{1}{\sqrt{5}} \cdot \frac{2\sqrt{5}}{2} = 1$$

Induction Hypothesis:

Induction Step:

$$\begin{aligned} a_{n+2} &= a_{n+1} + a_n \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{1+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{1-\sqrt{5}}{2} \right) \right] \\ &\quad + \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \cdot 1 - \left(\frac{1-\sqrt{5}}{2} \right)^n \cdot 1 \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{3+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{3-\sqrt{5}}{2} \right) \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{1-\sqrt{5}}{2} \right)^2 \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right] \quad \square \end{aligned}$$

NOTE: Necessary & Sufficient Conditions

If $P \Rightarrow Q$: Q is "necessary" for P .

If $P \Leftarrow Q$: Q is "sufficient" for P .

$$(\neg Q \Rightarrow \neg P)$$

A lot of higher maths revolves around finding necessary & sufficient conditions which are easy to check.

→ equivalences.

Approaches to Writing Proofs

• Bottom-Up Approach

- i) First state & prove lemmas / theorems leading up to your result
- ii) Then, state & prove your main result using the above lemmas / results.

• Top-Down Approach ← my personal preference.

- i) Start by stating & proving your main result, making assumptions about smaller results in the form of hypotheses / claims along the way
- ii) Prove your claims.

Q Prove that $\sqrt{2}$ is irrational.

(Q2) Prove that $\sqrt{2}$ is irrational

Ans. Assume that $\sqrt{2}$ is rational.

$$\sqrt{2} = \frac{a}{b} \text{ with } a \text{ and } b \text{ being co-prime}$$

$$\therefore \frac{a^2}{b^2} = 2 \Rightarrow 2b^2 = a^2 \Rightarrow a^2 \text{ is even}$$

which $\rightarrow$ This shows that a^2 is even, and so is a .
new Replace a with $2p$. Q2m1.

$$2b^2 = (2p)^2 \Rightarrow 2b^2 = 4p^2 \Rightarrow b^2 = 2p^2$$

which shows b is even.

but this means a and b , both are even which is a contradiction to the Assumption. $\Rightarrow \Leftarrow$

Hence by proof by contradiction $\sqrt{2}$ is irrational.

Claim 1: if a^2 is even then a is even.

because odd $\times$ odd, $(2n+1)^2 = 2(2n^2 + 2n) + 1$ is always odd and even $\times$ even that is $2n \times 2n = 4n^2$ is even.

Hence proved.

claim after main proof.

(top-down)

~ Anuvindan

// Extra Topics.

Induction is d-dimensional.

$P: \forall n_1, n_2, \dots, n_d \in \mathbb{N} \quad P(n_1, n_2, \dots, n_d)$

i) Identify base cases for n_1 .
 $\rightarrow n_{11}, n_{12}, n_{13}, \dots, n_{1k_1}$ (k_1 base cases)
 $P(n_1) \leftarrow 1, 2, 3, \dots, k_1$

ii) Prove $P(n_1, n_2, n_3, \dots, n_d)$ using
(d-1) dimensional induction on $n_2, n_3, \dots, n_d$

$P(n_{12}), P(n_{13}), \dots$ Do the same replacing n_{11} w/ other base cases.

iii) Now, perform induction on n_1 to
prove $P(n_1) \Rightarrow P(n_1 + 1) \quad \forall n_1 \geq n_{1k_1}$

Very similar to 2D

last base case

$\hookrightarrow$ Permute $(n_1, n_2, \dots, n_d)$ as convenient.

Out of scope for exams.

// Also discussed in passing:

- Combinatorial Induction / Induction as Recursion
- Zero knowledge proofs.

= END OF PHASE.