

Proof Writing & Mathematical Reasoning

Lec 1

ISI & CMI Crash Course 2024

2024-03-04 05

⊛ Introduction

⊙ What is a set?

- (old) "well-defined collection of objects"
- (new) A set is a mathematical structure possessing a well-defined (unambiguous) notion of inclusion.

Every set defines which elements it contains, and nothing else. So a set is something whose membership we can check.

• Eg.: $S = \dots$

i) $\{1, 2, 3, a, b, c\} \rightarrow$ Is $a \in S$? Yes
Is $\exists \in S$? No. "im"

ii) $\{k \in \mathbb{N} \mid k \text{ is even}\} \rightarrow$ Is $1 \in S$? No
 $4 \in S$? Yes
 $0 \in S$? No

iii) $\{A \mid A \text{ is a set}\} \rightarrow$ Is this a set?

Call this U . Let U be a set.

$$R := \{x \in U \mid x \notin x\}$$

LHS
"is defined"
w/
RHS

$R \in R$? $\rightarrow$ Suppose $R \in R \Rightarrow R \in U \wedge R \notin R \Rightarrow$

$\rightarrow$ Suppose $R \notin R$. By defn of R , $R \in R \Rightarrow$

$\therefore R$ is not a set $\Rightarrow U$ is not a set.

contradiction

Russell's Paradox.

∴ Seemingly "normal" "sets" can have disorders inside them.

⇒ You should be able to unambiguously answer a membership check for a set.

⊙ Basics of Reasoning

- $\wedge, \cdot$ AND "conjunction"
 - $\vee, +$ OR "disjunction"
 - $\neg, \overline{(\cdot)}$ NOT "negation"
 - $\Rightarrow$ "implies" / "is sufficient for" / "only if"
 - $\Leftarrow$ "is implied by" / "is necessary for"
 - $\Leftrightarrow, \equiv$ equivalence "equivalent to" / "if and only if"
 - ↳ "iff"

- Truth Tables. 0 = False, 1 = True.

<u>A</u>	<u>B</u>	<u>$\neg A = \overline{A}$</u>	<u>$A \cdot B$</u>	<u>$A + B$</u>	<u>$A \oplus B$</u> ^{XOR}
0	0	1	0	0	0
0	1	1	0	1	1
1	0	0	0	1	1
1	1	0	1	1	0

Check:

$$\begin{array}{l} (A \oplus B) = (A \cdot B) + (\overline{A} \cdot \overline{B}) \\ \overline{(A + B)} = \overline{A} \cdot \overline{B} \\ (A \cdot B) = \overline{\overline{A} + \overline{B}} \end{array} \left. \vphantom{\begin{array}{l} (A \oplus B) = (A \cdot B) + (\overline{A} \cdot \overline{B}) \\ \overline{(A + B)} = \overline{A} \cdot \overline{B} \\ (A \cdot B) = \overline{\overline{A} + \overline{B}} \end{array}} \right\} \text{de Morgan Law} \quad \parallel \quad \overline{\overline{A}} = A$$

commutative

Order of precedence: NOT > AND > OR
 $A \cdot B = B \cdot A$, $A + B = B + A$, associative
 distributive: $A \cdot (B + C) = A \cdot B + A \cdot C$

- $A \Rightarrow B$ when A is true, B must be true

<u>A</u>	<u>B</u>	<u>$A \Rightarrow B$</u>	<u>$\bar{A} + A \cdot B$</u>
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

they
are
same!

$A \Leftrightarrow B$ A and B are always same.

By defn: $(A \Rightarrow B) \Leftrightarrow (B \Leftarrow A)$

Also, $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (A \Leftarrow B)$
 $\Leftrightarrow \neg (A \oplus B)$

○ Basic Predicate Logic

- $\in$ inclusion "in" / "belongs to" } $x \in A$ same
 $\supset$ containment "contains" } $A \supset x$ same
 $\exists$ "there exists"
 $\exists!$ "there exists unique"
 $\forall$ "for all"

- Eg: (---)

⊙ Basic Set Operations

- $A \subseteq B$ "subset" $x \in A \Rightarrow x \in B$ ∃ st. such that
 $A \supseteq B$ "superset" $B \subseteq A$ ↓
 $A \subsetneq B$ "proper subset" $A \subseteq B, \exists x \in B \mid x \notin A$

- $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
 $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
 $A \setminus B = \{x \in A \mid x \notin B\}$
 $A \Delta B = A \setminus B \cup B \setminus A$

HW Verify comm., assoc, distributive, de Morgan, etc. hold.

- $\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup \dots \cup A_n$
 $\bigcup_{\alpha \in A} S_\alpha = \{x \mid (\exists \alpha \in A \mid x \in S_\alpha)\}$
↘ indexing set
(same for intersections)

⊙ Power Set

- The power set of A , denoted by $P(A)$ or 2^A is the set of all subsets of A , including itself and $\emptyset$ (the empty set)

- Result: $A = 2^A \Leftrightarrow A = \emptyset$

⊛ Relations and Functions

⊙ Cartesian Product

• Defⁿ: $A \times B = \{ \overbrace{(a, b)}^{2\text{-tuple / ordered pair}} \mid a \in A, b \in B \}$

• Eg.: $\{1, 2, 3\} \times \{10, 11\}$ ✓

⊙ Relation

• Defⁿ: A relation R from A to B is simply a subset of $A \times B$: $R \subseteq A \times B$

A relation R on A : $R \subseteq A \times A$

• We say $x R y$ iff $(x, y) \in R$

⊙ Properties of relations on a set

Say $R \subseteq A \times A$

• Reflexivity $\forall a \in A, a R a$

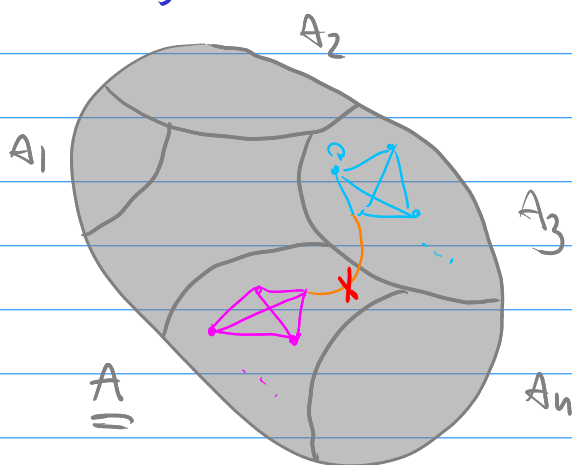
• Symmetry $a R b \Rightarrow b R a$

• Transitivity $a R b, b R c \Rightarrow a R c$

A relation which is reflexive, symmetric & transitive is called an equivalence relation.

- Observe: An equivalence relation $\mathcal{R}$ on A partitions A into non-overlapping, exhaustive equivalence classes $A_1, A_2, \dots, A_k$

Inside each class, all elements are related to each other, and elements of two distinct classes are not related.



SIDE NOTE

All partitions are isomorphic to equivalence relations.

equiv. classes $\hookrightarrow$ A partition of $A = \{A_i\}$ st. $\forall i \neq j, A_i \cap A_j = \emptyset$
 $\bigcup_i A_i = A$
 $\subseteq 2^A \rightarrow$ subsets pairwise disjoint
 $\hookrightarrow$ exhaustive
 Corresp $\mathcal{R} := \bigcup_i A_i^2$ $\hookrightarrow A_i \times A_i$
 (HW) Justify $\uparrow$

(6) Write the relation explicitly, state & prove if they are R, S, T. If all 3, what are the equivalence classes?

i) $\mathcal{R} \subseteq \mathbb{Z}^2, a \mathcal{R} b$ iff $a \leq b$
 $a > b$

ii) $\mathcal{R}_k \subseteq \mathbb{N}_0^2, a \mathcal{R}_k b$ iff $k \mid a-b$

$\hookrightarrow k$ divides $a-b$.

① Functions

- Defn: $f \subseteq A \times B$ is said to be a function from A to B
iff: $\forall a \in A, \exists! b \in B \mid (a, b) \in f$

This is written as: $f: \overset{\text{domain}}{A} \rightarrow \overset{\text{codomain}}{B}$
 $\underbrace{a}_{\text{pre-image of 'b'}} \mapsto \underbrace{b =: f(a)}_{\text{image of 'a' of 'f'}} \leftarrow \text{"maps to"}$

- Suppose, $A' \subseteq A$ $f(A') := \{f(a) \mid a \in A'\} \subseteq B$
Now, $f(A)$, the set of all possible images is called range

- Inverses: Consider $f: A \rightarrow B \ni b$

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

= set of all pre-images of b

- Injective / One-One functions.

$f: A \rightarrow B$, f is injective iff $\forall b \in B$
 $f^{-1}(b)$ has at most 1 element
 $\hookrightarrow$ No many-one mappings.

- Surjective / Onto functions.

$f: A \rightarrow B$, f is surjective iff $\forall b \in B$
 $f^{-1}(b)$ has at least 1 element
 $\hookrightarrow$ Codomain = Range

unique inverse /
one-one corresp. b/w
elements of
 A & B

• Bijjective / Inversible Functions

A function that is both injective & surjective is called bijective. Notice $\forall b \in B$, $f^{-1}(b)$ is a singleton, say $\{a\}$.
By abuse of notation, write $f^{-1}(b) := a$.

• Cardinality

• Very loosely, how "big" the set is.

• We say $A \cong B$ iff $\exists$ bijection $\varphi: A \rightarrow B$
Essentially, elements can be placed in one-one
If $A \cong B$, $|A| = |B|$ some cardinality corresp.

• $\forall n \in \mathbb{N}$, $N_n := \{1, 2, \dots, n\}$ (HW)
Now: $|N_n| := n$
 $|\emptyset| := 0$ } $\rightarrow$ for finite sets, $|A| =$ no. of elements in A ($\therefore$)

• For an infinite set A ,

i) if $A \cong \mathbb{N}$, we call A countable: $|A| = |\mathbb{N}| = \aleph_0$
ii) otherwise, we call A uncountable.

=

Up Next: $\mathbb{Z}$, $\mathbb{Q}$ are countable
 $\mathbb{R}$ is uncountable.

But first a bit about proofs...

(HW)

$$|2^A| = 2^{|A|}$$

$$|A \times B| = |A| |B|$$

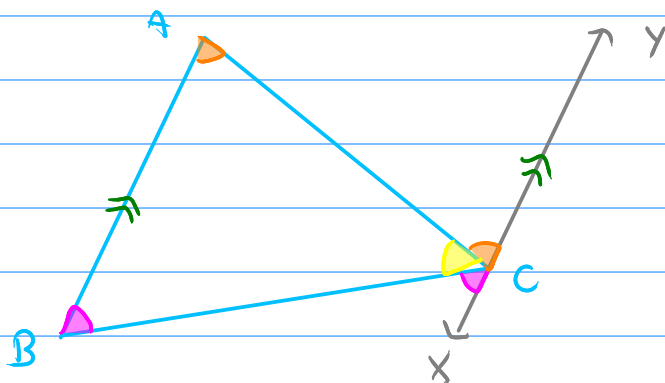
do for finite sets



Proofs

⊙ What is a proof?

- A proof is a sequence of logical steps from something known to be true, to some unknown proposition; o.e.: $\boxed{1 \Rightarrow P}$ is a proof of P .
- Why? Check $(1 \Leftrightarrow P) \Leftrightarrow P$. $\parallel$ If $1 \Rightarrow P$ and $P \Rightarrow 1 \quad \forall P$ then P
- An axiom is a statement taken to be true without proof. Eg.: ZF/ZFC in set theory.
Euclid's postulates in geometry.
- Eg.: Prove that the sum of angles of a triangle in Euclidean space is 180° .



$AB \parallel XY$

By alternate int. $\angle$ s

○ $\angle A = \angle ACY$;

● $\angle B = \angle BCX$;

● $\angle ACB = \angle ACB$

(+) $\Delta = 180^\circ$

↪ Classic direct proof.

angles on one side of a line...

⑥ Commonly Used Proving Techniques.

- Direct Proof. Like we just saw, start w/ a true statement, and manipulate:

$$\textcircled{1}^{\text{tautology}} \Rightarrow \dots \Rightarrow \dots \Rightarrow \dots \Rightarrow \textcircled{P} \quad \square$$

- Proof by Equivalence: Establish $P \Leftrightarrow Q$

Then proceed to prove Q . More relevant to researchers than students, as if Q is not proven yet, you can't prove Q . In research, often problems are shown to be equivalent to a known difficult conjecture / hypothesis (eg.: Riemann Hypothesis) and left at that. If that conjecture is proven later, all these problems are automatically solved. Conversely, if you prove any of them, all of them are solved. ($P=NP?$ like situation)

- Proof by (Successive) Reduction / Sufficiency.

Suppose you want to prove P . Show $P \Leftarrow Q$. Then try to prove Q . Q is sufficient for P $\Leftarrow$ (repeat this).

~ "Claim Chain" $\Rightarrow$

TST: $\dots$

Claim 1: $\underline{\hspace{2cm}}$

Claim 2: $\underline{\hspace{2cm}}$

(Later)

Proof of Claim 1:

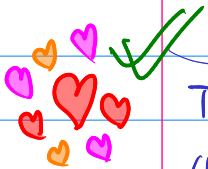
Proof of Claim 2

TST: $\dots$

suffices to show: $\boxed{\text{Answer}}$

top-down approach

bottom-up: Prove lemmas / claims first, main part later.



- Proof by Contradiction

Usually, we want $\boxed{1 \Rightarrow P}$ Negate both sides: $(\neg 1 \Leftarrow \neg P) \Leftrightarrow \boxed{\neg P \Rightarrow 0}$

Start with the opposite of P , and show that it leads to something impossible (i.e. a contradiction)

Eg: $\sqrt{2}$ is irrational (HW)

- Proof by Contrapositive

Suppose, you want to prove $P: X \Rightarrow Y$.
Equivalently, prove the contrapositive: $\neg Y \Rightarrow \neg X$
(HW) Hint: Use truth tables.

Commonly used to prove $\boxed{X \Leftrightarrow Y}$ statements.
i) First prove $X \Rightarrow Y$. (if part)
ii) Next, instead of proving $X \Leftarrow Y$, prove: $\neg X \Rightarrow \neg Y$. (only if part)

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

! IMPORTANT: Converse, unlike contrapositives are not equivalent.

- Proof by Induction (Later)

★ notations & terms differ from place to place & book to book.

① Countable / Uncountable Sets.

• (Recap) Sets $A \cong \mathbb{N}$ are called countable.

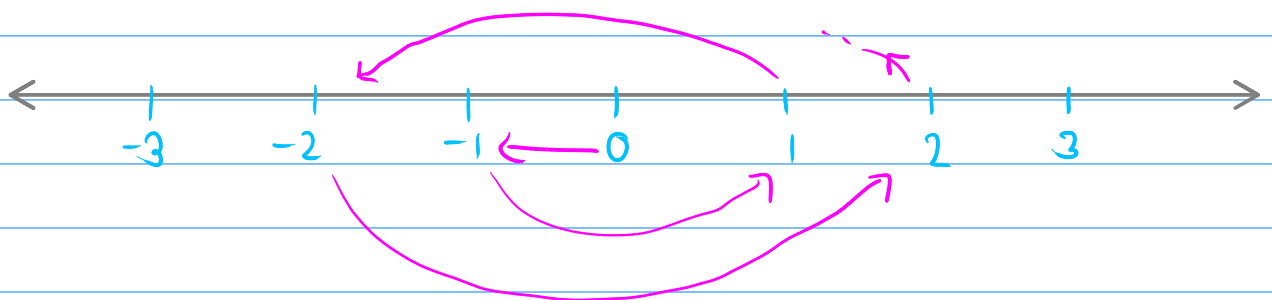
• **! IMPORTANT:** Finite sets are not countable.

• $\mathbb{N}_0$ is countable: $\varphi : \mathbb{N}_0 \rightarrow \mathbb{N}$ (HW)
 $a \mapsto a+1$
 check this is bijection ←

• $\mathbb{Z}$ is countable: $\varphi : \mathbb{Z} \rightarrow \mathbb{N}$
 $0 \mapsto 1$
 if $a \in \mathbb{N}$, $a \mapsto 2a+1$
 if $-a \in \mathbb{N}$, $a \mapsto -2a$

$\varphi :$

	-3	-2	-1	0	1	2	3
↓	6	4	2	1	3	5	7



So, in a sense, there are as many integers as there are natural numbers, even though $\mathbb{N} \neq \mathbb{Z}$

→ Infinities are weird!

(HW) Prove φ is really a bijection.

- $\mathbb{Q}$ is countable

https://proofwiki.org/wiki/Rational_Numbers_are_Countably_Infinite/Proof_2

Claim 1: If A, B countable, then $A \times B$ countable

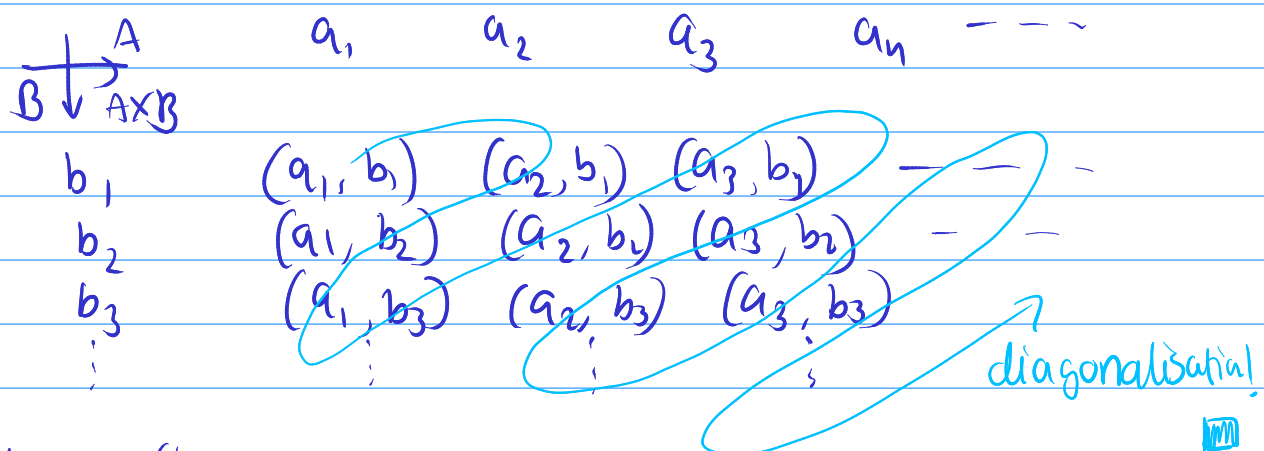
Claim 2: If $f: A \rightarrow B$ injective, B countable
then A is countable.

Now, for any $p/q \in \mathbb{Q} \mid p \in \mathbb{Z}, q \in \mathbb{N}$
 $\gcd(p, q) = 1$,
define $\varphi: \downarrow$
 (p, q) This is clearly injective.

$\therefore \varphi$ is an injection from $\mathbb{Q}$ to $\mathbb{Z} \times \mathbb{N}$.

By claim ① & ②: $\mathbb{Q}$ is countable. 
 $\because \mathbb{Z}, \mathbb{N}$ are countable $\Rightarrow \mathbb{Z} \times \mathbb{N}$ countable.

Proof of Claim 1: (H.W) Make this rigorous.



Proof of Claim 2: Each point in the range has
a unique pre-image.

$\therefore$ Range $\subseteq$ codomain, $|\text{range}| = |\text{domain}|$, countable
(or finite) 

• $\mathbb{R}$ is uncountable

W/o loss of generality, take $(0,1)$ only.

For $\mathbb{R}$, we use $f: \mathbb{R} \rightarrow (0,1)$

$$x \mapsto \frac{1}{2} + \frac{1}{\pi} \tan^{-1}(x)$$

famous
bijection.

TST: $(0,1)$ is uncountable.

Let us proceed by contradiction.

Suppose $(0,1)$ is countable $\Rightarrow \exists \phi: \mathbb{N} \rightarrow (0,1)$ bijection.

Denote $a_i = \phi(i)$, $i \in \mathbb{N}$.

$$\therefore (0,1) = \{a_1, a_2, a_3, \dots\}$$

Suppose we write a_i in normalised decimal form.

$$a_i = \sum_{j=1}^{\infty} d_{ij} 10^{-j}, \quad \left(\nexists N \in \mathbb{N} \mid \forall j > N, d_{ij} = 9 \right)$$

$d_{ij} \in \{0, 1, \dots, 9\}$

$\rightarrow 0.7999\dots \otimes$

Construct a_0 as follows.

i) $\Psi: \{0, 1, \dots, 9\} \rightarrow$ (non-trivial permutation)
say $0 \mapsto 1, 1 \mapsto 2, \dots, 8 \mapsto 9, 9 \mapsto 0$.

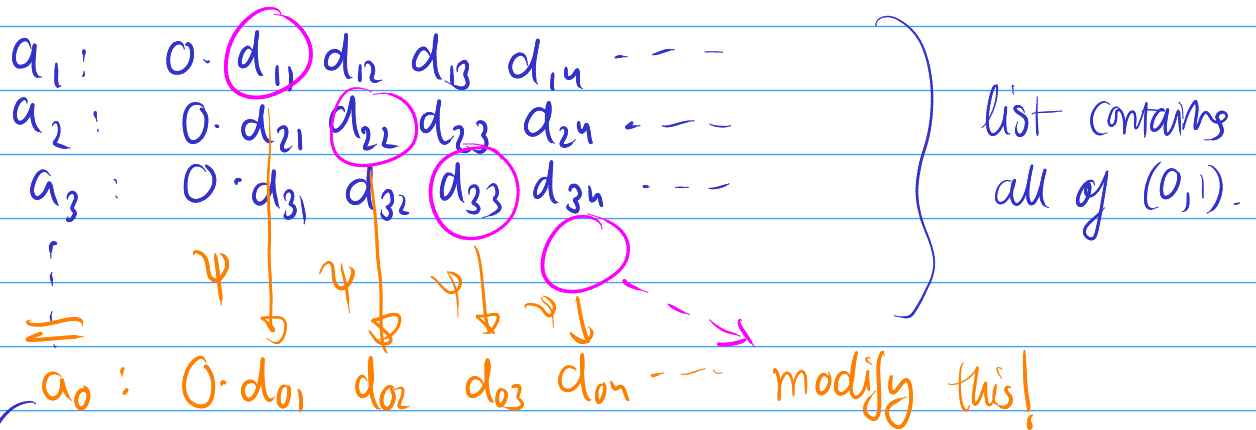
ii) $d_{0j} := \Psi(d_{ij}) \rightarrow \forall j \mid \Psi(d_{ij}) - d_{ij} \geq 1$.

iii) $a_0 := \sum_{j=1}^{\infty} d_{0j} 10^{-j}$ $\left\{ \begin{array}{l} \forall i, a_i \neq a_0 \\ \Rightarrow a_0 \notin (0,1) \end{array} \right\}$

Now, fix any $i \in \mathbb{N}$, $|a_0 - a_i| \geq |d_{0i} - d_{ii}| 10^{-i} \geq 10^{-i} > 0$

Small technicalities ignored.

Visualising:



$\Rightarrow$ differs from all of the above in at least one place
 $\Rightarrow$ NOT part of list
 $\Rightarrow$ list was not complete! $\Rightarrow \leftarrow$

⊙ Mathematical Induction

- Induction is typically used to prove $P: \forall n \in \mathbb{N} P(n)$.
Typically, $n \in \mathbb{N}$, (can be done for whole numbers, subsets, etc)

- The Idea: An "incremental" proof.

Weak Induction

- Prove a "base case" (typically $n=1$, sometimes $0, d$)
- Prove: $[P(k) \Rightarrow P(k+1)] \forall k \in \mathbb{N}$.
 (assume $P(k) \rightarrow$ induction hypothesis (IH)
 induction step (IS): Using the IH for k ,
 prove it for $k+1$ (might be complicated))

Then we have: $P(1) \Rightarrow P(2) \Rightarrow \dots \Rightarrow P(k) \Rightarrow \dots \infty$
 $\Rightarrow$ cascades

$\therefore P$ follows.

$\Rightarrow$ for strong form: $(\bigwedge_{i=1}^k P(i)) \Rightarrow P(k+1)$ (you assume $P(1), \dots, P(k)$ for proving $P(k+1)$).

- In a slightly more general setup, there may be multiple but finitely many base cases;
 and $\bigwedge_{i=1}^k P(i) \Rightarrow P(k+1)$ (weak) } may hold only after some $k \geq L$.
 $\bigwedge_{i=1}^k P(i) \Rightarrow P(k+1)$ (strong) }
 (before that, base cases & manual checking) for some $L \in \mathbb{N}$

② Prove by Induction: [2024 Yearlong p. 33-34]

HCU

- For $n \geq 3$, the sum of interior angles of an n -gon is $180^\circ \times (n-2)$.
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 $n \geq 0$.

Hint: i) Take out a single $\triangle$:



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

more examples (try to solve yourself as well)

② (Fibonacci numbers)

HCU

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



WARNING:

Always check if $P(k) \Rightarrow P(k+1)$ actually holds for base case k

$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \dots \Rightarrow P(k) \Rightarrow \dots$
 $\times \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark$

Ref: Cow Conundrum
 2024 Yearlong p. 37-38

irrelevant!