MATH 347

FUNDAMENTAL MATH

w/ Prof AJ Hildebrand

Meets @ Sidney Lu 2055, MWF 02:00 PM - 02:50 PM

Wednesday, January 22nd 2025

Set-theoretic Notations & Terminology

① Sets

Example: $\{1, 5, 7\}$ "set of three elements"

elements

use curly braces

→ $\{1, 5, 7\}$ same set as $\{1, 7, 5\}$

Order doesn't matter

→ $\{1, 7, 1, 5\}$ same set as $\{1, 7, 5\}$

duplicated elements don't count

Some standard sets

- $\mathbb{N} = \{1, 2, 3, \ldots\}$: natural numbers
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$: integer numbers
- $\mathbb{R}$: real numbers
- $\mathbb{Q}$: rational numbers
- ϕ (or $\{ \}$) : empty set

Set-builder notation:

things, constraint

- Example: $\{2k+1 : k \in \mathbb{Z}\} = \{\ldots, -3, -1, 1, 3, \ldots\}$

  "set of all $2k+1$ such that $k \in \mathbb{Z}$"

  "k is element of $\mathbb{Z}$", "k integer"

$\{2k+1 : k \in \mathbb{Z}\}$: set of all odd numbers

- Example: $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$

  Rational numbers are ratio of 2 integers

  Denominator $\neq 0$

Set operations:

- Union: $A \cup B = \{x : x \in A \text{ or } x \in B\}$

  non-exclusive

- Intersection: $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- Set-theoretic difference: $A \setminus B = \{x : x \in A \text{ and } x \notin B\} = \{x \in A : x \notin B\}$

Friday, January 24th 2025

Introduction to Proofs

① Structure

"If P, then Q"
"Suppose P. Then Q"
"Assume P. Then Q"
} same meaning $P \Rightarrow Q$

Ex: If $\overset{P}{\text{n, m even integer}}$, then $\overset{Q}{\text{n+m also even } \mathbb{Z}}$

Basic structure of a proof of a statement of form $P \Rightarrow Q$:

$\boxed{\text{Assume } P}$
$\downarrow$ logical deductions
$\boxed{\text{Therefore } Q}$

Proof construction

- Stage 1: scratch, come up w/ outline or flowchart
- Stage 2: write up in proper logical order

Practice: "Even/odd proofs"

Assumptions:

- Meaning/definitions of $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$
- Basic arithmetic operations $(+, -, \times, \div)$
- Not going to use any number theory (congruences, mod arithmetic)
- n even $\Leftrightarrow$ $n = 2k$ for some $k \in \mathbb{Z}$
- n odd $\Leftrightarrow$ $n = 2k+1$ for some $k \in \mathbb{Z}$
- Properties of addition and multiplication
  - Ex: commutative, associative
- Any integer is either even or odd, not both

proof Ex: Prove if n even and m even $\Rightarrow$ $n+m$ even

$\boxed{\text{Assume } n \text{ even and } m \text{ even}}$

$n = 2k$, $m = 2h$, where $k, h \in \mathbb{Z}$

$n+m = 2k+2h = 2(k+h)$

Notice that $k+h$ is an integer since $k, h \in \mathbb{Z}$

By definition of even numbers, $n+m$ is even

$\downarrow$

$\boxed{\text{Therefore } n+m \text{ even}}$

Monday, January 27th 2025

Proof Techniques

1. Direct : Assume P $\xrightarrow{\text{logical deduction}}$ Therefore Q $\boxed{P \Rightarrow Q}$
2. Contraposition : Assume Q false $\xrightarrow{\text{logical deduction}}$ Therefore P false $\boxed{\neg Q \Rightarrow \neg P}$
3. Contradiction : Assume Q false and P $\xrightarrow{\text{logical deduction}}$ Contradiction
4. Proof by cases : Split into different cases (often combined w/ other techniques)

Ex: 2(b) from Even/Odd WS ("Prove for $n \in \mathbb{Z}$, if $\underbrace{n^2 \in 2\mathbb{Z}}_{P}$, then $\underbrace{n \in 2\mathbb{Z}}_{Q}$")

→ Direct proof

$n^2 \in 2\mathbb{Z}$, then $\exists k \in \mathbb{Z}$ s.t. $n^2 = 2k$

$n = \sqrt{2k}$

DOESN'T WORK

→ Contraposition

Assume $n \notin 2\mathbb{Z}$, then $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$4k^2 + 4k \in \mathbb{Z}$, then $n \in 2\mathbb{Z}+1 \Rightarrow n^2 \in 2\mathbb{Z}+1$

$n \notin 2\mathbb{Z} \Rightarrow n^2 \notin 2\mathbb{Z}$ By contraposition: $n^2 \in 2\mathbb{Z} \Rightarrow n \in 2\mathbb{Z}$

Ex: 3 from Even/Odd WS ("Prove that a sum of two odd perfect squares is never a perfect square")

"If n and m are odd, then $n^2 + m^2$ can't be a perfect square"

Wednesday, January 29th 2025

Quiz next wednesday !!

Proof by Contradiction

What if only form Q ?

$P \Rightarrow Q$

Assume $P \wedge \neg Q$

↓

Contradiction

Ex: $\sqrt{2}$ is irrational

- Suppose $\sqrt{2}$ is rational
- Then by definition of rational numbers, $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{Z} \wedge q \neq 0$
- Squaring both sides, $2 = \frac{p^2}{q^2}$ and $p^2 = 2q^2$
- As q is an integer, q^2 also an integer, thus p^2 even
- If p^2 even, then $p = 2k$, $k \in \mathbb{Z}$
- $2 = \frac{4k^2}{q^2} \rightarrow q^2 = 2k^2$
- q^2 even, then $q = 2j$

Friday, January 31st 2025

Set-Theoretic Proofs

Ex: (i.) $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

(ii.) $A \setminus (A \setminus B) \subseteq B$

Tools: definition of set operations

- $x \in A \cup B \iff x \in A$ or $x \in B$
- $x \in A \setminus B \iff x \in A$ and $x \notin B$
- $x \notin A \setminus B \iff x \notin A$ or $x \in B$

Proof-template to prove $S \subseteq T$

Definition of $S \subseteq T$: If $\underbrace{x \in S}_{P}$, then $\underbrace{x \in T}_{Q}$.

Assume $x \in S$.

$\downarrow$

Therefore $x \in T$

Monday, February 3rd 2025

Logical Statements

Logical implication $\boxed{P \Rightarrow Q}$

- "P implies Q"
- "If P true, then Q true"

Truth Values of "$P \Rightarrow Q$"

- $P \Rightarrow Q$ false if P true and Q is false
- $P \Rightarrow Q$ true in all other case
- If P is false, "$P \Rightarrow Q$" is true regardless of Q
- Doesn't say anything abt truth of P or Q itself

Wednesday, February 5th 2025

Negations of logical statements

- $\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$
- $\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$ } Flip the sign!
- $\neg(P \Rightarrow Q) \iff P \wedge (\neg Q)$ $*$

Consequence of $(*)$: Negation of implication $P \Rightarrow Q$ is never equivalent to another implication involving P & Q and their negations

Ex: Negation of "If A is true, then B is true"

$\neg(A \Rightarrow B) \iff A \wedge \neg B$

Negation: "A is true and B is false"

Quantifiers ("for all", "exists")

- $\forall$: for all, example: for all $x \in \mathbb{R}$, $x < 5$: $\forall x \in \mathbb{R}, x < 5$
- $\exists$: exists, example: exists an $x \in \mathbb{R}$ such that $x < 5$: $\exists x \in \mathbb{R}$ s.t. $x < 5$
- Negation rules:
  - $(\forall x \in S)(P(x))$ "For all $x \in S$, $P(x)$ is true"

    $\neg(\forall x \in S)(P(x)) \iff (\exists x \in S)(\neg P(x))$ "Exists an $x \in S$ such that $P(x)$ is false"
  - $(\exists x \in S)(P(x))$ "Exists an $x \in S$ s.t. $P(x)$ is true"

    $\neg(\exists x \in S)(P(x)) \iff (\forall x \in S)(\neg P(x))$ "For all $x \in S$, $P(x)$ is false"

Ex: "All classrooms have at least one broken chair"

Negation: Exists a classroom that has no broken chairs

Ex: "If $x \notin \mathbb{Q}$, then $x^2 \notin \mathbb{Q}$"

$\forall x \in \mathbb{R}, x \notin \mathbb{Q} \Rightarrow x^2 \notin \mathbb{Q}$

Negation: $\exists x \in \mathbb{R}$ s.t. $x \notin \mathbb{Q}$ and $x^2 \in \mathbb{Q}$

Friday, February 5th 2025

Def: Assume f is a function from $\mathbb{R}$ to $\mathbb{R}$. (i.e. f maps $x \in \mathbb{R}$ to a unique $y \in \mathbb{R}$, $y = f(x)$)

$$f \text{ bounded} \iff \underbrace{(\exists M > 0)(\forall x \in \mathbb{R})[|f(x)| \leq M]}_{\text{definition of bounded function}}$$

Negation of a bounded function

$$\neg (\exists M > 0)(\forall x \in \mathbb{R})[|f(x)| \leq M]$$
$$(\forall M > 0)(\exists x \in \mathbb{R})[|f(x)| > M]$$

Ex: $f(x) = x$ is not bounded

Proof: Let $M > 0$ be given. Take $x = M+1$. Thus, $f(x) = M+1$, and evidently $M+1 > M$. Thus, we have shown that there exists an x such that $|f(x)| > M$ □

All functions from $\mathbb{R}$ to $\mathbb{R}$:

$$(\forall x \in \mathbb{R})(\exists M > 0)[|f(x)| \leq M]$$

Proof: Let $f(x)$ be an arbitrary function from $\mathbb{R}$ to $\mathbb{R}$. Let $x \in \mathbb{R}$ be given. Take $M = |f(x)| + 1$. Then evidently, $|f(x)| \leq |f(x)| + 1$ is true. Therefore, there does exists an M such that for all $x \in \mathbb{R}$ the statement is true □

Difference: $(\exists M > 0)(\forall x \in \mathbb{R})[|f(x)| \leq M]$ same M has to work for every x, M chosen first

$(\forall x \in \mathbb{R})(\exists M > 0)[|f(x)| \leq M]$ x picked first, so we can customize M according to needs

Monday, February 10th 2025

MIDTERM WEDNESDAY 26TH FEB

Assume $f: \mathbb{R} \to \mathbb{R}$

Definitions: a.) f is increasing (strictly increasing) $\iff (\forall x,y \in \mathbb{R})\,[x<y \Rightarrow f(x) < f(y)]$

b.) f is non-decreasing (weakly increasing) $\iff (\forall x,y \in \mathbb{R})\,[x<y \Rightarrow f(x) \leq f(y)]$

c.) f is decreasing (strictly decreasing) $\iff (\forall x,y \in \mathbb{R})\,[x<y \Rightarrow f(x) > f(y)]$

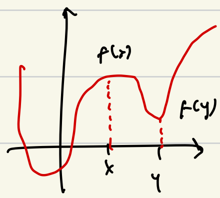
d.) f is non-increasing (weakly decreasing) $\iff (\forall x,y \in \mathbb{R})\,[x<y \Rightarrow f(x) \geq f(y)]$

NOT-increasing vs NON-increasing $\iff (\forall x,y \in \mathbb{R})\,[x<y \Rightarrow f(x) \geq f(y)]$

$\Updownarrow$

$(\exists x,y \in \mathbb{R})\,[x<y \wedge f(x) \geq f(y)]$

EX: Not increasing, but not non-increasing



Revisiting proof techniques:

1. $P \Rightarrow Q$ with direct : $P \Rightarrow Q$ logical structure
2. $P \Rightarrow Q$ with contraposition : $\neg Q \Rightarrow \neg P$ logical structure
3. $P \Rightarrow Q$ with contradiction : $(P \wedge \neg Q) \Rightarrow C$ logical structure

   false statement, contradiction
4. P with contradiction : $\neg P \Rightarrow C$ logical structure (*)

* Why does proof by contradiction work ?

$\boxed{\neg P \Rightarrow C}$

$\Updownarrow$

$\neg P$ true $\wedge$ C true

$\neg P$ false $\wedge$ C true

$\neg P$ false $\wedge$ C false

As C is always false

Then $\neg P$ must be false

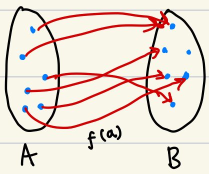
So P is true

$\iff \neg P$ false $\iff P$ true

Wednesday, February 12th 2025

Functions

DEF: Given non-empty sets A and B, a function f from A to B is an assignment of a unique element $f(a)$ to each element $a \in A$



Properties:
- Injective: one element of A maps to exactly one element in B
- Surjective: every element in B is mapped by elements in A
- Bijective: both injective and surjective

Ex: $f(x) = x^2$

① $f: \mathbb{R} \to \mathbb{R}$

Not injective since $f(x) = f(-x) = x^2$

Not surjective as cannot hit negative reals

② $f: \mathbb{N} \to \mathbb{N}$

Injective

Not surjective as only perfect squares possible

③ $f: [0,1] \to [0,1]$

Injective and surjective (bijective)

DEF: A function is called injective if and only if for every numbers $x, y \in A$ where $x \neq y$, then $f(x) \neq f(y)$.

f injective $\Leftrightarrow (\forall x, y \in A)[x \neq y \Rightarrow f(x) \neq f(y)] \Leftrightarrow (\forall x, y \in A)[f(x) = f(y) \Rightarrow x = y]$

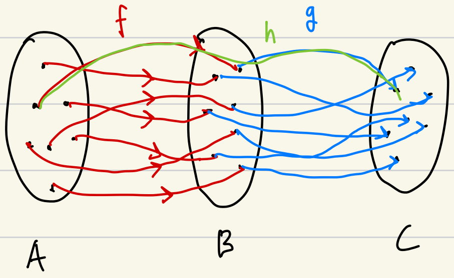
DEF: A function is called surjective if and only if for every numbers $b \in B$, there exists an $a \in A$ s.t. $f(a) = b$.

f surjective $\Leftrightarrow (\forall b \in B)(\exists a \in A)[f(a) = b]$

Friday, February 14th 2025

Composition of functions

Given $f: A \to B$ and $g: B \to C$. The composition of g and f is the function defined by $(g \circ f)(a) = g(f(a))$ where $a \in A$ and the output $g(f(a)) \in C$.



Proof of injectivity

Steps:

1. Let $x, y \in A$
2. Assume $f(x) = f(y)$
3. Logical deductions
4. Therefore, $x = y$

Conclusion: Hence, f is injective

Ex: Show that if f ∧ g injective, then $h = g \circ f$ injective.

Let $f: A \to B$, $g: B \to C$, and both f and g are injective. Let $x, y \in A$ be given, and assume $h(x) = h(y)$. Then, by the definition of composition, $g(f(x)) = g(f(y))$. Because g is injective, $f(x) = f(y)$. f is injective, thus it follows that $x = y$. We have shown that $h(x) = h(y)$ implies $x = y$. Thus, h is injective □

Monday, February 17th 2025.

Proofs of surjectivity

Def: f surjective $\Leftrightarrow (\forall b \in B)(\exists a \in A)[f(a) = b]$ "every $b \in B$ is a map of $a \in A$"

corollary: f not-surjective $\Leftrightarrow (\exists b \in B)(\forall a \in A)[f(a) \neq b]$

Assume $f: A \to B$, $g: B \to C$ and $h: A \to C$ is the composition $h = g \circ f$

Ex: "If h is surjective, then g is surjective"

Flow chart: Assume h surjective $\Leftrightarrow (\forall c \in C)(\exists a \in A)[h(a) = c]$

$\downarrow$

Assume $c \in C$

$\downarrow$ by def. of surjec (h)

$\exists a \in A$ s.t. $h(a) = c$

$\downarrow$ by def. of comp. (h)

$\exists a \in A$ s.t. $g(f(a)) = c$

$\downarrow$

Let $b = f(a)$. Then $g(b) = c$

Therefore g surjective

Ex: "If h is injective, then g is injective"

Counter-example!

Wednesday, February 19th 2025

Functions wrap-up

Suppose $f: \mathbb{R} \to \mathbb{R}$

$(\forall y \in \mathbb{R})(\exists x \in \mathbb{R})[f(x) = y]$

a.) Prove if f surjective, f is not bounded

$(\forall M > 0)(\exists x \in \mathbb{R})[|f(x)| > M]$

Assume M be given. There exists $x \in \mathbb{R}$ s.t. $f(x) = |M+1|$. Then, $f(x) > M$.

Friday, February 21st 2025

Sum / Product notations

DEF: $\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$

$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n$

Ex: $\sum_{i=1}^{5} i = 1+2+3+4+5 = 15$

$\sum_{i=1}^{n} 1 = \underbrace{1+1+1+\ldots+1}_{n \text{ terms}} = n$

$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$

Formulas: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

$\sum_{i=0}^{n} r^i = \frac{1-r^{n+1}}{1-r}$ for $n \neq 1$

$\sum_{i=0}^{\infty} r^i = \frac{1}{1-r}$ for $|r| < 1$

EX:
WS

1. $\sum_{i=1}^{n} 2 = 2n$
2. $\prod_{i=1}^{n} 2 = 2^n$
3. $\sum_{i=1}^{n} (n-i) = \frac{n^2-n}{2}$
4. $\prod_{i=1}^{n} (n-i) = (n-1)(n-2)\ldots(n-n) = 0$
5. $\prod_{i=1}^{n} i^n = 1^n \cdot 2^n \cdot 3^n \cdot \ldots n^n = (n!)^n$
6. $\prod_{i=1}^{n} n^i = n \cdot n^2 \cdot n^3 \cdots n^n = n^{\sum_{i=1}^{n} i} = n^{\frac{n(n+1)}{2}}$
7. $\sum_{i=1}^{n} \sum_{j=1}^{n} 1 = \sum_{i=1}^{n} n = n^2$
8. $\sum_{i=1}^{n} \sum_{j=1}^{n} (i+j) = \sum_{i=1}^{n} \left((i+1)+(i+2)+\ldots+(i+n)\right)$

$= \sum_{i=1}^{n} \left(ni + \frac{n(n+1)}{2}\right)$

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

Induction

Steps for induction: ① Base step: Prove $P(1)$ is true
② Induction step: $(\forall k \in \mathbb{N})[P(k) \Rightarrow P(k+1)]$

Used for proving $(\forall n \in \mathbb{N})\, P(n)$

Principle of induction: If ① and ② good, then $(\forall n \in \mathbb{N})\, P(n)$ follows

Ex: Gauss' sum formula $\underbrace{\sum_{i=1}^{n} i = \frac{n(n+1)}{2}}_{P(n)}$

$$\boxed{\Big(P(1) \wedge (\forall k \in \mathbb{N})[P(k) \Rightarrow P(k+1)]\Big) \Rightarrow (\forall n \in \mathbb{N})\, P(n)}$$

Let us test when $n=1$. Then, $\sum_{i=1}^{1} i = \frac{1(1+1)}{2} = \frac{1(2)}{2} = 1$. This is accurate. Proven for base case.

Assume for $n=k$, $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. For $n=k+1$, $\sum_{i=1}^{k+1} i = 1+2+\ldots+k+k+1 = \sum_{i=1}^{k} i + k+1 = \frac{k(k+1)}{2} + \frac{2(k+1)}{2}$

Then, $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$. This agrees with Gauss' formula. Thus, if $P(k)$ true, $P(k+1)$ true. Therefore, by induction, it's true □

Monday, February 24th 2025

Template for induction step:

① Let $k \in \mathbb{N}$ be given

② Assume $P(n)$ true for $n=k$

③ Logical step

④ Therefore $P(n)$ also true for $n=k+1$

Ex: Prove that $2^n > n$ for all $n \in \mathbb{N}$

- Base case

  Let $n=1$. Then, $2^n = 2 > 1 = n$. Therefore, proven for base case.

- Inductive case

  Let $k \in \mathbb{N}$ be given. Assume that $2^k > k$. Then, $2^{k+1} = 2 \cdot 2^k$. From our assumption, $2^k > k$. Therefore $2^{k+1} = 2(2^k) > 2k = k+k$. As $k \in \mathbb{N}$, $k+k \geq k+1$. Hence, $2^{k+1} > k+1$. We have shown that if $2^k > k$, then $2^{k+1} > k+1$.

Therefore, we have proved that $2^n > n$ for all $n \in \mathbb{N}$ by induction □

Friday, February 28th 2025

Fibonacci Numbers ($F_n = F_{n-1} + F_{n-2}$, $F_1 = F_2 = 1$ by definition)

~~Conjecture~~: The sum of the first n Fibonacci numbers $\sum_{i=1}^{n} F_i = F_{n+2} - 1$

THEOREM!

Proof:
- Base case for $n = 1$. Then, $\sum_{i=1}^{1} F_i = F_1 = 1$ by definition. RHS: $F_3 = 2$, thus $F_3 - 1 = 1$.
  Proven true for base case.
- Let $k \in \mathbb{N}$ given. Assume $\sum_{i=1}^{k} F_i = F_{k+2} - 1$
  Then, $\sum_{i=1}^{k+1} F_i = \sum_{i=1}^{k} F_i + F_{k+1}$. By using the assumption and the definition of Fibonacci sequence, $\sum_{i=1}^{k+1} F_i = F_{k+2} - 1 + F_{k+1} = (F_{k+1} + F_{k+2}) - 1 = F_{k+3} - 1$. This is $P(n)$ for $n = k+1$. Thus, if $P(n)$ true for k, then $P(n)$ also true for $k+1$.

By principle of induction, $\sum_{i=1}^{n} F_i = F_{n+2} - 1$ for all $n \in \mathbb{N}$ $\square$

Strong Induction

General version: $\boxed{P(1) \wedge (\forall k \in \mathbb{N}) \left[P(1) \wedge P(2) \wedge \ldots \wedge P(k) \Rightarrow P(k+1) \right] \Rightarrow (\forall n \in \mathbb{N}) P(n)}$

Fibonacci-type ver: $\boxed{P(1) \wedge P(2) \wedge (\forall k \geq 2) \left[P(k-1) \wedge P(k) \Rightarrow P(k+1) \right] \Rightarrow (\forall n \in \mathbb{N}) P(n)}$

Monday, March 3rd 2025

Fibonacci numbers: $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$

Binet formula: $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$???

Strong induction of Fibonacci type: $P(1) \wedge P(2) \wedge (\forall k \geq 2)\left[P(k-1) \wedge P(k) \Rightarrow P(k+1)\right] \Rightarrow (\forall n \in \mathbb{N})\, P(n)$

Let $a_1 = 2$, $a_2 = 10$, $a_n = 2a_{n-1} + 3a_{n-2}$ for $n \geq 3$.

<u>Conjecture</u>: $a_n = 3^n + (-1)^n$

↳ Proof: By the statement, $a_1 = 3 - 1 = 2$, which agrees with the definition of a_1. By the statement, $a_2 = 9 + 1 = 10$, which agrees with the def. of a_2. Now, let $k \geq 2$ be given. Assume that $a_{k-1} = 3^{k-1} + (-1)^{k-1}$ and also $a_k = 3^k + (-1)^k$. Then, by the definition of the sequence, we have $a_{k+1} = 2a_k + 3a_{k-1}$. Implementing the assumption, we now have that $a_{k+1} = 2 \cdot 3^k + 2(-1)^k + 3(3^{k-1}) + 3(-1)^{k-1} = 3^{k+1} + (-1)^{k+1}$. This is the statement for $n = k+1$. Statement true for $n = k-1$ and $n = k$ implies statement true for $n = k+1$. By Strong Induction, statement true.

Notes on logical structure: Case: $n=1$ $n=2$ $n=3$ $n=4$ . . . .

Base case covered by $P(1) \wedge P(2)$

Induction step involves $k-1$ and k, $k \geq 2$.
First case not covered is $n = 3$. $k+1$ must be 3.
First k must be $k = 2$

Statement: The n-th term of a Fibonacci sequence is $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$

Proof: F_1 by the statement is $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \frac{2\sqrt{5}}{2\sqrt{5}} = 1$, which fits the definition of F_1. F_2 by the statement is $\frac{1}{\sqrt{5}}\left(\frac{(1+\sqrt{5})^2 - (1-\sqrt{5})^2}{4}\right) = \frac{2\sqrt{5} \cdot 2}{4\sqrt{5}} = 1$, which fits the definition of F_2. Proven for base cases. Then, let $k \geq 2$ given. Assume that $F_{k-1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right)$ and $F_k = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right)$. By the definition of Fibonacci sequence, $F_{k+1} = F_{k-1} + F_k$ It follows that $F_{k+1} = F_k + F_{k-1}$. Implementing our initial assumptions, we have $F_{k+1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right)$

Notice that this involves the golden ratio, $\frac{1 \pm \sqrt{5}}{2}$ which is a solution to $x^2 - x - 1 = 0$.

"Any" = "$\forall$" for all

Wednesday, March 5th 2025

Ex: (Non formula) Show that an n-element set has exactly 2^n subsets

Proof: Consider base case where $n=1$. Then, $S = \{x\}$ can have 2 subsets, which is $S_1 = \{x\}$ and $S_2 = \phi$. Agrees with the statement, proven for base case. Let $k \in \mathbb{N}$ be given. Assume that the statement is true for $n=k$. Let A be an arbitrary set with $(k+1)$ elements. Then, $A' = A \setminus \{a\}$ where $a \in A$ and $|A'| = k$. A' has 2^k subsets by induction hypothesis. All subsets of A' doesn't include a. If we include a, we essentially have 2 times the amount of subsets. Thus, A has $2 \cdot 2^k$ subsets, or 2^{k+1}. $\square$

Monday, March 10th 2025

Cardinality and Countability

Cardinality: number of elements

Ex: $|\phi| = 0$, $|\{1,2,3\}| = 3$

Cantor's results:

- $\mathbb{R}$ is uncountable
- $\mathbb{Q}$ countable

DEF: Two sets A and B have the same cardinality if there exists a bijection between A & B

DEF: A set A is called finite if it's either the empty set or if it has the same cardinality as the set $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ (i.e. if there's a bijection between A and $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. or the otherway around)

DEF: A set is called countable if it has the same cardinality as $\mathbb{N}$ (i.e. if there is a bijection)

DEF: A set is called uncountable otherwise (ie if it's neither finite nor infinite)

DEF: Power set of A: "Set of all subsets of A"

$\hookrightarrow$ $P(A) = \{B : B \subseteq A\}$

DEF: Cartesian product: Set of ordered pairs (a,b): $a \in A$, $b \in B$

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

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

$$P(A) = \left\{ \begin{array}{l} \phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \\ \{2,3\}, \{1,3\}, \{1,2,3\} \end{array} \right\}$$

Ex: $$\{1,2,3\} \times \{0,1\} = \left\{ \begin{array}{l} (1,0), (1,1), (2,0), (2,1), \\ (3,0), (3,1), (4,0), (4,1) \end{array} \right\}$$

Friday, March 14th 2025

Operations that preserve countability

- Taking infinite subsets (if A countable and $B \subseteq A$ is an infinite subset of A, then B countable)

  Ex: $\mathbb{Q}$ is countable, so set of rationals in $[0,1]$ is also countable

- Adding one element to a countable set, or adding finitely many elements to a countable set

  Ex: $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ is countable as $\mathbb{N}$ is countable

- Adding countably many elements ("$A \cup B$ countable if $A \wedge B$ countable")

  Ex: $\mathbb{Z} = \mathbb{N} \cup \underbrace{\{-0, -1, -2, \dots\}}_{-\mathbb{N}_0}$. As both sets countable, then $\mathbb{Z}$ countable

  Proof. Let A and B be countable sets defined as $A = \{a_1, a_2, \dots\}$ and $B = \{b_1, b_2, \dots\}$. Then, $A \cup B = \{a_1, b_1, a_2, b_2, \dots\}$ is also countable. $\square$

  Corollary: $\bigcup_{i=1}^{k} A_i$ countable if A_i countable for $1 \le i \le k$ where $i, k \in \mathbb{N}$ (works also for $k \to \infty$ countable)

- Cartesian product of two countable sets (if A, B countable, then $A \times B$ is also countable)

  Remark: true for finitely many countable sets, but not for countably many sets

  Proof idea for $\bigcup_{i=1}^{\infty} A_i$ or the cartesian product equivalent: zig-zag method of enumerating

Hotel Infinity Paradox

Let the hotel be modeled as a one floor hotel with room numbers $1, 2, \dots$ and every room is occupied. Suppose an additional guest arrive, free up a room by reassigning room number k to $k+1$. Thus room one is now free. Bijection is $f(k) = k+1$. For 30 guests, we can have $f(k) = k+30$. Repeat on doing that for $k \to \infty$ (goes on and on), we free up countably many rooms. Function that works is $f(k) = 2k$. If there are countably many buses with countably many passengers, free up by using bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. In other words, $f(i, j)$ assigns passenger i in bus j where $i = 1, 2, 3, \dots$ and $j = 1, 2, 3, \dots$. For example, $f(i, j) = 2^{i-1}(2j-1)$

Monday, March 24th 2025.

THEOREM: $\mathbb{Q}$ is countable

Preliminary notes for the proof:

- $\mathbb{Q} = \underbrace{\mathbb{Q}_+}_{\text{positive rationals}} \cup \underbrace{\mathbb{Q}_-}_{\text{neg. rationals}} \cup \{0\}$
- $\exists f : \mathbb{Q}_+ \to \mathbb{Q}_-$ s.t. f is bijective ($f(x) = -x$)
- Sufficient to show $\mathbb{Q}_+$ countable for proving $\mathbb{Q}$ countable.

Proof. Let us construct a table of rational numbers where the column index is numerator and row is denom. This table contains all of the positive rational numbers.

$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	...
$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	...
$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	...
$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	...
$\vdots$		$\vdots$	$\vdots$	

Now, enumerate the elements in a "zigzag" fashion. That is:

$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	...
$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	...
$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	...
$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	...
$\vdots$				

Sequence: $\underset{r_1}{\frac{1}{1}}, \underset{r_2}{\frac{2}{1}}, \underset{r_3}{\frac{1}{2}}, \underset{r_4}{\frac{1}{3}}, \cancel{\frac{2}{2}}, \underset{r_5}{\frac{3}{1}}, \underset{r_6}{\frac{4}{1}}, \underset{r_7}{\frac{3}{2}}, \underset{r_8}{\frac{2}{3}} \dots$

Thus after finitely many steps, every element is hit. Therefore, $\mathbb{Q}_+$ is countable.
If $\mathbb{Q}_+$ is countable, then $\mathbb{Q}_-$ countable as $f : \mathbb{Q}_+ \to \mathbb{Q}_-$ where $f(x) = -x$ is a bijection.
Hence, as $\mathbb{Q} = \mathbb{Q}_+ \cup \mathbb{Q}_- \cup \{0\}$, we have that $\mathbb{Q}$ is countable. $\square$

Same proof idea:

- If A, B are countable sets, then $A \times B$ is countable
- If $A_1, A_2, \dots$ countable sets, then $A_1 \cup A_2 \cup \dots$ is countable
- If $A_1, A_2, \dots, A_k$ countable sets, then $A_1 \times A_2 \times \dots \times A_k$ is countable. (Not true when $k = \infty$)

Wednesday, March 26th 2025

"Benchmark" uncountable sets : $\mathbb{R}$, $P(\mathbb{N})$ "power set of $\mathbb{N}$", Set of infinite binary sequences

THEOREM: The set of all binary sequences is uncountable

Proof. Assume that the set of all binary sequences is countable. There are countably many infinite binary sequences, say S_1, S_2, S_3, etc. Arrange these sequences in a table manner :

Seq.						
S_1	0	1	1	0	1	...
S_2	1	1	0	1	0	...
S_3	1	0	1	0	1	...
S_4	1	0	1	0	0	...
...	...	...	...	...	...	...

Construct S^* be the diagonal sequence.
That is, $S^* = (0, 1, 1, 0, \ldots)$.
Now, construct S be the "flip" of S^*.
That is, $S = (1, 0, 0, 1, \ldots)$

Notice that S cannot be S_1 as it has different entry of the first term, cannot be S_2 as it has different second entry, and so-on. Therefore, S is a binary sequence NOT included in the enumeration. This implies a contradiction. Hence, the set is uncountable. $\square$

THEOREM: $P(\mathbb{N})$ is uncountable

Proof. Construct bijection between $P(\mathbb{N})$ and the set of all infinite binary sequences. Suppose $A \in P(\mathbb{N})$, $A = \{2, 5, 6, 8, \ldots\}$. Then, we can map the set A to an infinite binary sequence $(a_1, a_2, \ldots)$ where

$$a_k = \begin{cases} 1 & \text{if } k \in A \\ 0 & \text{if } k \notin A \end{cases} \qquad \forall A \in P(\mathbb{N})$$

Then, as a bijection exists, $P(\mathbb{N})$ has the same cardinality as the infinite binary set. Therefore, $P(\mathbb{N})$ is uncountable. $\square$

THEOREM: $\mathbb{R}$ is uncountable

Proof. By Cantor's diagonal argument on the decimal expansion of real numbers, $\mathbb{R}$ is uncountable $\square$

$$\boxed{\text{Idea: Just consider } x \in [0,2) \text{ s.t. decimal expansion contains only 0s and 1s}}$$

THEOREM: The set of all irrational real numbers is uncountable.

Proof. The set of irrational numbers, denoted as A, is precisely $A = \mathbb{R} \setminus \mathbb{Q}$. If A is countable, then $\mathbb{R} = A \cup \mathbb{Q}$ countable, which is a contradiction. Therefore, we require A to be uncountable. $\square$

Friday, March 28th 2025

THEOREM: Set of all finite sequences of natural numbers is countable

Proof. Let A_k be the set of such sequences of length k. The given set is $\bigcup_{i=1}^{\infty} A_i$. $A_1 = \mathbb{N}$, then A_1 countable. $A_2 = \mathbb{N} \times \mathbb{N}$, thus A_2 is countable. A_3 is $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$, or $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$. It follows that A_3 is countable. Hence, A_k is countable for all k. Therefore, $\bigcup_{i=1}^{\infty} A_k$ countable $\square$

THEOREM: Set of all infinite sequences of natural numbers are uncountable

Proof. The given set is the super set of the set of all infinite binary sequences. That set is uncountable, it follows that the given set is also uncountable $\square$

Sets of functions $f: A \to B$

Cases: A — finite / countable / uncountable, B — finite / countable / uncountable

Ex: $\{f: \mathbb{N} \to \{0,1\}\}$ uncountable as it's in bijection to set of all infinite binary sequences

Idea: each f generates a string of infinite binary sequences, thus we have uncountable

Ex: $\{f: \{0,1\} \to \mathbb{N}\}$ is countable as it's in bijection to $\mathbb{N} \times \mathbb{N}$

Idea: f maps 0 or 1 to an $x \in \mathbb{N}$, thus we have "2 choices", thus $\mathbb{N} \times \mathbb{N}$ bijection

Monday, March 31st 2025

CONGRUENCES

Def: Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. a is said to be "congruent b mod m" if $m \mid a-b$.
Equivalently, $a \equiv b \bmod m$ if $a = km + b$ for some $k \in \mathbb{Z}$.

Proposition: If $\left\{ \begin{array}{l} a \equiv b \bmod m \\ c \equiv d \bmod m \end{array} \right\}$ then $\begin{array}{l} a+c \equiv b+d \bmod m \\ ac \equiv bd \bmod m \end{array}$

Proof:

- $\left.\begin{array}{l} a \equiv b \bmod m \Rightarrow m \mid a-b \\ c \equiv d \bmod m \Rightarrow m \mid c-d \end{array}\right\} \Rightarrow m \mid (a+c)-(b+d)$
  $\Downarrow$ $a+c \equiv b+d \bmod m$

- $\left.\begin{array}{l} a \equiv b \bmod m \Rightarrow m \mid a-b \Rightarrow m \mid c(a-b) \\ c \equiv d \bmod m \Rightarrow m \mid c-d \Rightarrow m \mid b(c-d) \end{array}\right\} \Rightarrow m \mid ac - \cancel{bc} + \cancel{bc} - bd$
  (multiple of m)
  $m \mid ac - bd \Rightarrow ac \equiv bd \bmod m$ □

THEOREM (F. little): For any prime p and any integer a such that $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$

Divisibility / remainders of polynomials:

SAME IDEA LIKE QUADRATIC CONGRUENCES IN ZAHARESCU MATH 453 !!!

a.) Possible remainders of $n^4 \bmod 5$

$n \equiv 0, 1, 2, 3,$ or $4 \bmod 5$

$n^4 \equiv 0, 1^4, 2^4, 3^4,$ or $4^4 \bmod 5$

$n^4 \equiv 0$ or $1 \bmod 5$

b.) Do there exist $\mathbb{Z}$ s.t. $h^4 + k^4 + n^4 \equiv 4 \bmod 5$? No! Max: $3 \bmod 5$

c.) Let $S(n)$ be the sum of the digits of n. Then $9 \mid n$ iff $9 \mid S(n)$.

Proof: $n = 10^0 \cdot a_0 + 10^1 a_1 + \dots + 10^k a_k$

$n \equiv 10^0 a_0 + 10^1 a_1 + \dots + 10^k a_k \bmod 9$

$n \equiv a_0 + a_1 + \dots + a_k \bmod 9 \equiv S(n) \bmod 9$

Monday, April 7th 2025

RELATIONS

DEF: Given two sets S and T, a relation from S to T is a subset $R \subseteq S \times T$
A relation on S is a subset $R \subseteq S \times S$.

DEF: Write $x \sim y$ if $(x, y) \in R$ i.e. if x is related to y

Ex:
- $S = \mathbb{Z}$, congruence relation mod $m \in \mathbb{N}$ defined as $x \sim y \iff x \equiv y \text{ mod } m$
  For example, $m = 3$, $347 \sim 347$, $347 \sim 2$, etc.
- $S = \mathbb{N}$, divisor relation is defined as $x \sim y \iff x \mid y$. Or in other words,
  $x \sim y \iff \exists k \in \mathbb{Z}$ s.t. $y = kx$
- S arbitrary, equality relation is defined as $x \sim y \iff x = y$. Corresponds to set
  $R = \{(x, x) : x \in S\}$
- $S = \mathbb{R}$, order relation is defined as $x \sim y \iff x \leq y$

DEF: Given a relation on some set S that's denoted by $\sim$, properties that $\sim$ might have:
- Reflexive: $\forall x \in S$, $x \sim x$
- Symmetric: $\forall x, y \in S$, $x \sim y \Rightarrow y \sim x$
- Transitive: $\forall x, y, z \in S$, $x \sim y \wedge y \sim z \Rightarrow x \sim z$

DEF: If a given relation $\sim$ on some set S satisfies ALL of the three properties above, then $\sim$ is said to be an equivalence relation

Ex: Congruence relation mod m is an equivalence relation

Proof. Check the three properties
- Reflexivity: $x \sim x \iff x \equiv x \text{ mod } m \Rightarrow m \mid x - x \Rightarrow m \mid 0$
- Symmetricity: Let $x, y \in S$ be given. Assume $x \equiv y \text{ mod } m$. Then, $\exists k \in \mathbb{Z}$ s.t. $x = y + mk$.
  Rearrange to get $y = x + (-k)m$. $k \in \mathbb{Z} \Rightarrow -k \in \mathbb{Z}$, thus we get $x \sim y \Rightarrow y \sim x$
- Transitive: Let $x, y, z \in S$ be given. Assume $x \equiv y \text{ mod } m$ and $y \equiv z \text{ mod } m$. Then, $\exists k_1, k_2 \in \mathbb{Z}$ s.t.
  $x = y + k_1 m$ and $y = z + k_2 m$. It follows that $x = z + (k_1 + k_2)m$. $k_1, k_2 \in \mathbb{Z} \Rightarrow (k_1 + k_2) \in \mathbb{Z}$.
  Proven that if $x \sim y$ and $y \sim z$, then $x \sim z$

$\square$

Wednesday, April 9th 2025

DEF: Given an equivalence relation denoted as "$\sim$" on a set S, the set $[x] = \{y \in S : x \sim y\} = \{y \in S : y \sim x\}$ is called the equivalence class of x

Ex: The congruence relation mod 3 on $\mathbb{Z}$:

$[0] = \{y \in \mathbb{Z} : 0 \sim y\} = \{\ldots, -3, 0, 3, \ldots\}$

$[1] = \{y \in \mathbb{Z} : 1 \sim y\} = \{\ldots, -2, 1, 4, \ldots\}$

$[2] = \{y \in \mathbb{Z} : 2 \sim y\} = \{\ldots, -1, 2, 5, \ldots\}$

$[347] = \{y \in \mathbb{Z} : 347 \sim y\} = \{y \in \mathbb{Z} : 2 \sim y\} = [2]$

DEF: A partition of a set S is a collection of subsets $A_i \subseteq S$ satisfying:

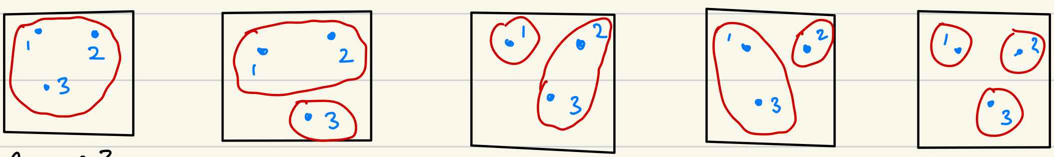
(i.) non-empty: $\forall i \in \mathbb{N},\ A_i \neq \emptyset$

(ii.) disjoint: $\forall i, j \in \mathbb{N}$ s.t. $i \neq j$, $A_i \cap A_j = \emptyset$

(iii.) Unions of all: $\bigcup_i A_i = S$

Ex: $S = \{1, 2, 3\}$

All partitions on S: $\{1,2,3\}$, $(\{1,2\}, \{3\})$, $(\{2,3\}, \{1\})$, $(\{1,3\}, \{2\})$, $(\{1\}, \{2\}, \{3\})$



$\{1,2,3\}$ $\quad$ $\{1,2\}, \{3\}$ $\quad$ $\{2,3\}, \{1\}$ $\quad$ $\{1,3\}, \{2\}$ $\quad$ $\{1\}, \{2\}, \{3\}$

THEOREM: Given an equivalence relation on a set S, the set of distinct equivalence classes on S forms a partition on S

Ex: $S = \mathbb{Z}$, congruence relation mod 3, the sets $[0]$, $[1]$, $[2]$ are the distinct equivalence classes for this relation, and therefore form a partition of $\mathbb{Z}$

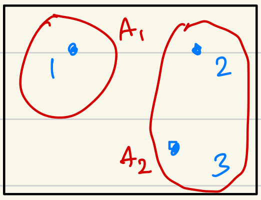
Friday, April 11th 2025

THEOREM: Given a partition A_i of a set S, the relation defined by

$$\boxed{x \sim y \iff x \in A_i \wedge y \in A_i \text{ (or alternatively) } R = \bigcup_i (A_i \times A_i)}$$

is an equivalence relation on S whose distinct equivalence classes are exactly the sets A_i of the given partition

INTUITION: $S = \{1,2,3\}$



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

EQUIVALENCE RELATION! EQUIV CLASSES:

- $[1] = \{1\}$
- $[2] = \{2,3\}$

Consequences of the theorem:

- There is a bijection between the set of all partitions on S and the set of all equivalence relations on S
- The number of equivalence relations on S is equal to the number of partitions on S

Monday, April 14th 2025

MAX, MIN, SUP, INF, COMPLETENESS AXIOM

DEF: Let $S \subseteq \mathbb{R}$ s.t. $S \neq \emptyset$. Then define max S and min S as:

- max S : largest element of S if it exists
- min S : smallest element of S if it exists

Ex: $\mathbb{N}$ has $\min \mathbb{N} = 1$, and $\max \mathbb{N}$ DNE

Ex: $S = \{1 - \frac{1}{n} : n \in \mathbb{N}\} = \{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\}$

$\min S = 0$, $\max S$ DNE

DEF: Given a set $S \subseteq \mathbb{R}$ such that $S \neq \emptyset$, a number $\alpha \in \mathbb{R}$ is called an:

- Upper bound for S if $\forall x \in S$, $\alpha \geq x$
- lower bound for S if $\forall x \in S$, $\alpha \leq x$

Remarks:

- max S is always an upper bound if it exists, similarly min S is a lower bound if it exists
- A bounded set S is defined as $\exists M \in \mathbb{R}$ s.t. $\forall x \in S$, $|x| \leq M$

  This implies that in a bounded set, $-M \leq x \leq M$. Therefore, upper bound M and lower bound $-M$.

DEF: Given non-empty set $S \subseteq \mathbb{R}$ and $\alpha \in \mathbb{R}$, α is called the least upper bound of S ($\sup S$) if:

- α is upper bound of S
- α is the smallest among all upper bounds of S

DEF: Given non-empty set $S \subseteq \mathbb{R}$ and $\alpha \in \mathbb{R}$, α is called the greatest lower bound of S ($\inf S$) if:

- α is lower bound of S
- α is the greatest among all lower bounds of S

DEF: Epsilonics definitions of sup S and inf S:

- $\alpha = \sup S \iff \forall x \in S,\ \alpha \geq x \ \wedge\ \forall \varepsilon > 0, \exists x \in S$ s.t. $x > \alpha - \varepsilon$
- $\alpha = \inf S \iff \forall x \in S,\ \alpha \leq x \ \wedge\ \forall \varepsilon > 0, \exists x \in S$ s.t. $x < \alpha + \varepsilon$

Wednesday, April 16th 2025

QUESTION: Let S be a non-empty subset of $\mathbb{R}$ that is bounded above. Let T be the set of all upper bounds of S. Then $T \subseteq \mathbb{R}$.

- $\inf T$ exists as the set is bounded below
- $\min T$ exists as $\sup S$ exists
- $\max T$ and $\sup T$ doesn't exist

- $T = \{x \in \mathbb{R} : x \geq \alpha\}$ where $\alpha = \sup S$

Significance of Completeness Axiom:

- Guarantees the existence of irrational numbers such as $\sqrt{2}$ or π within $\mathbb{R}$

Proof. For $\sqrt{2}$, consider the set $S = \{x \in \mathbb{Q} : x^2 \leq 2\}$ By Completeness Axiom, S must have a supremum. One can show by contradiction that $(\sup S)^2 = 2$. This implies that $\sup S = \sqrt{2}$ $\square$

- Guarantees the existence of infinite decimal expansions e.g. $3.14159\ldots$

Proof. Consider $S = \{3, 3.1, 3.14, \ldots\}$. S has an upper bound, by Completeness Axiom, S must have a supremum. $\sup S$ is the real number represented by the expansion $\square$

Friday, April 18th 2025

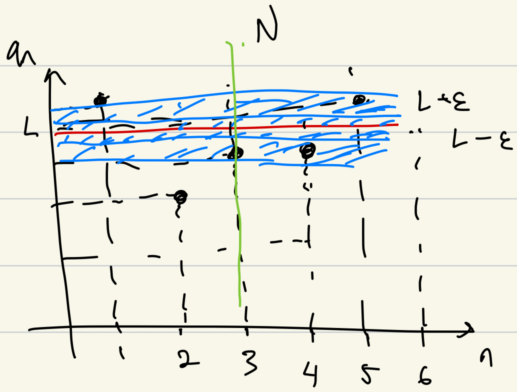
LIMITS

DEF: Given a sequence $\{a_n\}$ of real numbers and a real number L, we define

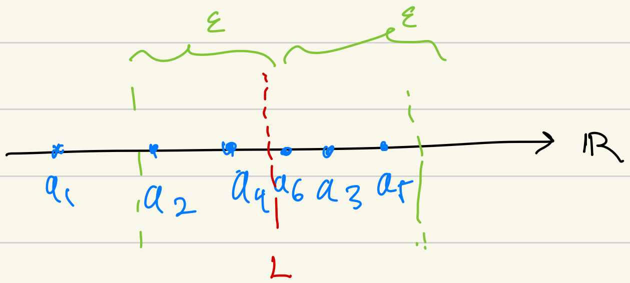
$a_1, a_2, a_3, \ldots$

$$\lim_{n\to\infty} a_n = L \iff \forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ s.t. } n \geq N \Rightarrow |a_n - L| < \varepsilon.$$

INTUITION:



INTUITION:



THEOREM: If $\lim_{n\to\infty} a_n = L$ and $\lim_{n\to\infty} a_n = M$, then $L = M$ (Uniqueness of Limits)

Proof. Assume $\lim_{n\to\infty} a_n = L$ and $\lim_{n\to\infty} a_n = M$ such that $L \neq M$. WLOG, we may assume $L < M$. Take $\varepsilon = \frac{1}{3}(M-L)$. Then the intervals $(L-\varepsilon, L+\varepsilon)$ and $(M-\varepsilon, M+\varepsilon)$ don't overlap. Since $\lim_{n\to\infty} a_n = L$, there exists N_1 such that $n \geq N_1 \Rightarrow |a_n - L| < \varepsilon$. Analogously, since $\lim_{n\to\infty} a_n = M$, there exists N_2 such that $n \geq N_2 \Rightarrow |a_n - M| < \varepsilon$. Let $n = \max(N_1, N_2)$, then we see that $n \geq N_1$ and $n \geq N_2$. For this n, both $|a_n - L| < \varepsilon$ and $|a_n - M| < \varepsilon$. But, $a_n < L + \varepsilon = L + \frac{1}{3}M - L = \frac{2}{3}L + \frac{1}{3}M$ and $a_n > M - \varepsilon = \frac{2}{3}M + \frac{1}{3}L$.

Monday, April 21st 2025

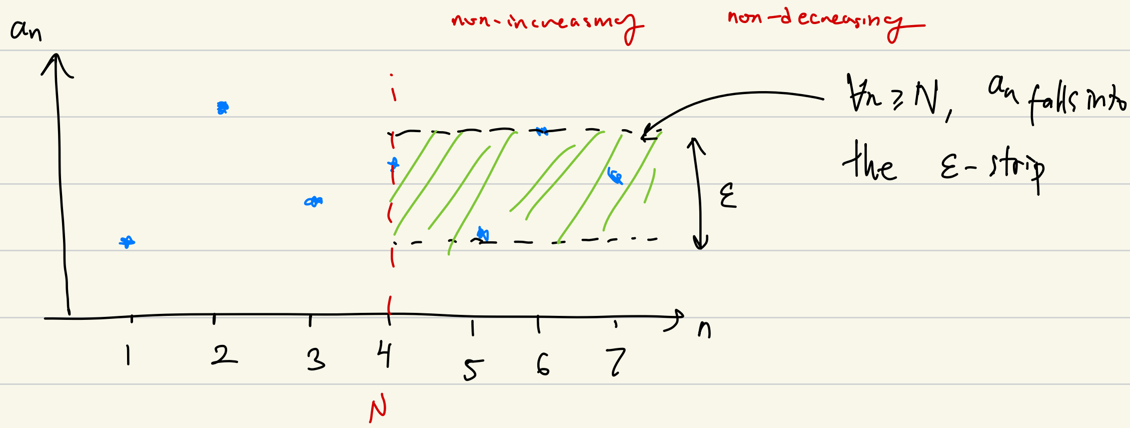
DEF: $\{a_n\}$ converges $\iff \exists L \in \mathbb{R}$ s.t. $\lim_{n\to\infty} a_n = L$

DEF: $\{a_n\}$ Cauchy $\iff \forall \varepsilon > 0, \ \exists N \in \mathbb{N}$ s.t. $n, m \geq N \Rightarrow |a_n - a_m| < \varepsilon$

DEF: $\{a_n\}$ bounded $\iff \exists M \in \mathbb{R}$ s.t. $\forall n \in \mathbb{N}, \ |a_n| \leq M$

DEF: $\{a_n\}$ is monotone $\iff \forall n \in \mathbb{N}, \ \underbrace{a_{n+1} \leq a_n}_{\text{non-increasing}}$ or $\underbrace{a_{n+1} \geq a_n}_{\text{non-decreasing}}$

INTUITION FOR CAUCHY:



THEOREM: A sequence is convergent iff it's Cauchy

THEOREM: Given two sequences $\{a_n\}$ and $\{b_n\}$ that has limits L and M respectively:

- $\lim_{n\to\infty} c a_n = cL$
- $\lim_{n\to\infty} a_n \pm b_n = \lim_{n\to\infty} a_n \pm \lim_{n\to\infty} b_n = L \pm M$
- $\lim_{n\to\infty} a_n b_n = \lim_{n\to\infty} a_n \lim_{n\to\infty} b_n = LM$
- If $b_n \neq 0$ for all $n \in \mathbb{N}$ and $M \neq 0$, $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{L}{M}$

THEOREM: If a sequence is monotone and bounded, then it's also convergent

Remark:
- Any convergent sequence is bounded
- The converse of the theorem is not true

Wednesday, April 23rd 2025

PROOF - PRACTICE

① Sum property ($\lim_{n\to\infty} a_n = L \wedge \lim_{n\to\infty} b_n = M \Rightarrow \lim_{n\to\infty} a_n + b_n = L+M$)

Proof. Let $\{a_n\}$ and $\{b_n\}$ be given such that $\lim_{n\to\infty} a_n = L$ and $\lim_{n\to\infty} b_n = M$ where $L, M \in \mathbb{R}$.
Then by definition of limits:

$$\forall \varepsilon > 0, \exists N_1 \in \mathbb{N} \text{ s.t. } n \geq N_1 \Rightarrow |a_n - L| < \varepsilon$$

$$\forall \varepsilon > 0, \exists N_2 \in \mathbb{N} \text{ s.t. } n \geq N_2 \Rightarrow |b_n - M| < \varepsilon$$

Let $\varepsilon = \varepsilon'/2$ where $\varepsilon' \in \mathbb{R}^+$. Then, there exists N_1 and N_2 such that both conditions work. Choose $n = \max(N_1, N_2)$. Then, it follows that

$$|a_n - L| + |b_n - M| < \varepsilon' \quad \text{(algebra)}$$

$$|(a_n - L) + (b_n - M)| < \varepsilon' \quad \text{(triangle inequality)}$$

$$|(a_n + b_n) - (L+M)| < \varepsilon' \quad \text{(algebra)}$$

ε' arbitrary. This is the problem statement. Hence, we have shown that $\lim_{n\to\infty} a_n + b_n = L+M$ □

CHECK THE WORKSHEET MODEL

② Convergent $\Rightarrow$ Bounded

Proof. Let $\lim_{n\to\infty} a_n = L$ where $L \in \mathbb{R}$. Let $\varepsilon = 1$. Then $\exists N_1 \in \mathbb{N}$ s.t. $\forall n \geq N_1$, $|a_n - L| < 1$. Choose $M_1 = |L| + 1$, $M_2 = \max(|a_1|, |a_2|, \ldots, |a_N|)$.

Friday, April 25th 2025

Proposition. If $\lim_{n\to\infty} a_n = 0$ and $\{b_n\}$ is bounded, then $\lim_{n\to\infty} a_n b_n = 0$

Proof (Idea.) $\lim_{n\to\infty} a_n = 0 \iff \forall \varepsilon' > 0, \exists N \in \mathbb{N}$ s.t. $n \geq N \Rightarrow |a_n| < \varepsilon'$

$\{b_n\}$ bounded $\iff \exists M \in \mathbb{R}$ s.t. $\forall n \in \mathbb{N}, |b_n| \leq M$

$\varepsilon' := \varepsilon / M$. Then $\exists N \in \mathbb{N}$ s.t. $n \geq N \Rightarrow |a_n b_n| < \varepsilon' M = \varepsilon$

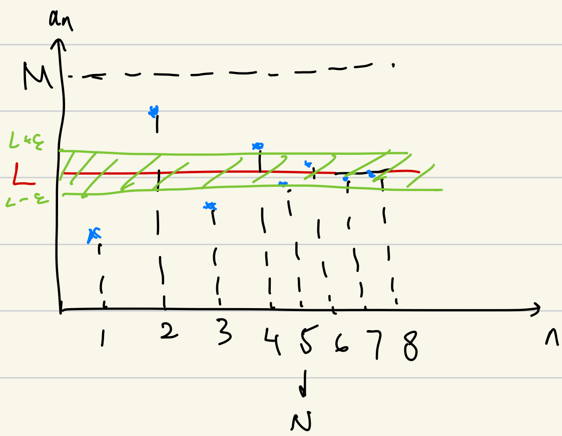
" ε/M trick"

Structure:
1. Assume $\lim_{n\to\infty} a_n = 0$ and $\{b_n\}$ bounded
2. Let $\varepsilon > 0$ be given
3. Since $\{b_n\}$ bounded, $\exists M \in \mathbb{R}$ s.t. $\forall n \in \mathbb{N}, |b_n| \leq M$
4. Since $\lim_{n\to\infty} a_n = 0$, $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N$, $|a_n| < \varepsilon' = \varepsilon/M$
5. Therefore $\forall n \geq N$, $|a_n b_n| = |a_n||b_n| < \varepsilon/M \cdot M = \varepsilon \iff n \geq N \Rightarrow |a_n b_n| < \varepsilon$
6. Hence, $\lim_{n\to\infty} a_n b_n = 0$ $\square$

Proposition. If $\{a_n\}$ convergent, then $\{a_n\}$ bounded

Proof. (Idea.) $\{a_n\}$ convergent $\iff \exists L \in \mathbb{R}$ s.t. $\lim_{n\to\infty} a_n = L$

$\{a_n\}$ bounded $\iff \exists M \in \mathbb{R}$ s.t. $\forall n \in \mathbb{N}, |a_n| \leq M$



1. Pick $\varepsilon = 1$ in def of $\lim_{n\to\infty} a_n = L$
2. Let N be s.t. $\forall n \geq N$, $|a_n - L| < 1$
3. Then $\forall n \geq N$, $|a_n| < \underbrace{|L| + 1}_{= M_1}$
4. Let $M_2 = \max(|a_1|, |a_2|, \ldots, |a_{N-1}|)$
5. Then $n \in \{1, 2, \ldots, N-1\} \Rightarrow |a_n| \leq M_2$ and

   $n \in \{N, N+1, \ldots\} \Rightarrow |a_n| \leq M_1$
6. Let $M = \max(M_1, M_2)$, then it follows $\forall n \in \mathbb{N}, |a_n| \leq M$ $\square$

bounded!

Monday, April 28th 2025

Propostion: $a_n = (-1)^n$ diverges

SCRATCH

$\{a_n\}$ Cauchy $\iff \forall \varepsilon > 0, \exists N \in \mathbb{N}$ s.t. $\forall m,n \geq N, |a_m - a_n| < \varepsilon$

$\{a_n\}$ Convergent $\iff \forall \varepsilon > 0, \exists N \in \mathbb{N}$ s.t. $\forall m,n \geq N, |a_m - a_n| < \varepsilon$

$\{a_n\}$ not-Convergent $\iff \underset{①}{\exists \varepsilon > 0}$ s.t. $\underset{②}{\forall N \in \mathbb{N}}$, $\underset{③}{\exists m,n \geq N}$ s.t. $\underset{④}{|a_m - a_n| \geq \varepsilon}$

Proof Structure:
1. Let ε = *insert something specific*
2. Choose an N value
3. Find $m,n \geq N$ specific value
4. Show that for all conditions above, $|a_m - a_n| \geq \varepsilon$

Choose $\varepsilon = 1$. Let N be given. Then choose $m = N+1$ and $n = N$. Then,
$|a_m - a_n| = |(-1)^{N+1} - (-1)^N| = |(-1)^N(-1-1)| = 2 > 1 = \varepsilon$ ✓

Proof. Let $\varepsilon = 1$. Then, let $N \in \mathbb{N}$ be given. Choose $m = N+1$ and $n = N$. Then, $|a_m - a_n| = |(-1)^{N+1} - (-1)^N| = |-1-1| = |-2| = 2 > 1 = \varepsilon$. We have found an $\varepsilon > 0$ such that for an arbitrary $N \in \mathbb{N}$, exists $m,n \geq N$ such that $|a_m - a_n| \geq \varepsilon$. This is the definition of a divergent sequence. Hence, proven that $a_n = (-1)^n$ divergent. □

Proposition: $\lim_{n \to \infty} \frac{(-1)^n}{\sqrt{n}} = 0$

SCRATCH

$\forall \varepsilon > 0, \exists N \in \mathbb{N}$ s.t. $\forall n \geq N, \left|\frac{(-1)^n}{\sqrt{n}}\right| < \varepsilon$

Square to get $\frac{1}{n} < \varepsilon^2$. Choose $N = \frac{1}{\varepsilon^2}$

Then $\left|\frac{(-1)^n}{\sqrt{n}}\right| = |\ \varepsilon\ |$

Proof. Let $\varepsilon > 0$ be given. Choose $N = \left\lceil \frac{4}{\varepsilon^2} \right\rceil$. Let $n \geq N$ be given. Then it follows that $\left|\frac{(-1)^n}{\sqrt{n}}\right| = \frac{1}{\sqrt{n}} \leq \frac{1}{\sqrt{N}} = \frac{\varepsilon}{2} < \varepsilon$. Hence, by the definition of limits, $\lim_{n \to \infty} a_n = 0$. □

Friday, May 2nd 2025

THEOREM: If $\{a_n\}$ monotone and bounded, then $\{a_n\}$ convergent (Monotone Convergence Thm.)

Proof. Suppose $\{a_n\}$ is bounded and monotone. WLOG, $a_n \leq a_{n+1}$ for all $n \in \mathbb{N}$. Let set S be defined as $S = \{a_n : n \in \mathbb{N}\}$. Then, as $S \neq \emptyset$ and bounded, by the Completeness Axiom, $\sup S$ exists. Let $L = \sup S$. Let $\varepsilon > 0$ be given. By definition of $\sup \{a_n\}$, there exists $N \in \mathbb{N}$ such that $a_N > L - \varepsilon$ and $a_N \leq L$. Since $\{a_n\}$ non-decreasing, we have that $L - \varepsilon < a_N \leq a_{N+1} \leq a_{N+2} \leq \ldots \leq L$. Hence for all $n \geq N$, $|a_n - L| < \varepsilon$. $\square$