Math 220-01: Mathematical Reasoning and Proof
Instructor: David Zureick-Brown ("DZB")

"Notes"
Last updated: February 5, 2024

These are very rough notes for the course, which mostly overlap with the class content.

Contents

MATH 220 HANDOUT 1 - LOGIC

A **statement** is a sentence for which ‘true or false’ is meaningful.

1. Which of these are **statements**?

(1) Today it is raining.
(2) What is your name?
(3) Every student in this class is a math major.
(4) $2 + 2 = 5$.
(5) $x + 1 > 0$.
(6) $x^2 + 1 > 0$.
(7) If it is raining, then I will wear my raincoat.
(8) Give me that.
(9) This sentence is false.
(10) If x is a real number, then $x^2 > 0$.

2. Which of these are true?

(1) (T or F) Every student in this class is a math major and a human being.
(2) (T or F) Every student in this class is a math major or a human being.
(3) (T or F) $2 + 2 = 5$ or $1 > 0$.
(4) (T or F) If x is a real number, then $x^2 \geq 0$.
(5) (T or F) If x is a complex number, then $x^2 \geq 0$.

3. Write the negations of the following.

(1) $2 + 2 = 5$
(2) $1 > 0$.
(3) $2 + 2 = 5$ or $1 > 0$.
(4) Every student in this class is a math major.
(5) Every student in this class is a math major or a human being.
(6) If x is a real number, then $x^2 > 0$.

4. Prove the following using truth tables.

(1) $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$,
(2) $(P \vee Q) \vee R = P \vee (Q \vee R)$. (We thus write $P \vee Q \vee R$ for both.)
(3) $\neg(P \vee Q) = \neg P \wedge \neg Q$,
(4) $\neg(P \wedge Q) =$ (make a guess similar to problem 3),
(5) $\neg(\neg P) = P$.

5. In exercise 6, you may use the following variants of exercise 4.

(1) $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$,
(2) $(P \wedge Q) \wedge R = P \wedge (Q \wedge R)$. (We thus write $P \wedge Q \wedge R$ for both.)
(3) $P \vee Q = Q \vee P$.
(4) $P \wedge Q = Q \wedge P$.

6. Prove or disprove the following *without* using truth tables.

(1) $\neg(P \wedge \neg Q) = \neg P \vee Q$.
(2) $P \vee ((Q \wedge R) \wedge S) = (P \wedge Q) \vee (P \wedge R) \vee (P \wedge S)$.
(3) $P \vee (Q \wedge R) \wedge S) = (P \vee Q) \wedge (P \vee R) \wedge (P \vee S)$.

7. Write the negations of the following implications.

(1) If n is even, then n^2 is even.
(2) If $1 = 0$, then $2 + 2 = 5$.
(3) If there is free coffee, then DZB will drink it
(4) If $1 = 0$ and $2 + 2 = 5$, then the sky is blue and kittens are popular on youtube
(5) If x and y are real numbers such that $xy = 0$, then $x = 0$ or $y = 0$.

8. Which of these are true?

(1) (T or F) For all $x \in \mathbf{Z}$, x is divisible by 2.
(2) (T or F) There exists an $x \in \mathbf{Z}$ such that x is divisible by 2.
(3) (T or F) For all $x \in \mathbf{R}$, if $x \neq 0$, then there exists a $y \in \mathbf{R}$ such that $xy = 1$.
(4) (T or F) For all $x \in \mathbf{R}$, there exists a $y \in \mathbf{R}$ such that $xy = 1$.

9. Write the negations of the following.

(1) For all $x \in \mathbf{Z}$, x is divisible by 2.
(2) There exists an $x \in \mathbf{Z}$ such that x is divisible by 2.
(3) $\neg(\forall x, P(x))$,
(4) $\neg(\exists x \text{ s.t. } Q(x))$
(5) $\forall x, (P(x) \wedge Q(x))$.
(6) If $\exists x \in \mathbf{R}$ such that $2x = 1$, then for all y, $y^2 < 0$.
(7) For all $x \in \mathbf{R}$, there exists a $y \in \mathbf{R}$ such that $xy = 1$.

10. Write the converse and contrapositive of the statements from problem 7.

MATH 220 HANDOUT 2 - DIVISIBILITY

(1) Show that if $d \neq 0$ and $d \mid a$, then $d \mid (-a)$ and $-d \mid a$.
(2) Show that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
(3) Suppose that n is an integer such that $5 \mid (n+2)$. Which of the following are divisible by 5?
   (a) $n^2 - 4$
   (b) $n^2 + 8n + 7$
   (c) $n^4 - 1$
   (d) $n^2 - 2n$
(4) Prove that the square of any integer of the form $5k + 1$ for $k \in \mathbf{Z}$ is of the form $5k' + 1$ for some $k' \in \mathbf{Z}$.
(5) Show that if $ac \mid bc$ and $c \neq 0$, then $a \mid b$.

(6) (a) Prove that the product of three consecutive integers is divisible by 6.
   (b) Prove that the product of four consecutive integers is divisible by 24.
   (c) Prove that the product of n consecutive integers is divisible by $n(n-1)$.
   (d) (Challenge problem) Prove that the product of n consecutive integers is divisible by $n!$.
(7) Find all integers $n \geq 1$ so that $n^3 - 1$ is prime. Hint: $n^3 - 1 = (n^2 + n + 1)(n - 1)$.
(8) Show that for all integers a and b,

$$a^2 b^2 (a^2 - b^2)$$

is divisible by 12.
(9) Suppose that a is an integer greater than 1 and that n is a positive integer. Prove that if $a^n + 1$ is prime, then a is even and n is a power of 2. Primes of the form $2^{2^k} + 1$ are called Fermat primes.
(10) Suppose that a and n are integers that are both at least 2. Prove that if $a^n - 1$ is prime, then $a = 2$ and n is a prime. (Primes of the form $2^n - 1$ are called Mersenne primes.)
(11) Let n be an integer greater than 1. Prove that if one of the numbers $2^n - 1, 2^n + 1$ is prime, then the other is composite.
(12) Show that every integer of the form $4 \cdot 14^k + 1$, $k \geq 1$ is composite. Hint: show that there is a factor of 3 when k is odd and a factor of 5 when k is even.

(13) Can you find an integer $n > 1$ such that the sum

$$1 + \frac{1}{2} + \frac{1}{3} + + \cdots + \frac{1}{n}$$

is an integer?

Week 3: proof by contradiction

Prove that for $x, y \in \mathbb{R}$,

$$x + y > 20 \implies \overbrace{\boxed{x > 10 \text{ or } y > 10}}^{P}.$$

Proof: Assume $x + y > 20$. Assump.

(Q is either true or false)

(either "Q" or $\neg Q$ is true)

Proceed by contradiction. Assume $\neg P$, i.e., $x \le 10$ and $y \le 10$. [Adding gives $x + y \le 20$.] This contradicts our assumption. Thus $\neg P$ must have been false, so P is true, i.e.,

$x > 10$ or $y > 10$. ∎

Q

Proof that $\neg P \Rightarrow Q$

Template for proof by contradiction

- We want to prove P.
- There are "2 cases": P is true or P is false.
- If we can rule out "P is false", then P must be true.
- To begin, Assume P is false, i.e. $\neg P$.
- "Argue"; i.e. exhibit some (correct) chain of reasoning. end up w/ a statement Q.

(I.E write out a proof of "$\neg P \Rightarrow Q$")

- Observe (or give a proof that) Q is false.
- Conclude that $\neg P$ is false.

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

Intuitions

- Chess "If I move here, if moves they have check. So I shouldn't make that move"

Prove that $x^2 - y^2 = 1$ has no positive integer solutions.

$(x,y) = (1,0)$

not positive.

Proof: Proceed by contradiction.

Assume that x, y is a positive integer solution to $x^2 - y^2 = 1$. Then $(x-y)(x+y) = 1$. There are 2 possibilities:

$x - y = 1$ and $x + y = 1$, or $x - y = -1$ and $x + y = -1$.

In the 1st case adding gives $2x = 2$

Then $x = 1$, but $x - y = 1$, $\boxed{y = 0.}$ Q_1 this

is a contradiction since y is positive.

In the 2nd case, adding gives $2x = -2$,

So $\boxed{x = -1.}$ Q_2 This is a contradiction

since x is positive.

In both cases, we get a contradiction.
Thus our assumption was wrong, and we conclude that there are no positive integer solutions to $x^2 - y^2 = 1$. $\blacksquare$

N.B. Really was a proof that

$$\neg P \Rightarrow (Q_1 \text{ or } Q_2)$$

need both to give a contradiction

IE if there are cases in conclusion, need each case to be false.

Prove that $x^2 = 4y + 3$ has no integer solutions. P

Proof: Proceed by contradiction. Assume that there are $x, y \in \mathbb{Z}$ s.t.

$$x^2 = 4y + 3.$$

There are 2 cases: x is even or x is odd.

If x is even then the LHS is even and the RHS is odd. This is a contradiction.

If x is odd, then $x = 2k+1$ for some $k \in \mathbb{Z}$. Plugging in gives

$$(2K+1)^2 = 4K^2+4K+1 = 4y+3.$$

This a contradiction, since the LHS has a remainder of 1 and the RHS has a remainder of 3. $\blacksquare$

<u>Recall</u>: An integer n is <u>prime</u> if its only divisors are ± 1 and $\pm n$.

$2, 3, 5, 7, 11, 13, 17, 19, 23,$ primes

$4, 6, 8, 12$ not prime

$65537 = 2^{2^4} + 1$

65538 not prime

Euclid's theorem: there exist infinitely many primes.

<u>Proof:</u> Proceed by contradiction. Assume there are only finitely many primes.
Let's name them $p_1, p_2, \ldots, p_r$.

$(p_1 = 2, p_2 = 3, p_3 = 5, \ldots \; p_r = ?)$

Label them so that $p_1 = 2$, $p_{i+1} > p_i$

let $N = p_1 p_2 p_3 \cdots p_r + 1$.

(what does the factorization look like?)

Since $N > p_r$, N isn't prime (b/c N is bigger than the biggest prime). By FTA (Fundamental thm of arithmetic), N

factors into primes. Let q be one of those primes. Since $p_1, \dots, p_r$ are <u>all</u> of the primes, $\exists\, i$ s.t. $q = p_i$.
Then $q \mid N$ and $q \mid p_1 \cdots p_i \cdots p_r$, thus by the 2 out of 3 rule,

$q \mid N - (p_1 \cdots p_r)$, i.e. $q \mid 1$. This is a contradiction since $q > 1$. Thus there are infinitely many primes. $\blacksquare$

Joke: There are no uninteresting ~~numbers~~. positive integers.

Proof: Proceed by contradiction.
Assume that some positive integers are uninteresting. Then there must be

a smallest uninteresting positive integer.

But that's pretty interesting!

(this is a proof technique: think about the "smallest" counterexample) if $a|b$ and $a|b+c$ then $a|c$

$a|-b$

$a|(b+c)+(-b) = c$

FTA (Fundamental THM of Arithmetic)

let $N \in \mathbb{Z}_{>1}$. Then

(i) $\exists\, p_1, \dots, p_r$ primes s.t.

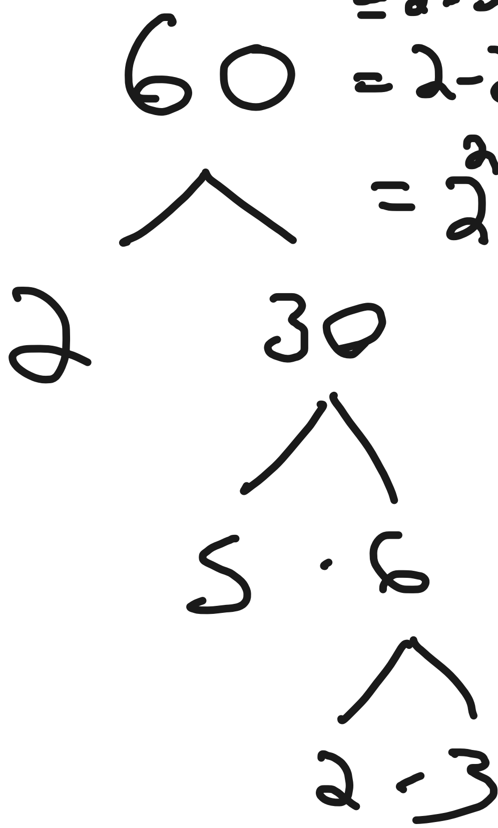
$$N = p_1 \cdots p_r$$

(ii) If $N = p_1 \cdots p_r = q_1 \cdots q_s$ s.t. $p_i \geq p_{i-1}$ and $q_j \geq q_{j-1}$, then $r = s$ and $\forall i$, $p_i = q_i$

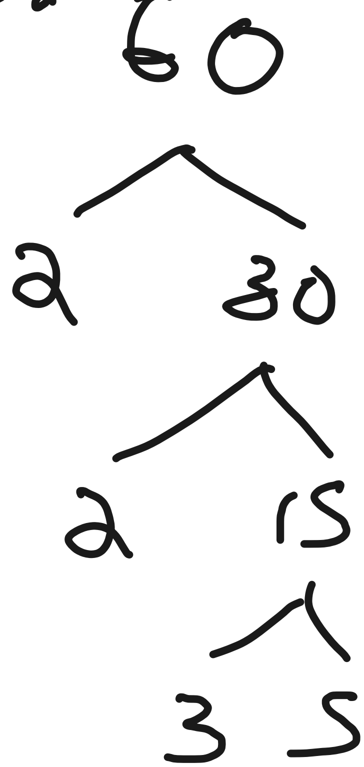
$= 2 \cdot 5 \cdot 2 \cdot 3$

$= 2 \cdot 2 \cdot 3 \cdot 5$

$= 2^2 \cdot 3 \cdot 5$



$2 \cdot 2 \cdot 3 \cdot 5$



Prove (i) Proceed by contradiction

Assume that some $N \in \mathbb{Z}_{>1}$ do not factor into primes. Let N be the smallest such integer. Then N is not prime, otherwise it is already factored

Thus N is composite. Write $N = ab$ where $1 < a, b < N$.
Since $a, b < N$ and N is the smallest integer that doesn't factor, a and b factor. Write $a = p_1 \cdots p_r$, $b = q_1 \cdots q_s$.
Then $N = ab = (p_1 \cdots p_r)(q_1 \cdots q_s)$.

This is a contradiction, since we just factored N. $\blacksquare$

Lecture 7 9/15/22 more contradiction

Want to prove P.

Assume $\neg P$. $\quad \neg P \Rightarrow Q$

Argue.

Conclude Q.

Observe that Q is false

Conclude P.

Prove that ($\forall n \in \mathbb{Z}$, n and $n+1$ have no common prime factors)

<u>Proof:</u> Proceed by contradiction. Assume $\exists n \in \mathbb{Z}$ s.t. n and $n+1$ have some common prime divisors. Let p be a prime s.t. <u>$p \mid n$</u> and <u>$p \mid n+1$</u>.

Then $p \mid (n+1) - n$, i.e., $p \mid 1$.
This is a contradiction, since p is prime, and primes are > 1. ∎

$\Rightarrow\Leftarrow$ ↯ ⨳

$d \mid a \wedge d \mid b \Rightarrow d \mid a+b$
$d \mid a \Rightarrow d \mid -a$
$d \mid a \wedge b \quad d \mid a-b$

Let $a,b,c \in \mathbb{Z}$. Sps $a^2+b^2=c^2$. Hyp

Show that abc is even.

Proof: Proceed by contradiction.

Assume $a^2+b^2=c^2$ and abc is odd.

Then a, b, and c are each odd. (BK if one were even, abc would be even)

Then $a^2, b^2, + c^2$ are odd (b/c products of odd integers are odd). Then $a^2 + b^2$ is even, but c^2 is odd. This is "even = odd" which is a contradiction. $\boxed{\mathcal{U}}$

$$\boxed{\begin{array}{l}\underline{\text{Defn}}\text{: A number } x \text{ is } \underline{\text{rational}} \text{ if} \\ \exists\, a,b \in \mathbb{Z} \text{ s.t. } b \neq 0 \text{ and } x = a/b.\end{array}}$$

A rational # is <u>reduced</u> if a and b have no common prime divisors

<u>Examples</u>: $\dfrac{2}{3} = \dfrac{4}{6}$

reduced not reduced.

<u>Fact</u>: every rational # can be reduced

Prove: $\sqrt{2} \notin \mathbb{Q}$. (It $\sqrt{2}$ is not Rational.)

Proof: Proceed by contradiction. Assume $\sqrt{2} \in \mathbb{Q}$. Then $\exists\, a, b \in \mathbb{Z}$ s.t. $b \neq 0$ and $\sqrt{2} = a/b$. Assume that a & b are reduced. In particular at least one of a or b is odd. Then

$b\sqrt{2} = a$. Then $b^2 \cdot 2 = a^2$.

Since the LHS is even, the RHS is even, i.e., a^2 is even. Thus a is even. (By HW1 if a is odd a^2 is odd.) Then $4 \mid a^2$; indeed, if $d \mid e$ + $f \mid g$ then $df \mid eg$). Write $a = 2k$ for some $k \in \mathbb{Z}$. Then $b^2 \cdot 2 = a^2$ $b^2 \cdot 2 = (2k)^2 = 4k^2$. Then $b^2 = 2k^2$. Since the RHS is even, b^2 is even so b is even. This is a contradiction, Since a+b are not both odd.

HW: $\sqrt{3} \notin \mathbb{Q}$

$3^{2/3}$

tan 1

$\pi = 3.141\ldots$

e

Prove: $\log_3 2 \notin \mathbb{Q}$.

Recall: $3^{\log_3 2} = 2$

__Proof:__ Proceed by contradiction.

Assume $\log_3 2 \in \mathbb{Q}$. Then $\exists\, a,b \in \mathbb{Z}$ s.t. $b \neq 0$ and $\log_3 2 = \frac{a}{b}$. WMA (we may assume) a & b are reduced.

Then $2 = 3^{\log_3 2} = 3^{a/b}$.

Then $2^b = 3^a$. $\left(\left(3^{a/b}\right)^b = 3^a \right)$

Since $b > 0$, the LHS is even.

But the RHS is odd. This is

a contradiction. $\boxed{M}$

Prove: if $a \in \mathbb{Q}$ and $b \notin \mathbb{Q}$, then $a+b \notin \mathbb{Q}$.

Proof: Assume $a \in \mathbb{Q}$ and $b \notin \mathbb{Q}$. Proceed by contradiction. Assume $a+b \in \mathbb{Q}$. Then $\exists\, c, d \in \mathbb{Z}$ s.t. $d \neq 0$ and $a = c/d$. Then $\exists\, e, f \in \mathbb{Z}$ s.t. $f \neq 0$ and $a+b = e/f$

Then $b = (a+b) - a = \frac{e}{f} - \frac{c}{d} = \frac{ed - cf}{fd}$.

Since $ed - cf, fd \in \mathbb{Z}$ and $fd \neq 0$, $b \in \mathbb{Q}$. This contradicts $b \notin \mathbb{Q}$.

We conclude that $a+b \notin \mathbb{Q}$. $\boxtimes$

Let a, b, c be odd. Let x be a solution to $ax^2 + bx + c = 0$. Prove $x \notin \mathbb{Q}$.

<u>Proof:</u> Assume a, b, c are odd.

Assume $ax^2 + bx + c = 0$.

Proceed by contradiction. Assume $x \in \mathbb{Q}$.

Then $\exists d, e \in \mathbb{Z}$ s.t. $e \neq 0$ and

$x = d/e$. WMA d & e are reduced.

Then $a\left(\frac{d}{e}\right)^2 + b\frac{d}{e} + c = 0$. \begin{equation}

Then $ad^2 + bde + ce^2 = 0$. (1.1)

Since d & e are reduced, at least one

is odd.

There are 3 cases: d & e are odd, d is even & e is odd, or d is odd & e is even

In case 1, the LHS of (1,1) is "odd + odd + odd = odd = even", a contradiction.

In case 2, the LHS is "e + e + 0 = e", $\Rightarrow\Leftarrow$

Case 3 is similar.

In each case, we have a contradiction ☒

2, 3, 5, 7, 11 ... $p \neq 1$ and $\forall a, b$ s.t. $p = ab$, $a = \pm 1$ or $b = \pm 1$

p is <u>prime</u> if "$p = ab \Rightarrow a = \pm 1$ or $b = \pm 1$"

<u>Fermat</u>: $1 = 1 \cdot 1 = 1 \cdot 1 \cdot 1 = \ldots$

Fermat:

$$2^0 + 1 = 1+1 = 2$$

$$2^1 + 1 = 2+1 = 3$$

$$2^2 + 1 = 4+1 = 5$$

$$2^4 + 1 = 16+1 = 17$$

$$2^8 + 1 = 256+1 = 257$$

$$2^{16} + 1 = 65536+1 = 65537$$

Fermat conj'd that $\forall n$, $2^{2^n}+1$ is prime.

False

Modern conj $2^{2^n}+1$ is never prime if $n \geq 5$.

$$2^3+1 = 8+1 = 9 = 3\cdot 3$$

$$2^5+1 = 32+1 = 33 = 3\cdot 11$$

$$2^7+1 = 128+1 = \underline{129} = 3\cdot 43$$

Problem: if 2^n+1 is prime then n is even.

Proof: Assume 2^n+1^n is prime.

Proceed by contradiction. Assume n is odd.

$$\left(\begin{aligned} &n^2-1 = (n-1)(n+1) \\ &x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots y^{n-1}) \end{aligned}\right)$$

Since n is odd, $(-1)^n = -1$.

Thus $2^n + 1 = 2^n + 1^n = 2^n - (-1)^n$.

This factors as $\left(2-(-1)\right)\left(2^{n-1} - 2^{n-2} + \cdots \pm 1\right)$

$$= 3 \cdot ?$$

If $2^n + 1 > 3$, it is not prime b/c 3 is a proper divisor. $\square$

<u>Induction:</u> Gauss S 10

$$1 + 2 + \dots + 100 = S$$

$$100 + 99 + \dots + 1 = S$$

$$\underbrace{101 + 101 \dots + 101}_{10} = 2S = 101 \cdot 100$$

$$S = \frac{101 \cdot 100}{2}$$

WTP: $\forall n \in \mathbb{Z}_{>0}$, $1+2+\dots+n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

$P(n)$

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

$n=2$ $\quad 1+2 = \frac{1\cdot 2}{2} + 2 = 2\left(\frac{1}{2}+1\right) = 2\left(\frac{3}{2}\right)$

$n=3$ $\quad 1+2+3 = \frac{2(3)}{2} + 3 = 3\left(\frac{2}{2}+1\right) = 3\left(\frac{4}{2}\right)$

$1+2+3+4 = \frac{3\cdot 4}{2} + 4 = 4\left(\frac{3}{2}+1\right) = 4\left(\frac{5}{2}\right)$

Proof: Proceed by induction. The statement is already true for $n=1$ b/c $\boxed{1 = \frac{1(2)}{2}}$ $=1$.

"Assume $P(n)$"

Assume that we already know the statement for n, I.E. assume that

this is $P(n)$.

$$1+2+\dots+n = n(n+1)/2.$$

Adding $n+1$ to both sides gives

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

The LHS of this is the LHS of what we want to prove. The RHS is

$$(n+1)\left(\frac{n}{2}+1\right) = (n+1)\left(\frac{n+2}{2}\right) = (n+1)\frac{(n+1)+1}{2}. \quad (*)$$

We conclude that $\forall n \in \mathbb{Z}_{>0}$,

$$1+2+\cdots+n = \frac{n(n+1)}{2}. \quad \blacksquare$$

$(*)$ to $(*)$ is a proof that $P(n) \Rightarrow P(n+1)$.

Let $P(n)$ be a statement which depends on some integer (usually pos) n.

(Ex: $P(n) =$ " $1+2+\cdots+n = \frac{n(n+1)}{2}$ ")

Goal: Prove $P(n)$ $\forall n \in \mathbb{Z}_{>0}$.

<u>Step 1</u>: Prove $P(1)$ "Base Case"

<u>Step 2</u>: Prove "$P(n) \Longrightarrow P(n+1)$" "Inductive step"

"Induction" = $P(1) \wedge$ "$\underline{P(n)} \Rightarrow P(\underline{n+1})$" $\Longrightarrow$

$$\forall n \in \mathbb{Z}_{>0}, P(n)$$

$P(1), P(2), P(3), P(4), \ldots, P(n), P(n+1), \ldots$

Warning:

$P(n) \neq \boxed{\frac{n(n+1)}{2}}$ ⟵ not "T or F"

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

Note: n is just a variable.

$P(1) \land P(n) \Rightarrow P(n+1)$ "prove the following case"

$P(a) \Rightarrow P(a+1)$

$P(a-1) \Rightarrow P(a)$

<u>Variant 3:</u> $P(0) \wedge P(n) \Rightarrow P(n+1)$

$P(2) \wedge P(n) \Rightarrow P(n+1)$

$\boxed{P(2) \wedge P(n) \Rightarrow P(n+2)}$

$\Rightarrow \forall n \in \mathbb{E}_{\geq 0}, P(n)$

$P(-1) \wedge P(n) \Rightarrow P(n-1)$

$\forall n \in \mathbb{Z}_{<0}, P(n)$

$P(-3), P(-2), P(-1)$

Define: a sequence $a_1, a_2, \ldots, a_n, \ldots$

$$\boxed{\begin{aligned} a_1 &= 2 = 2^1 \\ a_n &= 2 \cdot a_{n-1} \end{aligned}}$$

"recursive defn"

$a_m = 2 \cdot a_{m-1}$ $\quad \boxed{a_{n+1} = 2 \cdot a_n}$

$a_2 = 2 \cdot a_1 = 2 \cdot 2 = 4 = 2^2$

$a_3 = 2 \cdot a_2 = 2 \cdot 4 = 8 = 2^3$

$a_4 = 2 \cdot a_3 = 2 \cdot 8 = 16 = 2^4$

__Claim:__ $\forall n \in \mathbb{Z}_{>0}$, $\boxed{a_n = 2^n.}$

$P(n) =$ "$a_n = 2^n$"

Proof: Proceed by induction.

Base case: $P(1)$ is "$a_1 = 2^1$", i.e., "$2 = 2$". This is true.

$(P(n) \Rightarrow P(n+1))$

Inductive step: Assume $P(n)$, I.E., $a_n = 2^n$. (WTP $P(n+1)$, i.e., $a_{n+1} = 2^{n+1}$) Then $a_{n+1} = 2 \cdot a_n$ by the defn. of a_n. Then $a_{n+1} = 2 \cdot 2^n = 2^{n+1}$. Thus $P(n+1)$ is true. $\boxtimes$

Define: $a_1 = 0$

$$a_n = \sqrt{3 + 2a_{n-1}}$$

Prove: $\forall n \in \mathbb{Z}_{>0}$,

$a_n < 3$

$P(n) =$ "$a_n < 3$"

$a_1 = 0$

$a_2 = \sqrt{3 + 2 \cdot 0} = \sqrt{3}$

$a_3 = \sqrt{3 + 2 \cdot a_2} = \sqrt{3 + 2\sqrt{3}}$

$a_4 = \sqrt{3 + 2a_3} = \sqrt{3 + 2\sqrt{3 + 2\sqrt{3}}}$

Proof: Proceed by induction.

Base case: $P(1)$ is "$a_1 < 3$", i.e. "$0 < 3$". This is true.

I. S. Assume $P(n)$, i.e., "$a_n < 3$".

[WTP: $P(n+1)$, i.e., "$a_{n+1} < 3$"] Then, by defn,

$a_{n+1} = \sqrt{3+2a_n}$. Since $a_n < 3$,

$$a_{n+1} = \sqrt{3 + 2a_n} < \sqrt{3 + 2 \cdot 3} = \sqrt{3+6}$$
$$= \sqrt{9} = 3$$

Thus $a_{n+1} < 3$. $\boxtimes$

Claim: "$1+2+4+8+\cdots+2^{n-1} = 2^n - 1$" $\forall n \in \mathbb{Z}_{>0}$

Proof: Proceed by induction.

BC: $P(1)$ is "$1 = 2-1$". This is true.

IS: Assume $P(i)$, i.e., $1+2+\cdots+2^{i-1} = 2^i - 1$.

(WTP $P(i+1)$, i.e., $1+2+\cdots+2^{i+1-1} = 2^{i+1}-1$)

$1+2+\cdots+2^{i-1}+2^i = 2^{i+1}-1$

Adding 2^i to each side gives

$$1+2+\dots+2^{i-1}+2^i = 2^i-1+2^i.$$

The LHS is the LHS of $P(i+1)$.

The RHS is $2\cdot 2^i-1 = 2^{i+1}-1$.

This is the RHS of $P(i+1)$. $\blacksquare$

Claim: $\forall n \in \mathbb{Z}_{\geq 0}$, $\underbrace{3 \mid 4^n - 1}_{P(n)}$.

Proof: Proceed by induction.

BC: $P(0)$ is "$3 \mid 4^0 - 1$", i.e., "$3 \mid 0$"

which is true.

IS: Assume $P(n)$, i.e., $3 \mid 4^n - 1$.

(WTP $3 \mid 4^{n+1} - 1$) Then $\exists\, m \in \mathbb{Z}$ s.t.

$4^n - 1 = 3m$. Then $4^n = 3m + 1$.

Then $4^{n+1} - 1 = 4^n \cdot 4 - 1 = (3m+1) \cdot 4 - 1$

$= 12m + 4 - 1 = 12m + 3 = 3(4m+1)$.

Thus $3 \mid 4^{n+1} - 1$ $\blacksquare$

More Induction

WTP $\forall n \in \mathbb{Z}_{>0}, P(n)$

BC: Prove $P(1)$.

IS: Prove "$P(a) \Rightarrow P(a+1)$"

Prove: $\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Proof: Proceed by induction.

Base case: $P(1)$ is "$1^2 = 1(2)(3)/6$"

TE $1 = 1$.

Inductive step: Assume $P(a)$, i.e.,

$$1^2+2^2+\cdots+a^2 = a(a+1)(2a+1)/6.$$ $\left(\begin{array}{l}\text{WTP}\\ P(a)\Rightarrow P(a+1)\end{array}\right)$

Adding $(a+1)^2$ gives

$$1^2+2^2+\cdots+a^2+(a+1)^2 = \frac{a(a+1)(2a+1)}{6}+(a+1)^2.$$

The LHS is the LHS of $P(a+1)$.

The RHS is $\frac{a(a+1)(2a+1)}{6} + (a+1)^2 =$

$$(a+1)\left(\frac{a(2a+1)}{6} + \frac{6(a+1)}{6}\right) =$$

$$(a+1)\left(\frac{2a^2+a+6a+6}{6}\right) = (a+1)\left(\frac{2a^2+7a+6}{6}\right)$$

$$= \frac{(a+1)(a+2)(2a+3)}{6} =$$

$$\frac{(a+1)((a+1)+1)(2(a+1)+1)}{6}.$$ This is the

RHS of $P(a+1)$. $\boxtimes$

Claim: $\forall a \in \mathbb{Z}_{\geq 0}$, 3^a is odd.

Proof: BC: $P(0)$ is "3^0 is odd", i.e., "1 is odd". This is true.

IS: Assume $P(a)$, i.e., 3^a is odd.

(WTP: $P(a+1)$, i.e. 3^{a+1} is odd)

$$\parallel$$

$$\boxed{3^a} \cdot 3$$

Then $3^{a+1} = 3^a \cdot 3$. Since 3^a is odd & 3 is odd, and since the product of odd integers is odd, 3^{a+1} is odd. $\blacksquare$

Slogan: "Any time something "works" for 2 things, it works for many things".

Example: we know that "odd · odd = odd"

Pf: $\big((2a+1)\cdot(2b+1) = 4ab + 2(a+b) + 1 \big)$

rem. of 1.

<u>Claim:</u> If $a_1, \ldots, a_n$ are odd integers then $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ is odd. $P(n)$

<u>Pf:</u> Proceed by induction.

BC is $P(1)$ i.e., "if a_1 is odd, then a_1 is odd". This is true.

$P(2)$ is "if a_1, a_2 are odd, then $a_1 a_2$ is odd." This is true and we previously proved it.

<u>IS</u>: Prove that for $n \geq 2$, $P(n) \Rightarrow P(n+1)$

Assume $P(n)$, i.e., "if $a_1, \ldots, a_n$ are odd then $a_1 \cdots a_n$ is odd".

(WTP: $P(n+1)$ I.e. ["if $a_1, \ldots, a_{n+1}$ are odd" then $a_1 \cdots a_{n+1}$ is odd"],

Assume $a_1, \ldots, a_{n+1}$ are odd.

Then $a_1 \cdots a_n$ is odd because $P(n)$ is true. Then $(a_1 \cdots a_{n+1}) = (a_1 \cdots a_n) \cdot a_{n+1}$.

Since $(a_1 \cdots a_n)$ is odd and a_{n+1} is odd, since we know $P(2)$, their product is odd. Thus $a_1 \cdots a_{n+1}$ is odd ∎

$$a+b = b+a$$

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

---

2 base cases

$$P(1) \wedge P(2) \wedge \left(P(n) \Rightarrow P(n+1) \right)$$

The proof that $P(n) \Rightarrow P(n+1)$ doesn't work for $n=1$.

Prove: $\boxed{n! > 2^n}$ for $n \geq 4$.

$P(n)$

$$n! = n \cdot (n-1)(n-2) \cdots 1$$

$n =$	$P(n) =$
1	$1! = 1 > 2$
2	$2! = 2 > 4$
3	$3! = 6 > 8$
4	$4! = 24 > 16$

Proof: Proceed by induction.

BC: $P(4)$ is "$4! > 2^4$", i.e., "$24 > 16$". This is true.

Assume $n \geq 4$ and assume $P(n)$, i.e., $n! > 2^n$.

(WTP $P(n+1)$, i.e., $(n+1)! > 2^{n+1}$)

Multiplying $P(n)$ by $n+1$ gives

$$\boxed{(n+1)\,n! > (n+1)\,2^n.}$$

The RHS of this is $(n+1)!$.

Since $n \geq 4$, $n+1 \geq 5 \geq 2$.

Thus $\boxed{(n+1)\,2^n \geq 2 \cdot 2^n = 2^{n+1}.}$

We conclude that $(n+1)! > 2^{n+1}$ $\blacksquare$

Fibonacci #'s $F_1 = 1$, $F_2 = 1$, $F_3 = 1+1$

$F_4 = 3$, ...

Last perfect power

$1, 1, 2, 3, 5, \boxed{8}, 13, 21, 34, 55, 89, \boxed{144}, \ldots$

Defn:

$$\boxed{\begin{gathered} F_1 = 1, \; F_2 = 1 \\ F_n = F_{n-1} + F_{n-2} \end{gathered}}$$

Same as

$$F_{n+1} = F_n + F_{n-1}$$

$$F_n = F_{n-1} + F_{n-2}$$

$$F_{n+2} = F_{n+1} + F_n$$

$$F_{2n+2} = F_{2n+1} + F_{2n}$$

Claim: "$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$"

"$P(n)$"

Ex's 1, 1, 2, 3, 5, 8, 13, 21

Proof: (BC) $P(1)$ is "$F_1 = F_2$", i.e.,

"$1 = 1$". This is true.

IS: Assume $P(n)$, i.e.,

"$F_1 + F_3 + \dots + F_{2n-1} = F_{2n}$".

$2(n+1)-1 =$

$2n+2-1$

$2n+1$

Adding F_{2n+1} to both sides gives

$$F_1 + F_3 + \dots + F_{2n-1} + F_{2n+1} = F_{2n} + F_{2n+1}.$$

By the defn, $F_{2n} + F_{2n+1} = F_{2n+2}$.

Thus $F_1 + F_3 + \cdots + F_{2n+1} = F_{2n+2}$, i.e.,

$P(n+1)$ is true. ∎

"Lucas"

$2, 1, 3, 4, 7, 11, 18, 29, \ldots$

$L_1 = 2 \qquad L_2 = 1$

$L_n = L_{n-1} + L_{n-2}$

Claim: $\forall n \in \mathbb{Z}_{>0}$, "$F_n < 2^n$".

Proof: (BC) $P(1)$ is "$F_1 < 2^1$", i.e.,

$1 < 2$. $P(2)$ is "$F_2 < 2^2$", i.e.,

$1 < 4$. These are true.

IS: Assume $P(n)$ and $P(n+1)$, ~~IE~~,

$F_n < 2^n$ and $F_{n+1} < 2^{n+1}$.

(WTP $P(n+2)$, i.e., $F_{n+2} < 2^{n+2}$)

By defn, $F_{n+2} = F_{n+1} + F_n$. Since $P(n)$ and $P(n+1)$ are true, $F_{n+1} + F_n < 2^{n+1} + 2^n$.

IH, $F_{n+2} < 2^{n+1} + 2^n$. (want 2^{n+2})

Since $2^n < 2^{n+1}$, $2^{n+1} + 2^n < 2^{n+1} + 2^{n+1}$

$= 2 \cdot 2^{n+1} = 2^{n+2}$. Thus

$F_{n+2} < 2^{n+2}$. $\blacksquare$

$$P(1) \wedge P(2) \wedge \big(P(n) \wedge P(n+1) \Rightarrow P(n+2) \big)$$

$$P(1),\ P(2),\ P(3),\ P(4),\ P(5),\ \ldots$$

<u>Claim:</u> "$F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^n$" $= P(n)$

1, 1, 2, 3, 5, 8

<u>Proof:</u> "$P(2)$" is the statement

"$F_1 \cdot F_3 = F_2^2 + (-1)^2$", i.e.,

$$1 \cdot 2 = 1^2 + (-1)^2$$

$$2 = 2.$$ This is true.

IS: Assume $P(a)$, i.e., $F_{a-1} \cdot F_{a+1} = F_a^2 + (-1)^a$.

(WTP $P(a+1)$, i.e., $F_a \cdot F_{a+2} = F_{a+1}^2 + (-1)^{a+1}$)

By defn, $F_{a-1} + F_a = F_{a+1}$, i.e., $F_{a-1} = F_{a+1} - F_a$.

Subbing gives $(F_{a+1} - F_a) \cdot F_{a+1} = F_a^2 + (-1)^a$.

Then $F_{a+1}^2 - F_a \cdot F_{a+1} = F_a^2 + (-1)^a$.

then $F_{a+1}^2 - (-1)^a = F_a^2 + F_a \cdot F_{a+1}$.

Then $F_{a+1}^2 + (-1)(-1)^a = F_{a+1}^2 + (-1)^{a+1}$

$= F_a(F_a + F_{a+1}) = F_a F_{a+2}$ by the def. $\square$

def of fib.

Week 6: Sets

Set = "container", order does not matter
defined by what they contain

Defn: A *set* is a collection of objects.
An object of a set is called an *element*.
We write this as $a \in S$.

Examples

$S = \{1, 2, 3, 4, 5\}$

\{ ... \} in Latex

$1 \in S$, $0 \notin S$, $\pi \notin S$

$T = \{2, 1, 3, 4, 5\} = S$

$T = S$

$\{1, \sqrt{2}\}$, $\{\sqrt{2}, \pi\}$, $\{$David, Jenny, Sarah$\}$

$\{1, 2, \ldots, 10\}$ use "..." to indicate some pattern

\ldots vs ...

$\{2, 4, \ldots, 20\}$

Common Sets

$\mathbb{N} = \{1, 2, 3, \ldots\}$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ = complex #'s

$\sqrt{2} \notin \mathbb{Q}, \quad \sqrt{2} \in \mathbb{R}$

$\sqrt{-2} \notin \mathbb{R}$

$E = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}$

$d \in \mathbb{Z}_{\geq 1}$, we define

$d\mathbb{Z} = \{\text{'multiples of } d\text{'}\}$ $\boxed{!}$ More detail

$= \{\ldots, -2d, -d, 0, d, 2d, 3d, \ldots\}$

$= \{dn : n \in \mathbb{Z}\}$

$= \{n : n \in \mathbb{Z} \mid d \mid n\}$

$= \{n \in \mathbb{Z} \text{ s.t. } d \mid n\}$

General constructor:

$\{\text{formula} : \text{parameters} \mid \text{conditions}\}$

" : " = " | " = "such that" = "s.t."

Example: $a, b \in \mathbb{R}$

$[a, b] = \{x \in \mathbb{R} \text{ s.t. } a \leq x \leq b\}$

$[a, b) = \{x \in \mathbb{R} \text{ s.t. } a \leq x < b\}$

$\boxed{!}$ A set can contain anything

Example:

$$\mathrm{Fun}(\mathbb{R},\mathbb{R}) = \{\text{functions from } \mathbb{R}\to\mathbb{R}\}$$
$$= \{f : \mathbb{R}\to\mathbb{R}\}$$

$g(x) := x^2$, then $g \in \mathrm{Fun}(\mathbb{R},\mathbb{R})$

$h(x) := \sqrt{x}$ $\quad h \notin \mathrm{Fun}(\mathbb{R},\mathbb{R})$

$\quad h \in \mathrm{Fun}(\mathbb{R},\mathbb{C})$

":=" means "definition"

$$\mathbb{Q}[x] := \{a_0 + a_1x + \cdots + a_nx^n : n \in \mathbb{Z}_{\geq 0} \text{ and each } a_i \in \mathbb{Q}\}$$

$$\mathbb{R}[x] := \{\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \ \mathbb{R}\}$$
$$= \left\{\sum_{i=0}^{n} a_ix^i : n \in \mathbb{Z}_{\geq 0},\ a_i \in \mathbb{R}\right\}$$

$\boxed{!}$ Sets can be elements of sets.

Analogy: Big Amazon box containing many smaller boxes.

Examples:

$$T := \{ \{1\}, \{2\}, \{3,4\} \}$$

T has 3 elements, not 4

$\{1\} \in T$, $\{2\} \in T$, $\{3,4\} \in T$

$\boxed{\{1,2\} \notin T}$

$$S = \{ \{2\}, 3 \}$$

$3 \in S$

$\{2\} \in S$

$2 \notin S$

"$\in$" is not transitive

$x \in y \wedge y \in z \not\Rightarrow x \in z$

$2 \neq \{2\}$

$$R = \{ 1, \{1\} \}$$

$1 \in R$

$\{1\} \in R$

Empty set $\longleftrightarrow$ "empty box"

<u>Defn:</u> The empty set ϕ is the set with the property that $\forall x, x \notin \phi$. (I.E., $x \in \phi$ is always false.)

Defn: We say that 2 sets S and T are equal if $x \in S \iff x \in T$.

(i.e., S & T have the same elements)

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

$\{1,2\} \neq \{2,3\}$ b/c $1 \in \{1,2\}$ and $1 \notin \{2,3\}$

$\mathbb{Z} \neq \mathbb{Q}$ b/c $\frac{1}{2} \in \mathbb{Q}$ but $\frac{1}{2} \notin \mathbb{Z}$.

Defn: Let S and T be sets. We say that S is a subset of T if $x \in S \Rightarrow x \in T$. In this case we write $S \subseteq T$. (OR $S \subset T$)

(Equivalently: $\forall x \in S, x \in T$)

To show $S \not\subseteq T$

Find $x \in S$ s.t. $x \notin T$

$\neg$ $\exists x \in S$ s.t. $x \notin T$

Example: $\{1,2\} \subseteq \{1,2,3\}$

$\{1,2,3\} \not\subseteq \{1,2\}$

$\underset{3}{\cup\!\!\!\!\!\in}$ $\quad \underset{3}{\not\ni}$

Remark: $S = T \iff S \subseteq T$ and $T \subseteq S$

$$\begin{array}{ccccccccc}
 & & \frac{1}{2} & & \frac{1}{2} & & i & & i \\
 & & \not\in & & \in & & \not\in & & \in \\
\mathbb{N} & \subseteq & \mathbb{Z} & \subseteq & \mathbb{Q} & \subseteq & \mathbb{R} & \subseteq & \mathbb{C} \\
\not\ni & \neq & \ni & \neq & \not\ni & \neq & \ni & \neq & \\
-1 & & -1 & & \sqrt{2} & & \sqrt{2} & &
\end{array}$$

Proofs w/ sets

$P \implies Q$

Recall "$A \subseteq B$" means $x \in A \implies x \in B$

An implication

Start by "assuming the assumption"

1. "Assume $x \in A$"
2. Write out what "$x \in A$" means
   (I.E write out the defn)
3. "Argue" or "do calculations"

   $\boxed{?}$

4. Conclude that $x \in B$.

has some defn &

in step 3, you verify this

$d\mathbb{Z} = \{n : n \in \mathbb{Z} \mid d \mid n\}$

Prove or disprove:

(i) $6\mathbb{Z} \subseteq 2\mathbb{Z}$

(ii) $2\mathbb{Z} \subseteq 6\mathbb{Z}$

Proof: (ii) This is false b/c $2 \in 2\mathbb{Z}$, but $2 \notin 6\mathbb{Z}$ (b/c $6 \nmid 2$).

(i) Let $x \in 6\mathbb{Z}$. Then $x \in \mathbb{Z}$ and $6 \mid x$.

Since $2 \mid 6$, by transitivity, $2 \mid x$. Thus $x \in 2\mathbb{Z}$, $\blacksquare$.

$A = \{ 4^n - 1 : n \in \mathbb{Z}_{\geq 0} \} = \{ 0, 3, 15, 63, \dots \}$

$B = 3\mathbb{Z}_{\geq 0}$

$:= \{ n \in \mathbb{Z}_{\geq 0} \text{ s.t. } 3 \mid n \}$

We know from week 2 that $3 \mid 4^n - 1$. TE $A \subseteq B$

<u>Claim:</u> $A \subseteq B$.

<u>Proof:</u> Let $x \in A$. Then $\exists n \in \mathbb{Z}_{\geq 0}$ s.t. $x = 4^n - 1$.

By week 2, $3 \mid 4^n - 1$. Thus $4^n - 1 \in 3\mathbb{Z}$. $\blacksquare$

Converse? Is $B \subseteq A$? NO!

$6 \in B$ but $6 \notin A$.

__Lemma:__ Let A, B, C be sets. Suppose that $A \subseteq B$ and $B \subseteq C$. Then $A \subseteq C$.

$x \in A \Rightarrow x \in C$

__Proof:__ Assume $A \subseteq B$ and $B \subseteq C$. Let $x \in A$. Since $A \subseteq B$, $x \in B$. Since $x \in B$, and $B \subseteq C$, $x \in C$. $\blacksquare$

ϕ is the set s.t. "$x \in \phi$" is false $\forall x$.

Claim: $\forall$ set A, $\phi \subseteq A$.

Proof: "There is nothing to check" $\square$

Is every $x \in \phi$ also $x \in A$? Yes...

Contradiction: Suppose $\phi \not\subseteq A$.

($\phi \subseteq A$ means $\boxed{x \in \phi \Rightarrow x \in A}$)

I.E. suppose that $\exists x \in \phi$ s.t. $x \notin A$.

Since $x \in \phi$ is always false, we found a contradiction. $\square$

You can't disprove $\phi \subseteq A$.

Contrapositive: $x \notin A \Rightarrow x \notin \phi$.

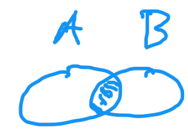
Suppose $x \notin A$. Well..... $x \notin \phi$ is true. $\square$

Week 7: More proofs w/ sets

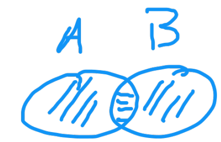
$A \subseteq B$ means $x \in A \Rightarrow x \in B$ "Let $x \in A$. ..... Thus $x \in B$."

$\forall x \in A, x \in B$

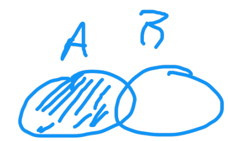
$A \cap B = \{x : x \in A \text{ and } x \in B\}$



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



$A - B = \{x \in A \mid x \notin B\}$



$\overline{B} = \{x : x \notin B\}$

$=$

$U - B$

$U =$ "everything"

Prove or disprove:

(i) $6\mathbb{Z} = 2\mathbb{Z} \cup 3\mathbb{Z}$ F

(ii) $6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$ T

$d\mathbb{Z} = \{n \in \mathbb{Z} \text{ s.t. } d \mid n\}$

Proof:

(i) This is false: $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, but $2 \notin 6\mathbb{Z}$.

(ii) "$=$" is "$\subseteq$" and "$\supseteq$"

"$\subseteq$" Let $x \in 6\mathbb{Z}$. Then $x \in \mathbb{Z}$ and $6 \mid x$.

(WTS: $x \in 2\mathbb{Z} \cap 3\mathbb{Z}$, i.e., $x \in 2\mathbb{Z}$ and $x \in 3\mathbb{Z}$, i.e., $x \in \mathbb{Z}$, $2 \mid x$ and $3 \mid x$)

Since $2 \mid 6$ and $3 \mid 6$, by transitivity of division, $2 \mid x$ and $3 \mid x$.
Thus $x \in 2\mathbb{Z}$ and $x \in 3\mathbb{Z}$, so $x \in 2\mathbb{Z} \cap 3\mathbb{Z}$.

"$\supseteq$" Let $x \in 2\mathbb{Z} \cap 3\mathbb{Z}$. Then $x \in 2\mathbb{Z}$ and $x \in 3\mathbb{Z}$. Then $x \in \mathbb{Z}$ and $2 \mid x$ and $3 \mid x$.

(WTS: $x \in 6\mathbb{Z}$, i.e., $6 \mid x$).

Since $\gcd(2,3) = 1$, $2 \cdot 3 \mid x$. Thus $x \in 6\mathbb{Z}$. ∎

$P \Rightarrow (Q \Rightarrow R)$

negation

$\neg$ $[B \subseteq C \wedge \exists x \in A - C$ s.t. $x \notin A - B]$

$x \in A - C \Rightarrow x \in A - B$

$P \Rightarrow Q$

Claim: $(B \subseteq C) \Rightarrow (A - C \subseteq A - B)$

Proof: $\boxed{\text{Let } \cancel{x \in B}.}$! #1 wrong answer

Assume $B \subseteq C$. Let $x \in A - C$. Then $x \in A$ and $x \notin C$.

(WTS: $x \in A - B$, i.e., $x \in A$ and $x \notin B$).

Proceed by contradiction. Assume $x \in B$. Since $B \subseteq C$, $x \in C$. This contradicts $x \notin C$. Thus $x \notin B$. Thus $x \in A - B$. ∎

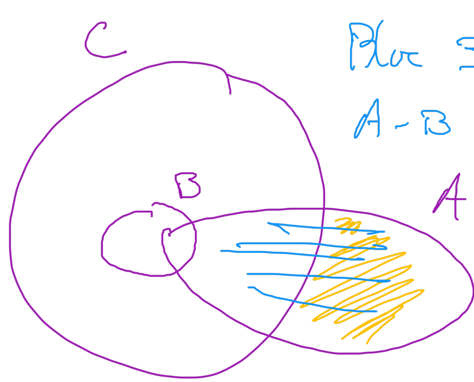
ALT. Proof.

... $x \notin C$. By the contrapositive of $B \subseteq C$, $x \notin B$.

$(x \in B \Rightarrow x \in C)$

Note: The contrapositive of "$B \subseteq C$" is

$x \notin C \Rightarrow x \notin B$



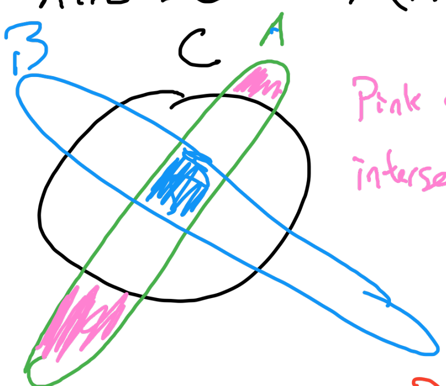
Blue ⊇ Yellow

$A - B \supseteq A - C$

$P \Rightarrow Q$

Claim: $A \cap B \subseteq C \Rightarrow (A-C) \cap B = \emptyset$

To prove "$D = \emptyset$", do proof by contradiction. "$D \neq \emptyset$", i.e. $\exists x \in D$.



Pink does not intersect B

Fine, but not ideal

"Let $x \in A - C \cap B$

..... $x \in \emptyset$"

Proof: ~~Let $x \in A \cap B$~~

Don't do this.

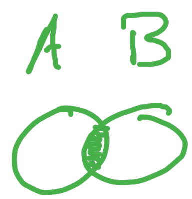
Suppose $A \cap B \subseteq C$. Proceed by contradiction. Assume $(A-C) \cap B \neq \emptyset$. Thus $\exists x \in (A-C) \cap B$. Then $x \in A - C$ and $x \in B$. Then $x \in A$ and $x \notin C$. Thus $x \in A \cap B$, so since $A \cap B \subseteq C$, $x \in C$. This is a contradiction, thus $A - C \cap B = \emptyset$. $\blacksquare$

De Morgan's Laws

$\overline{C} = \{x : x \notin C\}$

(a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

$\overline{A \cup B} = \overline{A} \cap \overline{B}$



Proof: "$\subseteq$" Let $x \in \overline{A \cap B}$. Then $x \notin A \cap B$.

(WTS $x \in \overline{A} \cup \overline{B}$ i.e.

$x \in \overline{A}$ or $x \in \overline{B}$ i.e.

$x \notin A$ or $x \notin B$)

$= \neg(x \in A \text{ and } x \in B) = \neg(x \in A \cap B)$

Thus $x \notin A$ or $x \notin B$. Thus $x \in \overline{A}$ or $x \in \overline{B}$.

Thus $x \in \overline{A} \cup \overline{B}$. $\boxtimes$

$ A \times B $

Products + Power Sets

Defn: let A and B be sets. The Cartesian Product $A\times B$ is the set $\{(a,b) : a\in A \text{ and } b\in B\}$.

Let $n\in\mathbb{N}$. then $A^n = \{(a_1,\dots,a_n) \text{ s.t. } \forall i\in\{1,\dots,n\}, a_i\in A\}$

$(A\times B\times C \ni (a,b,c),\ a\in A, b\in B, c\in C)$

Order matters $A\times B \neq B\times A$

$\boxed{\text{But}}$ A and B can be different.

1. $\mathbb{R}\times\mathbb{R} = \mathbb{R}^2 \ni (x,y),\ x,y\in\mathbb{R}$
2. $A=\{1,2\},\ B=\{3,4\}$

   $A\times B = \{(1,3),(1,4),(2,3),(2,4)\}$

   Ex. $(1,2)\notin A\times B$

   $A\times B \neq B\times A$

   $(1,3)\in A\times B,\ (1,3)\notin B\times A$ b/c $1\notin B$
3. $(a,b)\in A\times B \iff a\in A$ and $b\in B$
4. $\{-1,1\}\times\mathbb{Z} \ni (1,7)$
5. $\mathbb{R}\times \mathrm{Fun}(\mathbb{R},\mathbb{R}) \ni (\pi, f)$

$1\in\mathbb{Z}$ $\boxed{\mathbb{Z}\ni 1}$

$\mathbb{Z} \ni 1$ "$\ni$" = "s.t."

$A \supseteq B$ $A \supseteq B$

Lemma: Suppose $A \subseteq B$ and $C \subseteq D$.
Then $A \times C \subseteq B \times D$.

Proof: Suppose $A \subseteq B$ and $C \subseteq D$. Let $(a, c) \in A \times C$.

Then $a \in A$ and $c \in C$.

(WTK: $a \in B$ and $c \in D$)

Since $A \subseteq B$, $a \in B$. Since $C \subseteq D$, $c \in D$.

Thus $(a, c) \in B \times D$. ∎

Power Set: Let A be a set. Then we define the power set $P(A)$ to be

$$P(A) = \{ B \text{ s.t. } B \subseteq A \}$$

Examples: $A = \{1,2\}$ $\quad P(A) = \{ \{1\}, \{2\}, \phi, \{1,2\} \}$

$\{1\} \subseteq \{1,2\}$

$\{2\} \subseteq \{1,2\}$

$\emptyset \subseteq \{1,2\}$

$\{1,2\} \subseteq \{1,2\}$

$\{1\} \in P(\{1,2\})$

$1 \notin P(\{1,2\})$

Rule: $B \in P(A) \iff B \subseteq A$

$1 \notin P(\{1,2\})$ b/c $1 \not\subseteq \{1,2\}$

Claim: $\# P(A) = 2^{\# A}$

Ex: $A = \{7\}$ $\quad 1$

$P(A) = \{\phi, A\}$ $\quad 2^1$

Ex: $P(\phi) = \{ B : B \subseteq \phi \}$

$= \{ \phi \}$

$\# \phi = 0$

$\# \{\phi\} = 1 \qquad 1 = 2^0$

Ex: $\phi, A \in P(A)$ b/c $\phi \subseteq A$

$A \subseteq A$

$$P(\mathbb{Z}) = \{ \phi, \mathbb{Z}, \mathbb{E}, 3\mathbb{Z}, 4\mathbb{Z}, \ldots d\mathbb{Z}, \ldots \{1\}, \{2\}, \{3\}, \ldots \{1,2\}, \{1,2,3\}, \ldots \}$$

$\mathbb{E} \in P(\mathbb{Z})$

$d\mathbb{Z} \in P(\mathbb{Z})$

$\mathbb{R} \notin P(\mathbb{Z})$ b/c $\mathbb{R} \not\subseteq \mathbb{Z}$

Week 9: functions, images, & surjectivity

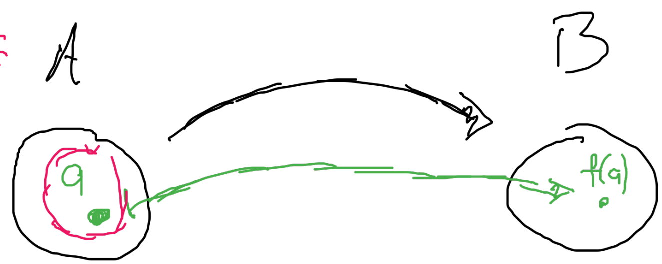
Let A, B be sets.

A <u>function</u> is a "rule" that associates, to each $a \in A$, some $b \in B$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \cup\!\!\!\mid & & \cup\!\!\!\mid \\ a & \longmapsto & f(a) \end{array}$$

Can't graph...

$W \subseteq$



Examples

$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

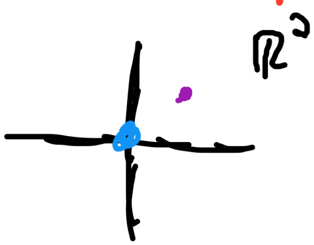
$(x,y) \longmapsto (x+y, xy)$

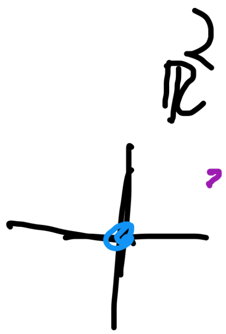
$f(x,y) = (x+y, xy)$

$f(0,0) = (0,0)$

$f(1,1) = (2,1)$

can't graph





"unambiguous" $:=$ $\forall a \in A$, $\exists$ exactly one output $f(a) \in B$.

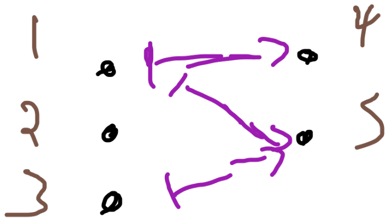
"not multivalued"

"passes the VLT" if $A = B = \mathbb{R}$

Let go of the formulas

$A = \{1,2,3\}, \; B = \{4,5\}$

$f(1) = 4 \quad f(2) = 4 \quad f(3) = 5$

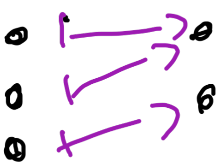


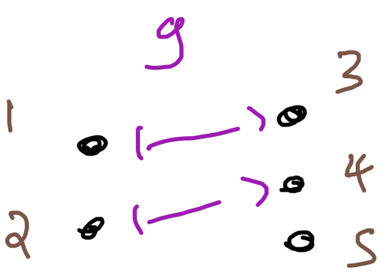
2 problems

Ambiguous (what is $f(1)$?)

Didn't define $f(2)$ . . .

From far away . . . just dots





5 is part of the codomain

5 is not an output

Domain	codomain	range = image
= inputs	potential outputs	Actual outputs

$A = \{x \mid x \text{ is a student in math dsc}\}$

$B = \{\text{yes}, \text{no}\}$

$$A \xrightarrow{f} B$$

$f(x) =$ Answer to "Is x wearing glasses"

$f(\text{Angela}) = \text{no}$

$f(\text{Jack}) = \text{no}$

$$\mathbb{Z} \xrightarrow{g} \mathbb{Z}$$

$$x \longmapsto \begin{cases} x/2 & \text{if } x \in \mathbb{E} \\ 3x+1 & \text{o/w} \end{cases}$$

otherwise

$g(1) = 4$

$g(2) = 1$

Caution

$$\mathbb{Z} \xrightarrow{h} \mathbb{Z}$$

$$x \longmapsto x/2$$

invalid b/c $x/2 \notin \mathbb{Z}$ if $x=1$

$$\mathbb{E} \longrightarrow \mathbb{Z}$$

$$x \longmapsto x/2$$

ok

Indicator fxn of $\mathbb{Q}$

$$\mathbb{R} \xrightarrow{f} \mathbb{R}$$

$$x \longmapsto \begin{cases} 0 & \text{if } x \notin \mathbb{Q} \\ 1 & \text{if } x \in \mathbb{Q} \end{cases}$$

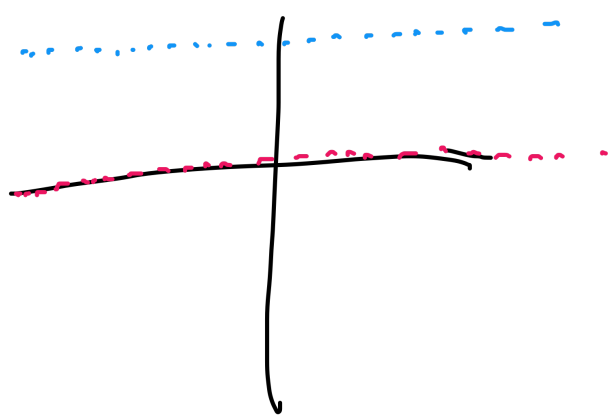
Unambiguous.

$g(0) = 1$ $\quad g(\sqrt{2}) = 0$

$g(22/7) = 1$ $\quad g(\pi) = 0$

$g(\tan 1) = ?$

$(x^5 + 7x + 1 = 0)$



What does it mean for $f = g$?

$f: A \to B$,

$g: C \to D$

<u>Defn:</u> We say that $f = g$ if

$A = C$, $B = D$, and $\forall a \in A$, $f(a) = g(a)$.

$\forall a, b \in A$, $f(a) = f(b)$ — constant

if $a = b$, $f(a) = f(b)$ — unambiguous

To show $f \neq g$, show $A \neq C$, $B \neq D$, or

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

Examples:

$$\mathbb{R} \xrightarrow{f} \mathbb{R}$$
$$x \longmapsto 2x$$

$f \neq g$ b/c different domains and codomains.

$$\mathbb{Z} \xrightarrow{g} \mathbb{Z}$$
$$x \longmapsto 2x$$

$g(\sqrt{2})$ is undefined b/c $\sqrt{2} \notin \mathbb{Z}$

$$\mathbb{Z} \xrightarrow{h} \mathbb{E}$$
$$x \longmapsto 2x$$

$h \neq g$

b/c different codomains.

$$\mathbb{Z} \xrightarrow{h_2} \mathbb{E}$$
$$n \longmapsto 2n$$

$h = h_2$

$$\forall b,\ \underset{\substack{\shortparallel \\ 2b}}{h(b)} = \underset{\substack{\shortparallel \\ 2b}}{h_2(b)}$$

$1 \overset{f}{\longmapsto} 2$, 3

$1 \overset{g}{\longmapsto} 3$, 2

$$f \neq g$$

$$\underset{\substack{\shortparallel \\ 2}}{f(1)} \neq \underset{\substack{\shortparallel \\ 3}}{g(1)}$$

$$f(n) = n+1$$

$$f(n) = 2n$$

invalid

$S \longmapsto S \cup 1$

$\mathcal{P}(\mathbb{Z}) \longrightarrow \mathcal{P}(\mathbb{Z})$

$\mathcal{P}(B) = \{A \subseteq B\}$

$A \in \mathcal{P}(B) \iff A \subseteq B$

$S \overset{f}{\longmapsto} S \cup \{1\} = f(S)$

$S \overset{g}{\longmapsto} S \cap \mathbb{E}$

$S \overset{h}{\longmapsto} S \cup \{\pi\}$

h is invalid

b/c $S \cup \{\pi\} \notin \mathcal{P}(\mathbb{Z})$

$f(\mathbb{E}) = \mathbb{E} \cup \{1\}$

$f(\mathbb{Z}) = \mathbb{Z} \cup \{1\} = \mathbb{Z}$

$f(\{2,3\}) = \{2,3\} \cup \{1\} = \{1,2,3\}$

$f(\emptyset) = \emptyset \cup \{1\} = \{1\}$

$g(\{2,3\}) = \{2,3\} \cap \mathbb{E} = \{2\}$

$g(\mathbb{Z}) = \mathbb{Z} \cap \mathbb{E} = \mathbb{E}$

$\mathbb{R} \longrightarrow P(\mathbb{R})$

$x \longmapsto (x, \infty)$

$x \longmapsto \{x\}$

$y \longmapsto y+1$ invalid

b/c $y+1 \notin P(\mathbb{R})$

$(x, \infty) = \{a \in \mathbb{R} \text{ s.t. } x < a\}$

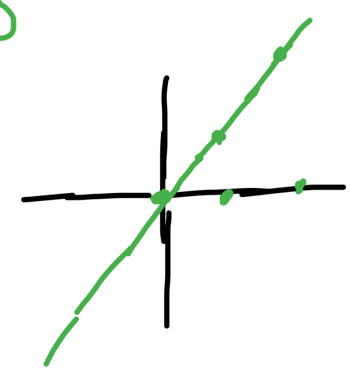
Common functions

$A \xrightarrow{id_A} A$ "do nothing"

$x \longmapsto x$ $A = \mathbb{R}$

$id_A(x) = x$

$id(x) = x$

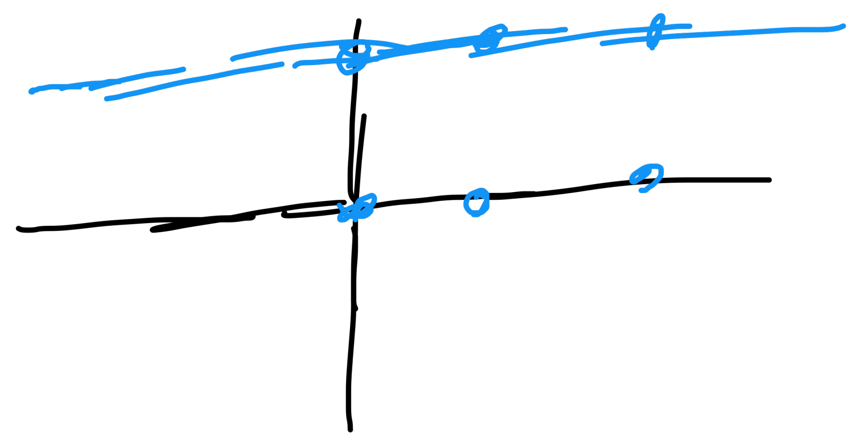


Sps $B \neq \emptyset$ and let $b \in B$.

$A \xrightarrow{c_b} B$ $A = B = \mathbb{R}$ $b = 1$

$a \longmapsto b$

$c_b(a) = b$



Defn: Let A and B be sets and $f: A \to B$ be a function.

The image (range) of f is

(write as $\operatorname{im} f$ or $f(A)$)

$$\operatorname{im} f = \{ f(a) : a \in A \}$$

If $W \subseteq A$, define

$$f(W) = \{ f(a) : a \in W \}$$

(onto)

We say that f is surjective if

$$f(A) = \operatorname{im} f = B$$

(I.E., "f takes every possible value")

$a \in A$, $f(a) \in B$ elements

$f(A)$ is a set

A not an elt

$f(W)$

$f(A) \subseteq B$

$\{ f(a) : a \in A \}$

To prove $f(A) = B$, only need to prove $B \subseteq f(A)$.

$A \xrightarrow{f} B$ $\quad$ f is surj.

$1 \mapsto 4$

$2 \mapsto 4$

$3 \mapsto 5$

$$f(A) = \{ f(a) : a \in A \}$$
$$= \{ f(a) : a \in \{1,2,3\} \}$$
$$= \{ f(1), f(2), f(3) \} = \{4,4,5\} = \{4,5\} = B$$

$W = \{1,2\}$

$$f(W) = \{ f(a) : a \in W \} = \{ f(1), f(2) \} = \{4,4\} = \{4\}$$

$A \xrightarrow{f} B$

$1 \longmapsto 2$

$ 3$

not surj.

$$f(A) = \{ f(1) \} = \{2\} \neq \{2,3\} = B.$$

$B \not\subseteq f(A)$ b/c $3 \in B$, but $3 \notin f(A)$

To prove $f(A) = B$, need to show

To prove $f(A) \neq B$, need to show

the defn of $b \in f(A)$

$\forall b \in B, \exists a \in A$ s.t. $f(a) = b$

$\exists b \in B$ s.t. $\forall a \in A, f(a) \neq b$

$\mathbb{R} \xrightarrow{f} \mathbb{R}$

$x \longmapsto x^2$

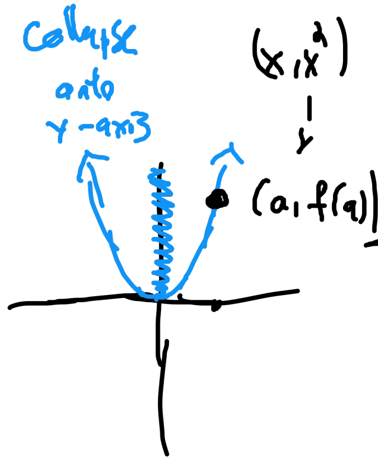
not surj b/c

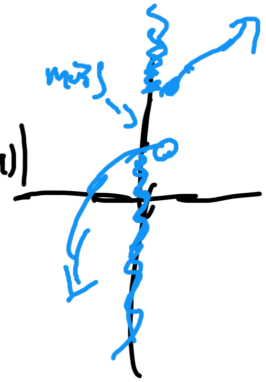
$-1 \notin \operatorname{im} f$

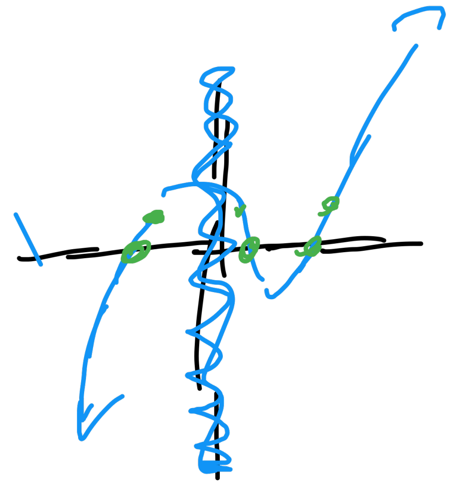
IE, $\nexists\, a \in \mathbb{R}$ s.t. $f(a) = -1$

IE $\nexists\, a \in \mathbb{R}$ s.t. $a^2 = -1$

b/c $a^2 \geq 0 \ \forall a \in \mathbb{R}$





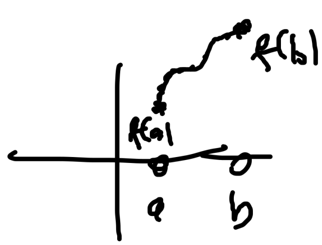


$\lim_{x \to \pm\infty} f(x) = \pm\infty$

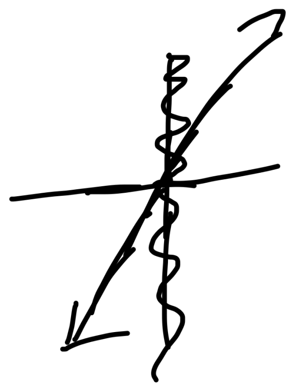
$f(\mathbb{R}) = \operatorname{im} f = \mathbb{R}_{\geq 0}$

(by "continuity")

$f(0) = 0$ AND $\lim_{x \to \infty} f(x) = \infty$



$$\mathbb{R} \xrightarrow{f} \mathbb{R}$$
$$x \longmapsto 2x+1$$
$$\text{im} f = \mathbb{R}$$



Pf: IVT, use continuity + limits.

Pf2: Claim: $f(\mathbb{R}) = \mathbb{R}$.

Automatic: $f(\mathbb{R}) \subseteq \mathbb{R}$.

Need: $\mathbb{R} \subseteq f(\mathbb{R})$.

Let $b \in \mathbb{R}$. (WTS $b \in f(\mathbb{R})$).

(Need $\exists\, a \in \mathbb{R}$ s.t. $f(a) = b$, i.e., $2a+1 = b$ $\qquad a = \frac{b-1}{2}$)

Let $a = \frac{b-1}{2}$. Then $a \in \mathbb{R}$ and $f(a) = 2\left(\frac{b-1}{2}\right)+1 = b-1+1$
$= b$.

Thus $b \in f(\mathbb{R})$ $\square$

Week 10, preimages

$f: A \longrightarrow B$

$a \longmapsto f(a)$

element

$W \subseteq A$

$f(W) = \{ f(a) : a \in W \}$

set

$f(W) \subseteq B$

b/c $f(a) \in B \ \forall a \in A$

Useful: $\forall a \in W,\ f(a) \in f(W)$

$P(A) \longrightarrow P(B)$

$W \longmapsto f(W)$

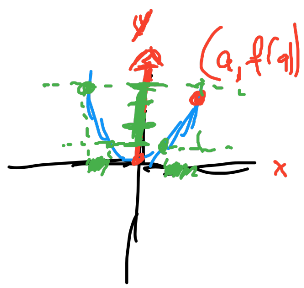
"Pre image" or "inverse image"

Defn: Let $A \xrightarrow{f} B$ be a fxn. Let $W \subseteq B$.
We define the preimage of W under f to be

$$f^{-1}(W) = \{a \in A \text{ s.t. } f(a) \in W\}$$

Caution! THIS IS NOT RELATED TO THE INVERSE FUNCTION

Examples: $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$



$W = \mathbb{R}_{\geq 0}$ $\quad f^{-1}(W) = \{a \in \mathbb{R} \text{ s.t. } \underset{a^2}{\underset{\shortparallel}{f(a)}} \in \mathbb{R}_{\geq 0}\}$

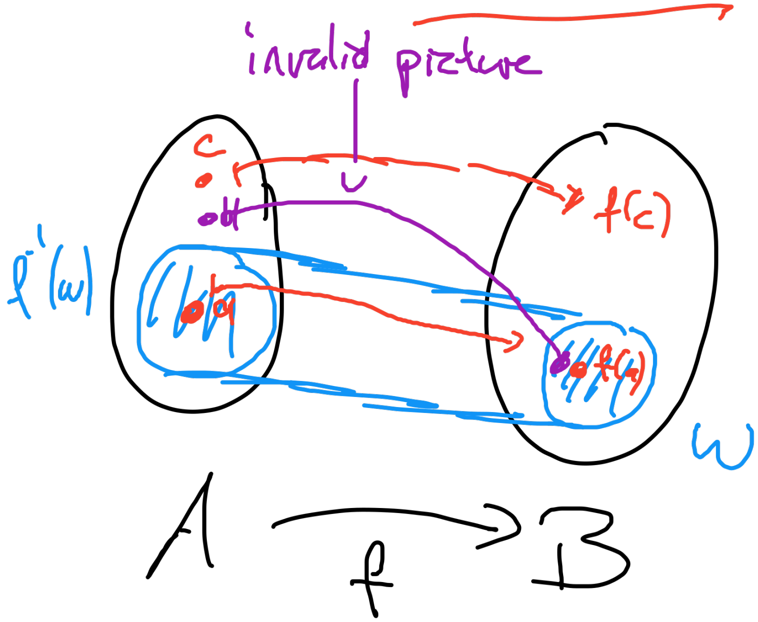
$= \mathbb{R}$

$W = [1,4]$

$f^{-1}(W) = [1,2] \cup [-2,-1]$

Useful: $a \in f^{-1}(W) \iff f(a) \in W$ ← this is either what we knew, or what we want to show

$c \notin f^{-1}(W) \iff f(c) \notin W$



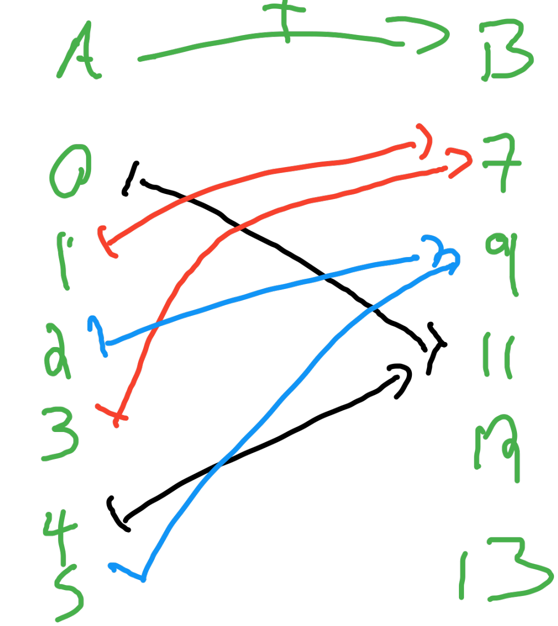
$A \xrightarrow{f} B \quad W = B \ ?$

Comment: $f^{-1}(B) = \{ a \in A \text{ s.t. } \boxed{f(a) \in B} \} = A$

Always true

(By the defn of fxn codomain)

Examples:



$f(0) = f(4) = 11$

$f(1) = f(3) = 7$

$f(2) = f(5) = 9$

$$f^{-1}(\{9, 11\}) = \{a \in A \text{ s.t. } f(a) \in \{9, 11\}\}$$
$$= \{0, 4, 2, 5\}$$

$$f^{-1}(\{7, 12\}) = \{1, 3\}$$

$$f^{-1}(\{7\}) = \{1, 3\}$$

$$f^{-1}(\{12, 13\}) = \emptyset$$

Example: $A \xrightarrow{f} B$

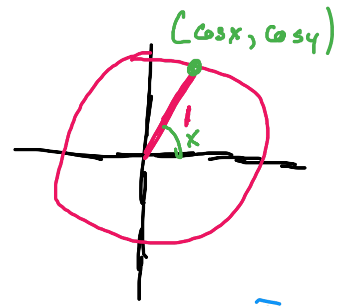
$W = \phi \subseteq B$

Always false

$$f^{-1}(\phi) = \{ a \in A \text{ s.t } \boxed{f(a) \in \phi} \} = \phi$$

Example: $f : \mathbb{R} \xrightarrow{\cos} \mathbb{R}$

$x \longmapsto \cos x$



$$f^{-1}([0,1]) = \{ a \in \mathbb{R} \text{ s.t. } \cos a \in [0,1] \}$$

$$= \ldots [-5\pi/2, -3\pi/2] \cup [-\pi/2, \pi/2] \cup [3\pi/2, 5\pi/2] \cup [7\pi/2, 9\pi/2] \ldots$$

$$(=) \bigcup_{n=-\infty}^{\infty} [-\pi/2 + 2n\pi, \pi/2 + 2n\pi]$$

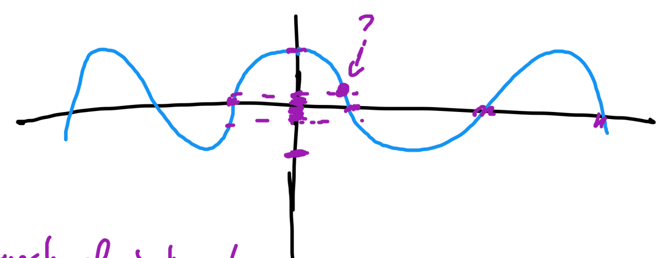
$$f^{-1}(\mathbb{R}_{\geq 0}) = f^{-1}([0,1])$$

Solve $\cos a = 0.17$

$a = \cos^{-1} .17$

$$f^{-1}([-1,1]) = \mathbb{R}$$

$$f^{-1}([2,3]) = \emptyset$$



$$f^{-1}([-0.23, 0.17]) = \text{bunch of intervals}$$

(w/ no nice formula)

$\mathbb{R} \xrightarrow{f} \mathbb{R}$, $x \mapsto x^2$ $\quad f^{-1}([1,4]) = [1,2] \cup [-2,-1]$.

$[a,b] = \{x \in \mathbb{R} \text{ s.t. } a \leq x \leq b\}$

Proof: "$\supseteq$" Let $x \in [1,2] \cup [-2,-1]$. Then $x \in [1,2]$ or $x \in [-2,-1]$.

Then $1 \leq x \leq 2$ or $-2 \leq x \leq -1$.

(WTS: $x \in f^{-1}([1,4])$ i.e., $f(x) \in [1,4]$ i.e., $1 \leq x^2 \leq 4$)

Case 1: $1 \leq x \leq 2$. Then squaring gives $1 \leq x^2 \leq 4$. Thus $x^2 = f(x) \in [1,4]$,

Thus $x \in f^{-1}([1,4])$.

Case 2: $-2 \leq x \leq -1$. Then squaring gives $1 \leq x^2 \leq 4$. Thus $x^2 = f(x) \in [1,4]$.

Thus $x \in f^{-1}([1,4])$.

"$\subseteq$" Let $x \in f^{-1}([1,4])$. Then $f(x) = x^2 \in [1,4]$. Then $1 \leq x^2 \leq 4$.

Then $1 \leq x \leq 2$ or $-2 \leq x \leq -1$. Thus $x \in [1,2]$ or $x \in [-2,-1]$,

Thus $x \in [1,2] \cup [-2,-1]$ ∎

18. For the following functions, compute the *inverse* image of the given subsets of the codomain. (No proofs are necessary.)

(a) $f: \mathbf{Z} \to \mathbf{Z}$, $f(n) = 3n + 1$; $W_1 = \mathbf{E}$, the set of even integers, $W_2 = \{4\}$, $W_3 = \{1, 5, 8\}$.

(b) $f: \mathbf{R} \to \mathbf{R}$, $f(x) = 3x + 1$; $W_1 = \{4\}$, $W_2 = \{1, 5, 8\}$, $W_3 = (4, \infty)$, $W_4 = (2, 4)$, $W_5 = \mathbf{Z}$, $W_6 = \mathbf{E}$, the set of even integers.

(c) $f: \mathbf{R} \to \mathbf{R}$, $f(x) = \cos x$; $W_1 = [-1, 1]$, $W_2 = \{x \in \mathbf{R} \mid x \geq 0\}$, $W_3 = \mathbf{Z}$.

(d) $f: \mathbf{R} \to \mathbf{R}$, $f(x) = e^x$; $W_1 = [-1, 0]$, $W_2 = \{x \in \mathbf{R} \mid x \geq 0\}$, $W_3 = \{1\}$.

(e) $f: \mathbf{Z} \to \mathbf{Z}$, $f(n) = \begin{cases} n, & \text{if } n \text{ is even} \\ n-1, & \text{if } n \text{ is odd} \end{cases}$; $W_1 = E$, $W_2 = \{1\}$, $W_3 = \{6\}$, $W_4 = \mathbf{O}$, the set of odd integers.

(a) $f^{-1}(\mathbb{E}) = \mathbb{O}$

"$\supseteq$" Let $a \in \mathbb{O}$. (WTS $a \in f^{-1}(\mathbb{E})$. $\exists$E, $f(a) \in \mathbb{E}$)

Then $f(a) = 3a+1$. Since a is odd, $3a$ is odd,

So $3a+1$ is even. Thus $f(a) \in \mathbb{E}$, thus $a \in f^{-1}(\mathbb{E})$.

"$\subseteq$" Let $a \in f^{-1}(\mathbb{E})$. Then $f(a) \in \mathbb{E}$. Thus $3a+1$ is even,

Thus $3a$ is odd, so $a \in \mathbb{O}$. ∎

e) $f(n) = \begin{cases} n & n \in \mathbb{E} \\ n-1 & n \in \mathbb{O} \end{cases}$

$f(0) = 0$ $\quad f(2) = 2$

$f(1) = 0$ $\quad f(3) = 2$

$f^{-1}(\{1\}) = \phi$ $\quad f^{-1}(\{6\}) = \{6, 7\}$

$f^{-1}(\mathbb{E}) = \mathbb{Z}$

Abstract proofs: $f: A \to B$

$X, Y \subseteq B$

$$f^{-1}(X \cup Y) \subseteq f^{-1}(X) \cup f^{-1}(Y)$$

Proof: Let $a \in f^{-1}(X \cup Y)$. Then $f(a) \in X \cup Y$.

Then $f(a) \in X$ or $f(a) \in Y$.

(WTS: $a \in f^{-1}(X) \cup f^{-1}(Y)$. IE $a \in f^{-1}(X)$ or $a \in f^{-1}(Y)$

IE $f(a) \in X$ or $f(a) \in Y$)

Thus $a \in f^{-1}(X)$ or $a \in f^{-1}(Y)$

Thus $a \in f^{-1}(X) \cup f^{-1}(Y)$.

"$\supseteq$" "every step is reversible", i.e., an "if and only if" ($\Longleftrightarrow$)

IE do the same proof backwards

$$f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$$

Switch "or" with "and" in prev. proof

(and $\cup$ w/ $\cap$)

"Let $\boxed{a \in f^{-1}(X \cap Y)}$ then $\boxed{f(a) \in X \cap Y.}$

Then $f(a) \in X$ and

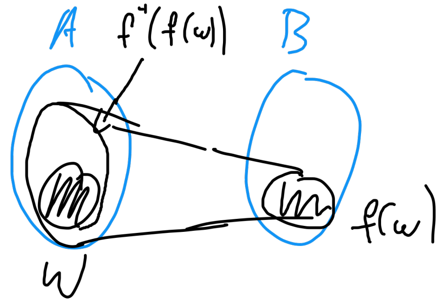
$f(a) \in Y$.

Then $a \in f^{-1}(X)$ and $a \in f^{-1}(Y)$.

Then $a \in f^{-1}(X) \cap f^{-1}(Y)$.

$A \xrightarrow{f} B$

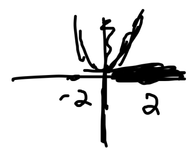
$W \subseteq A$



$\mathbb{R} \xrightarrow{x \mapsto x^2} \mathbb{R}$

$f^{-1}(f(W)) = f^{-1}(\mathbb{R}_{\geq 0}) = \mathbb{R}$

$W = \mathbb{R}_{\geq 0}$ $\quad f(W) = \mathbb{R}_{\geq 0}$



<u>Claim</u> $W \subseteq f^{-1}(f(W))$

Let $a \in W$. (WTS $a \in f^{-1}(f(W))$ IE $f(a) \in f(W)$)

$a \in W$ $\Downarrow$ defn of $f(W)$

Then $f(a) \in f(W)$ by defn of image.

Then $a \in f^{-1}(f(W))$. ☒
(defn of pre-im.)

$f^{-1}(f(W)) \subseteq W$ is false

$\mathbb{R} \subseteq \mathbb{R}_{\geq 0}$

for $W = \mathbb{R}_{\geq 0}$ $\quad f(x) = x^2$

Week 11: Injective functions or "one-to-one"

Defn: We say that a function $f: A \to B$ is injective if

$$\forall a, b \in A,\ a \neq b \Rightarrow f(a) \neq f(b)$$

"**Slogan**": "Distinct inputs give distinct outputs"

Contrapositive: $\forall a, b \in A,\ f(a) = f(b) \Rightarrow a = b$

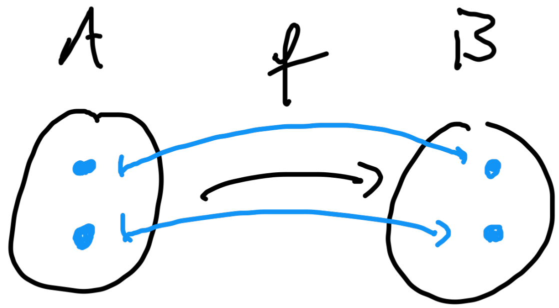
(often easier to do proofs with)

Negation: $\exists a, b \in A$ s.t. $a \neq b$ AND $f(a) = f(b)$

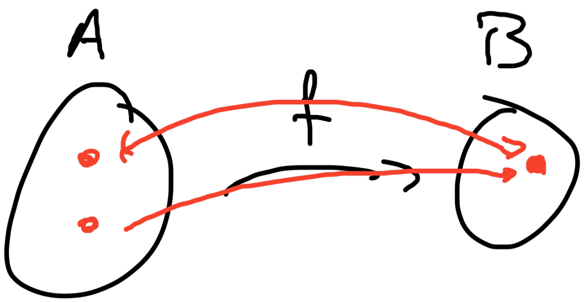
#1 Mistake: "$\forall a, b \in A,\ a = b \Rightarrow f(a) = f(b)$"

wrong

just.... the defn of a fxn

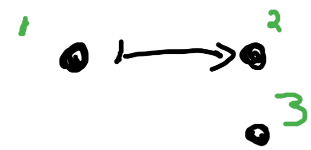


Inj

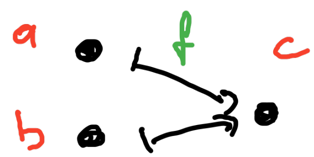


NOT I

"Test functions"



INJ

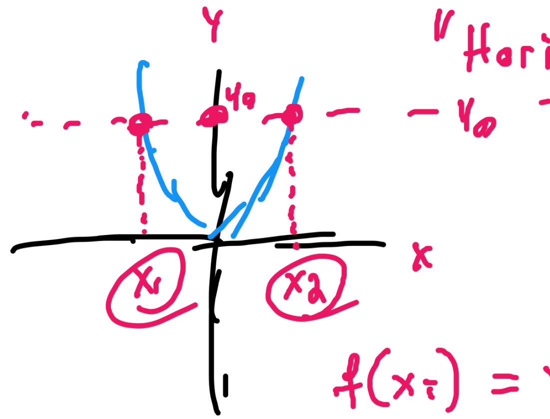


NOT INJ b/c
$a \neq b$ and $f(a) = f(b)$

Examples:

$g : \mathbb{R} \to \mathbb{R}$

$x \mapsto x^2$



$f(x_i) = y_0$

$\mathbb{R} \to \mathbb{R}$

"Horizon. line test":

$\forall$ Hor. line L, the intersection of L with the graph is at most one point

$\iff$

f is inj.

NOT INJ

$1 \neq -1$ and $\underbrace{g(1)}_{1} = \underbrace{g(-1)}_{1}$

Note: to prove a function $\boxed{\text{is}}$ inj., need an argument,

"$\forall a,b \in A,\ a \neq b \Rightarrow f(a) \neq f(b)$"

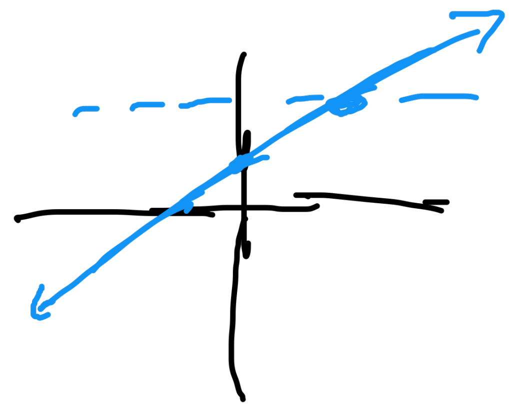
"$\forall a,b \in A,\ f(a) = f(b) \Rightarrow a = b$"

"Let $a,b \in A$. Assume $f(a) = f(b)$. $\boxed{\vdots}$ ... We conclude that $a = b$."

Argue

Examp: $\mathbb{R} \xrightarrow{f} \mathbb{R}$

$x \longmapsto \frac{x+1}{2}$



Claim: f is inj,

Proof: Let $a, b \in \mathbb{R}$. Suppose $f(a) = f(b)$. I.E.,

$\frac{a+1}{2} = \frac{b+1}{2}$. (WTS: $a = b$) Multiplying by 2 gives $a+1 = b+1$.

Subtracting 1 gives $a = b$. ☺

<u>Ei</u> $\mathbb{R}_{\geq 0} \xrightarrow{f} \mathbb{R}$

$x \longmapsto \frac{x-1}{x+1}$ I

<u>Proof:</u> Let $a,b \in \mathbb{R}_{\geq 0}$. Suppose $f(a)=f(b)$, i.e., $\frac{a-1}{a+1} = \frac{b-1}{b+1}$. Clearing denominators gives $(a-1)(b+1) = (b-1)(a+1)$, i.e.,

$ab-b+a-1 = ab-a+b-1$. Thus $-b+a = -a+b$, so $2a = 2b$, thus $a=b$. ∎

$$\frac{x-1}{x+1} = \frac{x+1-2}{x+1} = 1-\frac{2}{x+1} \Rightarrow 1-\frac{2}{a+1} = 1-\frac{2}{b+1}$$

$$\mathbb{R}^3 \xrightarrow{g} \mathbb{R}^2$$

$$(x,y,z) \longmapsto (x,y)$$

$$g(1,2,3) = (1,2)$$

$$g(1,2,4) = (1,2)$$

but $(1,2,3) \neq (1,2,4)$

g is <u>NOT</u> inj

$\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^3$ $\boxed{\text{I}}$

$(x,y) \longmapsto (x+y,\ x-y,\ x^2+y^2)$

$(0,0) \longmapsto (0,0,0)$

$(1,1) \longmapsto (2,0,2)$

$\vdots$

Proof: Sps $(a,b), (c,d) \in \mathbb{R}^2$. Sps $f(a,b) = f(c,d)$.

Thus $(a+b,\ a-b,\ a^2+b^2) = (c+d,\ c-d,\ c^2+d^2)$.

Thus $a+b = c+d$, $a-b = c-d$, $a^2+b^2 = c^2+d^2$.

Adding the 1st + 2nd eqn gives $2a = 2c$, so $a = c$.

~~Adding~~ Subtracting gives $2b = 2d$, thus $b = d$. We conclude that $(a,b) = (c,d)$ ∎

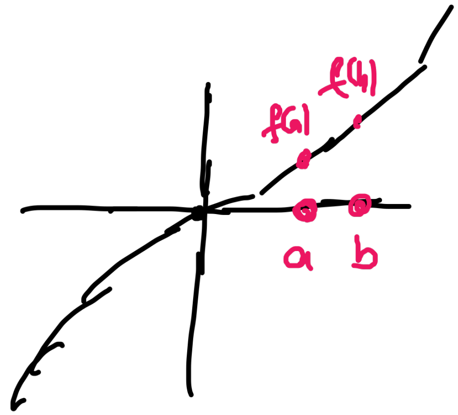
WTS $(a,b) = (c,d)$

$\Updownarrow$

$a = c \quad b = d$

Example: $\mathbb{R} \to \mathbb{R}$

$x \longmapsto x^3 + x$



or decreasing

Increasing $\overset{\text{HW}}{\Longrightarrow}$ inj

$$\boxed{b > a \Rightarrow f(b) > f(a)}$$

$a \neq b$ + f increasing

$\Downarrow$

$a < b \Rightarrow f(a) < f(b) \Rightarrow f(a) \neq f(b)$

or

$a > b \Rightarrow f(a) > f(b) \Rightarrow f(a) \neq f(b)$.

$x^3 + x = x(x^2+1)$

Try "usual" proof: Let $a, b \in \mathbb{R}$. Sps $f(a) = f(b)$. Then

$a^3 + a = b^3 + b$ . . .

f cts, diff Nowhere to go...

Calc I: $f'(x) > 0 \Rightarrow f$ is increasing

Proof: Since $f'(x) = 3x^2 + 1$, $f'(x) \geq 1$ $\forall x \in \mathbb{R}$. Thus f is increasing and therefore injective. ▨

Ex's:

$$f(x) = x^5 + 7x^3 + 3x$$

$$f'(x) = \boxed{5x^4 + 7x^2 + 3 \geq 3}$$

$\Rightarrow$ f is inj.

might need a small argument to show $f' > 0$.

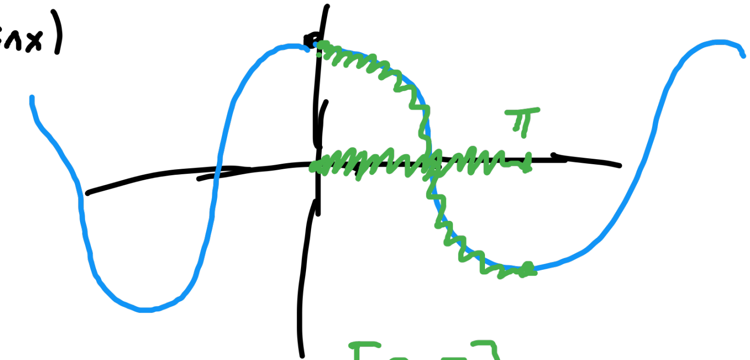
Example

$$\mathbb{R} \xrightarrow{\cos} \mathbb{R}$$

$$x \longmapsto \cos x$$

(cos x, sin x)

Not INJ



$[0,\pi]$

$\cos 0 = \cos 2\pi$

but $0 \neq 2\pi$.

Different fxns b/c different domains

$$[0,\pi] \longrightarrow \mathbb{R}$$

$$x \longmapsto \cos x$$

Is injective.

Pf: The der. of $\cos x$ is $-\sin x$. Since $-\sin x \leq 0$ $\forall x \in [0,\pi]$, $\cos$ is decreasing, and thus injective. $\blacksquare$

$\mathbb{C} \longmapsto \mathbb{C}$

$x \longmapsto x^2$

NI $(i)^2 = (-i)^2$

$-1 = (i)^2$, $(-i)^2 = (-1)^2 i^2 = 1(-1) = -1$

$$P(\mathbb{R}) \longrightarrow P(\mathbb{Z})$$

$$S \longmapsto S \cap \mathbb{Z}$$

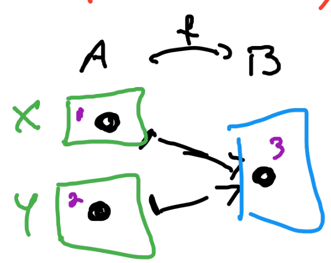
Not I: Are there sets $S_1, S_2 \subseteq \mathbb{R}$ s.t. $S_1 \neq S_2$ but $\boxed{S_1 \cap \mathbb{Z} = S_2 \cap \mathbb{Z}}$?

$\boxed{\{1, \pi\}} \cap \mathbb{Z} = \{1\} = \boxed{\{1, e\}} \cap \mathbb{Z}$

$A \xrightarrow{f} B$

$X, Y \subseteq A$

Recall: "$f(X) \subseteq f(Y) \implies X \subseteq Y$" is false.



"$\subseteq$"
$= f(X) = f(Y)$ but $X \not\subseteq Y$.

Counterexample
"~~Let A = {1}~~ B
let $A = \{1, 2\}$ ...

"Find the "correct" hypothesis"
NOT INJ.

L: Sps f is injective and $f(X) \subseteq f(Y)$. Then $X \subseteq Y$.

THE DEFN OF $f(X)$!

P: Sps f is inj and $f(X) \subseteq f(Y)$. Let $a \in X$. Then $f(a) \in f(X)$.

(To use the hypothesis "$f(X) \subseteq f(Y)$", need an elt of $f(X)$)

Since $f(a) \in f(X)$, and $f(X) \subseteq f(Y)$, $\boxed{f(a)} \in f(Y)$.

$c \in f(Y) \iff$
$\exists b \in Y$ s.t. $c = f(b)$
Apply w/ $c = f(a)$

Thus $\exists c \in Y$ s.t. $f(a) = f(c)$. Since f is injective, $a = c$. Since $c \in Y$, $a \in Y$. ∎

Week 12: Compositions of function

Defn: Let $f : A \to B$ and $g : B \to C$ be fxn.

We define the composition of g and f to be the fxn

$$g \circ f : A \longrightarrow C \quad \text{defined by}$$

(\circ)

$$a \longmapsto (g \circ f)(a) :\stackrel{\text{def}}{=} g(f(a)).$$

$$\in$$

ALT notation $gf = g \circ f$

Any time you do a proof w/ compositions, use the defn

Example:

$f : \mathbb{R} \to \mathbb{R}$ $\quad$ $g : \mathbb{R} \to \mathbb{R}$

$x \mapsto x^2$ $\quad$ $x \mapsto x+1$

$$(g \circ f)(1) = g(f(1)) = g(1) = 2$$

$$(f \circ g)(1) = f(g(1)) = f(2) = 4$$

Note: $g \circ f \neq f \circ g$ i.e., composition is not commutative,

Same domain & codomain $\boxed{\checkmark}$ but

$$(g \circ f)(1) \neq (f \circ g)(1)$$

Sometimes there is a "" formula for $g \circ f$

$$(g \circ f)(x) = g(f(x)) = g(x^2) = (x^2) + 1$$

$$(f \circ g)(x) = f(g(x)) = f(x+1) = (x+1)^2 = x^2 + 2x + 1$$

__Warning__: usually $f \circ g$ and $g \circ f$ don't __both__ make sense.

$f : A \to B$ $\quad$ $g : B \to C$

$g \circ f$ is ok. But

$f \circ g$ is not defined !

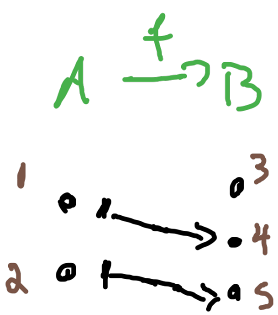
$(f \circ g)(b) = f(g(b))$ __but__

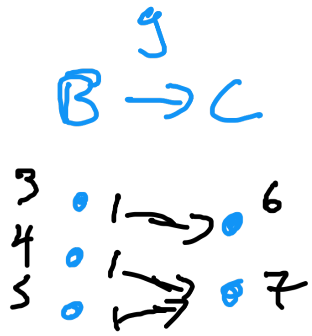
$b \in B \rightsquigarrow g(b) \in C$

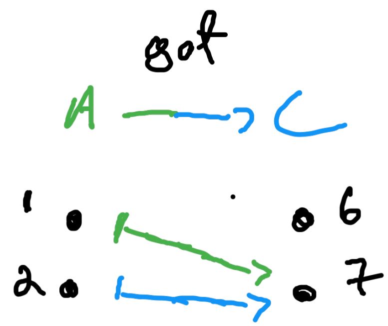
But domain of $f = A$

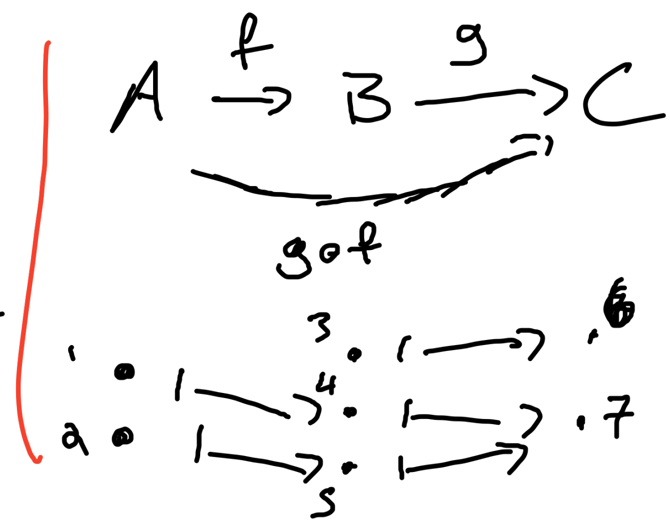
__If:__ $C \subseteq A$ we can fix this.

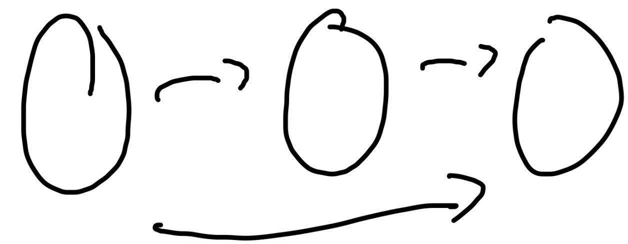
Examples:











$$(g\circ f)(1) = g(f(1)) = g(4) = 7$$

$$(g\circ f)(2) = g(f(2)) = g(5) = 7$$

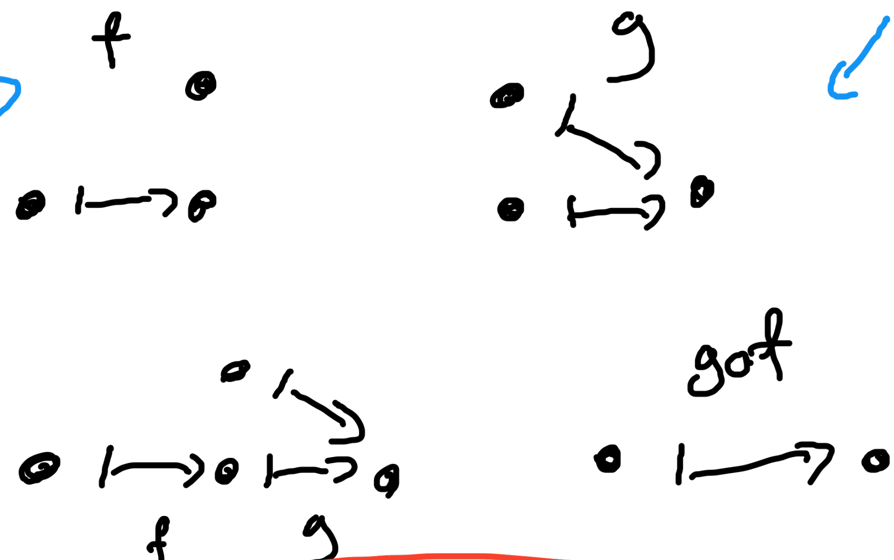
Note: f is inj + g is surj., but $g\circ f$ is neither inj or surj

Eg f inj $\not\Rightarrow$ $g\circ f$ inj

"Simplify" (TEST Functions)

"smallest" inj, not surj fxn

smallest surj, but not inj fxn



USEFUL FOR COUNTEREXAMPLES

(1) Let $f\colon \mathbf{R} \to \mathbf{R}$ be the function $f(x) = \frac{1}{1+x^2}$ and let $g\colon \mathbf{R} \to \mathbf{R}$ be the function $g(x) = e^x$.

(a) What is $(g \circ f)(0)$? $g \circ f(0) = (g \circ f)(0)$

(b) What is $(f \circ g)(0)$?

(c) Give a formula for $f \circ g$ and $g \circ f$.

$$(g \circ f)(0) = g(f(0)) = g(1) = e$$

$$(f \circ g)(0) = f(g(0)) = f(1) = \frac{1}{2}$$

$$(f \circ g)(x) = f(g(x)) = f(e^x) = \frac{1}{1+(e^x)^2} = \frac{1}{1+e^{2x}}$$

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{1}{1+x^2}\right) = e^{\left(\frac{1}{1+x^2}\right)}$$

(2) Let $f\colon \mathbf{R} \to \mathbf{Z}$ be the function $f(x) = \lfloor x \rfloor$ (i.e., round x down to the nearest integer) and let $g\colon \mathbf{Z} \to \mathbf{Z}$ be the function $g(n) =$ 'the number of distinct prime factors of n'. (So $g(0) = g(1) = 0$, $g(4) = 1$, $g(6) = 2$))

(a) What is $g \circ f(\pi)$?
(b) What is $g \circ f(91.1023124)$?
(c) Is $g \circ f$ injective? Surjective?

$f(1.1) = 1$, $f(1.0) = 1$

$f(x) =$ the largest integer y s.t. $y \le x$

$(g \circ f)(\pi) = g(f(\pi)) = g(f(3.14159\ldots)) = g(3) = 1$

$(g \circ f)(91.10\ldots) = g(f(91.\ldots)) = g(91) = 2$

$7 \cdot 13$

$g \circ f$ not surj b/c g is not surj , b/c $g(\cancel{x}) \geq 0$ $\forall x \in \mathbb{Z}$

$g \circ f$ not inj b/c f is not inj

$(g \circ f)(\boxed{1}) = g(f(1)) = g(1) = 0$

$(g \circ f)(\boxed{1.1}) = g(f(1.1)) = g(1) = 0$

(3) Let $f\colon \mathbf{Z} \to P(\mathbf{Z})$ be the function $f(n) = \{n\}$ and let $g\colon P(\mathbf{Z}) \to P(\mathbf{Z})$ be the function $g(S) = S \cap \{1\}$.

(a) What is $g \circ f(0)$?
(b) What is $g \circ f(1)$?
(c) Give a formula for $g \circ f$.

$$(g \circ f)(0) = g(f(0)) = g(\{0\}) = \{0\} \cap \{1\} = \emptyset$$

$$(g \circ f)(1) = g(f(1)) = g(\{1\}) = \{1\} \cap \{1\} = \{1\}$$

$$(g \circ f)(n) = g(f(n)) = g(\{n\}) = \{n\} \cap \{1\}$$

$$= \begin{cases} \{1\} & n = 1 \\ \emptyset & n \neq 1 \end{cases}$$

X, Y Sets

$$\mathrm{Fun}(X,Y) \overset{\text{def}}{:=} \{ f : X \to Y \}$$

$$\begin{array}{ccc}
\mathrm{Fun}(A,B) \times \mathrm{Fun}(B,C) & \xrightarrow{\circ} & \mathrm{Fun}(A,C) \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
(f, g) & \longmapsto & g \circ f
\end{array}$$

$$\begin{array}{ccc}
P(A) \times P(A) & \xrightarrow{\cap} & P(A) \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
(S, T) & \longmapsto & S \cap T
\end{array}$$

$h \circ g \circ f$

Lemma: Composition is associative, I.E.,

let $f: A \to B$, $g: B \to C$, $h: C \to D$ be fxns. Then

Then $h \circ (g \circ f) \overset{(*)}{=} (h \circ g) \circ f$.

Proof: The domain + codomain agree.

(WTS: $\forall a \in A$, $(h \circ (g \circ f))(a) = ((h \circ g) \circ f)(a)$)

Let $a \in A$. Then $(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$.

Also $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

These are equal, so $h \circ (g \circ f) = (h \circ g) \circ f$. ⊠

NOTE: to prove for 4 or more, induct, using $(*)$ as base case

$$f \circ (g \circ (h \circ w)) = (f \circ g) \circ (h \circ w) \ldots$$

use $\bullet \mapsto \bullet \mapsto \bullet$ to check truth

(4) Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Prove or disprove each of the following:

(a) If f and g are injections, then gf is an injection.
(b) If f and g are surjections, then gf is a surjection.
(c) If f and g are bijections, then gf is a bijection.
(d) If gf is an injection, then f and g are injections.
(e) If gf is a surjection, then f and g are surjections.
(f) If gf is a bijection, then f and g are bijections.
(g) If gf is an injection, then f is an injection.
(h) (HW) If gf is an injection, then g is an injection.
(i) (HW) If gf is a surjection, then f is a surjection.
(j) (HW) If gf is a surjection, then g is a surjection.
(k) If gf is a bijection, then f is a bijection.
(l) If gf is a bijection, then g is a bijection.
(m) If gf is an injection and g is a bijection, then f is an injection.

bij = inj AND surj

g inj means

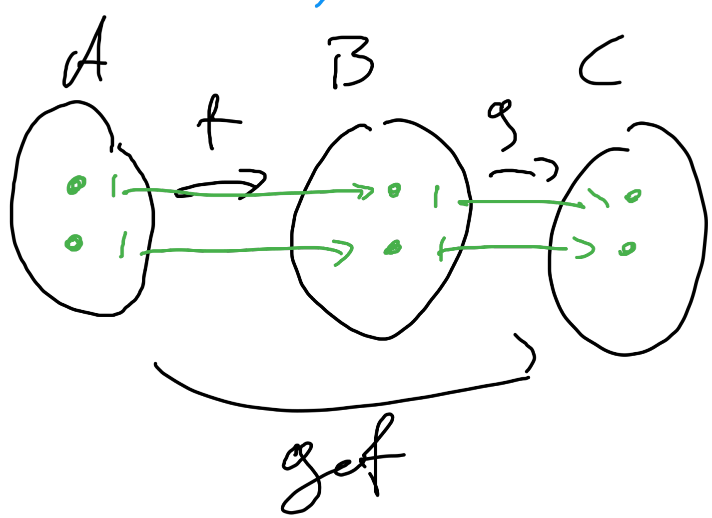
$g(x) = g(y) \implies x = y$

Apply w/ $x = f(a)$
$y = f(b)$

4a, proof: Sps f and g are inj. (WTP: $g \circ f$ is inj, i.e., $\forall a, b \in A$, $(g\circ f)(a) = (g \circ f)(b) \implies a = b$)

Let $a, b \in A$. Assume $(g\circ f)(a) = (g\circ f)(b)$. Then $g(f(a)) = g(f(b))$.

Since g is inj, $f(a) = f(b)$. Since f is inj, $a = b$. ∎



$$\begin{tikzcd} A \arrow[r, "f"'] \arrow[rr, bend left, "g \circ f"] & B \arrow[r, "g"'] & C \end{tikzcd}$$

4h) Sps f and g are surj. (WTS: $g \circ f$ is surj. IE im $g \circ f = C$, IE $(g \circ f)(A) = C$, IE $\underline{\forall x \in C, \exists a \in A \text{ s.t. } (g \circ f)(a) = x}$)

Let $x \in C$. Since g is surj, $\exists b \in B$ s.t. $g(b) = x$. Since f is surj, $\exists a \in A$ s.t. $f(a) = b$. Then $(g \circ f)(a) = g(f(a)) = g(b) = x$. $\boxtimes$

(4) Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Prove or disprove each of the following:

- (a) If f and g are injections, then gf is an injection.
- (b) If f and g are surjections, then gf is a surjection.
- (c) If f and g are bijections, then gf is a bijection.
- (d) If gf is an injection, then f and g are injections.
- (e) If gf is a surjection, then f and g are surjections.
- (f) If gf is a bijection, then f and g are bijections.
- (g) If gf is an injection, then f is an injection.
- (h) (HW) If gf is an injection, then g is an injection.
- (i) (HW) If gf is a surjection, then f is a surjection.
- (j) (HW) If gf is a surjection, then g is a surjection.
- (k) If gf is a bijection, then f is a bijection.
- (l) If gf is a bijection, then g is a bijection.
- (m) If gf is an injection and g is a bijection, then f is an injection.

a and b → c

Counterexample to d f e,

not coex to g

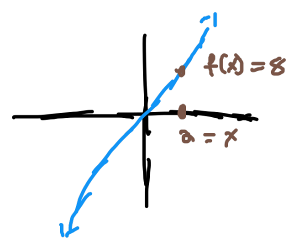
Proof of g: Sps $g \circ f$ is inj. Let $a, b \in A$. Suppose $f(a) = f(b)$. Then $g(f(a)) = g(f(b))$, and since $g \circ f$ is inj, $a = b$. ∎

Week 13: Inverse functions

Idea: f^{-1} "undoes" f

$f(x) = x^3$

$f^{-1}(x) = x^{1/3}$



$f^{-1}(8) = 2$

$f(3) = 27$

$f^{-1}(27) = 3$

$f(x) = x^3 = y$ & solve for x

$x = y^{1/3}$

"Works", but isn't the defn

"the x s.t. $f(x) = 26$" $= f^{-1}(26) = 26^{1/3} = 2.\ldots?$

IE solve the eqn $f(x) = 26$ for x

(*) $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(x^3) = (x^3)^{1/3} = x = id_{\mathbb{R}}(x)$

$f^{-1} \circ f = id_{\mathbb{R}}$

$\mathrm{id}_A : A \to A$ "the" identity fxn

$x \mapsto x$

$\mathrm{id}_A(x) = x, \forall x \in A$

<u>Prop</u>: Let $f : A \to B$ be <u>any</u> fxn. Then

(i) $f \circ \mathrm{id}_A = f$ $\quad A \xrightarrow{\mathrm{id}_A} A \xrightarrow{f} B$

(ii) $\mathrm{id}_B \circ f = f$ $\quad A \xrightarrow{f} B \xrightarrow{\mathrm{id}_B} B$

<u>Proof</u>: (i) $f \circ \mathrm{id}_A$ and f have the same domain & codomain.

Let $a \in A$. Then $(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(a)) = f(a)$. ∎

(ii) is similar.

Defn: We say that a fxn $f: A \to B$ is <u>invertible</u> if $\exists g: B \to A$ s.t.

$$f \circ g = id_B$$
$$g \circ f = id_A.$$

When such a g exists, we call g an <u>inverse</u> of f and sometimes write $g = f^{-1}$.

<u>Warnings</u>: (i) $f^{-1} \neq \frac{1}{f}$ $\boxed{!!!}$

(ii) not every f has an inverse!

$A = B = \mathbb{R}$

$f : A \to A$

$x \mapsto x^3$

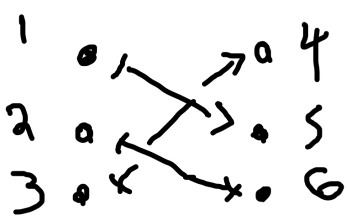
$g : x \mapsto x^{1/3}$

$$(g \circ f)(x) = g(f(x)) = g(x^3) = (x^3)^{1/3} = x = \mathrm{id}_{\mathbb{R}}(x)$$

$$(f \circ g)(x) = f(g(x)) = f(x^{1/3}) = (x^{1/3})^3 = x = \mathrm{id}_{\mathbb{R}}(x)$$

Example:

$A \xrightarrow{f} B$

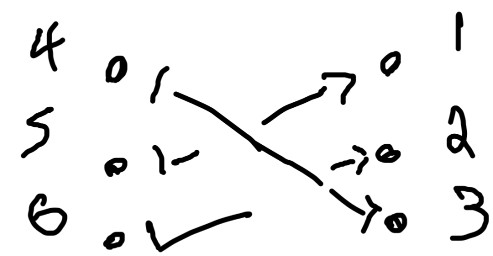


what is the inverse g of f?

$f \circ g = \mathrm{id}_B$

$g \circ f = \mathrm{id}_A$

$B \xrightarrow{g} A$



$$(g \circ f)(1) = g(f(1)) = g(5) = 1$$

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

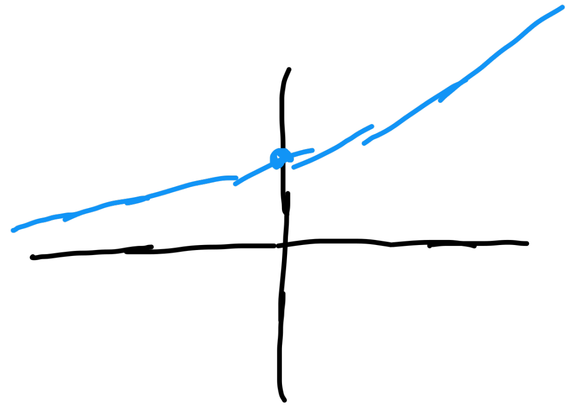
$$\begin{matrix} \| \\ g(y) = z \end{matrix}$$

"$g(x)$ is the solution to $f(z) = x$"

$$\boxed{g(x) = z \iff x = f(z)}$$

__Example:__ $\mathbb{R} \xrightarrow{e} \mathbb{R}_{>0}$

$x \longmapsto e^x$



This has an inverse $\ln$

$\mathbb{R}_{>0} \xrightarrow{\ln} \mathbb{R}$

$x \longmapsto \ln x$

$\ln \circ e = \mathrm{id}_{\mathbb{R}}$

$e \circ \ln = \mathrm{id}_{\mathbb{R}_{>0}}$

$\Longleftrightarrow$

$e^0 = 1$

$\ln 1 =$ "the solution to $e^x = 1$"

$= 0$

$e^\pi = e^\pi \quad \ldots$

$\ln(e^\pi) = \pi$

$\ln(e^x) = x$

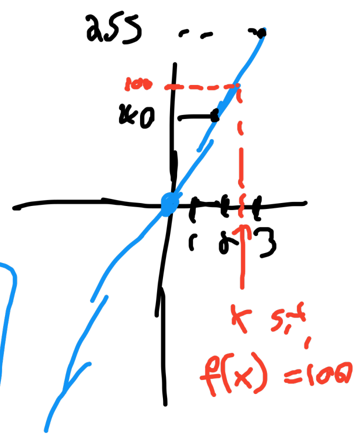
$e^{\ln x} = x$

$e^x = y \iff$

$\ln y = x$

$\mathbb{R} \xrightarrow{f} \mathbb{R}$

$x \longmapsto x^5 + 4x$



$$\boxed{\begin{aligned} f'(x) &= 5x^4 + 4 \\ &\geq 4 \end{aligned}}$$

$\Rightarrow f$ is inj

IVT $\Rightarrow$ surj

HS way

solve $x^5 + 4x = y$ for x

... can't do this nicely

$\boxed{\text{FACT}}$ f has an inverse g.

$f(0) = 0 \qquad g(0) = 0$

$f(1) = 5 \qquad g(5) = 1$

$f(x) = y \iff g(y) = x$

$f(2) = 40 \qquad g(40) = 2$

$f(x) = -5 \iff g(-5) = x$

$\iff$

$x^5 + 4x = -5 \iff x = -1$

Thus $g(-5) = -1$

$g(100) = x \iff f(x) = 100$

$\iff x^5 + 4x = 100$

$\iff x^5 + 4x - 100 = 0$

By IVT, has a sol, b/c

$f(2) = 40$

$f(3) = 3^5 + 4 \cdot 3 = 255$

So $\exists\, x \in [2,3]$ s.t. $f(x) = 100$

$f^{-1}(100) =$ this $x = 2. \ldots$

Sometimes f has no inverse

$$\mathbb{R} \xrightarrow{f} \mathbb{R}$$
$$x \longmapsto x^2$$

1. What is $f^{-1}(-1)$?

   There is no input s.t. $f(x) = -1$

Need surj to have an inverse

Math hack: replace codomain of image.

2. What is $f^{-1}(4)$?

   $f(2) = 4$

   $f(-2) = 4$

   $\boxed{!}$ Problem: is $f^{-1}(4) = 2$ or -2?

need inj to have an inverse

What about $x^{1/2}$?

- not def. for $x < 0$
- ambiguous (+ & − root)

THM: $f: A \to B$ has an inverse $\iff$ f is bijective.

Proof: "$\Rightarrow$" Assume f has an inverse g.

(Inj, WTS $\forall a, b \in A$, $f(a) = f(b) \Rightarrow a = b$)

Let $a, b \in A$. Suppose $f(a) = f(b)$. Then, $g(f(a)) = g(f(b))$.

Since $g = f^{-1}$, $g \circ f = id$, so $a = b$. ($(g \circ f)(a) = g(f(a)) = id(a) = a$)

(S, WTS $\forall b \in B$, $\exists a \in A$ s.t. $f(a) = b$)

Let $b \in B$. Let $a = g(b)$. Then $f(a) = f(g(b)) = (f \circ g)(b) = id_B(b) = b$.

"$\Leftarrow$" Assume f is bijection. Let's define $g: B \to A$ as follows.

Let $b \in B$. Since f is surj, $\exists a \in A$ s.t. $f(a) = b$. Since f is inj, there is only one such a. Define $g(b) = a$. Then

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

$(f \circ g)(b) = f(g(b)) = b$.

(1) USE THM → to help w/ proofs

→ to help w/ counterexamples

(2) Given f, to find f^{-1}, "solve" the eqns

$$f \circ g = \mathrm{id}_B \qquad \text{for } g$$
$$g \circ f = \mathrm{id}_A$$

(2') If you have a guess for g, verify your guess by plugging g into

(i) x^2 not inj $\Rightarrow$ not invertible

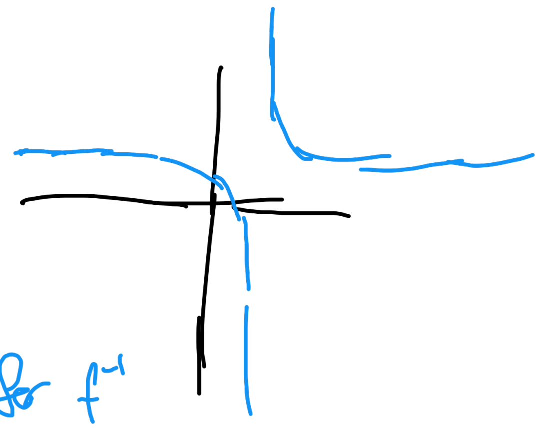
(ii) $f(x) = x^5 + x^3 + x$ is inv. by Thm

b/c bij.

(Still need to explain why f is bij)

$\underline{\text{Ex:}}$ $\mathbb{R}-\{1\} \xrightarrow{f} \mathbb{R}-\{1\}$

$$x \longmapsto \frac{x+1}{x-1}$$



How to find a formula for f^{-1}

$$f(x) = y \iff x = g(y)$$

"$g(y)$ is the x s.t. $f(x)=y$"

$$\frac{x+1}{x-1} = y \qquad \frac{2}{x-1} = y-1 \Rightarrow \frac{x-1}{2} = \frac{1}{y-1}$$

$$\frac{x+1}{x-1} = \frac{x-1+2}{x-1} = 1+\frac{2}{x-1} = y$$

$$\Rightarrow x-1 = \frac{2}{y-1}$$

$$\Rightarrow x = \boxed{1+\frac{2}{y-1}} = g(y)$$

$\underline{\text{IE}}$ $(f\circ g)(x) \overset{?}{=} x$

$$(f\circ g)(x) = f\left(1+\frac{2}{x-1}\right) = \frac{\left(1+\frac{2}{x-1}\right)+1}{\left(1+\frac{2}{x-1}\right)-1} = x$$

MAW

Example:

$$\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^2$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x-y \\ x+y \end{pmatrix}$$

$$\mathbb{R}^2 \xrightarrow{g} \mathbb{R}^2$$

$$\begin{pmatrix} s \\ t \end{pmatrix} \longmapsto \begin{pmatrix} \frac{s+t}{2} \\ \frac{-s+t}{2} \end{pmatrix}$$

$$(g \circ f)\begin{pmatrix} x \\ y \end{pmatrix} = g\left(f\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

$$= g\begin{pmatrix} x-y \\ x+y \end{pmatrix}$$

$$= \begin{pmatrix} \frac{(x-y)+(x+y)}{2} \\ \frac{-(x-y)+(x+y)}{2} \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

$f \circ g$ vs id

Week 14: Relations (4.2)

Informally: a "relation" is a way to compare "things"

Example: $S = \mathbb{R}$, $\geq$ is a relation

I.E., $\forall\, a,b \in S$, "$a \geq b$" is either true or false

Defn: Let S be a set. A relation on S is a subset $R \subseteq S \times S$.

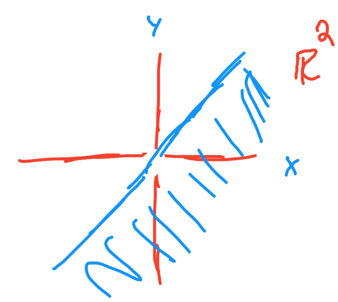
If $(a,b) \in R$, we say that "a is related to b" and write $\boxed{a \sim b}$ (or $a \underset{R}{\sim} b$).

usually use $\sim$

Example: $S = \mathbb{R}$

$R \subseteq \mathbb{R} \times \mathbb{R}$ given by

$$R \overset{\text{def}}{=} \{(a,b) \in \mathbb{R}\times\mathbb{R} \text{ s.t. } a \geq b\}$$



Example: $S = \{0,1,2\}$

$R \subseteq S \times S$

$$R \overset{\text{def}}{=} \{(0,1), (0,2), (1,2)\}$$

$0 \sim 1$ true b/c $(0,1) \in R$

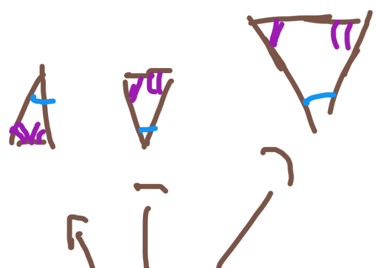
$1 \sim 2$ true

$2 \sim 0$ false b/c $(2,0) \notin R$

"Equivalence" Relations

Axiomatize the notion of "the same" or "more or less the same"

there are many properties of Δ's which don't depend on size or orientation.



basically the same

not literally the same

Examples ①

$$\frac{2}{3} = \frac{4}{6}$$

Defn: Let S be a set. Let R be a relation on S.
We say that R is an equivalence relation if

(R) $\forall a \in S, a \sim a$ · Reflexive

(S) $\forall a,b \in S, a \sim b \Rightarrow b \sim a$ · Symmetric

(T) $\forall a,b,c \in S, a \sim b \wedge b \sim c \implies a \sim c$ · transitive

Let $a \in S$. We define the equivalence class of a to be

$$[a] \stackrel{\text{def}}{=} \{b \in S \text{ s.t. } b \sim a\}$$

Warning: not interval notation.

NOTE: if $b \in [a]$ then $[b] = [a]$

set sets

$a \in [a]$ b/c $a \sim a$

New notation $[a]$ vs $\{a\}$

more elts

the set whose only elt is a

Examples: $S = \mathbb{Z}$, $a \sim b$ if $2 \mid a-b$

$2 \sim 4$ b/c $2-4=-2$ and $2 \mid -2$

$1 \sim 3$ $\quad 1-3=-2$

$1 \not\sim 2$ $\quad 1-2=-1$ $\quad 2 \nmid -1$

$(2,4) \in R$

$(2,3) \notin R$

(i.e., $a \sim b$ if a and b have the same remainder when you divide by 2

IE, $a \sim b$ if they have the same parity)

Claim: this is an equiv. relation.

Pf: (R) Let $a \in \mathbb{Z}$. (WTP: $a \sim a$, i.e., $2 \mid a-a$)

Since $a-a=0$, $2 \mid a-a$, so $a \sim a$.

(S) Let $a,b \in \mathbb{Z}$. Suppose $a \sim b$. Then $2 \mid a-b$.

(WTP: $b \sim a$, i.e., $2 \mid b-a$). Since $b-a = -(a-b)$,

$2 \mid b-a$, so $b \sim a$.

(T) Let $a,b,c \in \mathbb{Z}$. Suppose $a \sim b$ and $b \sim c$. Then $\underline{2 \mid a-b}$ and $\underline{2 \mid b-c}$.

(WTS: $a \sim c$, i.e., $\underline{2 \mid a-c}$) then $2 \mid (a-b)+(b-c)$, so $2 \mid a-c$. Thus $a \sim c$. ∎

Q: What are the equiv. classes?

$[0] = \{a \in \mathbb{Z} \text{ s.t. } a \sim 0\}$ $\qquad a \sim 0 \iff 2 \mid a-0$

$= \{a \in \mathbb{Z} \text{ s.t. } 2 \mid a\}$ $\qquad \iff 2 \mid a$

$= 2\mathbb{Z} = \mathbb{E}$

$[1] = \{a \in \mathbb{Z} \text{ s.t. } a \sim 1\}$ $\qquad a \sim 1 \iff 2 \mid a-1$

$= \{a \in \mathbb{Z} \text{ s.t. } a \text{ is odd}\}$ $\qquad \iff a-1$ is even

$= 2\mathbb{Z}+1$ or $\mathbb{O}$ $\qquad \iff a$ is odd

NOTE: $[0] \cup [1] = \mathbb{Z}$ AND $[0] \cap [1] = \emptyset$ "partition"

$[2] = \{a \in \mathbb{Z} \text{ s.t. } a \sim 2\}$ $\qquad a \sim 2 \iff 2 \mid a-2$

$= \mathbb{E}$ $\qquad \iff 2 \mid a$.

$[0] = [2]$

$[0] \neq [1]$

$0 \in [0]$ but $0 \notin [1]$

$S = \mathbb{R}$ $\quad x \sim y$ if $x < y$

NOT AN E.R. b/c

Not (R) or (S). (IS (T))

<u>Pf</u>: Let $a = 0$. Then $0 < 0$ is false, so $0 \not\sim 0$.

Thus $<$ is not reflexive.

Let $a = 0$ and $b = 1$. Then $0 < 1$, so $0 \sim 1$, but $1 \not< 0$, so $1 \not\sim 0$.

(T) $a < b \wedge b < c \Rightarrow a < c$.

$S = \mathbb{R}$, $x, y \in \mathbb{R}$, $x \sim y$ if $x - y \in \mathbb{Q}$

$\pi \sim \pi + 1$ $\quad \pi - (\pi + 1) = -1 \in \mathbb{Q}$

$0 \not\sim \sqrt{2}$ b/c $\sqrt{2} - 0 = \sqrt{2} \notin \mathbb{Q}$

Claim: this is an E.R.

<u>Pf:</u> (R) Let $a \in \mathbb{R}$. Then $a - a = 0 \in \mathbb{Q}$. Thus $a \sim a$.

(S) Let $a, b \in \mathbb{R}$. Suppose $a \sim b$, i.e., $a - b \in \mathbb{Q}$.
Then $b - a \in \mathbb{Q}$, so $b \sim a$.

(T) Let $a, b, c \in \mathbb{R}$. Suppose $a \sim b$ and $b \sim c$, i.e., $a - b \in \mathbb{Q}$ and $b - c \in \mathbb{Q}$.
Adding gives $a - c = (a - b) + (b - c) \in \mathbb{Q}$, thus $a \sim c$. $\blacksquare$

A, B sets. Define $A \sim B$ if $\exists$ a bijection $f: A \to B$.

THM f is bij $\iff$ f has an inverse

$\{1\} \sim \{2\}$ via $f(1) = 2$

$\{1\} \not\sim \{1, 2\}$

<u>Claim</u>: this is an E.R.

<u>Pf</u>: (R) Let A be a set. (WTP: $A \sim A$, i.e., $\exists$ a bijection $A \xrightarrow{f} A$)

Then $f = id_A$ is a bijection from A to A, because the inverse of id_A is id_A, i.e., $id_A \circ id_A = id_A$.

(S) Let A, B be sets. Suppose $\exists$ a bijection $f: A \to B$.

By the THM, $\exists g: B \to A$ s.t. $g = f^{-1}$. Since g is invertible, g is a bijection.

(T) Let A, B, C be sets. Suppose $\exists f: A \to B$ and $g: B \to C$ s.t. f and g are bijective. Then $g \circ f: A \to B$ is bijective (b/c we proved in L 1d).

Thus $A \sim C$. $\boxtimes$

A, B sets, $A \sim B$ if

$\exists f : A \to B$ s.t.

f is surj.

$\sim$ is (R) & (T) (same pf)

But: not (S).

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

There are 2 fxns from $A \to B$

$f(1) = 2$

$g(1) = 3$

Neither is a surjection. $\blacksquare$

$\exists$ surj $B \to A$

$\nexists$ surj $A \to B$

$S = \mathbb{R}$ $x \sim y$ if $x = 1$ or $y = 1$

$1 \sim 1$ $2 \not\sim 2$

$1 \sim 2$ $2 \not\sim 3$

$2 \sim 1$.

TRUE

NOT (R) b/c $2 \not\sim 2$

(S) is true.

Pf: Let $a, b \in \mathbb{R}$. Sps $a \sim b$, i.e., $a = 1$ or $b = 1$.

(WTK: $b \sim a$, i.e., $b = 1$ or $a = 1$) Since "or" is commutative

$b = 1$ or $a = 1$. Thus $b \sim a$.

(T) let $a = 2$, $b = 1$, $c = 3$

then $a \sim b \wedge b \sim c$, but $a \not\sim c$

ER $\iff$ $R \wedge S \wedge T$

$\neg$ ER $\iff$ $\neg R \vee \neg S \wedge \neg T$