More Contradiction; some Induction

WTP P

Assume $\neg P$

Argue

Conclude Q

Observe Q is false

Conclude P

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

$P \Rightarrow Q$

$\neg Q \Rightarrow \neg P$

$\cancel{\neg P \Rightarrow \neg Q}$

Let $n \in \mathbb{Z}$.

Prove that n and $n+1$ have no common prime factors.

Assume n and $n+1$ have a common prime factor p. Then $p \mid n$ and $p \mid n+1$. $\Rightarrow p \mid (n+1)-n \Rightarrow p \mid 1$

By the 2 out of 3 rule, $p \mid 1$.

But the smallest prime is $p = 2$, so this is a contradiction.

$\boxtimes$

(10) Let a, b, c be integers satisfying $a^2 + b^2 = c^2$. Show that abc must be even. (Harder problem: show that a or b must be even.)

Proceed by contradiction. Assume a, b, and c are all odd, then a^2, b^2 & c^2 are odd. But since $a^2 + b^2 = c^2$, the LHS is even, and the RHS is odd. This is a contradiction. $\blacksquare$

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

(9) Prove that if $r^3 + r + 1 = 0$ then r is irrational.

Proceed by contradiction.

Assume $r^3 + r + 1 = 0$ and $r \in \mathbb{Q}$.

Since $r \in \mathbb{Q}$, $\exists\, a, b \in \mathbb{Z}$ s.t. $b \neq 0$ and $r = a/b$. Moreover, WMA (we may assume) that a and b are "reduced", i.e., they have no common factors. (In particular, at least one of a or b is odd.) Thus, $\left(\frac{a}{b}\right)^3 + \frac{a}{b} + 1 = 0$.

Clearing denominators

$$a^3 + ab^2 + b^3 \overset{(*)}{=} 0$$

Case 1: a is even. Then b is odd. Then the LHS of $(*)$ is odd, but 0 is even. This is a contradiction.

Case 2: b is even. This is the same as case 1.

Case 3: a and b are both odd. But then the LHS of $(*)$ is odd, but the RHS is even, a contradiction.

We conclude that $r \notin \mathbb{Q}$. $\blacksquare$

$$\neg P \Rightarrow (Q_1 \vee Q_2 \vee Q_3)$$

$$\neg(Q_1 \vee Q_2 \vee Q_3) = \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3$$

$a^{\log_a b} = b$

$\log_a x = b \iff x = a^b$ $\qquad \log_a(a^b) = b$

$\log_{10} 100 = 2$

$\log_a x$ and a^x are inverse

(13) Prove that $\log_{10} 7$ is irrational.

Proceed by contradiction. Assume that $\log_{10} 7 \in \mathbb{Q}$. Thus, $\exists\, a, b \in \mathbb{Z}$ s.t. $b \neq 0$ and $\log_{10} 7 \overset{(*)}{=} a/b$. WMA a & b have no common prime factors. Moreover, at least one of a or b is not negative.

Applying 10^x to equation $(*)$ gives

$7 = 10^{\log_{10} 7} = 10^{a/b}$. Thus $7^b \overset{(*)}{=} 10^a$.

① If a or b is negative, we get that an integer is equal to a non integer, $\lightning$

② If a and b are both not negative, then, since $b > 0$, the LHS of $(*)$ is a multiple by 7, but the RHS is not a multiple of 7, $\lightning$.

We conclude that $\log_{10} 7 \notin \mathbb{Q}$. $\blacksquare$

Induction $\forall n \in \mathbb{Z}_{>0}$

$P(n)$ $\quad 1+2+3+\dots+n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$

Base case

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

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

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

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

Proof that $P(n-1) \implies P(n)$

Proof: Suppose we already knew that (Assum $P(n-1)$)

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

Adding n to both sides gives (Proof)

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

The RHS of this is

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

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

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

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

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

Define a sequence $a_1, a_2, a_3, \ldots$ as

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

"recursive definition"

$$a_2 = 2 \cdot a_1 = 2 \cdot 2 = 4 = 2^2$$
$$a_3 = 2 \cdot a_2 = 2 \cdot 4 = 8 = 2^3$$
$$a_4 = 2 \cdot a_3 = 2 \cdot 8 = 16 = 2^4$$
$$\vdots$$

Claim: $\forall n \in \mathbb{Z}_{>0},\ a_n = 2^n$

Idea: $2^{n-1} \cdot 2 = 2^n$

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

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

BASE CASE

$P(1) =$ " $a_1 = 2^1$ " true by definition

Assume that $P(n)$ is true, i.e., assume that $a_n = 2^n$. Then $a_{n+1} = 2 \cdot a_n$.

By our hypothesis, $a_{n+1} = 2 \cdot a_n = 2 \cdot 2^n = 2^{n+1}$.

Thus $P(n+1)$ is <u>also</u> true

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

We conclude that $\forall n > 0,\ P(n)$.

$\boxed{\text{Induction}}$ 4

Let $P(n)$ be a statement which depends on an integer n

$\boxed{\text{Ex}}$ $P(n) =$ "$a_n = 2^n$" or

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

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

Step 1: Prove $P(1)$ "Base case"

Step 2: Prove "$P(n-1) \Rightarrow P(n)$" "Inductive step"

"Induction" $=$ $P(1)$ and "$P(n-1) \Rightarrow P(n)$" $\Rightarrow$ $\forall n \in \mathbb{Z}_{>0}, P(n)$

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

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

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

WTP $\forall n \in \mathbb{Z}_{>1}, P(n)$

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

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

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

3. We want to prove, by induction, that, for every positive integer n,

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

a) What is the open statement "$P(n)$"?

P(n) =

b) What is the statement "$P(1)$"? Why is $P(1)$ true?

P(1) =

c) What is the inductive step? Write out your assumption, your desired conclusion, and the inductive step (i.e., the proof that $P(n-1) \Rightarrow P(n)$).

Assume that

We want to show that

(Inductive step)

Week 5: More induction

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

Base Case: Prove $P(1)$

Inductive Step: Prove $P(n) \Rightarrow P(n+1)$

ok To prove $P(a) \Rightarrow P(a+1)$

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

$P(n)$ = " $2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$ "

Want: $\forall n \in \mathbb{Z}_{\geq 0}$, $P(n)$

<u>Proof:</u> Proceed by induction. The base case $P(1)$ is " $2^0 = 2^1 - 1$ ", i.e., $1 = 1$ which is true.

Assume $P(n)$ is true. I.e.,

$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

(WTS: $P(n+1)$, i.e., $2^0 + 2^1 + \cdots + 2^{(n+1)-1} = 2^{n+1} - 1$)

Then, adding 2^n to each side gives

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^{n-1} + 2^n &= 2^n - 1 + 2^n \\ &= 2(2^n) - 1 \\ &= 2^{n+1} - 1. \end{aligned}$$

$\boxed{\text{Ivy}}$

$$\underbrace{\text{Let's try } P(n-1) \Rightarrow P(n).}$$

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^{(n-1)-1} + 2^{n-1} &= 2^{(n-1)} - 1 + 2^{n-1} \\ &= 2(2^{n-1}) - 1 \\ &= 2^n - 1 \end{aligned}$$

Define:

$a_0 = 0$

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

$a_1 = \sqrt{3+2a_0} = \sqrt{3+0} = \sqrt{3}$

$a_2 = \sqrt{3+2a_1} = \sqrt{3+2\sqrt{3}}$

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

$\vdots$

Claim: $\forall n \in \mathbb{Z}_{\geq 0}$,

$a_n < 3$.

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

Proof: Base case: $P(0)$ is the statement "$a_0 < 3$", i.e., "$0 < 3$", which is true.

Suppose that $P(n-1)$ is true. I.e., $a_{n-1} < 3$.

Then by definition, $a_n = \sqrt{3+2a_{n-1}}$.

Combining these gives

$$a_n = \sqrt{3+2a_{n-1}} < \sqrt{3+2\cdot 3} = \sqrt{3+2\cdot 3} = \sqrt{9} = 3. \quad \blacksquare$$

Scratch $\quad a_{n-1} < 3$

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

$< \sqrt{3+2(3)}$

$= \sqrt{3+6} = \sqrt{9} = 3$

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

Example: we know that if a, b are odd, then ab is odd.

$$\left(a = 2k+1,\ b = 2m+1,\ ab = (2k+1)(2m+1) = 4km + 2(k+m) + 1 = 2(2km + k + m) + 1 \right)$$

Lemma: Let $a_1, \ldots, a_n$ be odd integers. Then $a_1 a_2 \cdots a_n$ is odd.

Notes: $P(1)$ is just "if a_1 is odd, then a_1 is odd". $P \Rightarrow P$

$P(2)$ is true.

needed 2 base cases

Proof. We already know $P(1)$ and $P(2)$.

Assume $P(n-1)$ is true. Let $a_1, \ldots, a_n$ be odd integers.

$$\left(a_1 a_2 \cdots a_n = \underbrace{(a_1 a_2 \cdots a_{n-1})}_{\text{by } P(n-1), \text{ is odd}} \cdot a_n \right)$$

by $P(2)$ this is odd.

By induction (i.e., by $P(n-1)$), $a_1 \cdots a_{n-1}$ is odd.

By $P(2)$ (applied to $b_1 = (a_1 \cdots a_{n-1})$ and $b_2 = a_n$)

$(a_1 \cdots a_{n-1}) a_n$ is odd. ☒

Other examples

$a + b = b + a$ can rearrange as I wish

$$a_1 + a_2 + \cdots + a_n = (a_1 + \cdots + a_{n-1}) + a_n$$

$$(ab)(c) = a(bc)$$

$$a_1(a_2 \cdots a_n) = (a_1 a_2)(a_3 \cdots a_n)$$

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

$$f_1 \circ (f_2 \circ \cdots \circ f_n)$$

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

$$3^a = (2k+1)^a = \cdots$$

binomial expansion

$p(n) =$

Prove: $\forall n \in \mathbb{Z}_{\geq 0},\ 3 \mid 4^n - 1$.

Base Case: $P(0)$, i.e., $3 \mid 4^0 - 1$, i.e., $3 \mid 0$.

This is true. $(0 = 3x$, yeah, $x = 0)$

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

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

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

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

$$= (3m)4 + 4 - 1$$
$$= 3m4 + 3.$$

This is divisible by 3 by 2 out of 3 rule. ∎

$$\underbrace{(4^n - 1)4}_{3 \mid} = \underbrace{4^{n+1} - 4}_{3 \mid} = (4^{n+1} - 1) - \underbrace{3}_{3 \mid}$$

Apply 2 out of 3 rule.

Fibonacci #'s

$F_0 = 0$

$F_1 = 1$

$F_2 = 1$

$F_3 = 2$

$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$

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

the defn

Lucas #'s

$L_1 = 2, \; L_2 = 1$

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

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

Confusing Points:

$F_{a+2} = F_{a+1} + F_a \quad (\forall a)$

$F_{n+1} = F_n + F_{n-1} \quad (a = n-1) \quad (n-1)+2 = n+1$

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

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

Prove: $\forall n \in \mathbb{Z}_{>0}$, $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

Proof: Base case: $P(1)$ is "$F_1 = F_2$", i.e., "$1 = 1$", which is true.

($n=2$: $F_1 + F_3 = F_4$, i.e., $1 + 2 = 3$)

Assume $P(n)$ is true, i.e.,

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}.$$

(WTP $P(n+1)$, i.e., $F_1 + \cdots + F_{2(n+1)-1} = F_{2(n+1)}$

$2(n+1) - 1 = 2n+1$ $\qquad$ $2n+2$)

Then, adding F_{2n+1} to both sides gives

$$F_1 + F_3 + \cdots + F_{2n-1} + F_{2n+1} \overset{(*)}{=} F_{2n} + F_{2n+1}.$$

Since, by definition, $F_{2n+2} = F_{2n+1} + F_{2n}$, the RHS of $(*)$ is the RHS of $P(n+1)$. ∎

<u>Prove:</u> $\forall n \in \mathbb{Z}_{>0}$, $F_n < 2^n$.

Base cases:

$P(1) =$ "$F_1 < 2$", i.e., $1 < 2$, true

$P(2) =$ "$F_2 < 2^2$", i.e., $1 < 4$. True.

~~Inductive step: assume~~

$$\left(F_n = F_{n-1} + F_{n-2} < 2^{n-1} + 2^{n-2} < 2^{n-1} + 2^{n-1} = 2(2^{n-1}) > 2^n \right)$$

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

$\wedge$ = and

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

$$F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^{n+1} \qquad P(n)$$

$$P(0) = \text{"} F_0 F_2 = F_1^2 + (-1)^1 \text{"}$$

$$\text{"} 0 \cdot 1 = 1^2 + (-1)^1 = 0 \text{"}$$

$$P(1) = \text{"} F_1 F_3 = F_2^2 + (-1)^2 \text{"}$$

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

Assume $P(n)$ is true, i.e.,

$$F_{n-1} F_{n+1} = F_n^2 + (-1)^{n+1}$$

(WTP $P(n+1)$, i.e.,

$$F_n F_{n+2} = F_{n+1}^2 + (-1)^{n+2} \text{)}$$

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

$$(F_{n+1} - F_n) F_{n+1} = F_n^2 + (-1)^{n+1}$$

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

$$\Rightarrow$$

$$F_{n+1}^2 - (-1)^{n+1} = F_n^2 + F_n F_{n+1}$$

$$F_{n+1}^2 + (-1)^{n+2} = F_n (F_n + F_{n+1}) = F_n F_{n+2} \quad \square$$

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 $g \in \mathrm{Fun}(\mathbb{R},\mathbb{R})$

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

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

" $:=$ " means "definition"

$$\mathbb{Q}[x] := \{a_0 + a_1 x + \cdots + a_n x^n : n \in \mathbb{Z}_{\geq 0} \text{ and each } a_i \in \mathbb{Q}\}$$

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

$\boxed{!}$ 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 $\emptyset$ is the set with the property that $\forall x.\ x \notin \emptyset$. (I.E., $x \in \emptyset$ 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. $x \notin T$

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

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

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

$\underset{3}{\ni}$ $\quad$ $\underset{3}{\not\ni}$

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

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

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

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

<u>Prove or disprove</u>:

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

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

<u>Proof</u>: (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 $6|x$.

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

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

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

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

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

Claim: $A \subseteq B$.

Proof; 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" $\blacksquare$

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. $\blacksquare$

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. $\blacksquare$

Week 7: More proofs w/ sets

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

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

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

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

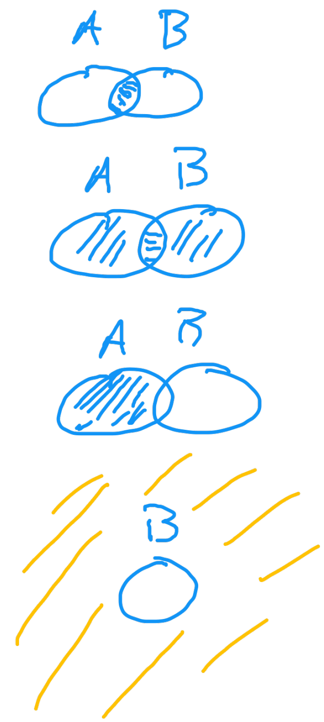
$A - B = \{x \in A \mid x \notin B\}$

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

$=$

$U - B$

$U =$ "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. $x \notin A-B$]

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

$\quad P \Rightarrow Q$

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 $x \notin B$).

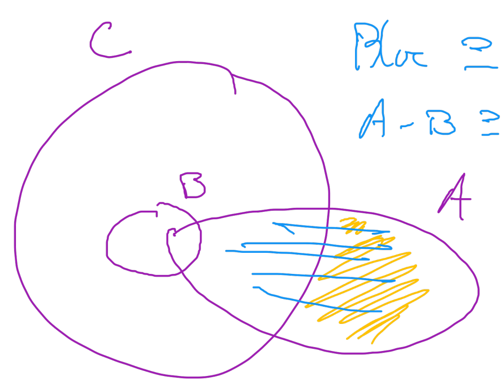
Proceed by contradiction. Assume $x \in B$. Since $B \subseteq C$, $x \in C$. This contradicts $x \notin C$. Thus $x \notin B$. Thus $x \in A-B$. ☺

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

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



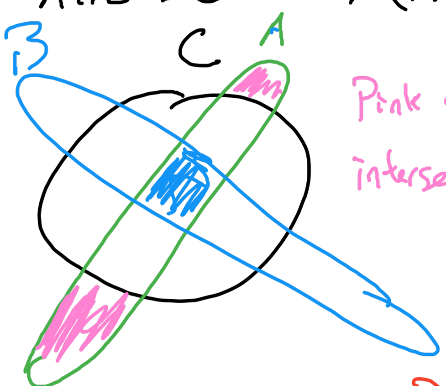
Blue ⊇ Yellow

$A-B \supseteq A-C$

$P \Rightarrow Q$

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: $\boxed{\text{Let } \cancel{x \in A \cap B}}$

Don't do this.

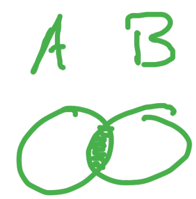
Suppose $A \cap B \subseteq C$. Proceed by contradiction. Assume $(A-C) \cap B \neq \emptyset$. Thus $\exists x \in (A-C) \cap B$. Then $x \in A - C$ and $x \in B$. Then $x \in A$ and $x \notin C$. Thus $x \in A \cap B$, so since $A \cap B \subseteq C$, $x \in C$. This is a contradiction, thus $A - C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

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

<u>Defn</u>: let A and B be sets. The <u>Cartesian Product</u> $A \times B$ 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 differentï

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

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

$$A \times B = \left\{ \begin{matrix} (1,3), (1,4) \\ (2,3), (2,4) \end{matrix} \right\}$$

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. $\mathbb{R} \times \operatorname{Fun}(\mathbb{R}, \mathbb{R}) \ni (\pi, f)$

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

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

"$\ni$" = "s.t."

$A \subseteq B$ $\quad$ $A \supseteq B$

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 $\phi \subseteq A$

$A \subseteq A$

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

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

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

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

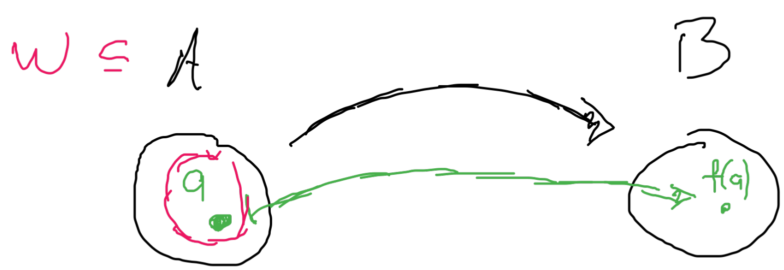
Week 9: functions, images, & surjectivity

Let A, B be sets.

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

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

Can't graph . . .



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

"not multivalued"

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

Examples

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

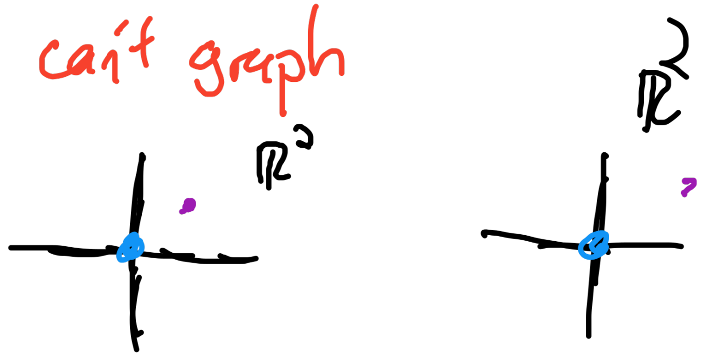
$(x, y) \longmapsto (x+y, xy)$

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

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

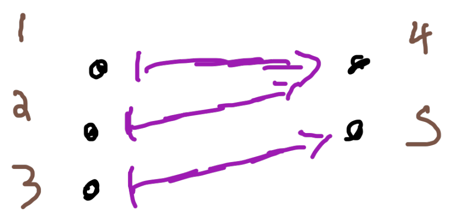
$f(1,1) = (2,1)$

can't graph

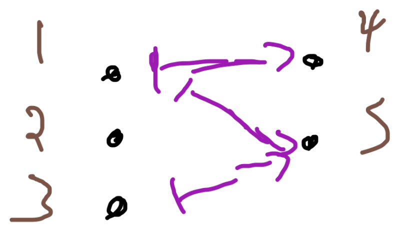


Let go of the formulas

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



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

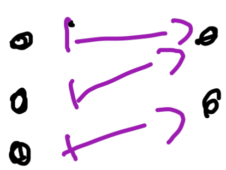


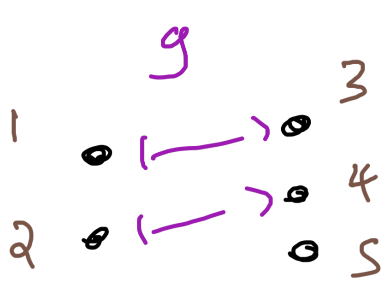
2 problems

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 = inputs

codomain: potential outputs

range = image: Actual outputs

$A = \{ x \mid x \text{ is a student in math 3SC} \}$

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

$$A \xrightarrow{f} B$$

$f(x) =$ 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 $\mathbb{Q}$

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

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

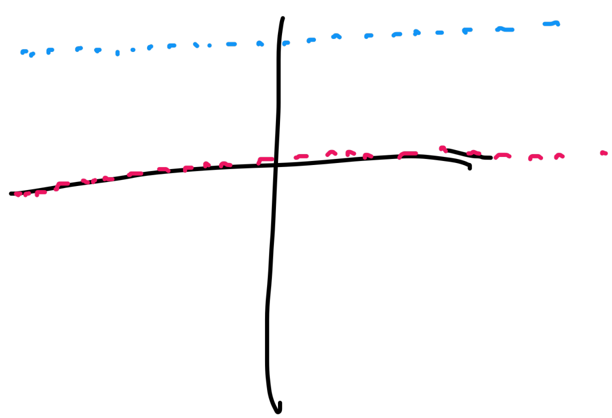
Unambiguous.

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

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

$g(\tan 1) = \, ?$

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



What does it mean for $f = g$?

$f : A \to B$,
$g : C \to D$

Defn: We say that $f = g$ if
$A = C$, $B = D$, and $\forall a \in A$, $f(a) = g(a)$.

To show $f \neq g$, show $A \neq C$, $B \neq D$, or
$\exists a \in A$ s.t. $f(a) \neq g(a)$.

consistent

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

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

unambiguous

Examples:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ x & \longmapsto & 2x \end{array}$$

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

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{g} & \mathbb{Z} \\ x & \longmapsto & 2x \end{array}$$

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

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{h} & \mathbb{E} \\ x & \longmapsto & 2x \end{array}$$

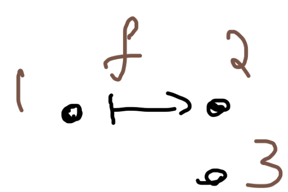
$h \neq g$

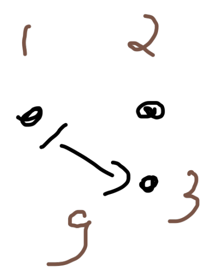
b/c different codomains.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{h_2} & \mathbb{E} \\ n & \longmapsto & 2n \end{array}$$

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

$h = h_2$





$f \neq g$

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

$f(n) = n+1$

$f(n) = 2n$

invalid

$S \mapsto S \cup 1$

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

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

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

$S \xmapsto{f} S \cup \{1\} = f(S)$

$S \xmapsto{g} S \cap \mathbb{E}$

$S \xmapsto{h} S \cup \{\pi\}$

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

h is invalid

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

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

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

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

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

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

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

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

$x \longmapsto \{x\}$

$y \longmapsto y+1$ invalid

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

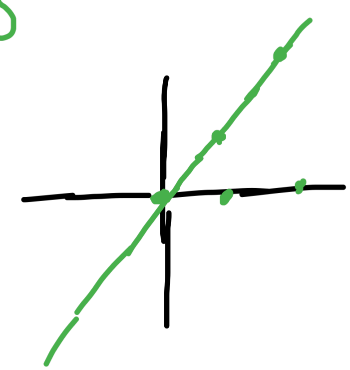
Common functions

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

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

$id_A(x) = x$

$id(x) = x$



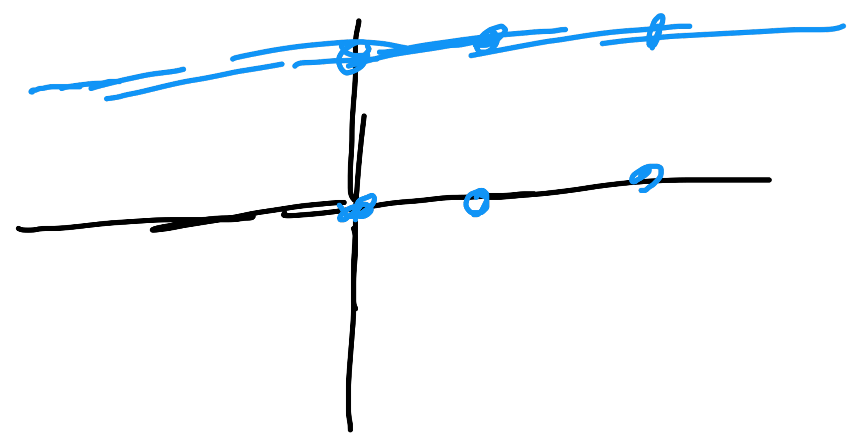
Sps $B \neq \emptyset$ and let $b \in B$.

$A \xrightarrow{c_b} B$

$a \longmapsto b$

$c_b(a) = b$

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



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

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

We say that f is **surjective** (onto) if

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

(IE, "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 $B \subseteq f(A)$.

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

$1 \mapsto 4$
$2 \mapsto 4$
$3 \mapsto 5$

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

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

$A \xrightarrow{f} B$

$1 \mapsto 2$
3

not surj

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

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

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

To prove $f(A) = B$, need to show $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$

To prove $f(A) \neq B$, need to show $\exists b \in B$ s.t. $\forall a \in A$, $f(a) \neq b$

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

$x \longmapsto x^2$

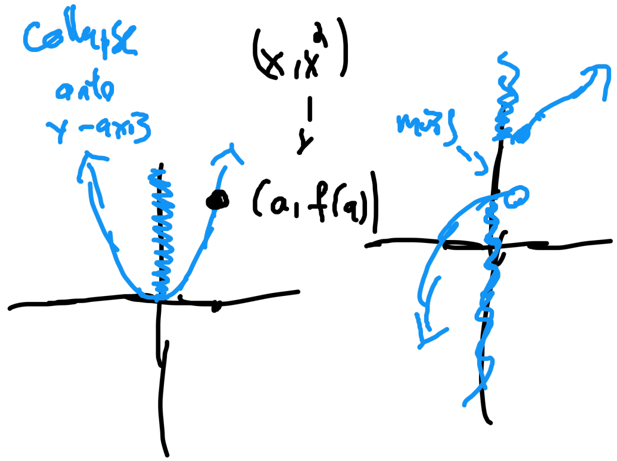
not surj b/c

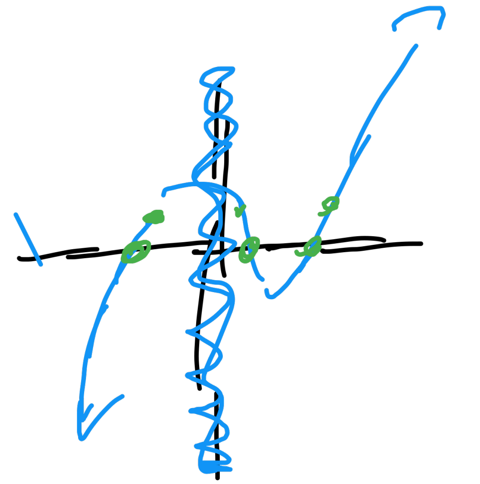
$-1 \notin \text{im } f$

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

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

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

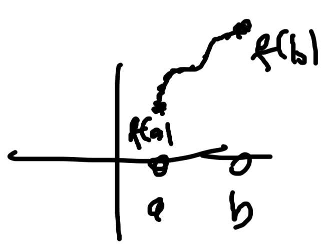




$f(\mathbb{R}) = \text{im } f = \mathbb{R}_{\geq 0}$

(by "continuity")

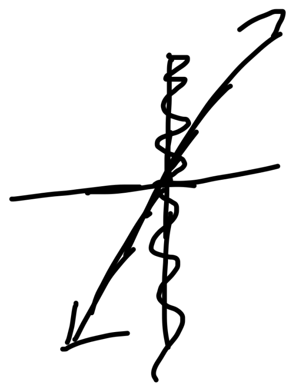
$f(0) = 0$ AND $\lim_{x \to \infty} f(x) = \infty$



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

$x \longmapsto 2x+1$

$\operatorname{im} f = \mathbb{R}$



Pf: IVT, use continuity + limits.

Pf 2: 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., $2a+1 = b$ $\quad a = \frac{b-1}{2}$)

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

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

$W \longmapsto f(W)$

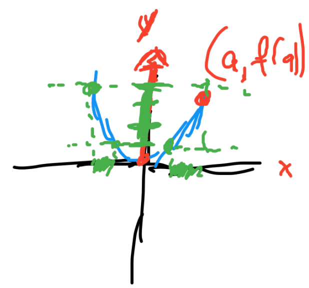
"Preimage" or "inverse image"

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

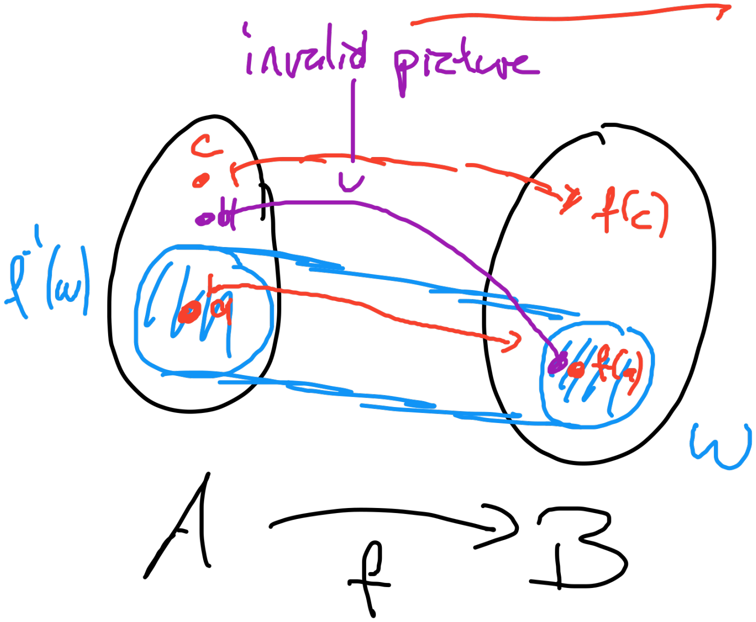
Examples: $f: \mathbb{R} \to \mathbb{R}$
$x \longmapsto x^2$



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

$W = [1,4]$
$f^{-1}(W) = [1,2] \cup [-2,-1]$

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



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

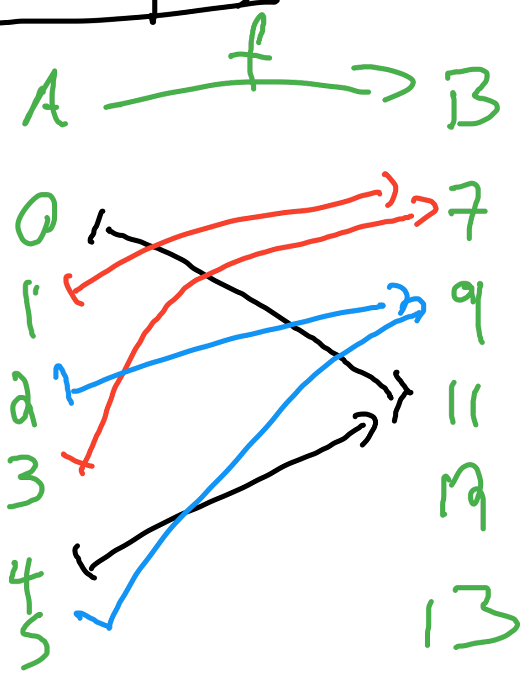
$A \xrightarrow{f} B \quad W = B$?

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

Always true

(By the defn of fxn codomain)

Examples:



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

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

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

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

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

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

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

<u>Example</u>: $A \xrightarrow{f} B$

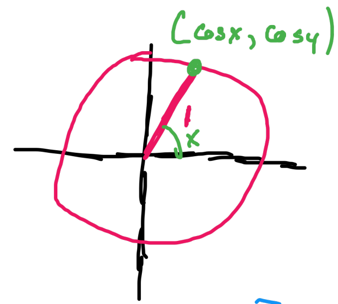
$W = \phi \subseteq B$

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

Always false

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

$x \longmapsto \cos x$



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

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

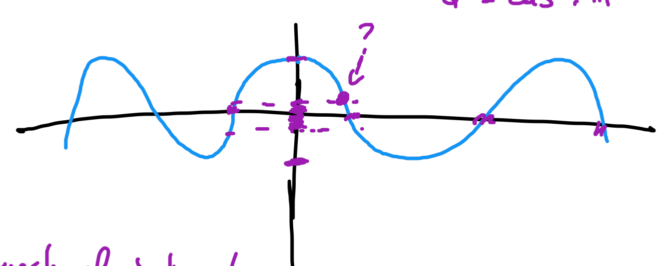
(Σ) $\displaystyle\bigcup_{n=-\infty}^{\infty} [-\pi/2 + 2n\pi, \pi/2 + 2n\pi]$

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

Solve $\cos a = 0.17$

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

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



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

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

(w/ no nice formula)

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

$x \mapsto x^2$

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

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

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

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

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

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

__Case 2:__ $-2 \le x \le -1$. Then squaring gives $1 \le x^2 \le 4$. 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 $1 \le x^2 \le 4$.

Then $1 \le x \le 2$ or $-2 \le x \le -1$. 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) $f\colon \mathbf{Z} \to \mathbf{Z}$, $f(n) = 3n + 1$; $W_1 = \mathbf{E}$, the set of even integers, $W_2 = \{4\}$, $W_3 = \{1, 5, 8\}$.

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

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

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

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

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

"$\supseteq$" Let $a \in \mathbb{O}$. (WTS $a \in f^{-1}(\mathbb{E})$. i.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) $f(n) = \begin{cases} n & n \in \mathbb{E} \\ n-1 & n \in \mathbb{O} \end{cases}$

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

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

$f^{-1}(\{3\}) = \emptyset$ $\qquad f^{-1}(\{6\}) = \{6, 7\}$

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

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 $\cup \mapsto \cap$)

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

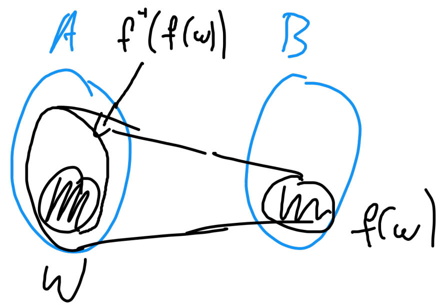
Then $f(a) \in X$ and $f(a) \in Y$.

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

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

$A \xrightarrow{f} B$

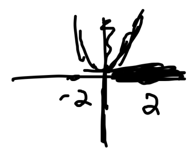
$W \subseteq A$



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

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

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



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

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

$a \in W \overset{\text{defn of } f(W)}{\Downarrow}$

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

Then $a \in f^{-1}(f(W))$, $\boxtimes$

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

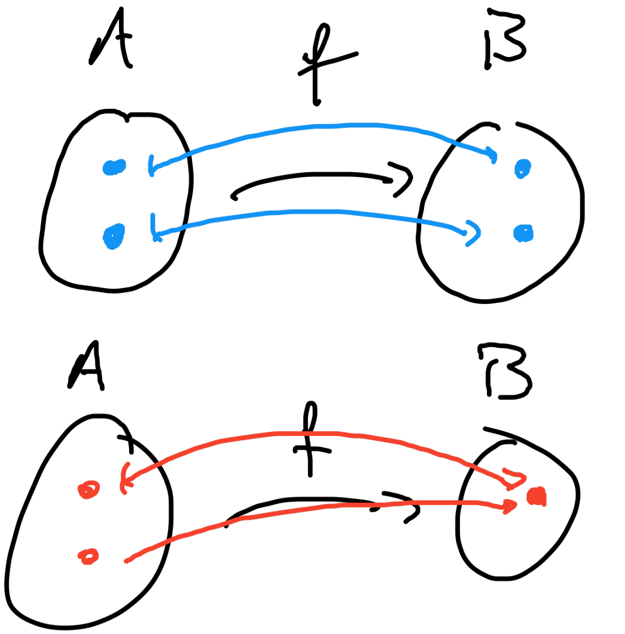
(often easier to do proofs with)

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

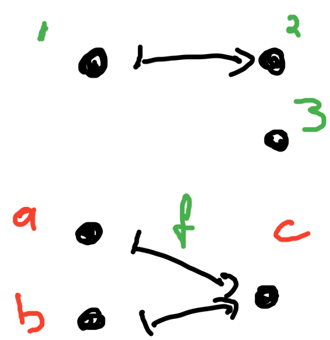
just.... the defn of a fxn



Inj

NOT I

"Test functions"



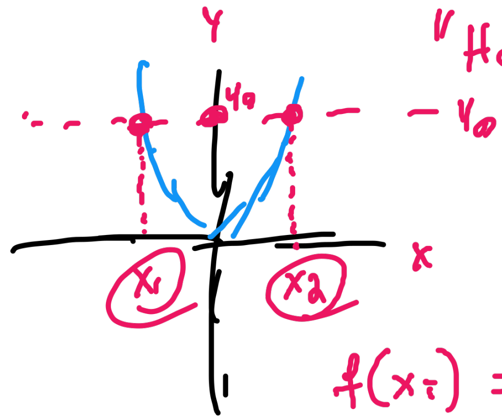
INJ

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

Examples:

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

$x \longmapsto x^2$



$f(x_i) = y_0$

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

"Horizon. line test":

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

$\Longleftrightarrow$

f is inj.

NOT INJ

$1 \neq -1$ and $g(1) = g(-1)$

$\quad\quad\quad\quad\quad\;\; \shortparallel \quad\;\; \shortparallel$

$\quad\quad\quad\quad\quad\quad\;\; 1$

<u>Note</u>: to prove a function $\boxed{13}$ inj., need an argument,

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

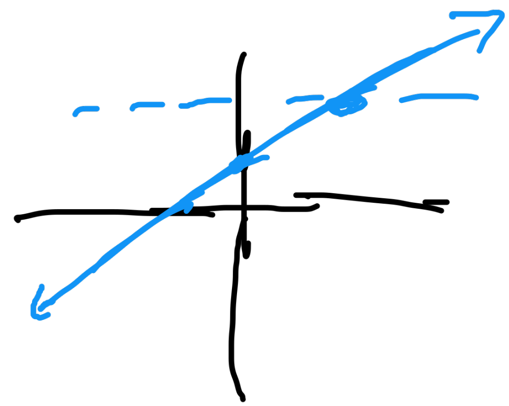
"$\forall a,b \in A,\ f(a) = f(b) \Rightarrow a = b$"

"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>E:</u> $\mathbb{R}_{\geq 0} \xrightarrow{f} \mathbb{R}$

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

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

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

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

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

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

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

$\vdots$

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

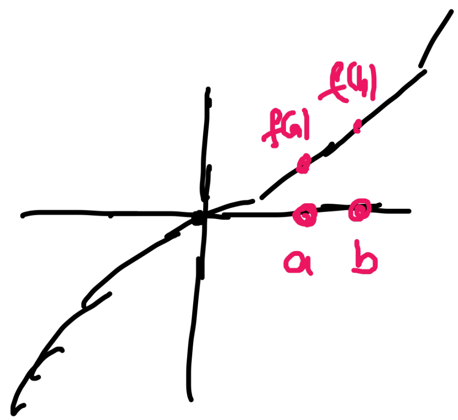
Adding the 1^{st} + 2^{nd} eqn gives $2a = 2c$, so $a=c$.

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

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

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

$x \longmapsto x^3+x$



Increasing $\overset{\text{(HW)}}{\Longrightarrow}$ inj
or decreasing

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

$a \neq b$ + 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

$a^3+a = b^3+b \ldots$

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. $\blacksquare$

Ex's:

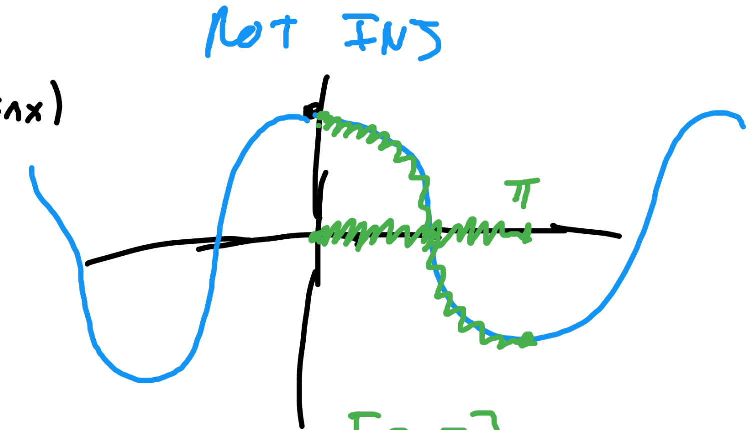
$$f(x) = x^5 + 7x^3 + 3x$$

$$f'(x) = \boxed{5x^4 + 21x^2 + 3 \geq 3}$$

$\Rightarrow f$ is inj.

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

Example



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

$x \longmapsto \cos x$

$\cos 0 = \cos 2\pi$
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. ∎

$$\mathbb{C} \longmapsto \mathbb{C}$$
$$x \longmapsto x^2$$

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

$$\begin{array}{ccc} (i)^2 & = & (-i)^2 \\ \| & & \| \\ -1 & & (-1)^2 i^2 \\ & & \| \\ & & 1(-1) = -1 \end{array}$$

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

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

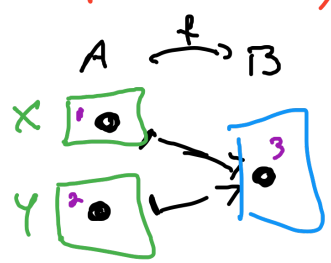
Not I: Are there sets $S_1, S_2 \subseteq \mathbb{R}$ s.t. $S_1 \neq S_2$ but $\boxed{S_1 \cap \mathbb{Z} = S_2 \cap \mathbb{Z}}$?

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

$A \xrightarrow{f} B$

$X, Y \subseteq A$

<u>Recall</u>: "$f(X) \subseteq f(Y) \Rightarrow X \subseteq Y$" is false.



"$\subseteq$"

$= f(X) = f(Y)$

but $X \nsubseteq Y$.

Counterexample

"~~Let A = {1}~~ B

let $A = \{1, 2\}$ ...

"Find the "correct" hypothesis"

NOT INJ.

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

THE DEFN OF $f(X)$

<u>P</u>: 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 $f(X) \subseteq f(Y)$, $\boxed{f(a)} \in f(Y)$.

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

$c \in f(Y) \Leftrightarrow$

$\exists b \in Y$ s.t. $c = f(b)$

Apply w/ $c = f(a)$

Week 12: Compositions of function

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

We define the <u>composition</u> of g and f to be the fxn

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

(\circ)

$$a \mapsto (g \circ f)(a) :\overset{\text{def}}{=} g(f(a)).$$

ALT notation $gf = \underline{g \circ f}$

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

Example:

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

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

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

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

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

Same domain & codomain ☑ but

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

Sometimes there is a "~~[illegible]~~" 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

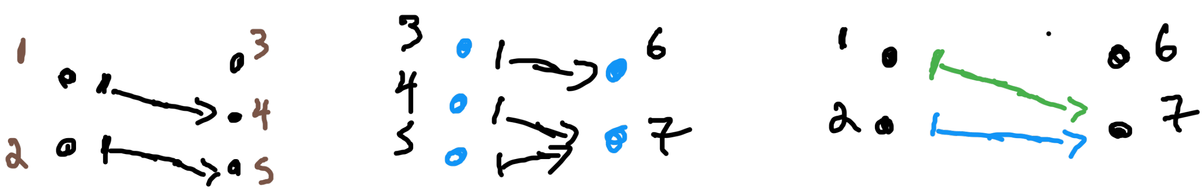
$b \in B \rightsquigarrow g(b) \in C$

But domain of $f = A$

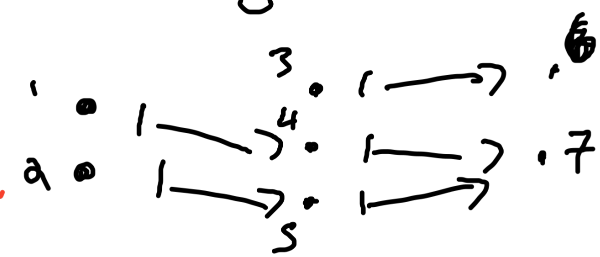
If: $C \subseteq A$ we can fix this.

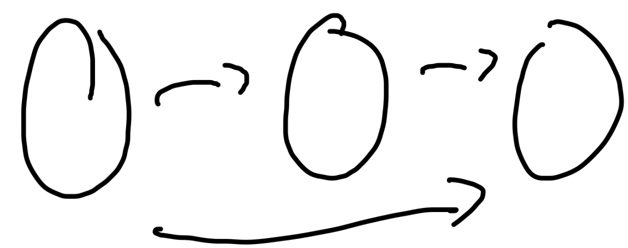
Examples:

$A \xrightarrow{f} B$ $\qquad$ $B \xrightarrow{g} C$ $\qquad$ $A \xrightarrow{g \circ f} C$



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





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

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

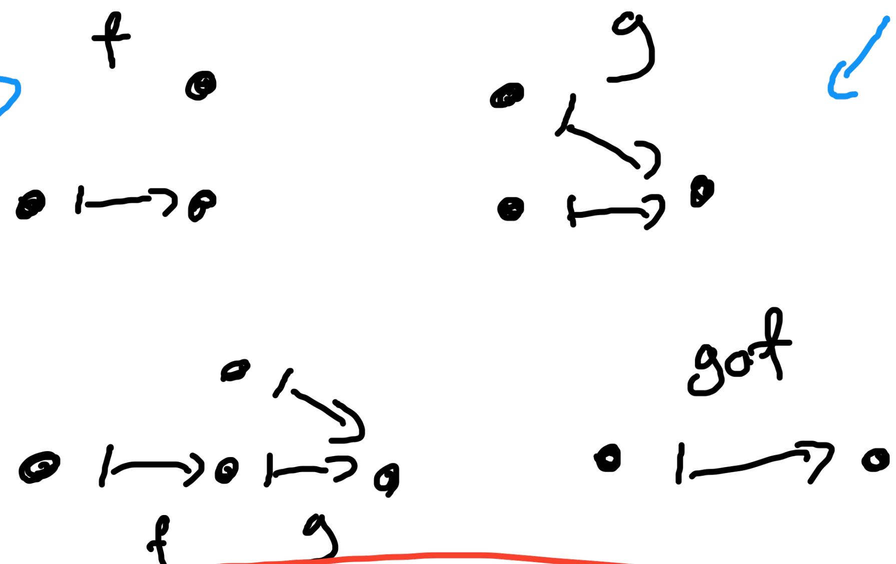
Note: f is inj + g is surj, but $g \circ f$ is neither inj or surj

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. $y \le x$

$(g \circ f)(\pi) = g(f(\pi)) = g(f(3.14\,19\ldots)) = g(3) = 1$

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

$7 \cdot 13$

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

$g \circ f$ 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 $\cdot \mapsto \cdot \mapsto \cdot$ 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

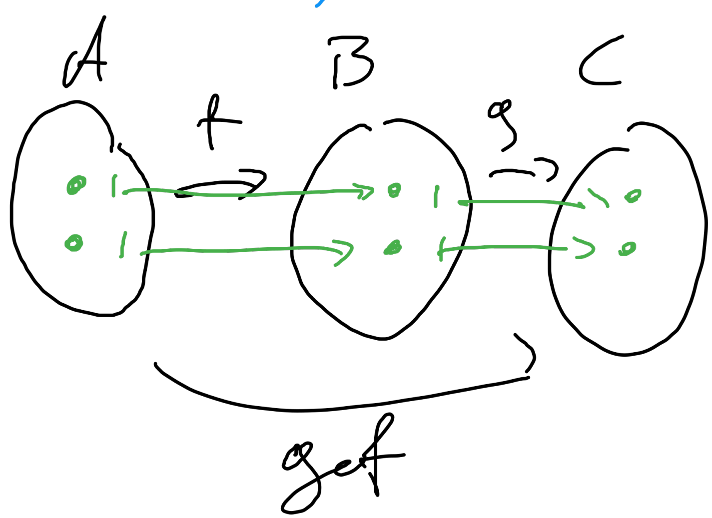
$g(x) = g(y) \implies x = y$

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 $\forall x \in C, \exists a \in A$ s.t. $(g \circ f)(a) = x$

IE $\operatorname{im} g \circ f = C$, IE $(g \circ f)(A) = C$)

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 $(g \circ f)(a) = g(f(a)) = g(b) = x$. $\blacksquare$

(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

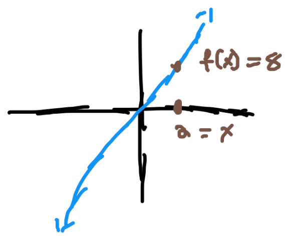
<u>Proof of g</u>: Sps $g \circ f$ is inj. Let $a, b \in A$. Suppose $f(a) = f(b)$. Then $g(f(a)) = g(f(b))$, and since $g \circ f$ is inj, $a = b$. ∎

Week 13: Inverse functions

Idea: f^{-1} "undoes" f

$f(x) = x^3$

$f^{-1}(x) = x^{1/3}$



$f^{-1}(8) = 2$

$f(3) = 27$

$f^{-1}(27) = 3$

"the x s.t. $f(x) = 26$" $= f^{-1}(26) = 26^{1/3} = 2.\ldots?$

FE solve the eqn $f(x) = 26$ for x

(*) $(f^{-1} \circ f)(x) = \underline{f^{-1}(f(x))} = f^{-1}(x^3) = (x^3)^{1/3} = \underline{x} = id_{\mathbb{R}}(x)$

$f^{-1} \circ f = id_{\mathbb{R}}$

$\boxed{\begin{array}{l} f(x) = x^3 = y \text{ + solve for } x \\ x = y^{1/3} \end{array}}$

"Works", but isn't the defn

$\mathrm{id}_A : A \to A$ "the" identity fxn

$x \mapsto x$

$\mathrm{id}_A(x) = x, \ \forall x \in A$

Prop: Let $f : A \to B$ be <u>any</u> fxn. then

(i) $f \circ \mathrm{id}_A = f$ $\qquad A \xrightarrow{\mathrm{id}_A} A \xrightarrow{f} B$

(ii) $\mathrm{id}_B \circ f = f$ $\qquad A \xrightarrow{f} B \xrightarrow{\mathrm{id}_B} B$

<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!

$A = B = \mathbb{R}$

$f : A \to A$

$x \mapsto x^3$

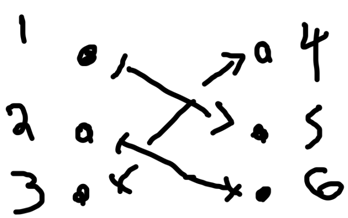
$g : x \mapsto x^{1/3}$

$$(g \circ f)(x) = g(f(x)) = g(x^3) = (x^3)^{1/3} = x = id_{\mathbb{R}}(x)$$

$$(f \circ g)(x) = f(g(x)) = f(x^{1/3}) = (x^{1/3})^3 = x = id_{\mathbb{R}}(x)$$

Example:

$A \xrightarrow{f} B$

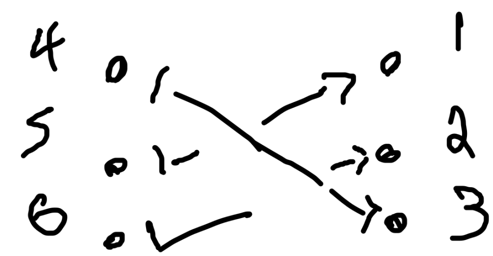


what is the inverse g of f?

$f \circ g = id_B$

$g \circ f = id_A$

$B \xrightarrow{g} A$



$$(g \circ f)(1) = g(f(1)) = g(5) = 1$$

$$(g \circ f)(z) = g(f(z)) = z$$

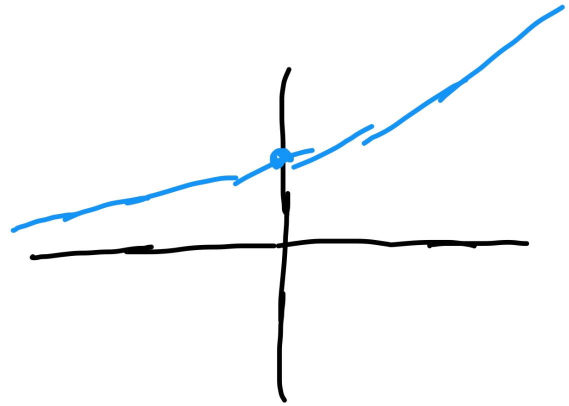
$$\begin{gathered} g(f(z)) \\ \parallel \\ g(y) = z \end{gathered}$$

"$g(x)$ is the solution to $f(z) = x$"

$$\boxed{g(x) = z \iff x = f(z)}$$

<u>Example:</u> $\mathbb{R} \xrightarrow{e} \mathbb{R}_{>0}$

$x \longmapsto e^x$



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 $e^x = 1$"

$= 0$

$e^\pi = e^\pi \quad \ldots$

$\ln(e^\pi) = \pi$

$\ln(e^x) = x$

$e^{\ln x} = x$

$e^x = y \quad \Longleftrightarrow$

$\ln y = x$

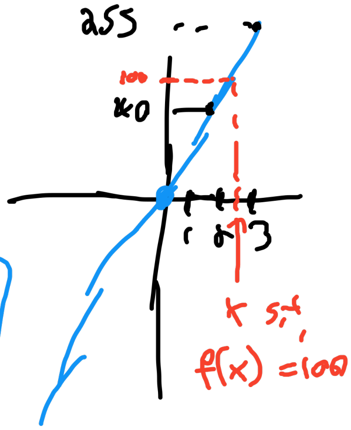
$\mathbb{R} \xrightarrow{f} \mathbb{R}$

$x \longmapsto x^5 + 4x$

$$\boxed{\begin{aligned} f'(x) &= 5x^4 + 4 \\ &\geq 4 \end{aligned}}$$

$\Rightarrow f$ 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

$(g \circ f)(a) = g(f(a)) = a$. ∎

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

(1) USE THM → to help w/ proofs
→ to help w/ counterexamples.

(2) Given f, to find f^{-1}, "solve" the eqns

$$\left.\begin{aligned} f \circ g &= \mathrm{id}_B \\ g \circ f &= \mathrm{id}_A \end{aligned}\right\} \text{ for } g$$

(2') If you have a guess for g, verify your guess by plugging g into

(i) x^2 not inj $\Rightarrow$ not invertible

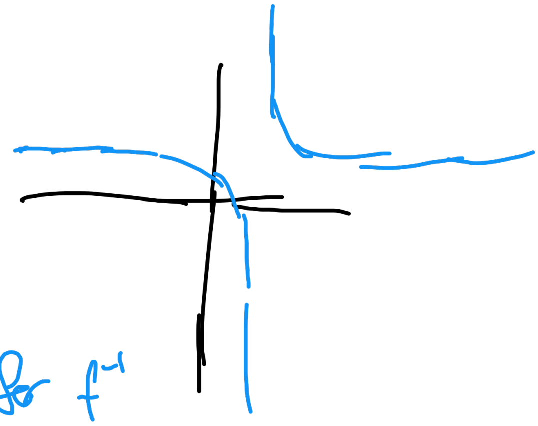
(ii) $f(x) = x^5 + x^3 + x$ is inv. by Thm

b/c bij.

(Still need to explain why f is bij)

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. $f(x)=y$"

$$\frac{x+1}{x-1}=y \qquad \frac{2}{x-1}=y-1 \Rightarrow \frac{x-1}{2}=\frac{1}{y-1}$$

$$\|$$

$$\frac{x-1+2}{x-1} = 1+\frac{2}{x-1} = y$$

$$\Rightarrow x-1=\frac{2}{y-1}$$

$$\Rightarrow x=\boxed{1+\frac{2}{y-1}}=g(y)$$

IE $(f\circ g)(x) \overset{?}{=} x$

$$\|$$

$$f\left(1+\frac{2}{x-1}\right)=\frac{\left(1+\frac{2}{x-1}\right)+1}{\left(1+\frac{2}{x-1}\right)-1} = x$$

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 $R \subseteq S \times S$.

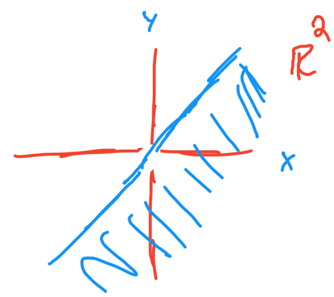
usually use $\sim$

If $(a,b) \in R$, we say that "a is related to b" and write $\boxed{a \sim b}$ (or $a \underset{R}{\sim} b$).

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 $(0,1) \in R$

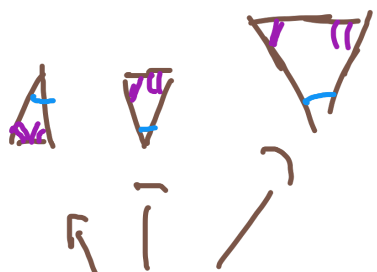
$1 \sim 2$ true

$2 \sim 0$ 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) $\forall a,b,c \in S, a \sim b \wedge b \sim c \Longrightarrow a \sim c$ · transitive

Let $a \in S$. We define the equivalence class of a to be

$$[a] \overset{\text{def}}{=} \{ b \in S \text{ s.t. } b \sim a \}$$

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?

$$[0] = \{a \in \mathbb{Z} \text{ s.t. } a \sim 0\}$$
$$= \{a \in \mathbb{Z} \text{ s.t. } 2 \mid a\}$$
$$= 2\mathbb{Z} = \mathbb{E}$$

$a \sim 0 \iff 2 \mid a-0$
$\iff 2 \mid a$

$$[1] = \{a \in \mathbb{Z} \text{ s.t. } a \sim 1\}$$
$$= \{a \in \mathbb{Z} \text{ s.t. } a \text{ is odd}\}$$
$$= 2\mathbb{Z}+1 \text{ or } \mathbb{O}$$

$a \sim 1 \iff 2 \mid a-1$
$\iff a-1$ is even
$\iff a$ is odd

NOTE: $[0] \cup [1] = \mathbb{Z}$ AND $[0] \cap [1] = \phi$ "partition"

$$[2] = \{a \in \mathbb{Z} \text{ s.t. } a \sim 2\}$$
$$= \mathbb{E}$$

$a \sim 2 \iff 2 \mid a-2$
$\iff 2 \mid a$.

$[0] = [2]$

$[0] \neq [1]$

$0 \in [0]$ 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))

Pf: 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) $a < b \wedge b < c \Rightarrow a < c$.

$S = \mathbb{R}$, $x, y \in \mathbb{R}$, $x \sim y$ iff $x - y \in \mathbb{Q}$

$\pi \sim \pi + 1$ $\quad \pi - (\pi+1) = -1 \in \mathbb{Q}$

$0 \not\sim \sqrt{2}$ 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 $a \sim c$. $\boxtimes$

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 $f(1) = 2$

$\{1\} \nsim \{1, 2\}$

<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 $y = 1$

$1 \sim 1$ $\quad$ $2 \nsim 2$

$1 \sim 2$ $\quad$ $2 \nsim 3$

$2 \sim 1$.

TRUE

NOT R) b/c $2 \nsim 2$

(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 $a \sim b$ ∧ $b \sim c$, but $a \nsim c$

ER $\iff$ $R \wedge S \wedge T$

$\neg$ER $\iff$ $\neg R \vee \neg S \wedge \neg T$