MAT 108

Winter 2021

RIGHT BOARD

Math	English	Prop?	
$\sin(\sqrt{1000})$	the brown dog	No	no = or verb.
$\sin(\sqrt{1000}) < \frac{1}{2}$ P	My dog is brown Q	Yes	
$\sin(x) < \frac{1}{2}$	The dog is brown.	No	undef. variable
$\sin(x) < 2$	The dog is brown or not brown.	Yes	always true.
$P = NP$	Jan 5 2022 will be rainy in Davis.	Yes	hard to evaluate
$x = \sqrt{1000}$ and $\sin(x) < \frac{1}{2}$		Yes.	
similar possible but tricky.	This sentence is false.	No	(paradox.)

In break out rooms:

Find examples of proposition.

and not propositions.

(Maybe a sentence for which it is not clear.).

Building new propositions from old ones.

If P and Q are propositions

write $\sim P$ for not P

$P \wedge Q$ for P and Q (A),

$P \vee Q$ for P or Q.

Summarize via a truth table:

P	Q	$\sim P$	$P \wedge Q$	$P \vee Q$	$\sim P \vee Q$	$\sim[P \wedge \sim Q]$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	T
F	F	T	F	F	T	T

call $\sim P \vee Q$

and $\sim[P \wedge \sim Q]$

equivalent.

P Q

Equiv. Eng. sentences:

My dog is either not brown or outside.

has propositional form:

$$\sim P \vee Q$$

My dog is not both brown and inside.

$\sim[P \wedge \sim Q]$

So as above these English sentences are equivalent.

210106

$\sim P \vee Q$
T
F
T
T

Names:

$\sim$	not	, negation , denial
$\wedge$	and	, conjunction
$\vee$	or	, disjunction

$\Longrightarrow$ implies, conditional, if - then -

$\Longleftrightarrow$ iff, if and only if, biconditional

$P \Longrightarrow Q$ means if $\underbrace{P}_{\text{antecedent}}$ then $\underbrace{Q}_{\text{consequent}}$.

converse to $P \Longrightarrow Q$ is $Q \Longrightarrow P$

contrapositive to $P \Longrightarrow Q$ is $(\sim Q) \Longrightarrow (\sim P)$.

Break out rooms!

Even Find 2 Eng. sentences involving conditions which have the same meaning but diff. prop. forms

Odd Find two diff equiv. prop. forms inv. condit. and then

find Eng. sentences
modeling the form.

Ex: $P \Rightarrow Q$

If im inside I on att. Zoom U.

$\sim Q \Rightarrow \sim P$ (contraps.

If im not att Zoom im outside.

Ex: Im a student at UC Davis P

I'm a math major $\Rightarrow$ Q.

$$\left.\begin{array}{l} P \Rightarrow Q \\ Q \Rightarrow P \end{array}\right]$$ clearly not equ.

equiv.

$P \Leftrightarrow Q$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
T	T
F	F
F	F
T	T

Rules for getting equivalent propositional forms:

Thm 1.1.1

$\sim\sim P$ eq P

$P \wedge Q$ eq $Q \wedge P$

$P \wedge (Q \wedge R)$ eq $(P \wedge Q) \wedge R$

$P \wedge (Q \vee R)$ eq $(P \wedge Q) \vee (P \wedge R)$

De Morgan $\sim(P \vee Q)$ eq $(\sim P) \wedge (\sim Q)$

$\sim(P \wedge Q)$ eq $(\sim P) \vee (\sim Q)$.

Ex: Find a prop. form ~~for~~ equiv to

$\sim(P \Rightarrow Q)$ without conditionals ($\Rightarrow$, $\Leftrightarrow$).

Ans: Truth Table:

P	Q	$\sim(P \Rightarrow Q)$	$P \wedge \sim Q$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	F	F

✓

Ans: $\boxed{P \wedge \sim Q}$

Another Ans: $P \Rightarrow Q$ is eq. to

$\sim P \vee Q$

(from before).

so $\sim(P \Rightarrow Q)$ eq. $\sim[\sim P \vee Q]$

eq $\boxed{P \wedge \sim Q}$

210108

Here a universe (of discourse) is the set over which all ~~q~~ quantifiers are taken.
(eg: $\forall x$ mean $\forall x \in$ the universe)

$\boxed{\text{Problem: With a paradox like this sentence is false}}$

Consider the denial of this sentence:

Somebody ~~Nobody~~ I know dislikes chocolate and likes coffee.

$$(\exists x \in \{\text{ppl I know}\})\big(\sim P(x) \wedge Q(x)\big)$$

Not everyone I know likes chocolate or dislikes coffee.

$$\sim(\forall x \in \{\text{ppl I know}\})\big(P(x) \vee \sim Q(x)\big)$$

$\exists$ is there exists:

$$(\exists x \in \mathbb{Z})\ (x^2 = 1)$$

Means there is some integr x with $x^2=1$

or

In the universe $\mathbb{Z}$.

$$(\exists x)\ (x^2=1).$$

In the universes below which are true?

$P(x)$ is $x^2 = 5$

all integers $= \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

U	$\mathbb{Z}$	$\mathbb{R}$	$\mathbb{R}_{\geq 0}$	$\{-\sqrt{5}, \sqrt{5}\}$
$(\forall x) P(x)$	F	F	F	T
$(\exists x) P(x)$	F	T	T	T
$(\exists! x) P(x)$	F	F	T	F

Notation: $\exists!$ is there is exactly one.

(there exists a unique).

Proof of Thm 1.3.1.a:

Let $\mathcal{U}$ be any universe.

The sentence $\sim(\forall x)P(x)$ is true in $\mathcal{U}$

iff $(\forall x)P(x)$ is false in $\mathcal{U}$

if and only if

iff the truth set for P in U is not all of U

iff the truth set for $\sim P$ in U is not empty.

iff $(\exists x) \sim P(x)$

Thus $\sim (\forall x)\, P(x)$ is equv. to $(\exists x) \sim P(x)$ in any universe.

210111

Thm: If a is an odd integer then a^2+1 is an even integer.

Proof: Assume that a is an odd integer. Hence there is an integr n with

$$a = 2n+1.$$

Hence $a^2+1 = (2n+1)^2+1 = 4n^2+4n+1+1$

$$= 2\left[2n^2+2n+1\right]$$

and $2n^2+2n+1$ is an integer.

Therefore $\boxed{a^2+1 \text{ is an even integer.}}$

q.e.d. latin for: that which was to be proved

Why is it true?

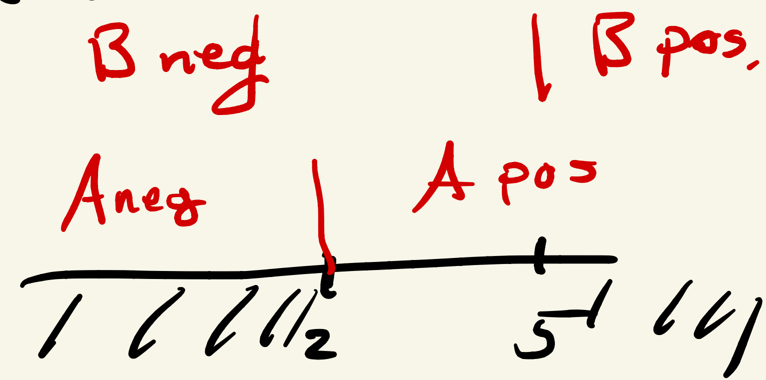
work backward and forward:

$x^2 - 7x > -10$

or

$x^2 - 7x + 10 > 0$

or



Eqv

$(x-2)(x-5) > 0$

A or B

or

A & B are both pos or A & B are both neg

or $x < 2$ or $x > 5$

$x^2 \leq 1$ or $-1 \leq x \leq 1$

hence $x < 2$

Proof Plan: Show $x^2 \leq 1$ implies $x < 2$

then hence $x-2<0$ & $x-5<0$

then $(x-2)(x-5)>0$

done $x^2-7x>-10$

Try a similar approach to show:

Thm: If x is a real number with $x<1$ then $x^2+6>5x$.

Proof:

Assume $x < 1$.

Hence $x < 2$.

Hence $(x-3)(x-2) > 0$.

Hence $x^2 + 6 > 5x$. q.e.d.

210113 Another direct proof:

Def: If a and b are integers then a <u>divides</u> b if $(\exists n \in \mathbb{Z})$ with $n \cdot a = b$

Claim: If a, b and c are integers and a divides both b and c then a divides $b - c$.

Proof: Assume a, b and c are integers with a dividing b and c.

Hence there ~~is a~~ are integers n and m with $n \cdot a = b$ and $m \cdot a = c$.

Hence $n - m$ is an integer.

Hence: $b - c = n \cdot a - m \cdot a = (n - m) \cdot a$.

Therefore a divides $b - c$. $\boxed{\text{qed}}$

Understand!

eg $5 = m$ $\quad 5^2 = 25$ odd $\quad$ so 5 odd ✓

$4 = m$ $\quad 4^2 = 16$ even $\quad$ so 4 even ✓

Logic: $(\forall m \in \mathbb{Z})\ \ \underline{P \Rightarrow Q}$

P is m^2 is odd

Q is m is odd.

use this.

or equivalently: $\boxed{\sim Q \Rightarrow \sim P}$

A: Assume: $\sim Q$ or m is even

or $\exists t$ with $2 \cdot t = m$

Conclusion: $\sim P$ or m^2 is even

or $\exists s$ with $2 \cdot s = m^2$

Ideas: $m^2 = (2t)^2 = 4t^2 = 2\underbrace{(2t^2)}_{\text{an int.}}$ ✓

Claim: Assume a is an integer. 4 does not divide $a^2 - 2$.

2/01/15

Recall §1.7 read often.

claim ② getting started:

Understand: eg: $6^2 - 2 = 34 = 2 \cdot 17$ not a mult of 4

Logic: P is 4 divides $a^2 - 2$

$(\forall a \in \mathbb{Z}) \sim P$

or for contradiction equiv!

$\underbrace{\sim [(\forall a \in \mathbb{Z}) \sim P]}_{eg} \Rightarrow \underbrace{[Q \wedge \sim Q]}_{F}$ still get to choose Q.

$$\boxed{[(\exists a \in \mathbb{Z}) P] \Rightarrow [Q \wedge \sim Q]}$$

Ass/Concl:

Assume there is some int. a with 4 dividing a^2-2 (2)

or $(\exists t \in \mathbb{Z})\ 4t = a^2-2$

Concl: Q and $\sim Q$ still get to choose Q,

Ideas: $4t = a^2 - 2$

(3) so $4t+2 = 2(2t-1) = a^2$

so a^2 is even so by Claim ① a is even

so there is $s \in \mathbb{Z}$ with $2s = a$

so $4t = (2s)^2 - 2 = 4s^2 - 2$

so $2 = 4(s^2 - t)$

5 | so $1 = 2\underbrace{(s^2 - t)}_{\text{an integer}}$ 4

Q

so 1 is even

D Know 1 is not even $\sim Q$

$\sim Q$

Quote! §1.7 Go over your proof and
- check for things not needed
- Make sure the order is best
- Make sure it is complete.

Def: Write $a \in \mathbb{Q}$ or a is rational

if $\exists p \in \mathbb{Z}, \exists q \in \mathbb{N}$ with $a = \frac{p}{q}$.

Claim 3: If a is rational $\forall a \in \mathbb{Q}$ P

and $a = \frac{p}{q}$ with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$

and the deminator q as small as possible

then either p is odd Q or q is odd. R

U: $a = \frac{24}{132} = \frac{12}{66} = \frac{2}{11}$ ← odd ✓

$a = \frac{3}{5}$ ← odd

$a = \frac{3}{10}$

$L: (\forall a \in \mathbb{Q})\ \underbrace{P}_{\text{complicated}} \Longrightarrow \underbrace{Q}_{\text{simple}} \vee \underbrace{R}$

or contrapositive:

$(\forall a \in \mathbb{Q})\ \sim(Q \vee R) \Rightarrow \sim P$

or

$\boxed{(\forall a \in \mathbb{Q})\ (\sim Q \wedge \sim R) \Rightarrow \sim P}$

Thm (Pythagoreans ~ 230 BC)

$\sqrt{2} \notin \mathbb{Q}$

or $\sqrt{2}$ is not rational

$\sqrt{2} \neq \frac{7}{5}$

Claim ④ There is an integer n with $n^2+15 < 8n$

Proof: Take $n=4$.

Hence $n^2+15 = 31$

and $8n = 32 > 31$.

qed.

210120

so $2q^2 = 2(2m+1)^2 = 8m^2+8m+2$

$\parallel$

$p^2 = (2k)^2 = 4k^2$

so $4m^2+4m+1 = 2k^2$

so $1 = 2k^2-4m^2-4m$

$= 2[k^2-2m^2-2m]$

$k^2-2m^2-2m \in \mathbb{Z}$

1 is even] Q ⑧

know 1 is not even] ~Q ⓪

From §1.7 (read often)
Always use complete sentences in a proof.

Multiple quantifiers:

① $\exists!$ both $\exists$ and $\forall$ something else.

② $\forall - \exists -$ or $\exists - \forall -$.

Example: 3 possibly false statements:

(3) $(\exists!\ x \in \mathbb{R})\quad x^2 - 4x + 3 = 0$

(4) " " " 4 " "

(5) " " " 5 " "

BrkOut Rm Questions:

(A) which is(are) true?

(B) which want a proof by contradiction?

(C) " " " example?

Claim: $\sim\left[(\exists!\, x \in \mathbb{R})\ x^2-4x+5=0\right]$

Proof: It suffices to show:

(sketch) $\sim\left[(\exists\, x \in \mathbb{R})\ x^2-4x+5=0\right]$

Computing: $x^2-4x+5 = (x^2-4x+4)+1$

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

For contradiction: assume $x \in \mathbb{R}$ and

$x^2-4x+5=0$ so $(x-2)^2+1=0$

so $(x-2)^2 = -1 < 0$

Know $(x-2)^2 \geq 0$

Therefore $(x-2)^2 \geq 0$ and $(x-2)^2 < 0$

a contradiction so $\sim(\exists x \in \mathbb{R})\ x^2-4x+5=0$

QED.

210122

Ex:

a	b	gcd(a,b)	lcm(a,b)
3	18	3	18
10	35	5	70
91	91	91	91
256	81	1	$256 \cdot 81$

Def: (pg 82 ex 16)

If a, b and m are nonzero integers then $\operatorname{lcm}(a,b) = m$ iff

(i) a and b both divide m (say m is a common multiple of a and b)

(ii) every common multiple of a and b is at least m.

$(\forall a, b, m \in \mathbb{Z}_{\neq 0})\ \operatorname{lcm}(a,b) = m \Longleftrightarrow$

$$[(\exists s,t \in \mathbb{Z})\ (a \cdot s = m) \land (b \cdot t = m)] \land$$

$$[(\forall e \in \mathbb{Z})\ [(\exists u,v \in \mathbb{Z})\ (a \cdot u = e) \land (b \cdot v = e)]$$

$$\Rightarrow (e \geq m)]$$

Shortening ~~strategy~~ gg:

Def: $\underbrace{a|e}_{\text{a divides e}} \Leftrightarrow (\exists s \in \mathbb{Z})\ a \cdot s = e$

Def: Call a and b <u>relatively prime</u>

or <u>coprime</u> if $(a,b)=1$.

Approach to ⓐ:

U: $a=20$ $\quad$ $b\neq 30$ / $\gcd(20,30)\neq 10$

$b=$

$a=11$ $\quad$ $b=13$ $\quad$ $\gcd(11,13)=1 \wedge 11<13$,

L: $(\forall a)(\exists b)\ P \wedge Q$

P is $P_i \wedge P_{ii}$

$\boxed{P_i \text{ is } 1 \text{ divides both.}}$ always true

P_{ii} any common div. is at most 1

A/C: $\forall$ .. assume $a \in \mathbb{N}_{\geq 0}$

find (our choice) b

conclude: $P \wedge Q$.

I: eg $a = 20$

choose $b = 23$ ✓

if $a = 65$

choose: $b = 83$ ✓

a

$b = a+1$

Try:

If d is a common div of

a and $a+1$

$\exists\ s,t \in \mathbb{Z}$ with

$$d \cdot s = a \quad \text{and} \quad d \cdot t = a+1$$

so $\quad d \cdot t - d \cdot s = a+1-a = 1$

$$d(t-s)$$

210125

Ex: 2 is a lin comb of 10 and 14.

since: $2 = 10 \cdot 3 + 14 \cdot (-2)$

1 is not a lin. comb. of 10 and 14

since: For contradiction assume

$1 = 10 \cdot x + 14 \cdot y = 2 \cdot [5 \cdot x + 7 \cdot y]$

so 1 is odd and 1 is even. a contradiction.

Ex of 1.8.1:

The smallest positive linear combination of 10 and 14 is 2.

Also $\gcd(10,14)=2$.

Ex: If $a=10$, $b=14$ then

$$14 = 10\cdot 1 + 4 \quad \text{and} \quad 0 \le 4 < 10$$

Euclid's Alg. Example: from $a=10$, $b=14$

$$14 = 10 \cdot 1 + 4$$

$$10 = 4 \cdot 2 + \boxed{2} = r_k$$

$$4 = 2 \cdot \underbrace{2}$$

No

$q_1 = 1$

$q_2 = 2$

$q_3 = 2$

$k = 2$

$r_k = 2$

$$256 = 81 \cdot 3 + 13$$
$$81 = 13 \cdot 6 + 3$$
$$13 = 3 \cdot 4 + \boxed{1} \quad r_2 = \gcd(256, 81).$$
$$3 = 1 \cdot 3$$

U: $p = 3$ $\quad a = 4 \quad b = 9$

$p = 6$ $\quad a = 4 \quad b = 9 \quad ab = 36$

not true

p div ab but not a or b

p is prime must be used.

$L: (\forall a, b, p \in \mathbb{Z})(P \wedge Q) \Rightarrow \underbrace{(S \vee T)}_{\sim S \Rightarrow T},$

P is p is prime

Q is $p \mid ab$

divides.

S is $p \mid a$

T is $p \mid b$

equivalently:

$$\boxed{\top (\forall a, b, p \in \mathbb{Z})(P \wedge Q \wedge \sim S) \Rightarrow T}$$

Ass: $P, Q, \sim S$

Cond: T

I: 1 p is prime] only divis are 1 and p

p | ab] so 3 $ab = pn$ for some int. n.

$p \nmid a$] so $\gcd(p,a) = 1$

does not divide

By Thm. 1.8.1 2 so $1 = p \cdot x + a \cdot y$ for some ints x and y.

$\exists x, y \in \mathbb{Z}$

lin. comb. of p and a

gcd(p,a)

Playing with these:

$(\forall p, a \in \mathbb{Z}_{\neq 0})(\exists x, y)$ $\gcd(a,b) = a \cdot x + b \cdot y$

$ab = pn$

$[1 = p \cdot x + a \cdot y$

④

want $\quad b \stackrel{?}{=} p \cdot t \qquad (T)$.

⑤

$b = p \cdot x \cdot b + a \cdot y \cdot b$

$= p \cdot xb + p \cdot n \cdot y$

$= p[xb + ny]$ $\quad$ so $\quad p$ div b.

✓

210127

Chapter 2: Set Theory -

Notes: 1. Will consider set theory using first order logic.

2. Also any first order logic involves sets (a) the universe $\mathcal{U}$ is a set.

(b) If $P(x)$ is a proposition with variable in a universe $\mathcal{U}$, then the truth set of P is

$$\{x \in \mathcal{U} \mid P(x) \text{ (is true)}\}$$

Consider relationships between operations on sentenceses and on sets.

Def: If A and B are sets then A is a subset of B if

$$(\forall x)\left[(x \in A) \Rightarrow (x \in B)\right]$$

In this case write $A \subseteq B$.

Venn diag.

Lemma: If A is a set then

$$\{\} \subseteq A.$$

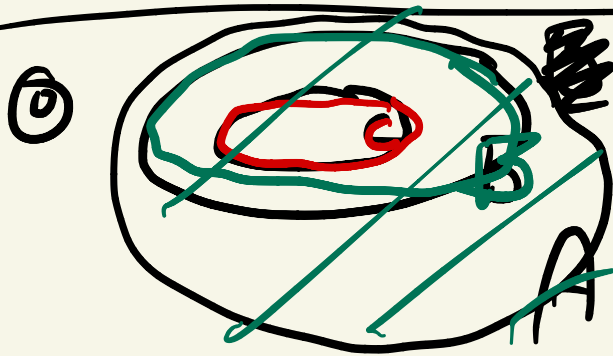
Proof: $(\forall x)\ (x \notin \{\})$

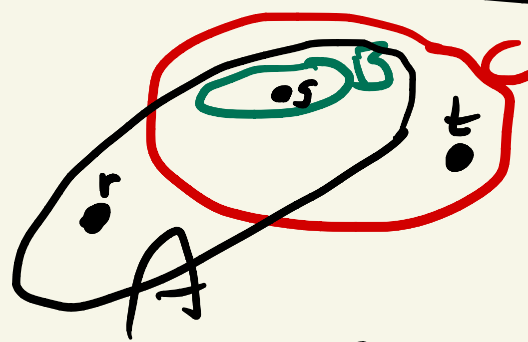
so $(x \in \{\})$ is false

and implies $(x \in A)$.

~~then~~ Therefore: $(\forall x)[(x \in \{\}) \Rightarrow (x \in A)]$.

qed.





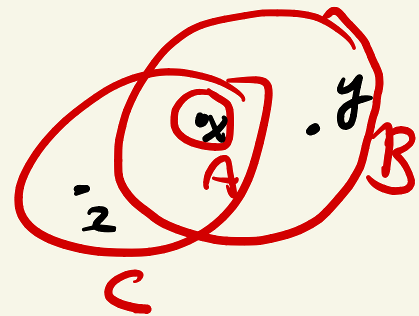
True; Example: $A = \{r, s\}$

$B = \{s\}$

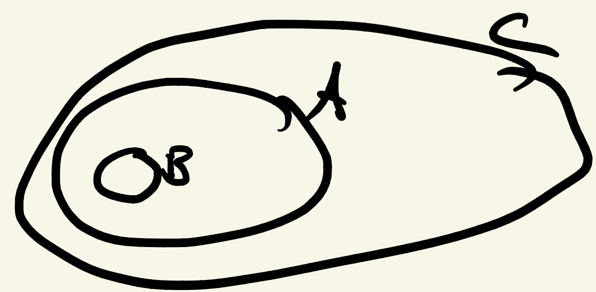
$C = \{s, t\}$

check ✓

① $A = \{x\}$
$B = \{x, y\}$
$C = \{x, z\}$



② $A = \{x, y\}$
$B = \{x, y\}$
$C = \{x, y\}$



③

④ False: Proof idea:

Know: $B \subseteq A$ so
$(\forall x)\ (x \in B) \Rightarrow (x \in A)$
$A \subseteq C$ so
$(\forall x)\ (x \in A) \Rightarrow (x \in C)$

so $(\forall x)\ (x \in B) \Rightarrow (x \in C)$.

so $B \subseteq C$.

210129

Claim: $\{x \in \mathbb{R} \mid |x+3| = 5 - |x|\} = \{-4, 1\}$.

Pf plan: (U) check: 1 in? try $|1+3| \stackrel{?}{=} 5 - |1| = 4$ ✓.

(L) Need to show: $A \subseteq B$ and $B \subseteq A$.

(C) • Assume $x \in A$ and show $x \in B$

• A ⋯ $x \in B$ " " $x \in A$

(I): $A = LHS = \{x \in \mathbb{R} \mid \ldots\}$ $B = RHS = \{-4, 1\}$.

To show $B \subseteq A$ just plug both in.

To show $A \subseteq B$

$|\cdot|$ suggests cases:

$2x = -8$ or $x = -4$

$x < -3$: $-(x+3) = 5 + x$ or $2x = -8$ or $x = -4$ ✓

$-3 < x < 0$ $x+3 = 5 + x$ or $3 = 5$ no soln

$0 < x$: $x + 3 = 5 - x$ or $2x = 2$ ✓

Proof: Check: $\{-4, 1\} \subseteq \{x \in \mathbb{R} \mid |x+3| = 5 - |x|\}$

If $x = 1$ then $|x+3| = 5 - |x| = 4$ ✓.

If $x = -4$ then $|x+3| = 5 - |-x| = 1$ ✓

qed.

Check: $\underbrace{\{-4, 1\}}_{B} \supseteq \underbrace{\{x \in \mathbb{R} \mid |x+3| = 5 - |x|\}}_{A}$

Assume $x \in A$. Either $0 < x$ or $-3 < x \leq 0$

or $x < -3$.

If $0 < x$ then $x + 3 = 5 - x$ so $x = 1 \in B$.

If $-3 \leq x \leq 0$ then $x + 3 = 5 + x$ so $3 = 5$

a contradiction. so $x \in B$.

If $x<-3$ then $-x-3=5-x$ so $x=-4\in B$.

Therefore $x\in B$. qed.

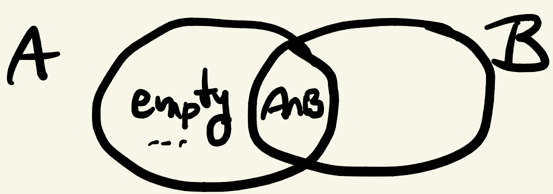
Problem: Which is true;

① If A & B are sets then
$$A\subseteq B \text{ iff } A\cap B=A.$$

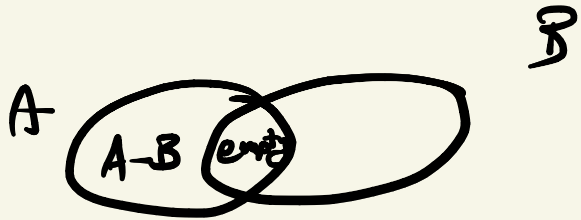
② If A & B are sets then
$$A\subseteq B \text{ iff } A-B=A.$$

Ans: Approach:

1



2



] false.

For 2 Find a counterexample:

Set $A = \{1\}$ $\quad B = \{2\}$.

compute: $A - B = \{1\} = A$] RHS true

but $A \not\subseteq B$.] LHS false.

210201

$A = \{\cancel{1}, \cancel{2}\}$ $\qquad$ $B = \{3\}$

$C = \{4\}$ $\qquad$ $D = \{\cancel{5}\}$

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

$$C \times D = \{\cancel{(4,5)}\}.$$

$$(A \cup C) \times (B \cup D) = \{\cancel{(1,3)}, \cancel{(2,3)}, (4,3), \cancel{(1,5)}, \cancel{(2,5)}, \cancel{(4,5)}\}$$

so $\quad A \times B = C \times D = \{\}$

but $\quad (A \cup C) \times (B \cup D) = \{(4,3)\}$

Asside: $\{\} \times \{3\} = \{ \}$

Note: For any set B

$$\{\} \times B = \{\}$$

$(0 \cdot b = 0)$ ✓

Ex: $\{\{\}\} \times \{3\} = \{(\{\},3)\}$

Note: If A has a elements
and B has b elements
then $A \times B$ has $a \cdot b$ elements.

Note: $\{\} \subseteq B$ for any set B.

Proof that ($\forall A, B, C, D$ sets)

$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

Assume: (x, y) is in $A \times B$

so x is in A and y is in B.

Hence since $A \subseteq A \cup C$ and $B \subseteq B \cup D$

also have $x \in A \cup C$ and $y \in B \cup D$.

Therefore (x, y) is in $(A \cup C) \times (B \cup D)$.

If (x, y) is in $C \times D$ then similarly.

(x, y) is in $(A \cup C) \times (B \cup D)$.

qed.

Def: If $\mathcal{Q}$ is a family of sets.

write $\bigcup_{A \in \mathcal{Q}} A$ for the union

so $x \in \bigcup_{A \in \mathcal{Q}} A$ iff $(\exists A \in \mathcal{Q})\ x \in A$

If $\mathcal{Q} = \{A_\alpha \mid \alpha \in \Delta\}$ is an indexed family of sets then $x \in \bigcup_{\alpha \in \Delta} A_\alpha$ iff

$(\exists \alpha \in \Delta)\ x \in A_\alpha$

Ex: 1: $\bigcup_{A \in \mathcal{A}} A = \bigcup_{\alpha \in \{a,b,c\}} A_\alpha = \{1,2,3,4,5\}$

2 $\bigcup_{B \in \mathcal{B}} B = \bigcup_{\alpha \in [0,2)} B_\alpha = [0,5)$

Def: $x \in \bigcap_{A \in \mathcal{A}} A$ iff $(\forall A \in \mathcal{A})\ x \in A$

$x \in \bigcap_{\alpha \in \Delta} A_\alpha$ iff $(\forall \alpha \in \Delta)\ x \in A_\alpha$

210203

Proof Planning:

U: $n=1$ $\quad 1^2 = 1$ ✓

$n=2$ $\quad 2^2 = 1+3$ ✓

$n=3$ $\quad 3^2 = 1+3+5$ ✓

L: $(\forall n \in \mathbb{N}) \quad P(n)$] correct logic for induction.

I: To show the formula for $n=4$

$$\underbrace{4}_{n+1}{}^2 = \underbrace{(3+1)^2}_{(n+1)^2} = \overbrace{\underbrace{3}_{n}{}^2 + 2\cdot\underbrace{3}_{n} + 1}$$

$$= \left(1+3+5\right) + (2\cdot 3+1)$$

$$= 1+3+5+\underbrace{7}_{2\cdot 4-1} \quad ✓$$

Or more generally:

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

$$= \left(1+3+\cdots+(2n-1)\right) + (2n+1)$$

$$= 1+3+\cdots\cdots + \left(2(n+1)-1\right)$$

Got $P(n+1)$ using $P(n)$

Claim: For every natural number n it is true that $n+3 < 5n^2$.

Proof: Check the base case with $n=1$ which is $1+3 \leq 5 \cdot 1^2$ which is true.

Assume for induction that $n+3 < 5n^2$

hence $5(n+1)^2 = 5n^2 + 1 + 10n + 9$

$> 5n^2 + 1 > n + 3 + 1 = (n+1) + 3.$

Therefore by PMI the claim holds.

qed.

Bad Proof:

Claim: Any group of n horses are all the same color.

"Proof" (look for error).

Check the base case with $n=1$ which is that any one horse is one color and is true,

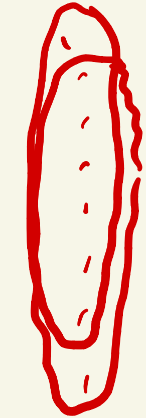
Assume for induction that

any group of n horses are all the same color.

Hence in any group of $n+1$ horses the first n are all the same color and the last n are all the same color and these two groups both contain the middle horses so all $n+1$ horses are all the same color.

Therefore by PMI the claim holds.

[illegible]



Proof Plan:

Consider this an inductive statement: $(\forall n \in \mathbb{N})$ $\nexists a \in \mathbb{Z}$ with $\frac{a}{n} = \sqrt{2}$

base case with $n=1$

is $\sqrt{2} \neq \frac{a}{1}$ an integer:

sine $0^2 \neq 2$, $1^2 \neq 2$

and if $|a| \geq 2$ then $a^2 > 2$ ✓

Assume for induction that for any $n \leq m$ $\nexists$ $\frac{a}{n} = \sqrt{2}$.

Hence: Assume for contradiction that $\exists$ $b \in \mathbb{Z}$ with $\frac{b}{m+1} = \sqrt{2}$.

so $b^2 = 2(m+1)^2$ so b^2 is even

so $b = 2k$ is even

so $4k^2 = 2(m+1)^2$

so $2k^2 = (m+1)^2$ so $(m+1)^2$ is even

so $m+1 = 2r$ is even

so $\quad \dfrac{k}{r} = \dfrac{2k}{2r} = \dfrac{b}{m+1} = \sqrt{2}$

but $\dfrac{m+1}{2} = r \leq m$ contradicting the induction hypothesis.

216205

Proof sketch for Claim 1:

U: Note $\gcd(1,1)=1$

$\gcd(1,2)=1$

$\gcd(2,3)=1$

$\gcd(3,5)=1$

$\vdots$

L: $(\forall n \in \mathbb{N})\ P(n)$

with $P(n)$ being: $\gcd(f_n, f_{n+1})=1$

C/A: Use induction:

- Check $n=1$ base case. 2

$\underbrace{\text{• Assume } P(n) \text{ and show } P(n+1)}_{\text{PMI}}$ 3.

$\underbrace{\left(\text{Assume } \forall k \le n \text{ have } P(k) \right) \text{ and show } P(n+1)}_{\text{GPMI}}$

I:

$$\underbrace{\gcd(13, 8) = \gcd(8+5, 8) \stackrel{?}{=} \underbrace{\gcd(5, 8) = 1}_{P(5)}}_{}$$

$P(6)$

More generally: $\gcd(f_{n+1}, f_{n+2}) = \gcd(f_{n+1}, f_{n+1}+f_n)$

$\overset{?}{=} \gcd(f_{n+1}, f_n) \underset{\text{ind hyp}}{=} 1$ ✓.

Claim ②: If f_n are the Fibonacci numbers then f_{4n} is divisible by 3.

Sketch for ②:

U:	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
	1	1	2	3	5	8	13	21
				3 div				3 div

L: $(\forall n \in \mathbb{N})\ P(n)$

here: $P(n)$ is 3 divides f_{4n}

A/C: Use induction:

base case $n=1$ $(f_4=3)$ ✓

Assume for induction $P(n)$

conclude $P(n+1)$.

I: $f_{4(n+1)} = f_{4n+4} = f_{4n+3} + f_{4n+2}$

$= f_{4n+2} + f_{4n+1} + f_{4n+2}$

$= 2 f_{4n+2} + f_{4n+1}$

$= 2(f_{4n+1} + f_{4n}) + f_{4n+1}$

$$= 3 f_{4n+1} + 2 f_{4n}$$

and by the ind. hyp. $f_{4n} = 3 \cdot S$

so $f_{4(n+1)} = 3(f_{4n+1} + 2S)$.

210208

Ex: §2.3 : Set families proof;

Prove that if $\mathcal{Q} = \{A_\alpha \mid \alpha \in \Delta\}$

(10a) and $\Gamma \subseteq \Delta$.

then $\bigcup_{\alpha \in \Gamma} A_\alpha \subseteq \bigcup_{\alpha \in \Delta} A_\alpha$

Proof: Assume $a \in \bigcup_{\alpha \in \Gamma} A_\alpha$.

Hence $(\exists \alpha \in \Gamma)$ with $a \in A_\alpha$.

and since $\Gamma \subseteq \Delta$ we have $\alpha \in \Delta$.

Therefore $a \in \bigcup_{\alpha \in \Delta} A_\alpha$. qed.

Thm 2.5.2: (Division Algorithm):

If $0 < m \leq n$ are natural numbers then there are unique q and r with

$$n = q \cdot m + r \quad \text{and} \quad 0 \leq r < m.$$

Proof of uniqueness:

Assume $0 < m \leq n$ and $n = q \cdot m + r$

and $n = \tilde{q} \cdot m + r$ and $0 \leq r < m$

and $0 \leq \tilde{r} < m$.

Hence: $-m < \tilde{r} - r < m$.

Also $0 = n - n = (q - \tilde{q}) \cdot m + (r - \tilde{r})$

Hence $\tilde{r} - r = (q - \tilde{q}) \cdot m$

so $\dfrac{\tilde{r} - r}{m} = q - \tilde{q}$.

Since $-1 < \dfrac{\tilde{r} - r}{m} < 1$ is an integer

se hae $\dfrac{\tilde{r} - r}{m} = 0$.

Hence $\tilde{r} - r = 0 = (q - \tilde{q}) \cdot m$.

Therefore $\tilde{r} = r$ and $\tilde{q} = q$. qed.

210212 Notation around Relations:

Def: If A and B are sets then a <u>relation from A to B</u> is a subset $R \subseteq A \times B$.

Write: aRb or a is related to b if $(a,b) \in R$

$a \not{R} b$ or a is not related to b if $(a,b) \notin R$

The domain of a relation R from A to B is

$$\mathrm{Dom}(R) = \{a \in A \mid (\exists b \in B)\ aRb\}$$

and the range is

$$\mathrm{Rng}(R) = \{b \in B \mid (\exists a \in A)\ aRb\}$$

A relation from A to A is a relation on A.

Ex: The identity relation on A is $I_A = \{(a,a) \in A \times A\}$.

The inverse to a relation R

from A to B is the relation R^{-1} from B to A with

$$R^{-1} = \{(b,a) \mid (a,b) \in R\}.$$

Note: $I_A^{-1} = I_A$

Def: If R is a relation from A to B and S is a relation from B to C

Then the <u>composition</u> relation

Diagram

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

$$S \circ R = \{(a,c) \in A \times C \mid (\exists b \in B)\ (aRb) \wedge (bSc)\}$$

from A to C

Ex: ⓐ $I_B \circ R = R$

ⓑ $R \circ I_A = R$

$$\begin{tikzcd}
A \arrow[r, "I_A"] \arrow[rr, bend right, "R \circ I"'] & A \arrow[r, "R"] \arrow[rr, bend right, "I \circ R"'] & B \arrow[r, "I_B"] & B
\end{tikzcd}$$

Pf: Sketch:

Understand: R and $I_B \circ R$ are relations and hence sets

Logic: so we must show $I_B \circ R \subseteq R$ and $I_B \circ R \supseteq R$

Ass/Concl: • Assume $(a,b) \in I_B \circ R$ and show $(a,b) \in R$.

• Assume $(a,b) \in R$ and show $(a,b) \in I_B \circ R$.

Idea: ↳ If $(a,b) \in I_B \circ R$

then $(a,b) \in I_B \circ R = \{(a,b) \in A \times B \mid (\exists \tilde{b} \in B)(a R \tilde{b}) \wedge (\tilde{b} I_B b)\}$.

$$\begin{tikzcd}
b & \tilde{b} & a \\
\rotatebox[origin=c]{-90}{$\in$} & \rotatebox[origin=c]{-90}{$\in$} & \rotatebox[origin=c]{-90}{$\in$} \\
B & B \arrow[l, "I_B"'] & A \arrow[l, "R"'] \arrow[ll, bend left, "I_B \circ R"]
\end{tikzcd}$$

but $\tilde{b} I_B b$

iff $b = \tilde{b}$

so $(a R \tilde{b}) \wedge (\tilde{b} I_B b)$

iff $a R b$ and $b = \tilde{b}$

210217

Claim: -4 is not in the range of T

Proof: $\operatorname{Rng}(T) = \{y \mid (\exists x \in \mathbb{R}) \ x \, T \, y\}$.

$= \{y \mid (\exists x \in \mathbb{R}) \ x^2 = y\}$.

Assume for contradiction that $-4 \in \operatorname{Rng} T$.

Hence there is $x \in \mathbb{R}$ with $x^2 = -4 < 0$.

If $x \in \mathbb{R}$ then $x^2 \geq 0$.

Hence $x^2 \geq 0$ and $x^2 < 0$ a contradiction.

Therefore $-4 \notin \operatorname{Rng} T$.

Claim: If R is a relation from A to B.

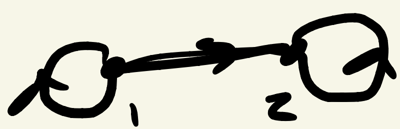
then $\mathrm{Dom}(R^{-1}) = \mathrm{Rng}(R)$.

Proof: $\mathrm{Rng}(R) = \{y \mid (\exists x \in A)\ xRy\}$

$= \{y \mid (\exists x \in A)\ y R^{-1} x\}$

$= \mathrm{Dom}(R^{-1})$.

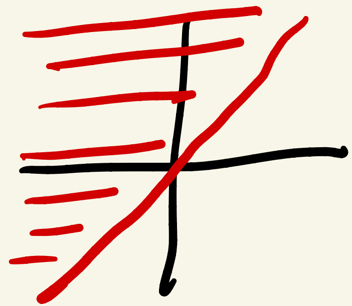
qed

Ex: $R =$ 

refl: Yes (all loops are there).

Sym: No: $1R2$ but $2 \not R 1$

trans: Yes. check for every pair of composable arrows.

Ex: $U =$  $= \{(x,y) \mid x \leq y\}$

refl: Yes: $\{(x,x) \mid x \in \mathbb{R}\} \subseteq U$

sym: No: $0 U 1$ but $1 \not U 0$.

trans: Yes: if x,y,z with $x \leq y$, $y \leq z$ then $x \leq z$.

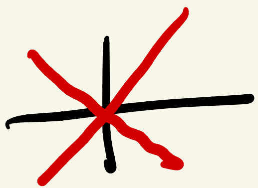
that is if $x, y, z \in \mathbb{R}$.

and $x \,\mathcal{U}\, y$ and $y \,\mathcal{U}\, z$

then $x \le y$ and $y \le z$

so $x \le z$

so $x \,\mathcal{U}\, z$.

Ex: $V =$  $= \{(x,y) \mid x=y \text{ or } x=-y\}$.

refl: Y since the line (x,x) is in V.

sym: Y since the graph is preserved by reflection over $x=y$

~~trans~~!

or!

if $x V y$

then either $y = x$ or $y = -x$

if $y = x$ then $y V x$.

if $y = -x$ then $y V x$

~~done~~

trans: Υ $V = \{(x,y) \mid x = y \text{ or } x = -y\}$

$= \{(x,y) \mid x^2 = y^2\}$

so if x, y, z with $x V y$, $y V z$

so $x^2 = y^2$ and $y^2 = z^2$

so $x^2 = z^2$ so $x V z$.

Hence V is an equivalence relation

Sketch:

Logic: Need $\Rightarrow$ and $\Leftarrow$] for iff.

$\Rightarrow$ Assume R is sym. and show: $\subseteq$ and $\supseteq$

$\Leftarrow$ Assume $R = R^{-1}$ and show symmetric.

210219

If R is a relation on a set A

define:

if $x \in R$ write $\bar{x} = \{y \in A \mid xRy\}$.

Write: $A/R = \{\bar{x} \mid x \in A\}$

a family of subsets of A.

Def: If A is a nonempty set and $\mathcal{F}$ is a family of subsets of A then $\mathcal{F}$ is a <u>partition</u> of A if

(i) $\emptyset \notin \mathcal{F}$

(ii) If $E, F \in \mathcal{F}$ then $[(E = F) \text{ or } (E \cap F = \emptyset)]$

(iii) $\displaystyle\bigcup_{E \in \mathcal{F}} E = A.$

Thm 3.3.1: If R is an equivalence relation on a nonempty set A then A/R is a partition of A.

210222

Ex: 7.a:

Find R an equiv. reln on $\mathbb{N}$ so that $\mathbb{N}/R = \{\{1, 2, \ldots, 9\}, \{10, \ldots, 99\}, \{100, \ldots 999\}, \ldots\}$.

Ans: $R = \{(a, b) \mid$ if a and b have the same number of digits$\}$.

§3.4: Mod. Arith:

Consider for any $m \in \mathbb{N}$

there is an equiv. reln: on $\mathbb{Z}$

$$R_m = \{(a,b) \mid m \text{ divides } a-b\}.$$

Write $\mathbb{Z}_m = \mathbb{Z}/R_m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{m-1}\}$

$\overline{0} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$

$\overline{m-1} = \overline{-1}$

and call this set the integers mod m.

Def: if $\bar{a}, \bar{b} \in \mathbb{Z}_m$, $k \in \mathbb{N}$ then:

$\bar{a} + \bar{b} = \overline{a+b}$ write $a+b \pmod m$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ $\quad a \cdot b \pmod m$

$\bar{a}^k = \overline{a^k}$ $\quad a^k \pmod m$

Claim: $+$ is well defined in $\mathbb{Z}_m$.

Equivalently:

Claim: If $\underbrace{a \equiv c \pmod m}_{\text{a is congruent mod m to c}}$ and $b \equiv d \pmod m$

then $a+b \equiv c+d \pmod m$

Proof: Since m divides $a-c$ and $b-d$

there ae integrs k and l with

$mk = a - c$ and $ml = b - d$

so $mk + ml = (a+b) - (c+d)$

$\parallel$

$m(k+l)$

so m divides $(a+b) - (c+d)$

so $a+b \equiv c+d \pmod{m}$

qed.

2 10224

Def: If A and B are sets then a function f from A to B is a relation from A to B with

(i) $\text{domain}(f) = A$

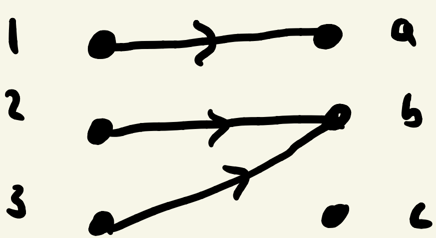
and (ii) if $a \in A$ and $b, c \in B$ with $(a,b) \in f$ and $(a,c) \in f$ then $b = c$.

Equiv:

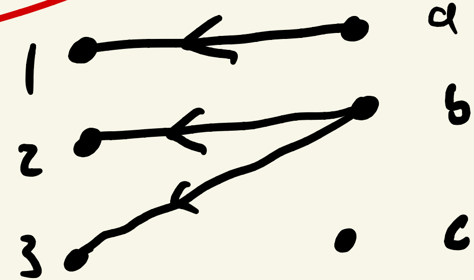
A relation f from A to B is a function iff

$$(\forall a \in A)\ (\exists!\, b \in B)\quad (a,b) \in f.$$

Ex: directed graph:



reln from $\{1,2,3\}$ to $\{a,b,c\}$



reln from $\{a,b,c\}$ to $\{1,2,3\}$

range $= \{a,b\}$

codom could be
$\{a,b\}$
$\{a,b,c\}$
$\{a,b,c,\varepsilon\}$
$\vdots$

Claim: Example 1 is a function:

$$f = \{(x,y) \in \mathbb{R}^2 \mid y = x^2 - 4\}.$$

Notation for functions:

If f is a function from A to B

write: $(a,b) \in f$ or equiv afb

or equiv $f(a) = b$

A <u>codomain</u> for a function is any set containing the range.

Sketch of proof:

U: Note: vertical line test holds ✓

L: (i) for domain: $\forall x \in \mathbb{R}$ have $\exists y$ $f(x)=y$.

(ii) for second (uniqueness) condition: $\forall$ $f(x)=y$ & $f(x)=z$

have $y=z$.

I: (i) $\forall x$ choose $y=x^2-4$ ✓

(ii) if $x^2-4=y$ & $x^2-4=z$

then $y=z$ ✓.

Ex: If A is any set then $I_A = \{(a,a) \mid a \in A\}$ is a function from A to A called the <u>identity</u> on A.

Note: this relation is also an equivalence relation.

Sketch: U: see above I_A is both,

L: Need to show $f \subseteq I_A$

Ass: f is a fn and eqv reln.

and $f \supseteq I_A$.

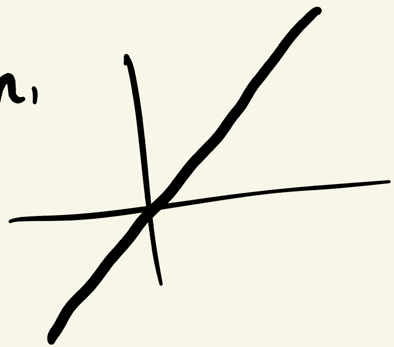
I: $\supseteq$ since f is an eq-reln

f is reflexive

so $\forall a \in A$ have $(a,a) \in f$.

$\subseteq$ since f is a function,

if $f(a) = b$ and $f(a) = c$ then $b = c$



but $f(a) = a$ since $I_A \subseteq f$.

An attempt to define a function using a relation which is not one is called <u>not well defined</u>.

216226

Sketch:

U: The relation is

$$f = \{(\bar{x}, [x]) \mid x \in \mathbb{Z}\}.$$

$$= \{(\bar{0}, [0]), (\bar{1}, [1]), \ldots \}.$$

L: Want to show f is not a function.

$\sim$ [ⓘ $\forall a \in \mathbb{Z}_3 \quad \exists b \in \mathbb{Z}_6$ with $(a,b) \in f$.

and ⓘⓘ $\forall a \in \mathbb{Z}_3, \; b, c \in \mathbb{Z}_6$ with $(a,b), (a,c) \in f$.

have $b = c$]

$\sim$ i or $\sim$ iv.

I: $\sim$ ii is likely the problem:

$\{(\bar{0}, [0]) \ldots, (\bar{3}, [3])$

$\bar{3} = \bar{0}$, $[3] \neq [0]$

$\therefore \sim$ ii, $\exists\, a \in \mathbb{Z}_3,\ b, c \in \mathbb{Z}_6$ with $(a,b), (a,c) \in f$

$\sim (b = c)$

$(b \neq c)$,

Recall: $\bar{x}, \bar{y} \in \mathbb{Z}_3$

then $\bar{x} = \bar{y}$ if 3 divides $x - y$.

$[x], [y] \in \mathbb{Z}_6$

then $[x] = [y]$ if 6 divides $x-y$

eg: $\bar{0}, \bar{3} \in \mathbb{Z}_3$ and 3 divides $0-3=-3$ ✓

Sketch:

u: $g = \{([x], \bar{x}) \mid x \in \mathbb{Z}\}$, $= \{([0], \bar{0}), \dots\}$,

Note: $g = f^{-1}$ the inverse relation.

L: (i) $\forall a \in \mathbb{Z}_6 \quad \exists\, b \in \mathbb{Z}_3$ with

$(a,b) \in g$

(ii) $\forall a \in \mathbb{Z}_6, \quad b, c \in \mathbb{Z}_3$ with

$(a,b), (a,c) \in g$ have $b = c$.

I: (i) $\forall a \in \mathbb{Z}_6 \quad \exists\, n \in \mathbb{Z}$ with $a = [n]$

and $([n], \bar{n}) \in g$ so take $b = \bar{n}$ ✓.

(ii) If $a \in \mathbb{Z}_6$ and $b, c \in \mathbb{Z}_3$

with $(a,b), (a,c) \in \mathcal{G}$

so there is $n \in \mathbb{Z}$ with $a = [n]$

and $k, l \in \mathbb{Z}$ with $b = \overline{k}$

$c = \overline{l}$

and $([k], \overline{k}) = (a,b)$

$([l], \overline{l}) = (a,c)$

so $[k] = [l]$

so 6 divides $k-l$ so $k-l = 6t$

$= 3\cdot(2t)$

so 3 divides $k-l$ so $\overline{k} = \overline{l}$ so $b = c$.

More functions:

Characteristic functions:

If S is a subset of A

then $\chi_S = \{(s,1) \mid s \in S\} \cup \{(a,0) \mid a \in A - S\}$

is a function from A to $\{0,1\}$.

In particular $\chi_S(s) = 1$ if $s \in S$

$\chi_S(a) = 0$ if $a \in A$ and $a \notin S$

Inclusion functions:

If S is a subset of A

the $i_S = \{(s,s) \mid s \in S\}$.

from S to A.

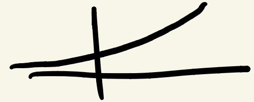
Restrictions of functions:

If S is a subset of A

and f is a function from A to B

then $f|_S = \{(s, f(s)) \mid s \in S\}$

from S to B

Examples: 

Consider: $f(x) = e^x$ from $\mathbb{R}$ to $\mathbb{R}$ or $\mathbb{R}_{>0}$

and $g(x) = x+3$ from $\mathbb{R}$ to $\mathbb{R}$

Find: $f^{-1}(x) = \ln(x)$ from $\mathbb{R}_{>0}$ to $\mathbb{R}$

$g^{-1}(x) = x-3$ from $\mathbb{R}$ to $\mathbb{R}$

$(f \circ g)(x) = e^{x+3}$ from $\mathbb{R}$ to $\mathbb{R}_{>0}$

$(g \circ f)(x) = e^x + 3$ from $\mathbb{R}$ to $\mathbb{R}$

or $\mathbb{R}$ to $\mathbb{R}_{>0}$

Claim 4.2.1: If g & f are functions as above then $g \circ f$ is a function.

Claim 4.21: If g is a function from B to C and f is a function from A to B then $g \circ f$ is a function from A to C.

Proof: For existence:

If $a \in A$ then $f(a) = b$ is in B so $g(b)$ is in C and (a, c) is in $g \circ f$.

For uniqueness:

If (a, c) and $(a, \tilde{c})$ are in $g \circ f$ then there are b and $\tilde{b}$ with

(a,b) and $(a,\tilde{b})$ in f so $b=\tilde{b}$

and (b,c) and $(b,\tilde{c})$ in g so $c=\tilde{c}$.

qed.

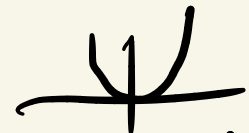
§4.3:

Def: A function f from A to B is <u>onto</u> or <u>surjective</u> if $\text{range}(f)=B$.

A function g from A to B is <u>one to one</u> or <u>injective</u> if every x and y in A with $f(x)=f(y)$ has $x=y$.

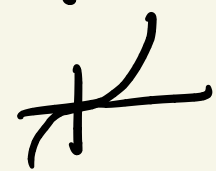
Examples: Which of the following are onto and/or one to one as functions from $\mathbb{R}$ to $\mathbb{R}$?

① $x^2 = f(x)$



② $e^x = g(x)$

③ $x^3 = h(x)$



Note: g is one to one if every horizontal line hits the graph at most once.

f is surjective if every horizontal line hits the graph at least once.

$$\begin{tikzcd} c & b \arrow[l, mapsto] & a \arrow[l, mapsto] \\ \rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} \\ C & B \arrow[l, "g"'] & A \arrow[l, "f"'] \arrow[ll, bend left, "g\circ f"] \end{tikzcd}$$

Sketch:

U: Need

L: $\forall c \in C$ want $\exists b \in B$ with $g(b) = c$.

I: Know: $g \circ f$ is onto so $\exists a \in A$ with $(g \circ f)a = c$

$$\begin{array}{l} (g\circ f)a = c \\ \quad \| \\ g(f(a)) = g(b) \quad \checkmark \end{array}$$

so take $b = f(a)$ in B

Sketch:

L: $P \not\Rightarrow Q$

$\to P$

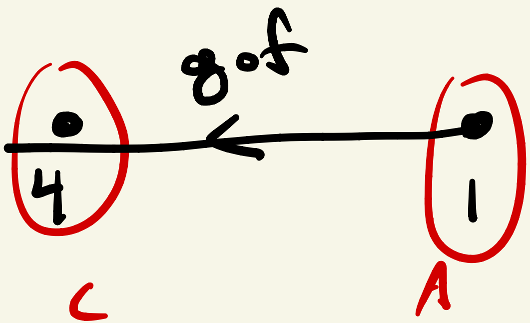
Q is f is onto

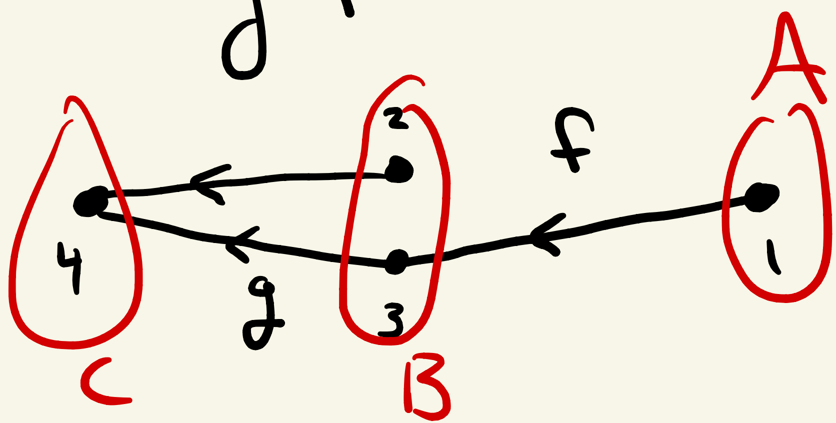
equivalent:

$\exists\, f, g$ as above with f not onto.

I: Find an example:

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





If $A \subseteq B$

restriction: If $f : B \longrightarrow C$

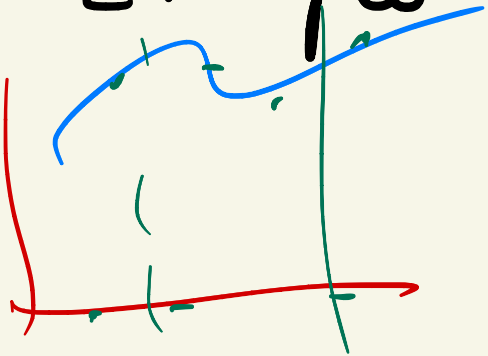
then the restriction of f to A

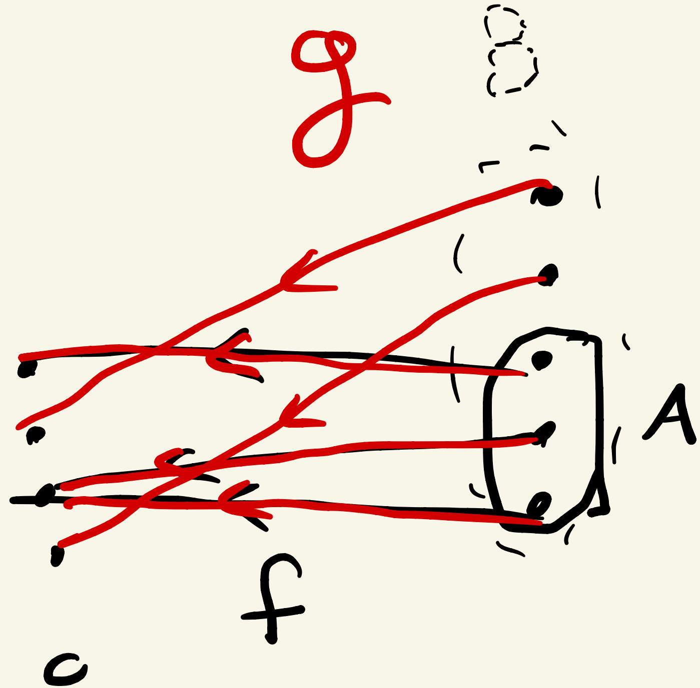
is $f|_A : A \longrightarrow C$

with $f|_A(a) = f(a)$

extension: f is an <u>extension</u> of $f|_A$.

Example:





f is a fn from A to C

an ext. g to B of f

210303

Cor 4.4.3:

If a relation f from A to B is a bijective function then the relation f^{-1} from B to A is also a bijective function.

Proof: Assume f is a relation from A to B which is a bijective function.

Since f is bijective if b is in B

there is a unique a in A with (a, b) in f or equivalently (b, a) in f^{-1}

so f^{-1} is a function.

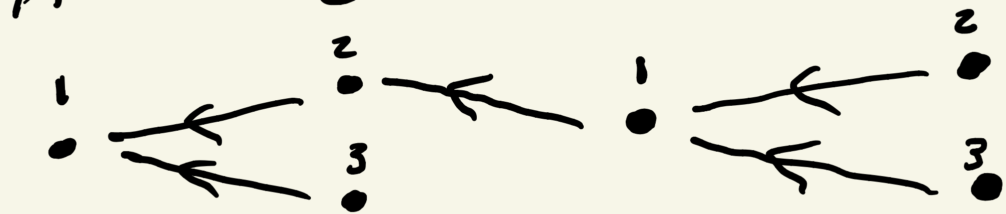
Since f is a function if a is in A there is a unique b in B with (a, b) in f or equivalently (b, a) in f^{-1}

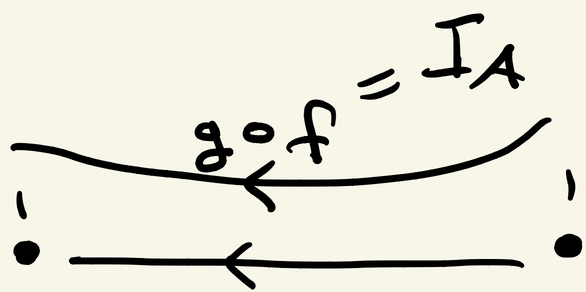
so f^{-1} is a bijection. qed.

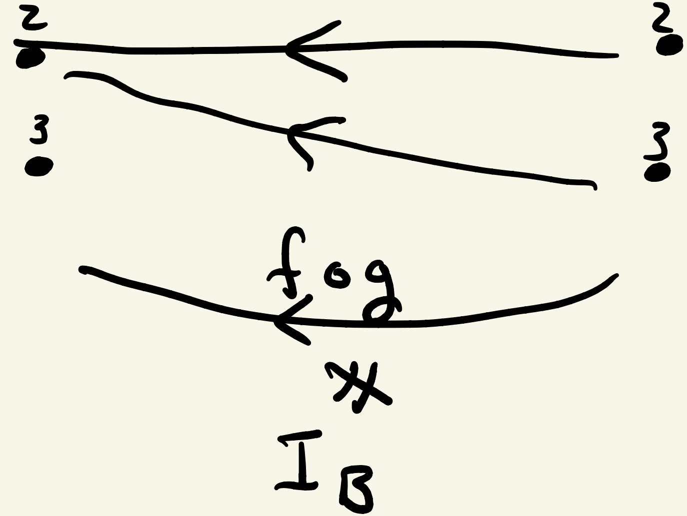
Sketch for Claim:

Existential so look for an example.

$$A \xleftarrow{g} B \xleftarrow{f} A \xleftarrow{g} B$$







Sketch for Thm 4.4.4.a:

L: iff so need $\Rightarrow$ and $\Leftarrow$ — two things,

$\Rightarrow$ Assume $f=g^{-1}$ and

show 4 things;

$g \circ f \subseteq I_A$

$g \circ f \supseteq I_A$

$f \circ g \subseteq I_B$

$f \circ g \supseteq I_B$

$\Leftarrow$ Assume $g \circ f = I_A$ and $f \circ g = I_B$

and show 2 things:

$f \subseteq g^{-1}$

$f \supseteq g^{-1}$

I: $\Rightarrow$ If $(a, \tilde{a}) \in g \circ f$

then $\exists\, b \in B$ with

$(a, b) \in f$ and $(b, \tilde{a}) \in g$.

hence ~~$(\tilde{a}, b) \in f = g^{-1}$~~

~~and since f is a fn. $a = \tilde{a}$.~~

hence $(b, a) \in g = f^{-1}$

and since g is a fn.

have $a = \tilde{a} = g(b)$,

therefore $g \circ f \subseteq I_A$

Claim: $f: \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$

1 with $f(\bar{x}) = (\bar{x})^2$ is not a bijection

Claim: $f: \mathbb{Z}_5 \to \mathbb{Z}_5$

2 with $f(\bar{x}) = (\bar{x})^3$ is a bijection.

Claim: $f: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

3 with $f((a,b)) = 2^{a-1}(2b-1)$

is a bijection.

210305

Proof of Claim 3:

f is onto since if n is a natural number then $n = 2^{\alpha}\beta$ with β odd, $\alpha \geq 0$ and $\beta \geq 1$.

Take $a = \alpha+1$ and $b = \frac{\beta+1}{2}$. Hence $f((a,b)) =$

$$2^{\alpha}\left(2\frac{\beta+1}{2} - 1\right) = n$$

f is 1-1 since if $2^{a}(2b-1) = 2^{\tilde{a}}(2\tilde{b}-1)$ and if (for contradiction) $a > \tilde{a}$ then $2^{a-\tilde{a}}(2b-1) = 2\tilde{b}-1$ is both even and odd (a contradiction) so $a \leq \hat{a}$.

similarly $\tilde{a} \leq a$ so $a = \tilde{a}$.

Hence $2^{a-1}(2b-1) = 2^{a-1}(2\tilde{b}-1)$

so $2b-1 = 2\tilde{b}-1$

so $b = \tilde{b}$. qed.

Example: Some bijections:

(a) $a : (0,1) \longrightarrow (0,3)$

with $a(x) = 3x$ is a bijection.

Check: since if $g(y) = \frac{1}{3} y$

Check: $(a \circ g)(y) = a(g(y)) = 3 \cdot \frac{1}{3} y = y$

so $a \circ g = I_{(0,3)}$

and $(g \circ a)(x) = g(a(x)) = \frac{1}{3} \cdot 3 \cdot x = x$

so $g \circ a = I_{(0,1)}$

Find a bijection

$f: (0,1] \longrightarrow (0,1)$

and find $f(\frac{1}{2})$ and $f(\frac{1}{\pi})$

and $f(1)$.

Using: $b:(0,1) \longrightarrow (1,\infty)$ is a bijection.
$$b(x) = \frac{1}{x}$$

and $c:(0,1] \longrightarrow [1,\infty)$ is a bijection
$$c(x) = \frac{1}{x}$$

and $d: \mathbb{W} = \{0,1,2,\dots\} \longrightarrow \mathbb{N}$ is a bijection
$$d(n) = n+1$$

and $$e : [1, \infty) \longrightarrow (1, \infty)$$

$$e(x) = \begin{cases} x+1 & \text{if } x \in \mathbb{N} \\ x & \text{otherwise} \end{cases}$$ is a bijct.

210308

Some counting: If $\bar{\bar{A}} = 3$ find:

(a) $\overline{\overline{A \times A}}$

(b) $\overline{\overline{\mathcal{P}A}}$

(c) $\overline{\overline{\mathcal{P}(A \times A)}}$

$f \subseteq A \times A$

(d) $\overline{\overline{\{f \mid f \text{ is a relation from } A \text{ to } A\}}}$

equiv to partitions

(e) $\overline{\overline{\{f \mid f \text{ is an equivalence reln on } A\}}}$

(f) $\overline{\overline{\{f \mid f \text{ is a function from } A \text{ to } \mathbb{N}_2\}}}$

$\mathbb{N}_2 = \{1, 2\}$

(g) $\overline{\overline{\{f \mid f \text{ is a function from } A \text{ to } A\}}}$

(h) $\overline{\overline{\{f \mid f \text{ is a bijection from } A \text{ to } A\}}}$

Ans: (a) $\overline{\overline{A \times A}} = \bar{\bar{A}} \cdot \bar{\bar{A}} = 3 \cdot 3 = 9$

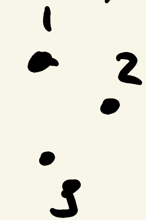
(b) $\overline{\overline{\mathcal{P}A}} = 2^{\bar{\bar{A}}} = 2^3 = 8$

(c) $\overline{\overline{\mathcal{P}(A \times A)}} = 2^9 = 512$

(d) the same as (c) since a sub set of $A \times A$ is the same as a reln from A to A. so 512 possible relations.

(e) the same as $\overline{\overline{\{\text{partitions of } \{1,2,3\}\}}}$

$$= \overline{\overline{\{\{\{1,2,3\}\}, \{\{1,2\},\{3\}\}, \{\{1,3\},\{2\}\}, \{\{2,3\},\{1\}\}, \{\{1\},\{2\},\{3\}\}\}}}.$$



$$= 5$$

(f) $\overline{\overline{\mathbb{N}_2}}^{\overline{\overline{A}}} = 2^3 = 8$

(g) $\overline{\overline{A}}^{\overline{\overline{A}}} = 3^3 = 27$

(h) $6 = \overline{\overline{A}}!$

- 3 choices $\quad 3 \cdot$
- 2 choices $\quad 2 \cdot$
- 1 choice $\quad 1$

Thm: 5.1.1

$\approx$ is an equivalence relation on the collection of sets.

Proof: Need to check:

→ symmetry.

- reflexivity.
- transitivity.

Check: symmetry: Need: If $A \approx B$ then $B \approx A$.

That is if $\exists f : A \to B$ a bij. function

then $\exists g : B \to A$ a bij. function

Proof: Assume $f: A \to B$ is a bij. function. Hence $f^{-1}: B \to A$ is also a bij. function. qed.

Overview of small cardinalities: no two columns are equivalent.

$\overline{\overline{\mathcal{P}\mathbb{N}}} \not\approx \mathbb{Q} \approx \mathbb{Q}_{>0} \approx \mathbb{N}\times\mathbb{N}$

$\mathbb{N}\times\mathbb{N} \approx \mathbb{Z} \supseteq \mathbb{W} \supseteq \mathbb{N}$

$(0,1] \not\approx \overline{\overline{\mathcal{P}(0,1)}}$

$(0,1] \supseteq \mathbb{R} \supseteq (a,b) \supseteq (0,1)$

$\emptyset \quad \mathbb{N}_1 \not\approx \mathbb{N}_2 \cdots \not\approx \mathbb{N}_n \not\approx \cdots \not\approx \mathbb{N} \not\approx (0,1)$

A

$0 \quad 1 \quad 2 \ldots n \ldots \quad \aleph_0 \quad c$

name of $\bar{\bar{A}}$

Thm: If $r < n$ then $\mathbb{N}_r \not\cong \mathbb{N}_n$.

Proof strategy:

Show there is no $\mathbb{N}_n \xrightarrow{f} \mathbb{N}_r$ which is injective (so no bijection)

Use induction. with $P(n)$ the proposition that $\forall r < n \ \nexists \ f: \mathbb{N}_n \longrightarrow \mathbb{N}_r$ which is injective.

Possible base steps for induction:

P(1) means: there is no injective map from $\{1\}$ to φ

which is true since the is no function from $\{1\}$ to φ.

P(2) means: there is no injective map from $\{1,2\}$ to $\underbrace{\{1\}}_{r=1}$ or $\underbrace{\varphi}_{r=0}$

but there is only one fn $f: \{1,2\} \to \{1\}$ and $f(1) = f(2) = 1$ so not inj.

and there are no ~~maps~~ fns from $\{1,2\}$ to φ.

210310

Thm 5.2.1: If $n \in \mathbb{N}$ then

$\mathbb{N}_n \not\approx \mathbb{N}$. ($\mathbb{N}$ is infinite),

Proof Plan: Show $\nexists\ f : \mathbb{N} \to \mathbb{N}_n$

injective.

Use 5.1.9: $\nexists\ g : \mathbb{N}_{n+1} \to \mathbb{N}_n$ injective.

Use contradiction.

Assume $f : \mathbb{N} \to \mathbb{N}_n$ is injective.

Hence $f|_{\mathbb{N}_{n+1}} : \mathbb{N}_{n+1} \to \mathbb{N}_n$ is injective.

a contradiction. q.e.d.

Proof of 5.2.4:

Assume $f: \mathbb{N} \to (0,1)$.

Write a_n for the n^{th} decimal digit of $f(n)$

and choose $b_n \neq a_n$ and $B \in (0,1)$

with digits b_n.

Claim: $B \notin \mathrm{Im}(f)$ so f is not onto.

Pf of claim: For contradiction assume $f(m) = B$

so $a_m = b_m$ a contradiction.

q.e.d.

Proof of 5.4.3:

Assume $f: A \to \mathcal{P}(A)$

Write $B = \{a \in A \mid a \notin f(a)\}$

Claim $B \notin \mathrm{Im}(f)$ so f is not onto.

Pf of claim:

For contradiction assume $f(a) = B$

Two cases: ① $a \in B$

or ② $a \notin B$.

In case ① $a \in f(a)$ so $a \notin B = f(a)$

a contradiction.

In case ② $a \notin f(a)$ so $a \in B = f(a)$

another contradiction. q.e.d.

210312 (Reread §1.7)

Proofs: Methods:

direct.
cases
contrapositive (not the converse).
contradiction
induction (PMI, Generalized).

Possible hints from logic:

$\forall$	start with	suppose	maybe direct
$\exists$	" "	choose	maybe construct

iff or $\Leftrightarrow$ two things $\Rightarrow$ { $\Leftarrow$

$=$ sets " " $\subseteq$ { $\supseteq$

Office hrs at 1 on Monday.

Ans: Outline @:

Need to show: reflexive (r)

symmetric (s)

transitive. (t)

Idea: (r): $\forall x \in \mathbb{R}$ $(x,x) \in S$

since $x - x = 0 \in \mathbb{Q}$ ✓

(s): $\forall x, y \in \mathbb{R}$ $(x,y) \in S \Rightarrow (y,x) \in S$

Assume $x - y \in \mathbb{Q}$

hence $-(x-y) = y - x \in \mathbb{Q}$ ✓

(t) $\forall x, y, z \in \mathbb{R}$ $[(x,y) \in S] \wedge ((y,z) \in S)$

$\Longrightarrow (x,z) \in S.$

Assume $x - y \in \mathbb{Q}$ and $y - z \in \mathbb{Q}$

hence $x - y + y - z = x - z \in \mathbb{Q}$ ✓

ⓒ Show $\overline{\Pi}$ is denumerable:

Proof idea: Need $\overline{\overline{\pi}} \approx \mathbb{N}$

or equiv: $\exists\ \overline{\overline{\pi}} \xrightarrow{f} \mathbb{N}$ a bijection

Note also know: (denumerable means $\overline{\overline{A}} = \aleph_0$),

$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{Z}$, $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$, $\mathbb{Q}$

so it suffices to find a bijctn.

from $\overline{\overline{\pi}}$ to any of

(Proved last time: $\nexists\ \mathbb{N} \xrightarrow{f} \mathbb{R}$ with f onto so $\overline{\overline{\mathbb{N}}} \neq \overline{\overline{\mathbb{R}}}$)

Consider $\overline{\overline{\pi}} \xrightarrow{f} \mathbb{Q}$

with $f(x) = x - \pi$

since $x \in \overline{\pi}$ know $(\pi, x) \in S$

so $\pi - x \in \mathbb{Q}$.

so $x - \pi \in \mathbb{Q}$.

eg $f(\underbrace{\pi + \tfrac{2}{3}}_{\in \overline{\pi}}) = \dfrac{2}{3}$

$$\frac{2}{3} = \pi + \frac{2}{3} - \pi$$

Finally: show f is a bijection:

How to do this: [Find an inverse to f.

or $\begin{cases} \text{show onto} \\ \text{and show 1-1} \end{cases}$ ✓

Consider $g(y) = y + \pi$

check: $(f \circ g)(y) = \cancel{g}\, f(g(y)) = f(y+\pi) = y$

and $(g \circ f)(x) = g(f(x)) = g(x-\pi) = x$

q.e.d.

Direct Proof of onto

Need: $\forall\, y \in \mathbb{Q}\ \exists\, x \in \overline{\pi}$ with $f(x) = y$.

Pf: Assume $y \in \mathbb{Q}$ take $x = y + \pi$

so $f(x) = f(y+\pi) = y + \pi - \pi = y$

$$\boxed{f(x) = x - \pi}$$

and $x \in \overline{\pi}$ since

$\pi - x = \pi - (y + \pi) = -y \in \mathbb{Q}.$

q'

$$\overline{\pi} = \{x \mid \pi - x \in \mathbb{Q}\}$$