Set Theory Review

natural numbers → $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$

integers → $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

rational numbers → $\mathbb{Q} = \left\{ \frac{x}{y} \mid \begin{array}{c} x, y \in \mathbb{Z} \\ y \neq 0 \end{array} \right\}$

real numbers → $\mathbb{R} = \{ x \mid x \text{ has a decimal expansion} \}$

$= \{\sqrt{3} \approx 1.732, 1 = 1.0, \frac{1}{2} = 0.5, \ldots\}$

$\{ \text{description of elements} \mid \text{condition on elements} \}$

Notation: Let A be a set. If x is in A we write $x \in A$. Otherwise we write $x \notin A$.

Def:

We s
if ev
an el

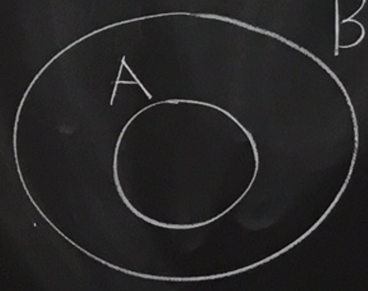
...A.
...A.

...mal}

..., $\frac{1}{2} = 0.5, \ldots$}

Def: Let A and B be sets.

We say that A is a subset of B if every element of A is also an element of B.



If A is a subset of B then we write $A \subseteq B$.

(Some people just write $A \subset B$.)

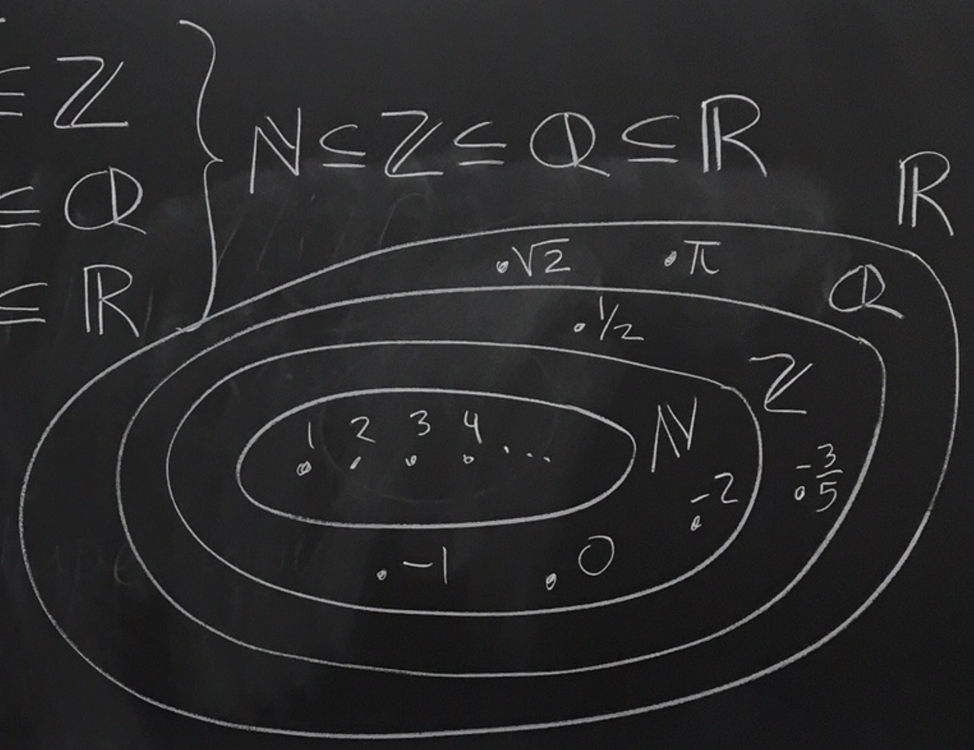
Ex:

$\mathbb{N} \subseteq \mathbb{Z}$

$\mathbb{Z} \subseteq \mathbb{Q}$

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

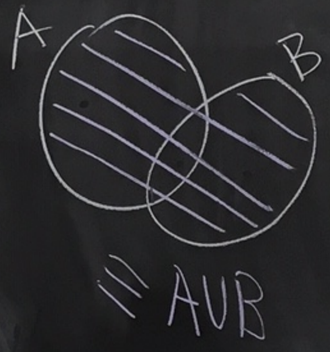


Method to show $A = B$ when A and B are sets

1. Show $A \subseteq B$
2. Show $B \subseteq A$

Def: Let A and B be sets.
The union of A and B is

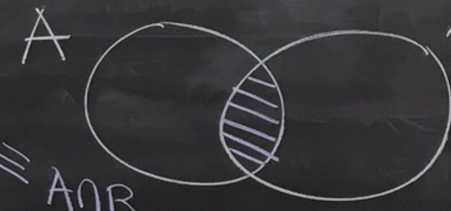
$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$



$\equiv A \cup B$

The intersection of A and B is

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



$\equiv A \cap B$

P	Q	P or Q	P and Q	If P, then Q
T	T	T	T	T
T	F	T	F	F
F	T	T	F	T
F	F	F	F	T

Ex: $A = \{1, 5, 7, 13, -\frac{1}{2}, \sqrt{2}\}$

$B = \{\sqrt{2}, 0, 52, -3.5, 7\}$

"$\underbrace{7 \in A}_{T}$ or $\underbrace{7 \in B}_{T}$" is True

So, $7 \in A \cup B$

$A \cup B = \{1, 5, 7, 13, -\frac{1}{2}, \sqrt{2}, 0, 52, -3.5\}$

"$\underbrace{0 \in A}_{T}$ or $\underbrace{0 \in B}_{F}$" is True

So, $0 \in A \cup B$

$A \cap B = \{\sqrt{2}, 7\}$

"$\underbrace{\sqrt{2} \in A}_{T}$ and $\underbrace{\sqrt{2} \in B}_{T}$" is True

So, $\sqrt{2} \in A \cap B$

Ren Q

EPSON

Ex: Let C, D, E be sets.

Prove that $C \cap (D \cup E) = (C \cap D) \cup (C \cap E)$

$C = \{1, 2, 3, 4, 5$
$D = \{3, 5, 7$
$E = \{2, 1, -6$

Proof:

$\subseteq$ We first show that $C \cap (D \cup E) \subseteq (C \cap D) \cup (C \cap E)$.

Let $x \in C \cap (D \cup E)$.

So, $x \in C$ and $x \in D \cup E$.

Thus, $x \in C$ and $(x \in D$ or $x \in E)$

$C = \{1, 2, 3, 4, 5\}$
$D = \{3, 5, 7\}$
$E = \{2, 1, -6\}$

$D \cup E = \{1, 2, 3, 5, 7, -6\}$
$C \cap (D \cup E) = \{1, 2, 3, 5\}$ ⟵

$C \cap D = \{3, 5\}$ $C \cap E = \{1, 2\}$
$(C \cap D) \cup (C \cap E) = \{1, 2, 3, 5\}$ ⟵

Hooray! They're equal

$\ldots \cap D) \cup (C \cap E)$.

⟹ So either
① $x \in C$ and $x \in D$
or ② $x \in C$ and $x \in E$

case 1: Suppose $x \in C$ and $x \in D$.
Then $x \in C \cap D$.
Hence $x \in (C \cap D) \cup (C \cap E)$.

case 2: Suppose $x \in C$ and $x \in E$.
Then, $x \in C \cap E$.
Ergo, $x \in (C \cap D) \cup (C \cap E)$.

⟹ So, in either case
$x \in (C \cap D) \cup (C \cap E)$.
Thus, if $x \in C \cap (D \cup E)$
then $x \in (C \cap D) \cup (C \cap E)$.

So,
$C \cap (D \cup E) \subseteq (C \cap D) \cup (C \cap E)$.

(2) Let's now show $(C \cap D) \cup (C \cap E) \subseteq C \cap (D \cup E)$

Let $w \in (C \cap D) \cup (C \cap E)$

So, $w \in C \cap D$ or $w \in C \cap E$.

case 1: Suppose $w \in C \cap D$.
Then $w \in C$ and $w \in D$.
Since $w \in D$ we know $w \in D \cup E$.
It follows that $w \in C$ and $w \in D \cup E$.
Consequently, $w \in C \cap (D \cup E)$.

case 2: Suppose $w \in C \cap E$.
Then $w \in C$ and $w \in E$.
Since $w \in E$ we know $w \in D \cup E$.
Since $w \in C$ and $w \in D \cup E$
we know $w \in C \cap (D \cup E)$.

$\triangleright$ We have show that if $w \in (C \cap D) \cup (C \cap E)$ then we must have $w \in C \cap (D \cup E)$.

So, $(C \cap D) \cup (C \cap E) \subseteq C \cap (D \cup E)$.

Therefore by parts $\boxed{\subseteq}$ and $\boxed{\supseteq}$ we know $(C \cap D) \cup (C \cap E) = C \cap (D \cup E)$.

$\square$

Weds, 8/28

Def: We say that two sets A and B are disjoint if $A \cap B = \emptyset$.

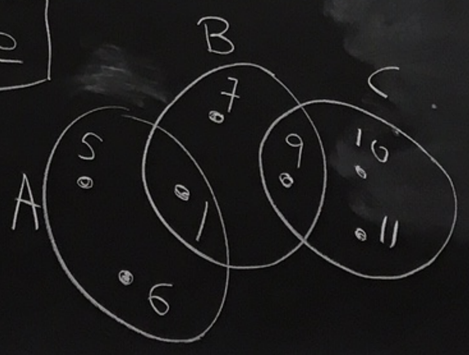
Ex: $A = \{1, 2, 4\}$
$B = \{7, 3\}$
$A \cap B = \emptyset$
So A and B are disjoint.

HW 2

⑦ Let A, B, C be sets.

Prove or disprove:
If $A \cap B \neq \emptyset$ and $B \cap C \neq \emptyset$ then $A \cap C \neq \emptyset$.

False



$A = \{1, 5, 6\}$
$B = \{1, 7, 9\}$
$C = \{9, 10, 11\}$

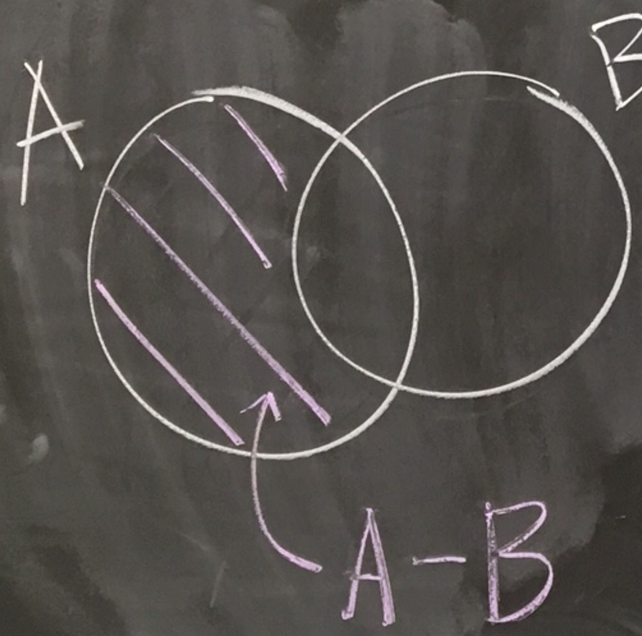
$A \cap B = \{1\} \neq \emptyset$
$B \cap C = \{9\} \neq \emptyset$
but
$A \cap C = \emptyset$.

This is called a counterexample.

Def: Let A and B be sets.

The **difference** of A and B is

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



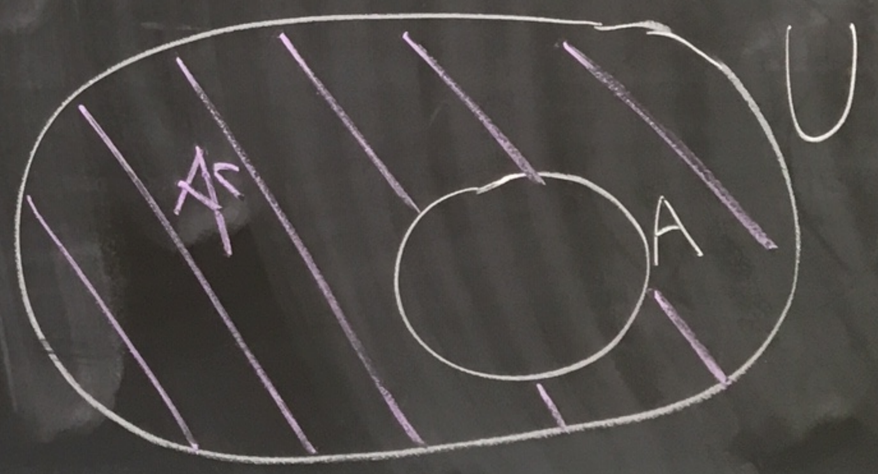
Ex: $A = \{\sqrt{2}, 4, 7, \frac{11}{3}, \pi^2\}$

$B = \{5, 7, \pi, 10, \frac{11}{3}\}$

$A - B = \{\sqrt{2}, 4, \pi^2\}$

Sometimes we have a "universal set" or "universe" that all our sets live in.

Def: Let A be a set where U is a universal set. The **complement** of A, denoted by $\overline{A}$ or A^c or A', is the set $A^c = U - A$.



Theorem: Let A and B be sets where U is a universal set. Then

① $(A \cup B)^c = A^c \cap B^c$

② $(A \cap B)^c = A^c \cup B^c$

(de Morgan's laws)

proof: ① ($\subseteq$) First let's show $(A \cup B)^c \subseteq A^c \cap B^c$.

Let $x \in (A \cup B)^c$.

So $x \in U - (A \cup B)$.

Thus $x \notin A \cup B$.

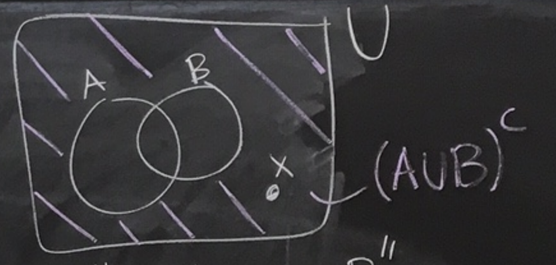
So the following is not true: "$x \in A$ or $x \in B$"

means $x \in A \cup B$

So, $x \notin A$ and $x \notin B$.

Thus, $x \in A^c$ and $x \in B^c$.

Ergo, $x \in A^c \cap B^c$.



$\neg$(P or Q) is ($\neg$P) and ($\neg$Q)

($\Leftarrow$) Now we show that $A^c \cap B^c \subseteq (A \cup B)^c$.

Let $x \in A^c \cap B^c$.

Then $x \in A^c$ and $x \in B^c$

So, $x \notin A$ and $x \notin B$.

Hence $x \notin A \cup B$.

Consequently $x \in (A \cup B)^c$.

By ($\Rightarrow$) and ($\Leftarrow$) we have $(A \cup B)^c = A^c \cap B^c$ ▨

T

P

Simpler:

$x \in (A \cup B)^c$

iff $x \notin A \cup B$

iff $x \notin A$ and $x \notin B$

iff $x \in A^c$ and $x \in B^c$

iff $x \in A^c \cap B^c$.

So, $(A \cup B)^c = A^c \cap B^c$.

Def: Let A and B be two sets.
The Cartesian product (or cross product)
of A and B is

$$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}$$

Ex: $A = \{1, -1, e\}$
$B = \{0, e\}$

$A \times B = \{(1,0), (1,e), (-1,0), (-1,e), (e,0), (e,e)\}$

For ordered pairs
by definition

$$(x,y)=(w,z)$$

if and only if

$$x=w \text{ and } y=z.$$

Wiener's definition [edit]

Norbert Wiener proposed the first set theoretical definition of the ordered pair in 1914:[6]

$$(a, b) := \{\{\{a\}, \emptyset\}, \{\{b\}\}\}.$$

He observed that this definition made it possible to define the types of *Principia Mathematica* as sets. *Principia Mathematica* had taken types, and hence relations of all arities, as primitive.

Wiener used {{*b*}} instead of {*b*} to make the definition compatible with type theory where all elements in a class must be of the same "type". With *b* nested within an additional set, its type is equal to $\{\{a\}, \emptyset\}$'s.

Hausdorff's definition [edit]

About the same time as Wiener (1914), Felix Hausdorff proposed his definition:

$$(a, b) := \{\{a, 1\}, \{b, 2\}\}$$

"where 1 and 2 are two distinct objects different from a and b."[7]

Kuratowski's definition [edit]

In 1921 Kazimierz Kuratowski offered the now-accepted definition[8][9] of the ordered pair (*a*, *b*):

$$(a,\ b)_K\ :=\ \{\{a\},\ \{a,\ b\}\}.$$

Note that this definition is used even when the first and the second coordinates are identical:

$$(x,\ x)_K = \{\{x\}, \{x,\ x\}\} = \{\{x\},\ \{x\}\} = \{\{x\}\}$$

Given some ordered pair *p*, the property "*x* is the first coordinate of *p*" can be formulated as:

$$\forall Y \in p : x \in Y.$$

The property "*x* is the second coordinate of *p*" can be formulated as:

$$(\exists Y \in p : x \in Y) \wedge (\forall Y_1, Y_2 \in p : Y_1 \neq Y_2 \rightarrow (x \notin Y_1 \vee x \notin Y_2)).$$

In the case that the left and right coordinates are identical, the right conjunct

Def: Let A be a set.

We define the power set of A to be the set of all subsets of A, that is

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

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

subsets of A

ϕ

$\{1\}$

$\{2\}$

$\{1, 2\}$

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

Note: $\phi \subseteq A$ for any set A

Def: $X \subseteq Y$ means

$(\forall x)(\text{If } x \in X, \text{ then } x \in Y)$

$(\forall x)(\text{If } x \in \phi, \text{ then } x \in A)$ ← True

F

T

Weds 9/4

Recall: Let A be a set.

The power set of A is

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

$$\mathcal{P}(\{a,b\}) = \{ \phi, \{a\}, \{b\}, \{a,b\} \}$$

Theorem: Let X and Y be sets. Then $X = Y$ if and only if $\mathcal{P}(X) = \mathcal{P}(Y)$.

Proof:

($\Rightarrow$) If $X = Y$, then $\mathcal{P}(X) = \mathcal{P}(Y)$.

($\Leftarrow$) Suppose $\mathcal{P}(X) = \mathcal{P}(Y)$.

We want to show that $X = Y$.

To show $X = Y$ we will show $X \subseteq Y$ and $Y \subseteq X$.

$\boxed{X \subseteq Y}$:

We know that $X \subseteq X$.

So $X \in \mathcal{P}(X)$.

But $\mathcal{P}(X) = \mathcal{P}(Y)$ so $X \in \mathcal{P}(Y)$.

So, $X \subseteq Y$.

$\boxed{Y \subseteq X}$: The same proof as above with X & Y interchanged shows that $Y \subseteq X$.

$\therefore$ Since $X \subseteq Y$ and $Y \subseteq X$ we have $X = Y$. ▨

A different approach to show $X \subseteq Y$ in the previous proof:

Let $a \in X$.

Then $\{a\} \subseteq X$ so $\{a\} \in \mathcal{P}(X)$.

Since $\mathcal{P}(X) = \mathcal{P}(Y)$ we have $\{a\} \in \mathcal{P}(Y)$.

Thus, $\{a\} \subseteq Y$.

Then $a \in Y$.

We have shown $X \subseteq Y$.

Families of sets

Def: When every element of a set A is itself a set then we call A a family or collection of sets.

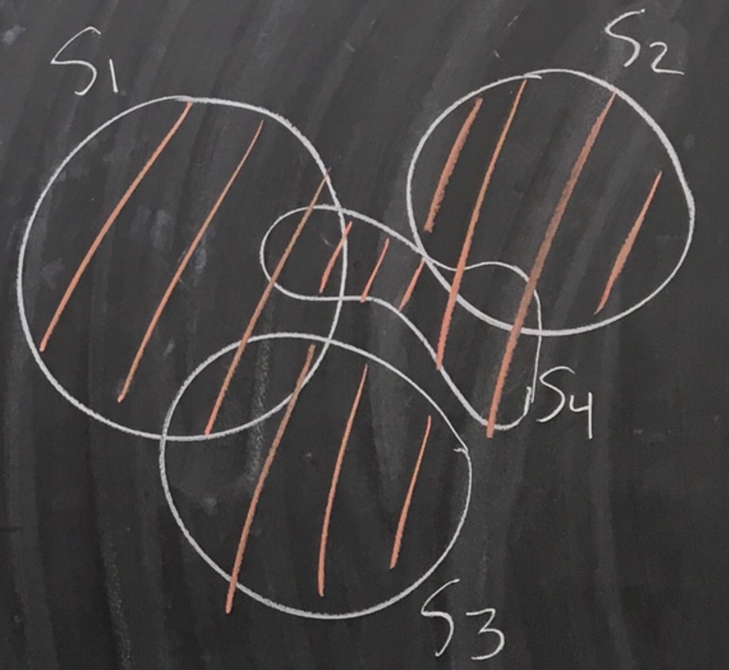
Ex: $\mathcal{P}(X)$ is a family of sets

Def: Let $\mathcal{A}$ be a non-empty family of sets.

We define the union over $\mathcal{A}$ to be

$$\bigcup_{S\in\mathcal{A}} S = \{x \mid x\in S \text{ for some } S\in\mathcal{A}\}$$
$$= \{x \mid \text{there exists } S\in\mathcal{A} \text{ with } x\in S\}$$

$\mathcal{A} = \{S_1, S_2, S_3, S_4\}$

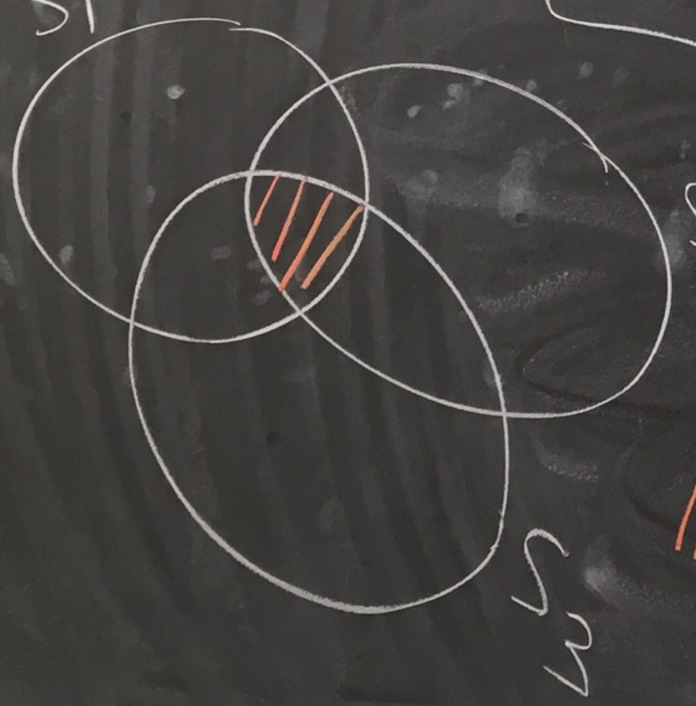


$$\text{III} = \bigcup_{S\in\mathcal{A}} S$$

We define the <u>intersection over $\mathcal{A}$</u> to be

$$\bigcap_{S\in\mathcal{A}} S = \{x \mid x\in S \text{ for all } S\in\mathcal{A}\}$$

$\mathcal{A}=\{S_1,S_2,S_3\}$



$\blacksquare = \bigcap_{S\in\mathcal{A}} S$

<u>Ex:</u>

$\mathcal{A}=\{\{1,\sqrt{2},3,e^4\},$
$\{5,3,e^4,\sqrt{6},78\},$
$\{i+1,1,10\}\}$

e

$A\}$

$\bigcup_{S \in A} S = \{1, \sqrt{2}, 3, e^4, 5, \sqrt{6}, 78, i+1, 10\}$

$\bigcap_{S \in A} S = \phi$

$, 78\},$

$\}$

Ex: $\mathcal{B} = \{ \{ n \in \mathbb{Z} \mid |n| \leq k \} \mid k \in \mathbb{N} \}$

$= \{ S_k \mid k \in \mathbb{N} \} = \{ S_1, S_2, S_3, \ldots \}$

where $S_k = \{ n \in \mathbb{Z} \mid |n| \leq k \}$

$S_1 = \{-1, 0, 1\}$

$S_2 = \{-2, -1, 0, 1, 2\}$

$S_3 = \{-3, -2, -1, 0, 1, 2, 3\}$

$$\bigcup_{S \in \mathcal{B}} S = \mathbb{Z} = \{\ldots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots\}$$

$$\bigcap_{S \in \mathcal{B}} S = S_1 = \{-1, 0, 1\}$$

Def: Let Δ be a non-empty set. Suppose that for each $\alpha \in \Delta$ there is a corresponding set A_α. The family

$\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ is called an <u>indexed family of sets</u>. The set Δ is called the <u>index set</u>. If $\alpha \in \Delta$ then α is called the index of A_α.

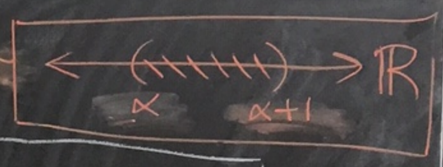
Given such a family of sets define

$$\bigcup_{\alpha\in\Delta} A_\alpha = \bigcup_{S\in\mathcal{A}} S = \{x \mid \text{there exists } \alpha\in\Delta \text{ with } x\in A_\alpha\}$$

$$\bigcap_{\alpha\in\Delta} A_\alpha = \bigcap_{S\in\mathcal{A}} S = \{x \mid x\in A_\alpha \text{ for all } \alpha\in\Delta\}$$

define these in terms of previous def.

Ex: Let's make sense of $\bigcup_{\alpha\in\mathbb{Z}} (\alpha,\alpha+1)$ in terms of the previous definition.



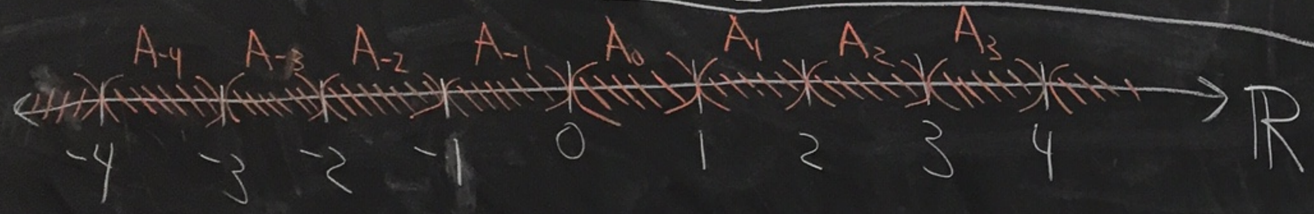
$\Delta = \mathbb{Z}$

Given $\alpha\in\Delta$,

set $A_\alpha = (\alpha,\alpha+1)$

$$\bigcup_{\alpha\in\mathbb{Z}} (\alpha,\alpha+1) = \mathbb{R}-\mathbb{Z}$$

$$\bigcap_{\alpha\in\mathbb{Z}} (\alpha,\alpha+1) = \emptyset$$



Some people write these sets like this:

$$\bigcup_{\alpha=-\infty}^{\infty} (\alpha,\alpha+1)$$

$$\bigcap_{\alpha=-\infty}^{\infty} (\alpha,\alpha+1)$$

It's understood that α ranges over $\mathbb{Z}$

Prop: Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets. Pick some $\alpha_0 \in \Delta$. Then:

① $A_{\alpha_0} \subseteq \bigcup_{\alpha \in \Delta} A_\alpha$

② $\bigcap_{\alpha \in \Delta} A_\alpha \subseteq A_{\alpha_0}$

Its understood that α ranges over $\mathbb{Z}$

9/9/19
Monday

HW 2

9(c) $A_n = (2 + \frac{1}{n}, n) \subseteq \mathbb{R}$

Calculate $\bigcup_{n=3}^{\infty} A_n$ and $\bigcap_{n=3}^{\infty} A_n$

$\bigcup_{n=3}^{\infty} A_n = (2, \infty)$

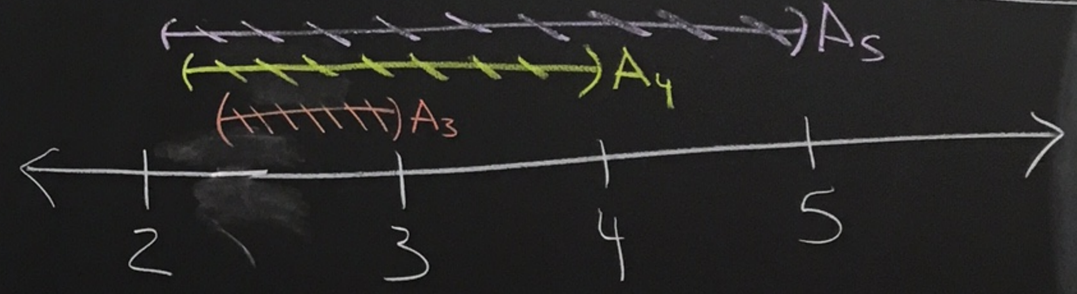
$\bigcap_{n=3}^{\infty} A_n = A_3 = (2 + \frac{1}{3}, 3)$

$= (\frac{7}{3}, 3)$

$A_3 = (2 + \frac{1}{3}, 3)$

$A_4 = (2 + \frac{1}{4}, 4)$

$A_5 = (2 + \frac{1}{5}, 5)$



From last time

Prop: Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets. Pick $\alpha_0 \in \Delta$. Then:

① $A_{\alpha_0} \subseteq \bigcup_{\alpha \in \Delta} A_\alpha$

② $\bigcap_{\alpha \in \Delta} A_\alpha \subseteq A_{\alpha_0}$

pf:

① Let $x \in A_{\alpha_0}$.

Recall that

$$\bigcup_{\alpha \in \Delta} A_\alpha = \left\{ y \;\middle|\; \begin{array}{l} \text{there exists } \alpha' \in \Delta \\ \text{where } y \in A_{\alpha'} \end{array} \right\}$$

Since $x \in A_{\alpha_0}$ there does indeed exist $\alpha' \in \Delta$ with $x \in A_{\alpha'}$, ie $\alpha' = \alpha_0$.

So $x \in \bigcup_{\alpha \in \Delta} A_\alpha$.

Thus, $A_{\alpha_0} \subseteq \bigcup_{\alpha \in \Delta} A_\alpha$.

② You try.

∎

(HW 3 Topic) — Equivalence relations & Well-defined operations & Modulo n

Def: A relation $\sim$ on a set S is a subset of $S \times S$. If (x,y) is an element of $\sim$ then we write $x \sim y$ and say that x is related to y.

If (x,y) is not an element of $\sim$ then we write $x \not\sim y$ and say that x is not related to y.

Ex: $S = \{\square, \$, ¢\}$

$\sim = \{(\square, ¢), (\square, \square), (\square, \$), (¢, \square), (¢, \$)\}$

$\square \sim ¢$ since $(\square, ¢) \in \sim$.

$¢ \sim \square$ since $(¢, \square) \in \sim$.

$\square \sim \square$ since $(\square, \square) \in \sim$.

$\$ \not\sim \$$ since $(\$, \$) \notin \sim$.

More common way to define a relation is like the following example.

Ex: $S = \mathbb{Z}$

Define $x \sim y$ to mean $x < y$.

Then $\sim$ is a relation on $\mathbb{Z}$.

We have

$2 \sim 3$ since $2 < 3$.

$2 \not\sim -1$ since $2 \not< -1$.

How can we think of $\sim$ as a subset of $\mathbb{Z} \times \mathbb{Z}$??

$$\sim = \{(x,y) \mid x < y\}$$

$$= \{(2,3), (-100, 0), (7, 777), \ldots\}$$

infinitely many more elements

Def: Let $\sim$ be a relation on a set S.

We say that $\sim$ is an <u>equivalence relation</u> on S if

① (reflexive) $x \sim x$ for all $x \in S$.

② (symmetric) If $x, y \in S$ and $x \sim y$, then $y \sim x$.

③ (transitive) If $x, y, z \in S$ and $x \sim y$ and $y \sim z$, then $x \sim z$.

can think of an equivalence relation as an "equals" sign.

Ex: Let $S = \{-15, 2, 0\}$

and $\sim = \{(0,0), (0,2), (2,0), (-15,2)\}$

(reflexive?) $0 \sim 0$ but $2 \not\sim 2$ and $(-15) \not\sim (-15)$.

So, $\sim$ is not reflexive.

(symmetric?) NO! $(-15) \sim 2$ but $2 \not\sim (-15)$.

(transitive?)
- $0 \sim 0$ and $0 \sim 2 \Rightarrow 0 \sim 2$ ✓
- $0 \sim 2$ and $2 \sim 0 \Rightarrow 0 \sim 0$ ✓
- $2 \sim 0$ and $0 \sim 0 \Rightarrow 2 \sim 0$ ✓

$0 \sim 0$ and $0 \sim 0 \Rightarrow 0 \sim 0$ ✓

$-15 \sim 2$ and $2 \sim 0$ but $-15 \not\sim 0$

So, $\sim$ is not transitive.

$\sim$ is NOT an equivalence relation

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

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

Is $\sim$ an equivalence relation? YES

reflexive

$1 \sim 1$
$2 \sim 2$
$3 \sim 3$

Yes

symmetric

Yes

If $x \sim y$, then $y \sim x$,

Ex: $1 \sim 3$ and $3 \sim 1$,

transitive

- $1 \sim 1$ and $1 \sim 1$. And $1 \sim 1$.
- $1 \sim 1$ and $1 \sim 3$. And $1 \sim 3$.
- $2 \sim 2$ and $2 \sim 2$. And $2 \sim 2$.
- $3 \sim 3$ and $3 \sim 3$. And $3 \sim 3$.
- $3 \sim 3$ and $3 \sim 1$. And $3 \sim 1$.
- $1 \sim 3$ and $3 \sim 3$. And $1 \sim 3$.
- $1 \sim 3$ and $3 \sim 1$. And $1 \sim 1$.
- $3 \sim 1$ and $1 \sim 1$. And $3 \sim 1$.
- $3 \sim 1$ and $1 \sim 3$. And $3 \sim 3$.

Yes

Def: Let $\sim$ be an equivalence relation on a set S. Let $x \in S$.

The <u>equivalence class</u> of x is

$$\overline{x} = \{ y \in S \mid x \sim y \}$$

$\overline{x}$ consists of all elements y that are related to x.

It doesn't matter if you define $\overline{x}$ as $\{ y \in S \mid x \sim y \}$ or $\{ y \in S \mid y \sim x \}$ since $\sim$ is symmetric.

Another notation for $\overline{x}$ is $[x]$.

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

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

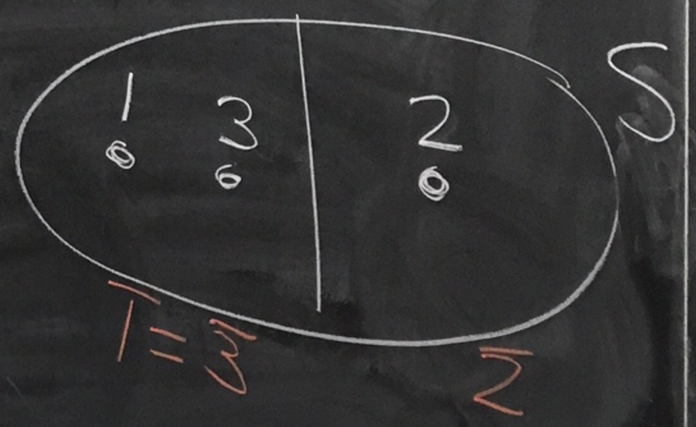
$\sim$ is an equivalence relation.

$\bar{1} = \{y \in S \mid 1 \sim y\} = \{1, 3\}$

$\bar{2} = \{y \in S \mid 2 \sim y\} = \{2\}$

$\bar{3} = \{y \in S \mid 3 \sim y\} = \{1, 3\}$

There are 2 equivalence classes $\bar{1} = \bar{3}$ and $\bar{2}$



Def: Let S be a set and $\sim$ be an equivalence relation on S. We denote the set of equivalence classes as $S/\sim$ read: "S mod $\sim$"

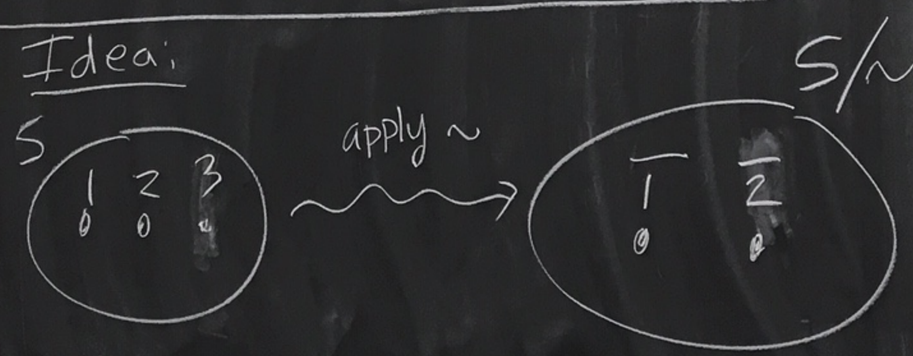
Ex: In the previous example

$$S/\sim = \{\bar{1}, \bar{2}\}$$

$\bar{1} = \bar{3}$

since $1 \sim 3$ we make 1 and 3 equal in the set of equivalence classes

Idea:



Weds
9/11

Hw 2

(16) Let A, B, C, and D be sets.

Prove: $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

proof:

We have that $(x,y) \in (A \times B) \cap (C \times D)$

iff $(x,y) \in A \times B$ and $(x,y) \in C \times D$

iff $x \in A$ and $y \in B$ and $x \in C$ and $y \in D$

iff $x \in A \cap C$ and $y \in B \cap D$

iff $(x,y) \in (A \cap C) \times (B \cap D)$

$\blacksquare$

Recall from last time

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

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

$\sim$ is an equivalence relation on S.

equivalence classes

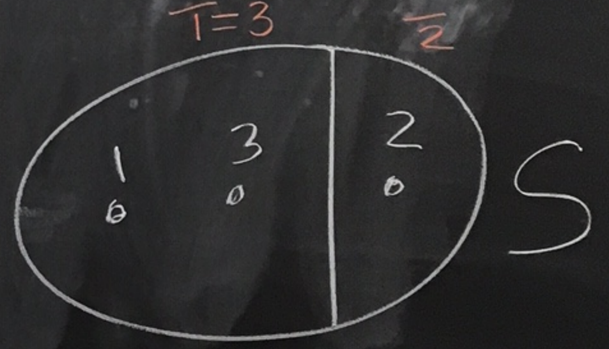
$\bar{1} = \{y \in S \mid 1 \sim y\} = \{1,3\}$

$\bar{2} = \{y \in S \mid 2 \sim y\} = \{2\}$

$\bar{3} = \{y \in S \mid 3 \sim y\} = \{3,1\}$

equal

$S/\sim = \{\bar{1}, \bar{2}\}$



Super-duper Equivalence relation Theorem

Let $\sim$ be an equivalence relation on a set S.

Let $x, y \in S$. Then:

① $x \in \bar{x}$

② $\bar{x} = \bar{y}$ iff $x \in \bar{y}$.

③ $\bar{x} = \bar{y}$ iff $x \sim y$.

④ $\bar{x} \cap \bar{y} = \emptyset$ iff $x \not\sim y$.

Examples from previous example

① $2 \in \bar{2}$

② $\bar{1} = \bar{3}$ and $1 \in \bar{3}$ (also $3 \in \bar{1}$)

③ $\bar{1} = \bar{3}$ and $1 \sim 3$.

④ $\bar{1} \cap \bar{2} = \{1,3\} \cap \{2\} = \emptyset$ and $1 \not\sim 2$.

Note ③ and ④ imply that either
$\bar{x}=\bar{y}$ OR $\bar{x}\cap\bar{y}=\phi$.

Proof: Let $x,y\in S$.

① Recall that
$\bar{x}=\{a\in S \mid x\sim a\}$.
Since $\sim$ is reflexive
we know that $x\sim x$.
So, $x\in\bar{x}$.

② ($\Rightarrow$): Assume that $\bar{x}=\bar{y}$.
We want to show that $x\in\bar{y}$.
By part 1, we know $x\in\bar{x}$.
Since $\bar{x}=\bar{y}$ we get that $x\in\bar{y}$.

($\Leftarrow$) Assume that $x\in\bar{y}$.
We need to show that $\bar{x}=\bar{y}$.

$\boxed{\bar{x} \subseteq \bar{y}}$: Let $z \in \bar{x} = \{a \in S \mid x \sim a\}$

So, $x \sim z$.

Since $x \in \bar{y} = \{a \in S \mid y \sim a\}$ we have $y \sim x$.

Since $y \sim x$ and $x \sim z$ and $\sim$ is an equivalence relation we have transitivity, so $y \sim z$.

Thus, $z \in \bar{y}$. So, $\bar{x} \subseteq \bar{y}$.

$\boxed{\bar{y} \subseteq \bar{x}}$: Let $z \in \bar{y}$.

Then, $y \sim z$.

Since $x \in \bar{y}$ we have $y \sim x$.

Since $\sim$ is symmetric and $y \sim x$ we have that $x \sim y$.

Since $x \sim y$ and $y \sim z$ by transitivity we have $x \sim z$.

So, $z \in \bar{x}$.

Thus, $\bar{y} \subseteq \bar{x}$.

Since $\bar{x} \subseteq \bar{y}$ and $\bar{y} \subseteq \bar{x}$ we have that $\bar{x} = \bar{y}$.

Thus, $\bar{x} = \bar{y}$ iff $x \in \bar{y}$
iff $y \sim x$
iff $x \sim y$.

P	Q	¬P	¬Q	P iff Q	(¬P) iff (¬Q)
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

③ By part 2,
$\bar{x} = \bar{y}$ iff $x \in \bar{y}$.
Note $x \in \bar{y}$ iff $y \sim x$.
Also since $\sim$ is symmetric
$y \sim x$ iff $x \sim y$.

④ Instead of proving
"$\bar{x} \cap \bar{y} = \emptyset$ iff $x \not\sim y$"
we prove
"$\bar{x} \cap \bar{y} \neq \emptyset$ iff $x \sim y$"

P iff Q
is equivalent to
(¬P) iff (¬Q)

($\Leftarrow$) Suppose $x \sim y$.
Then by part 2, $\bar{x} = \bar{y}$.
By part 1, $x \in \bar{x}$.
Since $\bar{x} = \bar{y}$ we have $\bar{x} \cap \bar{y} = \bar{x}$.
So, $x \in \bar{x} \cap \bar{y}$.
Thus, $\bar{x} \cap \bar{y} \neq \phi$.

($\Rightarrow$) Assume that $\bar{x} \cap \bar{y} \neq \phi$.
So, there exists $z \in S$
with $z \in \bar{x} \cap \bar{y}$.

$\Rightarrow$ So, $z \in \bar{x}$ and $z \in \bar{y}$.
Thus, $x \sim z$ and $y \sim z$.
By the symmetric-ness of $\sim$ we get that $z \sim y$.
By transitivity-ness of $\sim$ since $x \sim z$ and $z \sim y$ we get $x \sim y$.

DONE

HW 2

Recall: $\mathcal{P}(X) = \{Y \mid Y \subseteq X\}$

(14) (a) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Proof: $Y \in \mathcal{P}(A \cap B)$

iff $Y \subseteq A \cap B$

iff $Y \subseteq A$ and $Y \subseteq B$

iff $Y \in \mathcal{P}(A)$ and $Y \in \mathcal{P}(B)$.

iff $Y \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

FIN

Lemma: Let Y, A, and B be sets.
Then, $Y \subseteq A \cap B$ iff $Y \subseteq A$ and $Y \subseteq B$.

Proof:
($\Rightarrow$) Suppose $Y \subseteq A \cap B$.
Let $y \in Y$.
Then $y \in A \cap B$.
So, $y \in A$ and $y \in B$.
Thus, $Y \subseteq A$ and $Y \subseteq B$.

($\Leftarrow$) Suppose $Y \subseteq A$ and $Y \subseteq B$.

Let $y \in Y$.

Then from above $y \in A$ and $y \in B$.

So $y \in A \cap B$.

Thus, $Y \subseteq A \cap B$.

Lemma

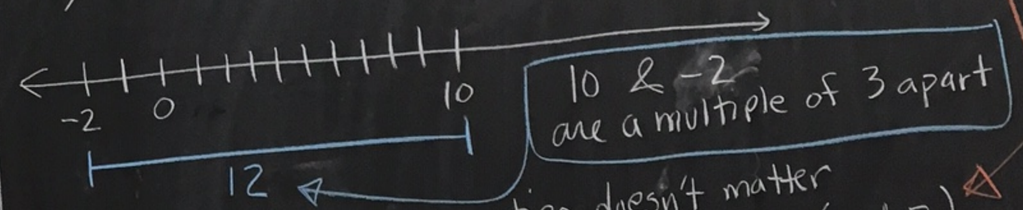
9/16
Monday

Def: Let $a, b \in \mathbb{Z}$. We say that a *divides* b if there exists $k \in \mathbb{Z}$ with $ak = b$. We write $a \mid b$ to mean that a divides b.
If a doesn't divide b we write $a \nmid b$.

Ex: $2 \mid 12$ since $12 = (2)(6)$, with $k = 6$

Def: Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$.
We say that *a and b are congruent modulo n* if $n \mid (a-b)$. If this is so then we write $a \equiv b \pmod{n}$.
If $n \nmid (a-b)$ we write
$a \not\equiv b \pmod{n}$

Ex: $n = 3$
Are -2 and 10 congruent modulo 3?
$(-2) - 10 = -12 \leftarrow 3 \mid (-12)$ since $-12 = 3(-4)$
So, $-2 \equiv 10 \pmod{3}$



Note: The order of subtraction doesn't matter
$10 - (-2) = 12 \leftarrow 3 \mid 12$ so $10 \equiv -2 \pmod{3}$

Ex: $n=3$

$10 \not\equiv 2 \pmod 3$

$10-2=8$ is not divisible by 3.

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$. Modulo n is an equivalence relation. That is,

1. $a \equiv a \pmod n$ for all $a \in \mathbb{Z}$.
2. If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
3. If $a, b, c \in \mathbb{Z}$ and $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

2.

on.

),

n).

proof:

① Let $a \in \mathbb{Z}$.
Then,
$a - a = 0 = n \cdot 0$.
So $a \equiv a \pmod{n}$.

② Let $a, b \in \mathbb{Z}$.
Assume that $a \equiv b \pmod{n}$.
Then $n \mid (a-b)$.
So, $a - b = nk$ for some $k \in \mathbb{Z}$.

Multiply by (-1) to get
$b - a = n(-k)$.
So, $n \mid (b-a)$.
Thus, $b \equiv a \pmod{n}$.

③ Let $a, b, c \in \mathbb{Z}$.
Assume that $a \equiv b \pmod{n}$
and $b \equiv c \pmod{n}$.
So, $n \mid (a-b)$
and $n \mid (b-c)$.

So there exists $k, \ell \in \mathbb{Z}$
with $a - b = nk$ and $b - c = n\ell$.
Adding the equations gives
$a - c = nk + n\ell$.

So,
$a - c = n[k + \ell]$.

Since $k + \ell \in \mathbb{Z}$ we get $n \mid (a-c)$.
Therefore, $a \equiv c \pmod{n}$.

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$. We denote the set of equivalence classes modulo n as $\mathbb{Z}_n$.

-9

Previously:

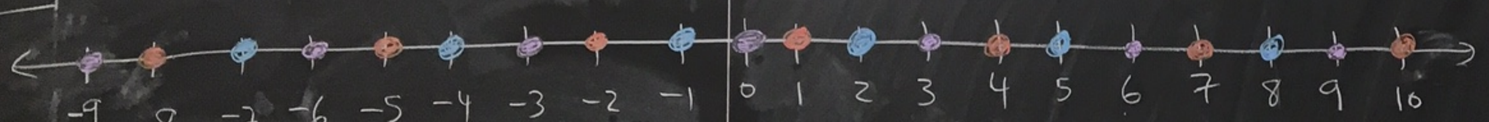
$\sim$ is an equivalence relation on S. The set of equivalence classes was denoted $S/\sim$.

Some people write $\mathbb{Z}/n\mathbb{Z}$ instead of $\mathbb{Z}_n$.

2.

Ex: Calculate $\mathbb{Z}_3$ (ie the equivalence classes modulo 3)

So, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.



$\bar{0} = \{x \in \mathbb{Z} \mid 0 \equiv x \pmod 3\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \bar{3}$

$\bar{1} = \{x \in \mathbb{Z} \mid 1 \equiv x \pmod 3\} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} = \overline{10}$

$\bar{2} = \{x \in \mathbb{Z} \mid 2 \equiv x \pmod 3\} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} = \bar{5}$

Use the super-duper equivalence class Theorem

$\bar{2} = \bar{5}$ since $2 \equiv 5 \pmod 3$

OR

$\bar{2} = \bar{5}$ since $5 \in \bar{2}$

$\mathbb{Z}$

... -9 -6 -3 0 3 6 9 ...	$\bar{0}$
... -8 -5 -2 1 4 7 10 ...	$\bar{1}$
... -7 -4 -1 2 5 8 11 ...	$\bar{2}$

Congruence modulo 3 breaks $\mathbb{Z}$ into 3 disjoint equivalence classes: $\bar{0}, \bar{1}, \bar{2}$

Division Algorithm on $\mathbb{Z}$

Let $a, b \in \mathbb{Z}$ and $a > 0$.
There exist unique integers q and r with

$$b = aq + r$$

and

$$0 \leq r < a.$$

Ex: $a = 5$, $b = 17$

$$17 = 5(3) + 2$$

3 → q; 2 → r

$0 \leq 2 < 5$
$0 \leq r < a$

$a = 5$
$b = -17$

$-17 = 5(-3) - 2$ doesn't work since r is negative

$-17 = 5(-4) + 3$
$a\,q + r$
$0 \leq r < a$

division algorithm

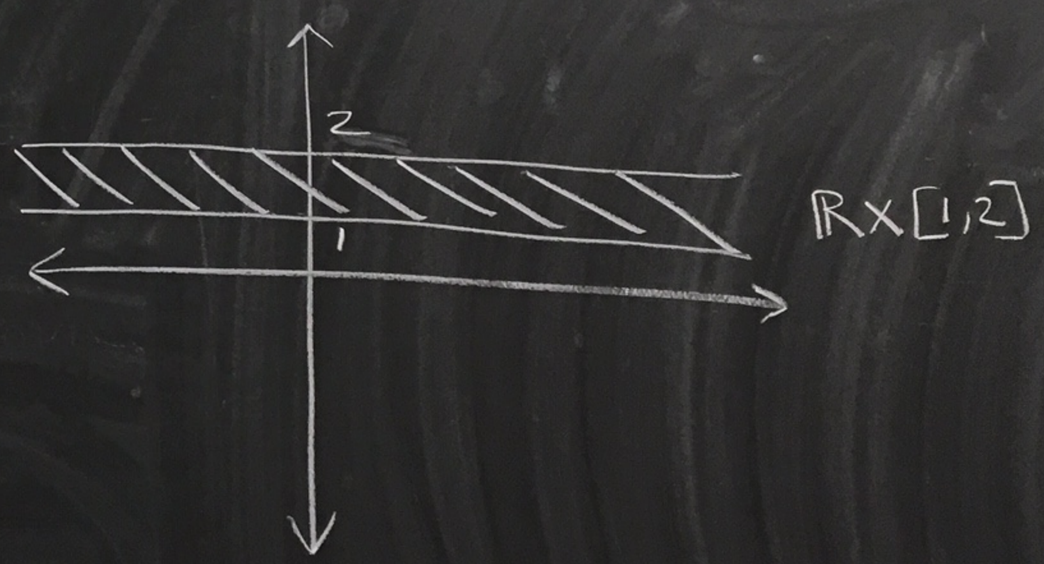
Hammock book 1.8

(7) (a) $\bigcup_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1]$

(b) $\bigcap_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1]$

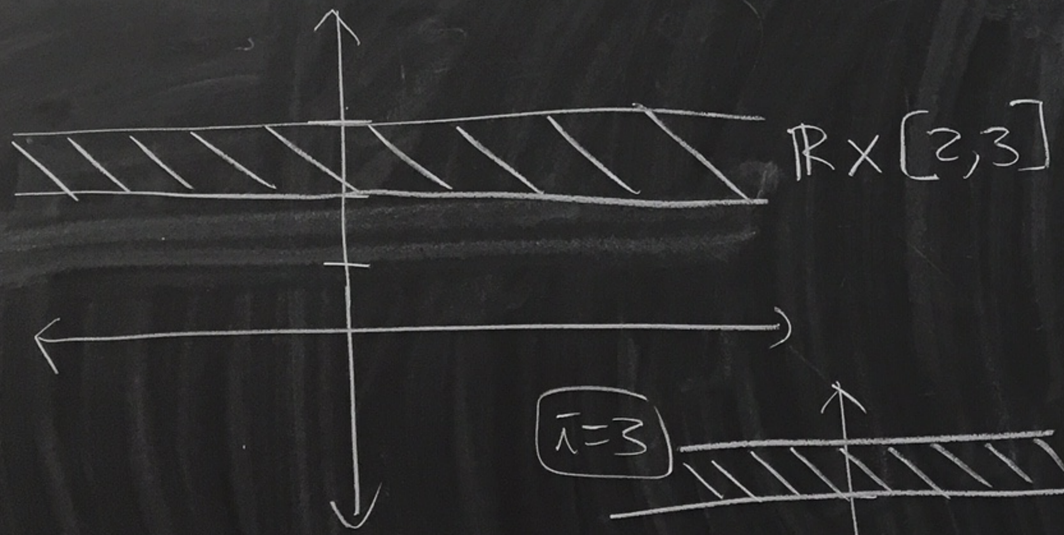
$i = 1$

$\mathbb{R} \times [1,2] = \{(x,y) \mid \begin{matrix} x \in \mathbb{R} \\ y \in [1,2] \end{matrix}\}$

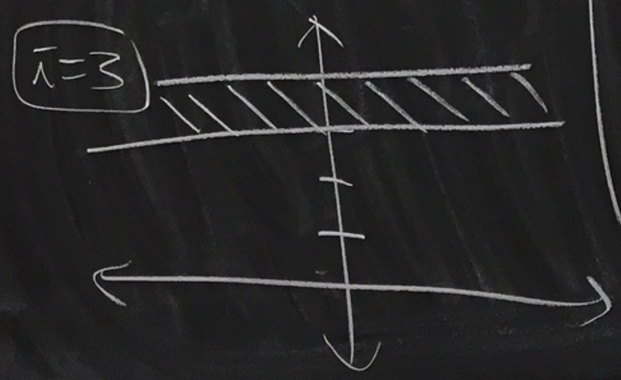


$\tilde{x}=2$

$R\times[2,3]=\{(x,y)\mid x\in R,\ y\in[2,3]\}$

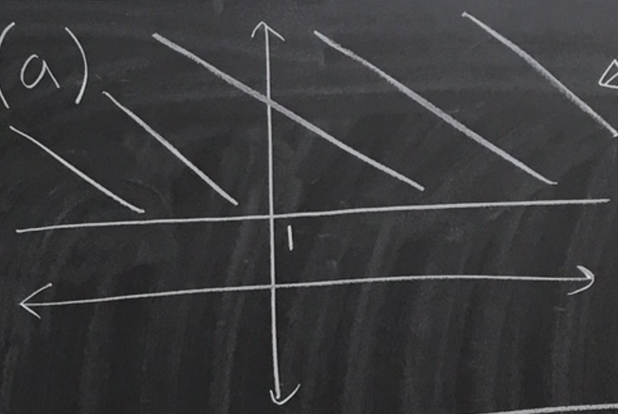


$\tilde{x}=3$



Answers

(a)



$\{(x,y)\mid x\in R,\ y\geq 1\}$

$=R\times[1,\infty)$

(b) $\emptyset$

Weds.
9/18

HW 2

④ Let A and B be sets.

Prove: $A \subseteq B$ iff $A - B = \emptyset$

Need to show

($\Rightarrow$) If $A \subseteq B$ then $A - B = \emptyset$

($\Leftarrow$) If $A - B = \emptyset$ then $A \subseteq B$

If P, then Q.

P iff Q
¬P iff ¬Q

Contradiction

If P, then Q.

pf: Assume P.
Show ¬Q leads to a contradiction

Thus, Q is true.

∎

Proof:

($\Longleftarrow$) Assume $A-B=\emptyset$.

We need to show that $A \subseteq B$.

Let $x \in A$.

Why is $x \in B$ true?

If $x \notin B$, then we would have $x \in A$ and $x \notin B$, implying $x \in A-B$.

But $A-B=\emptyset$ by assumption.

So $x \in B$.

Thus $A \subseteq B$.

($\Longleftarrow$) (Revised)

Assume $A-B=\emptyset$. ⇐ Assume P

By way of contradiction, suppose $A \not\subseteq B$. ⇐ what happens if $\neg Q$ is true?

Then there would exist $X \in A$ with $X \notin B$. ⇐ $A \subseteq B$ means: $\forall x$ (If $x \in A$, then $x \in B$)

Then $x \in A-B$.

But that contradicts $A-B=\emptyset$,

So, $A \subseteq B$. ⇐ Since $\neg Q$ leads to a contradiction, Q must be true

$A \not\subseteq B$ means: $\exists x$ where $x \in A$ and $x \notin B$.

$\forall$ for all

$\exists$ there exists

($\Rightarrow$) Suppose $A \subseteq B$. ← Assume P

We need to show that $A - B = \emptyset$. ← Need to show Q

By way of contradiction, suppose $A - B \neq \emptyset$. ← Assume $\neg Q$

There exists $x \in A - B$.

Then $x \in A$ and $x \notin B$.

But this contradicts that $A \subseteq B$. ← $\neg Q$ leads to a contradiction.

Thus, $A - B = \emptyset$. ← Therefore Q

□

Division Alg. continued

Ex: $a=5,\ b=17$

$b=aq+r$
$17=5\cdot 3+2$
$0\le r<5$

Define

$$S=\{b-ax \mid x\in\mathbb{Z} \text{ and } b-ax\ge 0\}$$

$$=\{b-ax \mid x\in\mathbb{Z} \text{ and } 17-5x\ge 0\}$$

$$=\{2,7,12,17,22,\dots\}$$

2 ← smallest integer in S

x	$b-ax=17-5x$
⋮	⋮
5	-8
4	-3
3	2
2	7
1	12
0	17
-1	22
⋮	⋮

not in S

in S

Division Algorithm Let $a, b \in \mathbb{Z}$ with $a > 0$.

Then there exists unique integers q and r with $b = aq + r$ and $0 \leq r < a$.

Proof:

(existence) Let

$$S = \{ b - ax \mid \begin{array}{l} x \in \mathbb{Z} \text{ and} \\ b - ax \geq 0 \end{array} \}.$$

Let's show that $S \neq \emptyset$.

case 1: Suppose $b \geq 0$.

Setting $x = -1$ gives

$b - ax = b + a > 0$

(because $b \geq 0$ & $a > 0$).

So, $b + a$ is a positive integer in S.

case 2: Suppose $b < 0$.

Setting $x = 2b$ gives

$b - ax = b - a(2b) = b(1 - 2a) > 0$

(since $b < 0$ and $\underbrace{a \geq 1}_{(a > 0)}$ gives $1 - 2a < 0$)

So, $b-a(2b) \in S$.

By case 1 and case 2, $S \neq \phi$.

Since S is not empty and S is a set of non-negative integers, S must have a smallest element.

Let r be the smallest element in S.

So there exists $q \in \mathbb{Z}$ with $r = b-aq$ and $r = b-aq \geq 0$.

So, $b = aq+r$ with $0 \leq r$.

We now show $r < a$.

Suppose that $r \geq a$.

Then $r-a \geq 0$.

And,

$r-a = (b-aq)-a = b-a(q+1)$.

Since $r-a \geq 0$ and $r-a = b-a(q+1)$ we know $r-a \in S$.

But $r-a < r$ since $a > 0$.

But then $r-a$ would be an element of S that is smaller than r.

This contradicts the assumption
that r is the smallest element in S.

So, $r < a$.

Thus, there exists $q, r \in \mathbb{Z}$ with $b = aq + r$ and $0 \leq r < a$.

(uniqueness) Suppose we have $b = aq + r$ and
$b = aq' + r'$ with $q, r, q', r' \in \mathbb{Z}$ and $0 \leq r < a$
and $0 \leq r' < a$.

We will show that $q = q'$ and $r = r'$.

Assume $r' \geq r$.
Then $r' - r \geq 0$.

Since
$$b = aq + r = aq' + r'$$
we have
$$a(q - q') = r' - r.$$
Thus, a divides $r' - r$.

But since $0 \leq r < a$ and $0 \leq r' < a$
and $r' - r \geq 0$ we know that
$$0 \leq r' - r < a.$$

$0 \leq r' < a$
$0 \leq r' - r < a - r < a$

Since $a \mid (r' - r)$ we
must have $r' - r = 0$.

So, $r' = r$.
Thus, $a(q - q') = r' - r = 0$.
Since $a > 0$, this gives $q - q' = 0$.
So, $q = q'$ ▨

new schedule

M	W
10/7	10/9
class Workshop review	Test 1
M	W
11/4	11/6
class Workshop review	Test 2

9/23

Monday

Recall

If $\sim$ is an equivalence relation on S, then $S/\sim$ is the set of equivalence classes for $\sim$

$\mathbb{Z}_n$ is the set of equivalence classes for the equivalence relation modulo n. $\mathbb{Z}_n = \mathbb{Z}/\equiv$

Ex: $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ and given any $x \in \mathbb{Z}$ either $\bar{x} = \bar{0}$ or $\bar{x} = \bar{1}$ or $\bar{x} = \bar{2}$

s an equivalence
n on S, then
is the set of
alence classes for ~

of equivalence
e equivalence
n.

$\mathbb{Z}_n = \mathbb{Z}/\equiv$

$\{\bar{0}, \bar{1}, \bar{2}\}$ and given any $x \in \mathbb{Z}$
either $\bar{x} = \bar{0}$ or $\bar{x} = \bar{1}$
or $\bar{x} = \bar{2}$

For example,
take $x = 32$.

$$3 \overline{)\,32}\quad 10$$
$$-30$$
$$2$$

the remainder is the equivalence class we want

$32 = 3(10) + 2$

$32 - 2 = 3(10)$

$3 \mid (32-2)$

So, $32 \equiv 2 \pmod 3$

So, $\overline{32} = \bar{2}$.

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$.

Then, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

Furthermore, if $0 \leq x \leq y \leq n-1$ and $\overline{x} = \overline{y}$, then $x = y$.

This part says that none of $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ are equal. They are all distinct.

Ex: $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

and none of these elements are equal

Proof of theorem

Let $S = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Let's show that $S = \mathbb{Z}_n$.

We know $S \subseteq \mathbb{Z}_n$ because S consists of equivalence classes.

Now let's show that $\mathbb{Z}_n \subseteq S$.

Recall that

$$\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\}.$$

Let $\bar{x} \in \mathbb{Z}_n$ where $x \in \mathbb{Z}$.

By the division algorithm there exist $q, r \in \mathbb{Z}$ with $x = qn + r$ and $0 \leq r < n$.

So, $x - r = qn$.

Thus, $n \mid (x - r)$.

Hence $x \equiv r \pmod{n}$.

So, $\bar{x} = \bar{r}$.

Ex:

$n = 3$

$x = 32$

$32 = 10 \cdot 3 + 2$

$x = qn + r$

So, $\overline{32} = \bar{2}$

Since $0 \le r \le n-1$ and $\bar{x} = \bar{r}$
we have $\bar{x} \in S$.

Therefore, $\mathbb{Z}_n = S = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Now we prove the furthermore part of the theorem.

Suppose $0 \le x \le y \le n-1$ and $\bar{x} = \bar{y}$
where $x, y \in \mathbb{Z}$.

We want to show that $x = y$.

Since $\overline{x}=\overline{y}$ we know by the super-duper equivalence class theorem that $x \equiv y \pmod{n}$.

So, $\boxed{n \mid (y-x)}$.

Using $0 \leq x \leq y \leq n-1$ we get $-x \leq 0 \leq y-x \leq n-1-x$.

Note that $n-1-x < n$.

So,

$$\boxed{0 \leq y-x < n}$$

Since $n \mid (y-x)$ we have $nq = (y-x)$ for some $q \in \mathbb{Z}$.

Note that $q \geq 0$ since $n \geq 2$ and $y-x \geq 0$.

Goal: Show $q=0$.

Suppose to the contrary that $q > 0$.

Then,

$$\underbrace{0 \leq y-x < n}_{\text{known}} \leq nq = y-x.$$

since $q \geq 1$

known

But then

$$y-x < y-x.$$

Contradiction.

So, $q = 0$ and $y-x = nq = 0$. Thus, $y = x$. ∎

Ex:

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\vdots$ $\qquad$ $\vdots$

Unsolved math problem

Given an integer m
can we express m in the form

$$m = x^3 + y^3 + z^3$$

where $x, y, z \in \mathbb{Z}$??

Ex:

$m = 0$

$$0 = 0^3 + 0^3 + 0^3$$

Ex: $m = 1$

$$1 = 1^3 + (-1)^3 + 1^3$$

Ex: $m = 2$

$$2 = 0^3 + 1^3 + 1^3$$

Ex: There are no solutions to

$$4 = x^3 + y^3 + z^3$$

$+0^3$

$+1^3$

Ex: $m=2$

$2=0^3+1^3+1^3$

Ex: There are no solutions to

$4=x^3+y^3+z^3$

Recently (2019)

$33=x^3+y^3+z^3$

and

$42=x^3+y^3+z^3$

were solved.

$33=8866128975287528^3$
$+(-8778405442862239)^3$
$+(-2736111468807040)^3$

It can be shown that if $m\equiv 4 \pmod 9$ or $m\equiv 5 \pmod 9$ then there do not exist $x,y,z\in\mathbb{Z}$ with $m=x^3+y^3+z^3$.

Theorem: Let $n, a, b, c, d \in \mathbb{Z}$ with $n \geq 2$.
If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$(a+c) \equiv (b+d) \pmod{n}$$

and $$ac \equiv bd \pmod{n}.$$

Proof: Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.
Then $n \mid (a-b)$ and $n \mid (c-d)$.

So, $nk = a-b$ and $n\ell = c-d$ where $k, \ell \in \mathbb{Z}$

Then

$$(a+c)-(b+d) = (a-b)+(c-d) = nk+n\ell = n[k+\ell].$$

Since $k+\ell \in \mathbb{Z}$ we get that $n \mid [(a+c)-(b+d)]$

So, $(a+c) \equiv (b+d) \bmod n$.

Also,

$$ac - bd = a\underbrace{(n\ell + d)}_{c} - \underbrace{(a - nk)}_{b}d$$

$$= an\ell + ad - ad + nkd$$

$$= n[a\ell + kd].$$

Since $a\ell + kd \in \mathbb{Z}$ we get that $n \mid (ac - bd)$.

So, $ac \equiv bd \pmod{n}$. ∎

Weds
9/25

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$

HW 3

(8) $S = \mathbb{N} \times \mathbb{N} = \{(a,b) \mid a \in \mathbb{N}, b \in \mathbb{N}\}$

$= \{(1,1), (2,5), (103, 301), \ldots\}$

Define $\sim$ on S by

$(a,b) \sim (c,d)$ means $a+d = b+c$

(a) Is $(3,6) \sim (7,10)$??

$3+10 = 6+7$.

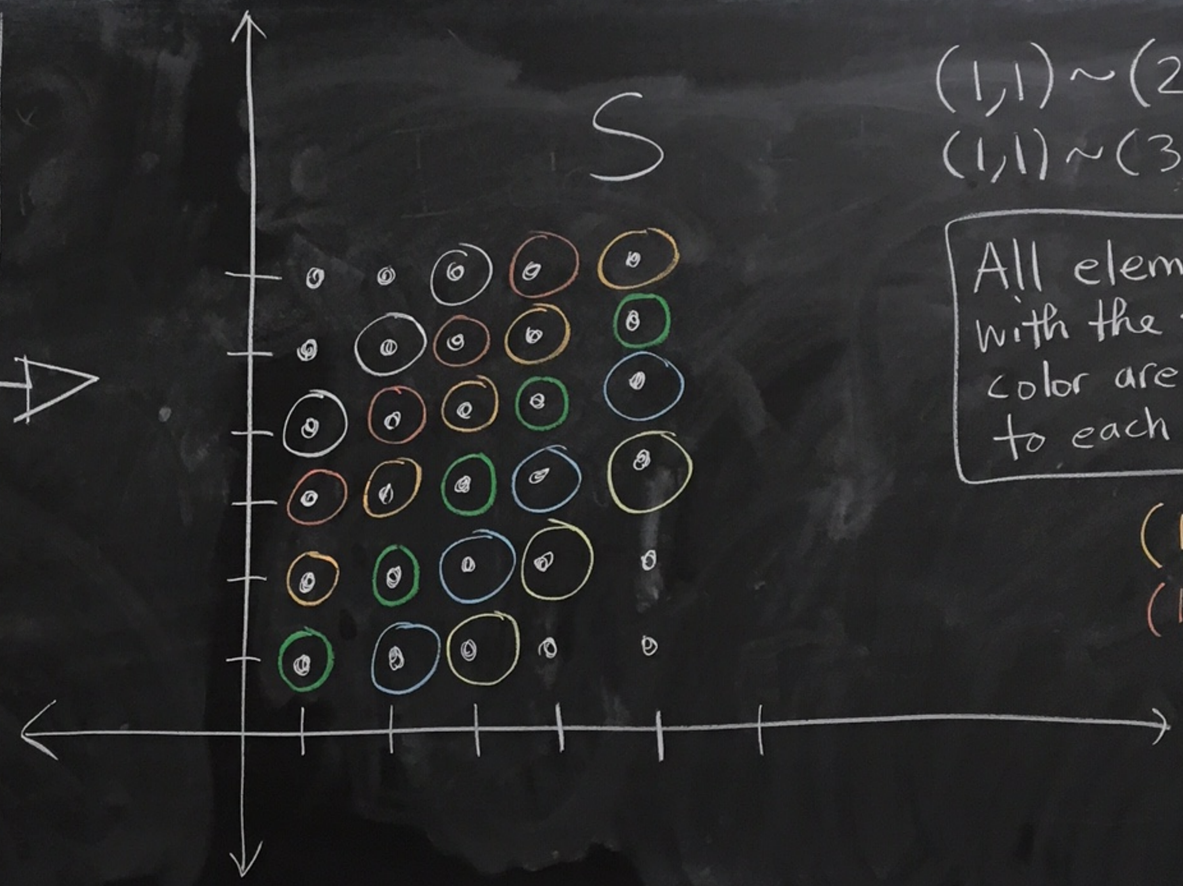
Yes $(3,6) \sim (7,10)$

(b) Is $(1,1) \sim (3,5)$?

No, $1+5 \neq 1+3$.

PICTURE TIME →

$(1,3) \sim (2,4)$



$(1,1) \sim (2,2)$

$(1,1) \sim (3,3)$

All elements with the same color are related to each other

$(1,2) \sim (2,3)$

$(1,2) \not\sim (2,1)$

$(1,2) \sim (1,2)$

$(a,b) \sim (c,d)$ if $a+d=b+c$

(c) Prove that $\sim$ is an equivalence relation on S.

(reflexive) Let $x \in S$.
Then $x=(a,b)$ where $a,b \in \mathbb{N}$
Since $a+b=b+a$ we know
$(a,b) \sim (a,b)$.
So, $x \sim x$.

(symmetric) Let $(a,b),(c,d) \in S$
where $a,b,c,d \in \mathbb{N}$.
And suppose $(a,b) \sim (c,d)$.
Then $a+d=b+c$.
So, $c+b=d+a$.
Thus, $(c,d) \sim (a,b)$.

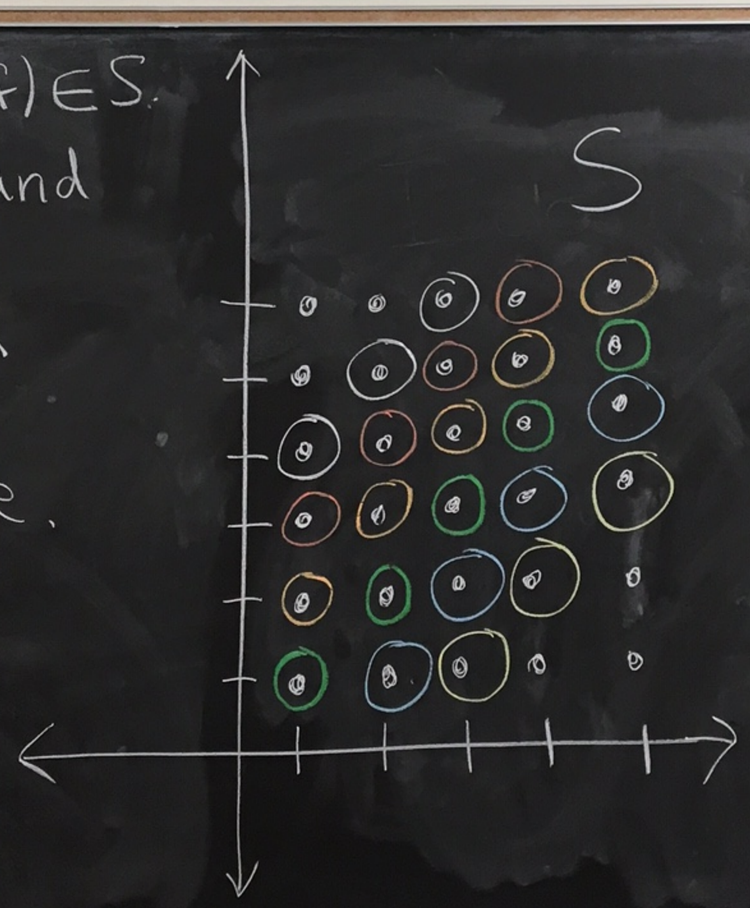
(transitive) Let $(a,b),(c,d),(e,f) \in S$.
Assume that $(a,b) \sim (c,d)$ and
$(c,d) \sim (e,f)$

Then, $a+d=b+c$ and
$c+f=d+e$.

So, $a+d+c+f=b+c+d+e$.

Thus, $a+f=b+e$.

So, $(a,b) \sim (e,f)$.



(d)

$\overline{(1,1)} = \{(1,1),(2,2),(3,3),(6,6),(10,10),\dots\}$

$\overline{(1,2)} = \{(1,2),(2,3),(3,4),(4,5),(20,21),\dots\}$

$\overline{(5,12)} = \{(5,12),(6,13),(7,14),(20,27),(10,17),\dots\}$

Well-defined operations

$\mathbb{Q} = \left\{ \frac{x}{y} \middle| \begin{array}{l} x, y \in \mathbb{Z} \\ y \neq 0 \end{array} \right\}$

Let's say one day you and your friend say "Hey let's make a new operation on $\mathbb{Q}$!" Your friend says "Totally! I concur!" You say "What about this operation $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$"

new operation symbol

And then joyfully you proceeded to calculate some calculations.

$\frac{2}{7} \oplus \frac{1}{5} = \frac{2+1}{7+5} = \frac{3}{12}$

$\frac{3}{11} \oplus \frac{49}{-1} = \frac{3+49}{11-1} = \frac{52}{10}$

equals sign

And then joyfully you proceeded to calculate some calculations.

$$\frac{2}{7} \oplus \frac{1}{5} = \frac{2+1}{7+5} = \frac{3}{12}$$

$$\frac{3}{11} \oplus \frac{49}{-1} = \frac{3+49}{11-1} = \frac{52}{10}$$

$$\frac{2}{1} \oplus \frac{5}{-1} = \frac{2+5}{1-1} = \frac{7}{0}$$ ← And then you're like "uh oh!"

One issue is that $\frac{7}{0}$ is not in $\mathbb{Q}$ ← No good

equals sign

$$\frac{2}{7} \oplus \frac{1}{5} = \frac{3}{12}$$

$$\frac{2}{11} \oplus \frac{1}{5} = \frac{4}{19}$$

Not equal even though $\frac{2}{7} = \frac{4}{14}$ ← No good

We say that $\oplus$ is NOT well-defined

Def: Let S be a set. An operation $\oplus$ on S is well-defined if

S is closed under $\oplus$

① For every $x, y \in S$ we have $x \oplus y \in S$.

② If some or all of the elements of S can be expressed in more than one way, we must show the following:

For every $a, b, c, d \in S$, if $a = b$ and $c = d$ then $a \oplus c = b \oplus d$

Let's make an operation on $\mathbb{Z}_n$.
Given $\overline{a}, \overline{b} \in \mathbb{Z}_n$ define

$$\overline{a} + \overline{b} = \overline{a+b}$$

and $$\overline{a} \cdot \overline{b} = \overline{ab}$$

[We can make this def. since $a, b \in \mathbb{Z}$ and we know how to compute $a+b$ and ab]

Ex: $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

$\overline{5} + \overline{0} = \overline{5+0} = \overline{5}$

$\overline{4} + \overline{6} = \overline{4+6} = \overline{10} = \overline{3}$

$10 \equiv 3 \pmod 7$
$7 \mid (10-3)$

$\overline{3} \cdot \overline{6} = \overline{3 \cdot 6} = \overline{18} = \overline{4}$

$18 \equiv 4 \pmod 7$

$\overline{4} + \overline{6} = \overline{3}$
$\| \quad \|$
$\overline{18} + \overline{-1} = \overline{18-1} = \overline{17} = \overline{3}$

the same!
$\overline{4} = \overline{18}$ and $\overline{6} = \overline{-1}$
$\overline{4+6} = \overline{18+-1}$

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$.
The following operations on $\mathbb{Z}_n$ are well-defined.
Given $\bar{a}, \bar{b} \in \mathbb{Z}_n$ define

$$\bar{a} + \bar{b} = \overline{a+b}$$

and $$\bar{a} \cdot \bar{b} = \overline{ab}$$

Proof:

① Given $\bar{a}, \bar{b} \in \mathbb{Z}_n$ with $a, b \in \mathbb{Z}$
we know that $a+b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$.
So, $\overline{a+b} \in \mathbb{Z}_n$ and $\overline{ab} \in \mathbb{Z}_n$.
That is $\bar{a}+\bar{b} \in \mathbb{Z}_n$ and $\bar{a}\bar{b} \in \mathbb{Z}_n$.

② Le
in
$\bar{a}$
S
S

② Let $a, b, c, d \in \mathbb{Z}$ with $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$ in $\mathbb{Z}_n$. We need to show that $\overline{a+c} = \overline{b+d}$ and $\overline{a}\,\overline{c} = \overline{b}\,\overline{d}$.

Since $\overline{a} = \overline{b}$ we know $a \equiv b \pmod{n}$.

Since $\overline{c} = \overline{d}$ we know $c \equiv d \pmod{n}$.

Super-duper equivalence class thm

From last class at the very end we proved that this implies that

$$(a+c) \equiv (b+d) \pmod{n}$$

and $$ac \equiv bd \pmod{n}.$$

duper ence thm

Thus, $\overline{a+c} = \overline{b+d}$

and $\overline{ac} = \overline{bd}$.

So, $\bar{a}+\bar{c} = \bar{b}+\bar{d}$

and $\bar{a}\bar{c} = \bar{b}\bar{d}$. ▨

9/30
Monday

HW 3
4460 HW 4

① (b) Is $11 \equiv -5 \pmod 5$?

$11 - (-5) = 16$

$5 \nmid 16$

So, No

$a \equiv b \pmod n$
means
$n \mid (a-b)$

In $\mathbb{Z}_n$
$\bar{a} = \bar{b}$ iff
$a \equiv b \pmod n$

Super-duper equivalence class thm

?

④ (c)

Is $\overline{1} = \overline{13}$ in $\mathbb{Z}_6$?

$1 - 13 = -12$

$-12 = (6)(-2)$

So, $6 \mid (1-13)$.

Thus $1 \equiv -13 \pmod 6$

So, $\overline{1} = \overline{-13}$ in $\mathbb{Z}_6$

⑥ (f) In $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ calculate the following and reduce your answer $\overline{a}$ so that $0 \leq a \leq 6$.

$\overline{5} \cdot \overline{2} + \overline{1} + \overline{2} \cdot \overline{4} \cdot \overline{6}$

$= \overline{10} + \overline{1} + \overline{8} \cdot \overline{6} = \overline{3} + \overline{1} + \overline{1} \cdot \overline{6} = \overline{4} + \overline{6}$

$= \overline{10} = \boxed{\overline{3}}$

$\overline{10} = \overline{3}$

$\overline{8} = \overline{1}$

Number Theory Applications

In number theory, people study integer solutions to Diophantine equations.

Diophantine equations are polynomials in as many variables as you want with integer coefficients.

Ex: Consider

$$x^2 + y^2 = z^2.$$

Q1: Are there solutions where $x, y, z \in \mathbb{Z}$?

Q2: If so, how many solutions are there?

Q3: Is there a formula for all the integer solutions?

Q1 Yes.

$(x,y,z)=(3,4,5)$ since $3^2+4^2=5^2$

$(x,y,z)=(5,12,13)$ since $5^2+12^2=13^2$

Q2: Infinitely many.

For example you can scale any solution.

$(x,y,z)=(3k,4k,5k)$ is a solution for any $k=1,2,3,4,\ldots$

$(3k)^2+(4k)^2=(5k)^2 \Longrightarrow$

More solutions: $(6,8,10)$, $(9,12,15)$, ...

$k=2$ $k=3$

Q3: Yes.

$x=k(m^2-n^2)$

$y=k(2mn)$

$z=k(m^2+n^2)$

where k,m,n are positive integers, $m>n$, and $\gcd(m,n)=1$, m and n have opposite parity (they can't both be even or both be odd)

MATH 4460

Gives all integer solutions to $x^2+y^2=z^2$

Ex: $m = 2$
$n = 1$
$k = 1$

$X = k(m^2 - n^2) = 1 \cdot (2^2 - 1^2) = 3$
$y = k(2mn) = 1 \cdot (2 \cdot 2 \cdot 1) = 4$
$z = k(m^2 + n^2) = 1 \cdot (2^2 + 1^2) = 5$

$m = 3$
$n = 2$
$k = 1$

$X = 1 \cdot (3^2 - 2^2) = 5$
$y = 1 \cdot (2 \cdot 3 \cdot 2) = 12$
$z = 1 \cdot (3^2 + 2^2) = 13$

One method to derive the formula:

Idea

$i^2 = -1$

$$z^2 = x^2 + y^2 = (x+iy)(x-iy)$$

Then you use properties of the Gaussian integers

$$\mathbb{Z}[i] = \{x+iy \mid x, y \in \mathbb{Z}\}$$

This set has a unique factorization theorem into primes.

2 is no longer prime in $\mathbb{Z}[i]$

$2 = (1+i)(1-i)$

$5 = (2+i)(2-i)$

$5 = 2^2 + 1^2$

5 is the sum of two squares

p factors iff $p \equiv 1 \pmod 4$

Ex: (Fermat's Last Theorem)

Fermat claimed to have a proof of:

There are no integer solutions to $x^n + y^n = z^n$ with $n > 2$ except if one of x, y, z are 0.

} Andrew Wiles proved this in 1995.

[NOVA documentary "The Proof"]

Fermat proved this case {

Ex: $x^3 + y^3 = z^3$ has no non-zero integer sols.

($0^3 + 2^3 = 2^3$ is called a trivial sol.)

4460
HW 4

(14) Prove that there are no integer solutions to $x^2-5y^2=2$.

You can't just check all x, y

x	y	x^2-5y^2
1	1	-4
2	1	-1
2	2	-16
10	1	95
⋮	⋮	⋮

Idea

If there was an integer solution to $x^2-5y^2=2$ then

$(x^2-5y^2) \equiv 2 \pmod{n}$

for any $n \geq 2$.

pf: Suppose there exists $x, y \in \mathbb{Z}$ with $x^2 - 5y^2 = 2$.
We will show that this leads to a contradiction
Since $x^2 - 5y^2 = 2$ we have that $(x^2 - 5y^2) \equiv 2 \pmod 5$

Note that $-5 \equiv 0 \pmod 5$.
So we get $x^2 \equiv 2 \pmod 5$.
This is a contradiction by the following table.

x	$x^2 \pmod 5$
0	(0)
1	(1)
2	(4)
3	$9 \equiv (4) \pmod 5$
4	$16 \equiv (1) \pmod 5$

The only squares modulo 5 are 0, 1, 4.

So, there is no x with $x^2 \equiv 2 \pmod 5$.
Thus, there are no integers x & y with $x^2 - 5y^2 = 2$. ∎

Hw 4 4460

(17) Prove that if $x \in \mathbb{Z}$, $x > 1$, and x ends in a 7 then x is not a square $\left[x \neq a^2 \text{ where } a \in \mathbb{Z} \right]$

Ex: 137 is not a square.

Method 1

$1^2 = 1$ $7^2 = 49$
$2^2 = 4$ $8^2 = 64$
$3^2 = 9$ $9^2 = 81$
$4^2 = 16$ $10^2 = 100$
$5^2 = 25$ $11^2 = 121$
$6^2 = 36$ $12^2 = 144$

Method 2

$137 = 130 + 7$

$\equiv 0 + 7 \pmod{10}$

$\equiv 7 \pmod{10}$

Show 7 is not a square modulo 10.

x	$x^2 \pmod{10}$
0	0
1	1
2	4
3	9
4	$16 \equiv 6 \pmod{10}$
5	$25 \equiv 5 \pmod{10}$
6	$36 \equiv 6 \pmod{10}$
7	$49 \equiv 9 \pmod{10}$
8	$64 \equiv 4 \pmod{10}$
9	$81 \equiv 1 \pmod{10}$

There are no 7's here.

For a general proof look online at solutions

10/2
Weds

Def: A partition of a set S is a family of sets $\mathcal{A}$

where

① Every $A \in \mathcal{A}$ satisfies $A \subseteq S$.

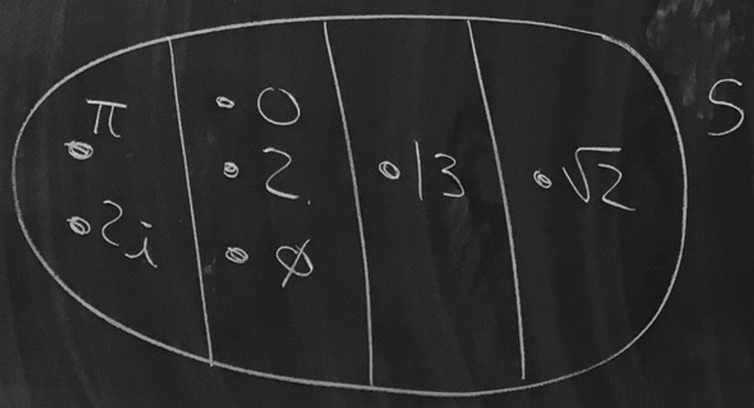
② $\bigcup_{A \in \mathcal{A}} A = S$

③ If $A, B \in \mathcal{A}$ and $A \neq B$
then $A \cap B = \emptyset$

Ex: $S = \{\pi, 13, 0, 2, \sqrt{2}, 2i, \phi\}$

$\mathcal{A}_0 = \{\{\pi, 2i\}, \{0, 2, \phi\}, \{13\}, \{\sqrt{2}\}\}$

$\mathcal{A}_0$ partitions S into 4 disjoint pieces.



$\mathcal{A}_0$ is a partition of S

① $\{\pi, 2i\} \subseteq S$
$\{0, 2, \phi\} \subseteq S$
$\{13\} \subseteq S$
$\{\sqrt{2}\} \subseteq S$

② $\bigcup_{A \in \mathcal{A}_0} A = \{\pi, 2i\} \cup \{0, 2, \phi\} \cup \{13\} \cup \{\sqrt{2}\} = S$

③ $\{\pi, 2i\} \cap \{0, 2, \phi\} = \phi$
$\{\pi, 2i\} \cap \{13\} = \phi$
$\{\pi, 2i\} \cap \{\sqrt{2}\} = \phi$
$\{0, 2, \phi\} \cap \{13\} = \phi$
$\{0, 2, \phi\} \cap \{\sqrt{2}\} = \phi$
$\{13\} \cap \{\sqrt{2}\} = \phi$

Ex: $S = \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\mathbb{Z}_3$ is a partition of $\mathbb{Z}$

$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$\bar{2} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

Theorem: Let S be a non-empty set.
Let $\sim$ be an equivalence relation on S.
The set of equivalence classes

$$S/_{\sim} = \{ \bar{a} \mid a \in S \}$$

is a partition of S.

Ex: $\mathbb{Z}_4 = \mathbb{Z}/_{(\equiv \bmod 4)} = \{ \bar{a} \mid a \in \mathbb{Z} \} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$

Ex:

$S = \mathbb{Z}$

$\sim$ is $\equiv \bmod 3$

$$\bigcup_{a \in \mathbb{Z}} \bar{a} = \bar{0} \cup \bar{1} \cup \overline{-1} \cup \bar{2} \cup \overline{-2} \cup \bar{3} \cup \overline{-3} \cup \dots$$

$$= \bar{0} \cup \bar{1} \cup \bar{2}$$

$$= \bigcup_{\bar{a} \in \mathbb{Z}_3} \bar{a}$$

Proof of theorem:

① Let $\bar{a} \in S/\sim$ where $a \in S$.

Then

$$\bar{a} = \{ b \mid b \in S \text{ and } a \sim b \} \subseteq S.$$

② Recall that if $\bar{a} \in S/\sim$ then $a \in \bar{a}$ by the super-equivalence class theorem.

Thus, $S = \bigcup_{a \in S} \{a\} \subseteq \bigcup_{a \in S} \bar{a} \subseteq \bigcup_{\bar{a} \in S/\sim} \bar{a}$

$\{a\} \subseteq \bar{a}$

So, $S \subseteq \bigcup_{\bar{a} \in S/\sim} \bar{a}$.

From ① each $\bar{a} \subseteq S$, so

$\bigcup_{\bar{a} \in S/\sim} \bar{a} \subseteq S$.

Thus,

$S = \bigcup_{\bar{a} \in S/\sim} \bar{a}$

③ By the super-duper equivalence class theorem, if $a, b \in S$ then either $\bar{a} = \bar{b}$ or $\bar{a} \cap \bar{b} = \emptyset$.

Theorem: Let S be a non-empty set.
Let $\mathcal{A}$ be a partition of S.
Define a relation on S by the following: Given $a, b \in S$, then $a \sim b$ iff there exists $A \in \mathcal{A}$ with $a \in A$ and $b \in A$.

Then:

1. $\sim$ is an equivalence relation on S.
2. $S/\sim = \mathcal{A}$

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

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

We now construct an equivalence relation $\sim$ on S using $\mathcal{A}$.

Examples: $1 \sim 2$ since $1 \in \{1,2,3\}$ and $2 \in \{1,2,3\}$

$4 \sim 4$ since $4 \in \{4\}$ and $4 \in \{4\}$

$\sim = \{(1,1), (1,2), (1,3), (2,2), (2,1), (2,3), (3,1), (3,2), (3,3), (4,4), (5,5)\}$

comes from $\{1,2,3\}$ — comes from $\{4\}$ — comes from 5

$\bar{1} = \{1,2,3\} = \bar{2} = \bar{3}$

$\bar{4} = \{4\}$

$\bar{5} = \{5\}$

} equivalence classes

$S/\sim = \{\bar{1}, \bar{4}, \bar{5}\} = \{\{1,2,3\}, \{4\}, \{5\}\} = \mathcal{A}$

Proof of theorem: Recall $a \sim b$ iff there exists $A \in \mathcal{A}$ with $a \in A$ and $b \in A$.

① (reflexive) Let $x \in S$.

By the def of partition, $S = \bigcup_{A \in \mathcal{A}} A$.

So, $x \in \bigcup_{A \in \mathcal{A}} A$.

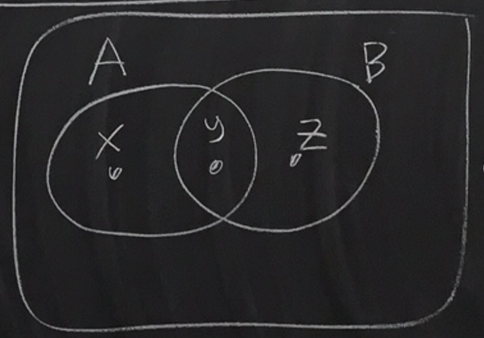
So, there exists $A \in \mathcal{A}$ with $x \in A$.

Thus, $x \sim x$ [since $x \in A$ and $x \in A$].

(symmetric) Let $x, y \in S$ and $x \sim y$.
Then there exists $A \in \mathcal{A}$ with
$x \in A$ and $y \in A$.
So, $y \in A$ and $x \in A$.
Thus, $y \sim x$.

(transitive) Let $x, y, z \in S$ and $x \sim y$ and $y \sim z$.
Since $x \sim y$ there exists $A \in \mathcal{A}$ with $x \in A$ and $y \in A$.
Since $y \sim z$ there exists $B \in \mathcal{A}$ with $y \in B$ and $z \in B$.

$\Rightarrow$ Since $y \in A \cap B$ we know $A \cap B \neq \phi$.
Since $\mathcal{A}$ is a partition we must have $A = B$ [since if $A \neq B$, the partition def part 3 would imply $A \cap B = \phi$].
Thus, $x \in A$ and $z \in A$.
So, $x \sim z$ (1)



(2) We want to show that $S/\sim = \mathcal{A}$.

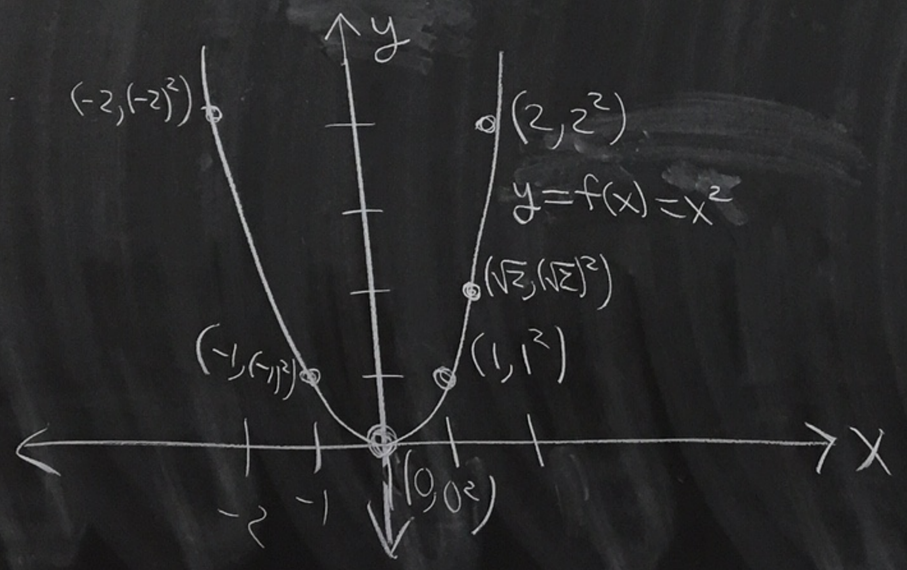
$\subseteq$: Let $\bar{a} \in S/\sim$.
Pick the unique $A \in \mathcal{A}$ with $a \in A$.
Then $\bar{a} = A$ by the def of $\sim$.
So, $\bar{a} \in \mathcal{A}$.

$\supseteq$: Let $A \in \mathcal{A}$.
Pick any $a \in A$.
Then by the def of $\sim$ we have $\bar{a} = A$.
So, $A \overset{\text{def}}{=} \bar{a} \in S/\sim$. ∎

Mon
10/7

Functions (HW 4 material)

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



How can we think of f as a set?

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

Here $f \subseteq \mathbb{R} \times \mathbb{R}$

Def: Let A and B be sets.
Let f be a subset of $A \times B$.
We say that f is a function from A to B if

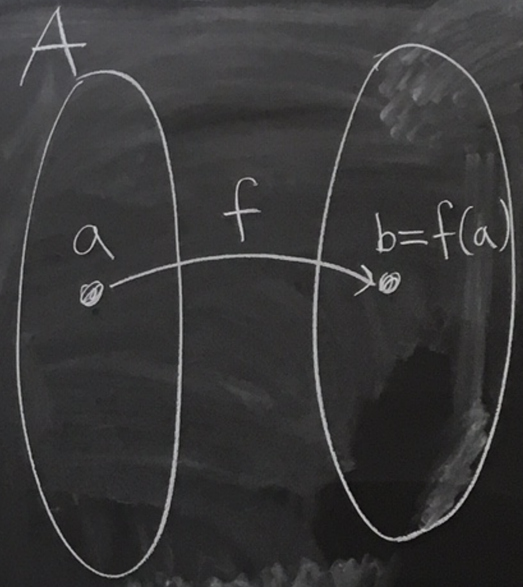
① For every $a \in A$ there exists $b \in B$ where $(a,b) \in f$.

and ② If (a,b_1) and (a,b_2) are in f, then $b_1 = b_2$.

This saying that we can plug any $a \in A$ into f and get b. b will be $f(a)$.

There is a unique b for each a. This is the vertical line test.

If this is the case, then we write $f: A \to B$ to mean that f is a function from A to B.



- The set A is called the <u>domain</u> of f.
- The set B is called the <u>codomain</u> of f.
- If $(a,b) \in f$ then we write $f(a)=b$.
  If $(a,b) \notin f$ then we write $f(a) \neq b$.

- The <u>range</u> of f is

$$\text{range}(f) = \{ b \in B \mid \exists a \in A \text{ with } f(a)=b \}$$

<u>Recall:</u> $\exists$ means "there exists"

Ex: $A = \{-1, 100, 3, \frac{72}{10}\}$

$B = \{\pi, -12, -1, \frac{1}{2}, 17, 14\}$

$f = \{(-1,-1), (100,\pi), (3,17), (\frac{72}{10},-1)\}$

Is f a function from A to B?

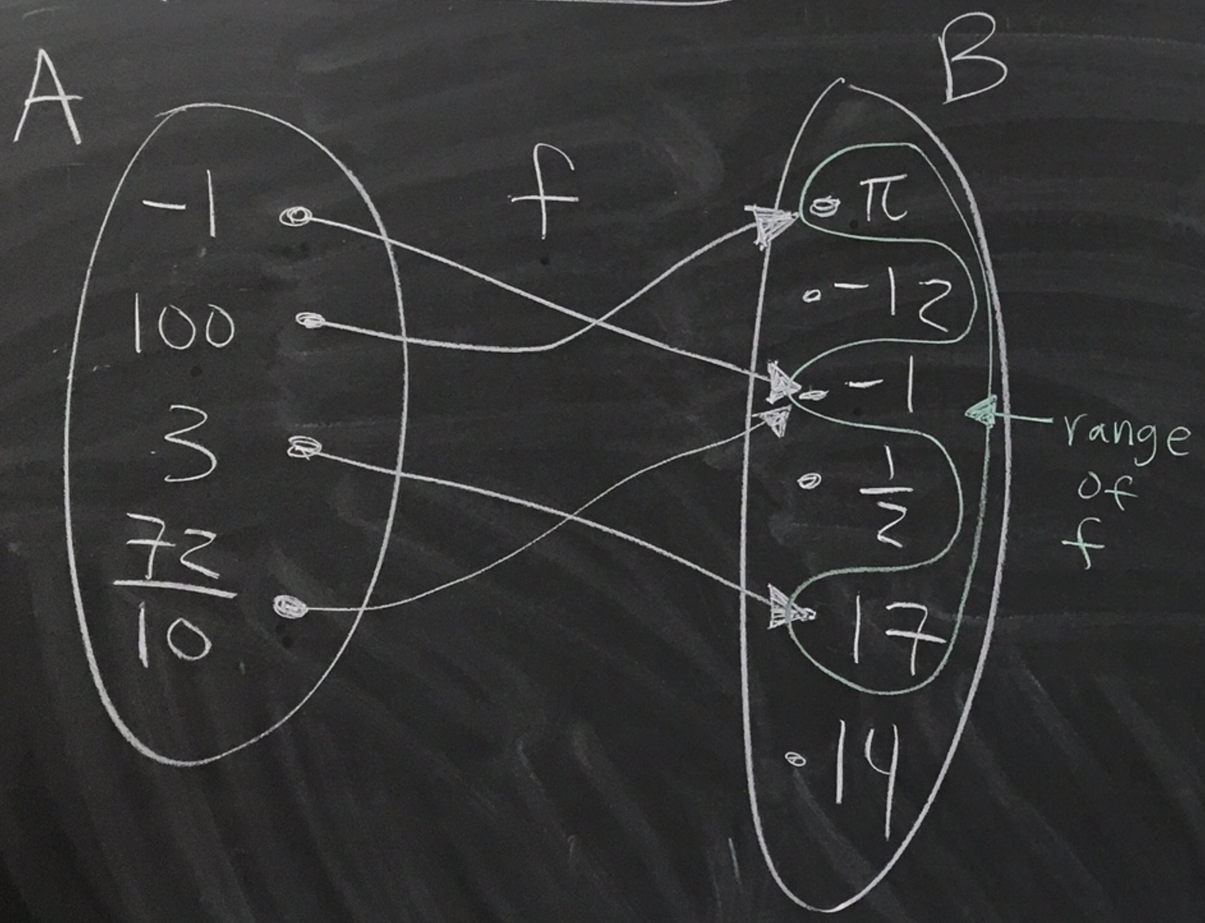
① ✓
② ✓
} Yes

$f(-1) = -1$
$f(100) = \pi$
$f(3) = 17$
$f(\frac{72}{10}) = -1$

f would not be a function if say $(-1,\pi)$ and $(-1,-12)$ were in f

$(-1,\pi) \leftarrow f(-1) = \pi$
$(-1,-12) \leftarrow f(-1) = -12$
} What is $f(-1)$?

Picture of f



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

$\text{codomain}(f) = B$

$\text{range}(f) = \{b \in B \mid \exists\, a \in A \text{ with } f(a) = b\}$

$= \{\pi, -1, 17\}$

For example, $\pi \in \text{range}(f)$ since $100 \in A$ and $f(100) = \pi$.

$-12 \notin \text{range}(f)$ since there is no $a \in A$ with $f(a) = -12$.

Ex:

Is
①
②

Ex: $A = \{-1, 100, 3, \frac{72}{10}\}$

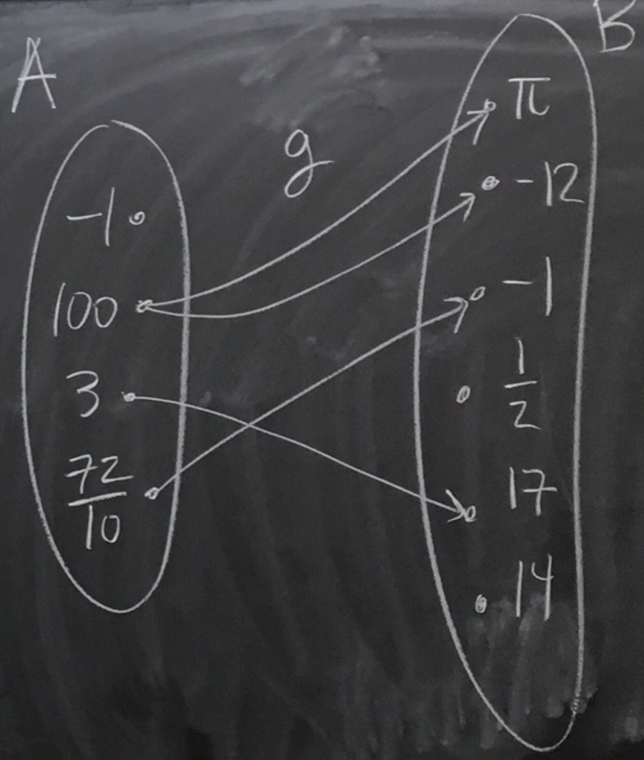
$B = \{\pi, -12, -1, \frac{1}{2}, 17, 14\}$

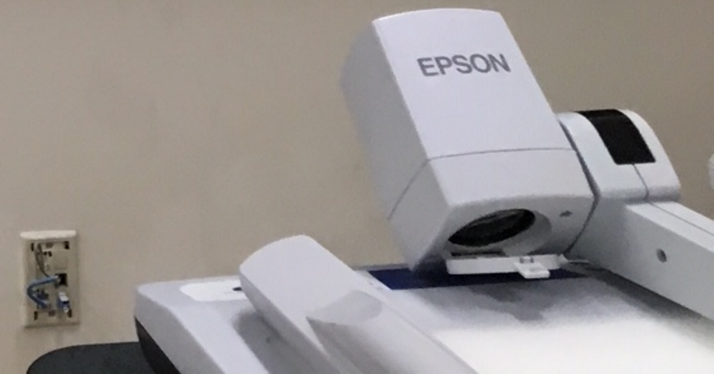
$g = \{(100, \pi), (3, 17), (\frac{72}{10}, -1), (100, -12)\}$

Is g a function from A to B? NO

① There is no $b \in B$ where $(-1, b) \in g$ or $g(-1) = b$.
① is not satisfied.

③ $(100, \pi)$ and $(100, -12)$ are both in g. Thats saying $g(100) = \pi$ and $g(100) = -12$. That's no good.





Test review — TOPICS

- HW 1 - set builder notation
- Hw 2 — set theory
- Hw 3 — equivalence relations modulo n

Structure

— calculations (4 prob.)

— proofs (3 prob.)

Hw 2

② Let $A = \{2k \mid k \in \mathbb{Z}\}$
and $B = \{3n \mid n \in \mathbb{Z}\}$
Prove $A \cap B = \{6m \mid m \in \mathbb{Z}\}$

proof:

$\subseteq$: Let $x \in A \cap B$.
Then $x \in A$ and $x \in B$.

So, $x = 2k$ where $k \in \mathbb{Z}$
and $x = 3n$ where $n \in \mathbb{Z}$.

Thus, $2k = 3n$.

Note that n cannot be odd because
if n was odd then $3n$ would be odd.
But $3n = 2k$ is even.

So n is even.
Thus $n = 2l$ where $l \in \mathbb{Z}$.
So, $x = 3n = 3(2l) = 6l \in \{6m \mid m \in \mathbb{Z}\}$.
So, $A \cap B \subseteq \{6m \mid m \in \mathbb{Z}\}$

⊇: Let $y \in \{6m \mid m \in \mathbb{Z}\}$

Then, $y = 6m$ where $m \in \mathbb{Z}$.

So, $y = 6m = 2(3m) \in A$

And, $y = 6m = 3(2m) \in B$.

Thus, $y \in A \cap B$.

Therefore, $\{6m \mid m \in \mathbb{Z}\}$.

By ⊆ and ⊇ we have $A \cap B = \{6m \mid m \in \mathbb{Z}\}$ ∎

HW 2

(15) Let A and B be sets.
Prove that A−B and B are disjoint.

pf: We need to show that $(A-B)\cap B=\phi$.
Suppose that $(A-B)\cap B\neq\phi$.
Then there exists $x\in(A-B)\cap B$.
So, $x\in A-B$ and $x\in B$.
Thus, $x\in A$ and $x\notin B$, and $x\in B$.

We can't have
$x\notin B$ and $x\in B$.
This is ridiculous!
So, $(A-B)\cap B=\phi$.
Thus, A−B and B are disjoint.

Hammock
Chapter 8

(13) Let A, B, C be sets. Then

$$A - (B \cup C) = (A - B) \cap (A - C).$$

Proof:

$\subseteq$: Let $x \in A - (B \cup C)$.

Then $x \in A$ and $\boxed{x \notin B \cup C}$.

What does $x \notin B \cup C$ mean?

It means that "$x \in B \cup C$" is not true.

We need the negation of "$x \in B$ or $x \in C$".

So "$x \notin B$ and $x \notin C$" is true.

$\neg(P \text{ or } Q)$

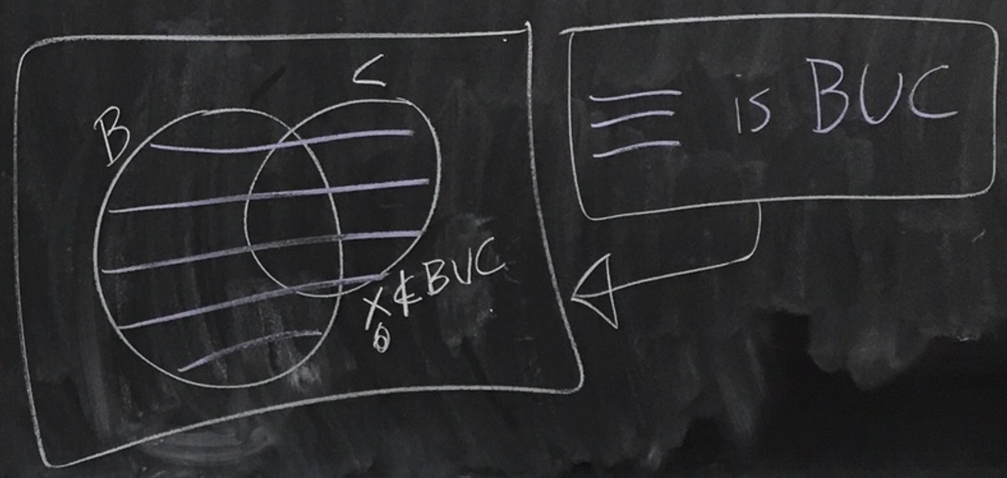
$(\neg P)$ and $(\neg Q)$

In summary, we have

$x \in A$ and $\underbrace{x \notin B \text{ and } x \notin C}_{\text{from } x \notin B \cup C}$,

So, $x \in (A - B)$ and $x \in (A - C)$.

Thus, $x \in (A - B) \cap (A - C)$.



$\equiv$ is $B \cup C$

(2): Let $x \in (A-B) \cap (A-C)$.

Then $x \in A-B$ and $x \in A-C$.

So, $x \in A$ and $x \notin B$, and $x \in A$ and $x \notin C$.

Thus, $x \in A$ and $\boxed{x \notin B \text{ and } x \notin C}$.

So, $x \in A$ and $\boxed{x \notin B \cup C}$.

Thus, $x \in A-(B \cup C)$.

Therefore, $(A-B) \cap (A-C) \subseteq A-(B \cup C)$.

Hammock 11.3

⑦ Define $\sim$ on $\mathbb{Z}$ by
$a \sim b$ iff $3a-5b$ is even.
Prove $\sim$ is an equivalence relation

pf:

(reflexive) Let $x \in \mathbb{Z}$.
Then $3x-5x = -2x = 2(-x)$ is even.
So, $x \sim x$.

(symmetric) Let $x, y \in \mathbb{Z}$.

Suppose $x \sim y$.

Then, $3x-5y$ is even.

So, $3x-5y = 2\Delta$ where $\Delta \in \mathbb{Z}$.

Adding $-8x+8y$ to both sides yields

$$3y-5x = 2(\underbrace{\Delta-4x+4y}_{\text{even}}).$$

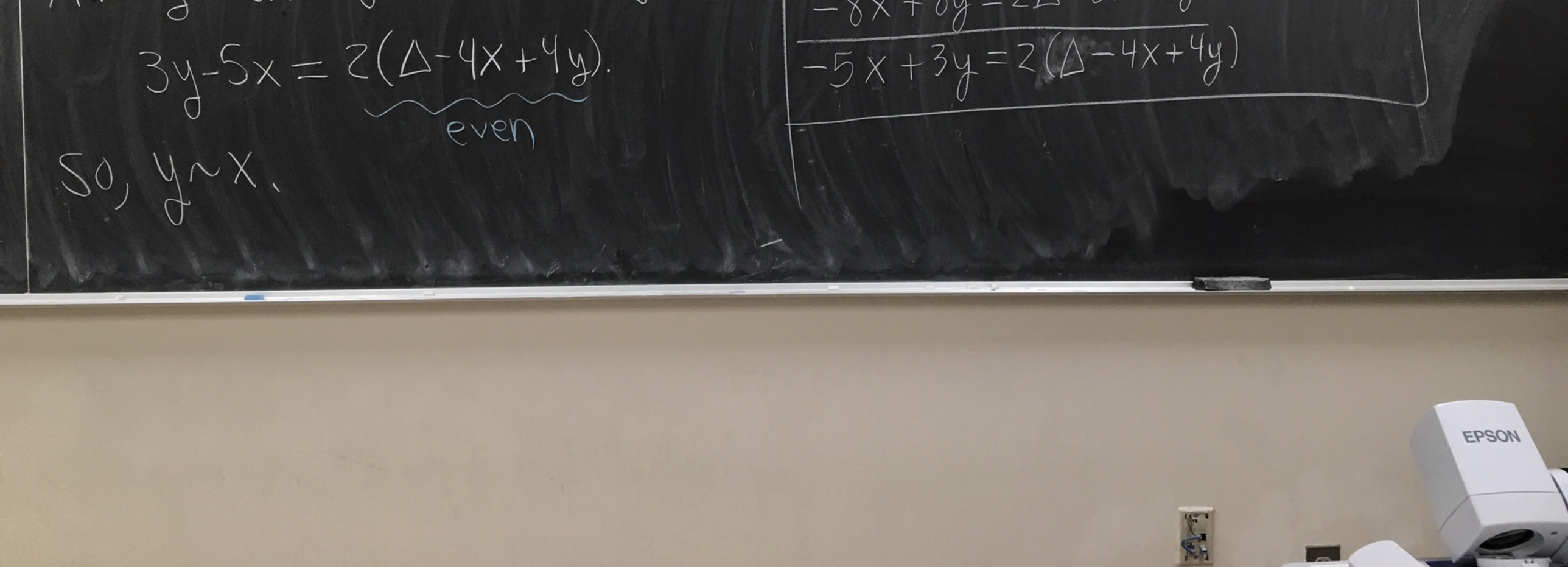
So, $y \sim x$.

Scratchwork

Given: $3x-5y = 2\Delta \leftarrow x \sim y$

Want: $3y-5x = 2(\text{integer}) \leftarrow y \sim x$

$$3x-5y = 2\Delta$$
$$-8x+8y = 2\Delta-8x+8y$$
$$-5x+3y = 2(\Delta-4x+4y)$$



Scratchwork

Given: $3x-5y=2k$

$3y-5z=2l$

Want: $3x-5z=2(?)$

Add

(transitive). Let $x,y,z\in\mathbb{Z}$.

Suppose $x\sim y$ and $y\sim z$.

Then, $3x-5y=2k$

and $3y-5z=2l$ where $k,l\in\mathbb{Z}$.

Adding these equations produces

$3x-2y-5z=2k+2l$.

So, $3x-5z=2(k+l+y)$.

Thus, $x\sim z$. ∎

MATH 4460 HW #4

(13) Prove that

$$15x^2 - 7y^2 = 1$$

has no integer solutions.

Pf: (By contradiction)

Suppose there exist $x, y \in \mathbb{Z}$ with $15x^2 - 7y^2 = 1$.

So in $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ we have

$$\overline{15x^2 - 7y^2} = \bar{1}.$$

Then,

$$\bar{15}\,\bar{x}^2 + \overline{-7}\,\bar{y}^2 = \bar{1}$$

in $\mathbb{Z}_7$.

So, $\bar{x}^2 = \bar{1}$ in $\mathbb{Z}_7$

But $\bar{x} = \bar{1}$ works in $\mathbb{Z}_7$.

So this leads nowhere.

In $\mathbb{Z}_7$,

$\bar{7} = \bar{0}$

$\bar{15} = \bar{1}$

Let's look in $\mathbb{Z}_3$ now.

So in $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ we have

$$\overline{15}\,\bar{x}^2 + \overline{-7}\,\bar{y}^2 = \bar{1}.$$

In $\mathbb{Z}_3$

$\overline{15} = \bar{0}$

$\overline{-7} = \bar{2}$

So, $\bar{2}\bar{y}^2 = \bar{1}$ in $\mathbb{Z}_3$.

There is no y with $\bar{2}\bar{y}^2 = \bar{1}$ in $\mathbb{Z}_3$ by the following table.

In $\mathbb{Z}_3$.

$\bar{y}$	$\bar{2}\bar{y}^2$
$\bar{0}$	$\bar{2}\cdot\bar{0}^2 = \bar{0}$
$\bar{1}$	$\bar{2}\cdot\bar{1}^2 = \bar{2}$
$\bar{2}$	$\bar{2}\cdot\bar{2}^2 = \bar{8} = \bar{2}$

$\bar{2}\bar{y}^2 = \bar{1}$ has no solutions in $\mathbb{Z}_3$

Hence, contradiction. So, there are no $x, y \in \mathbb{Z}$ with $15x^2 - 7y^2 = 1$. ∎

MATH 44

(13) Prove

Monday
10/14

Currently

Test 2 - Weds
Nov 6

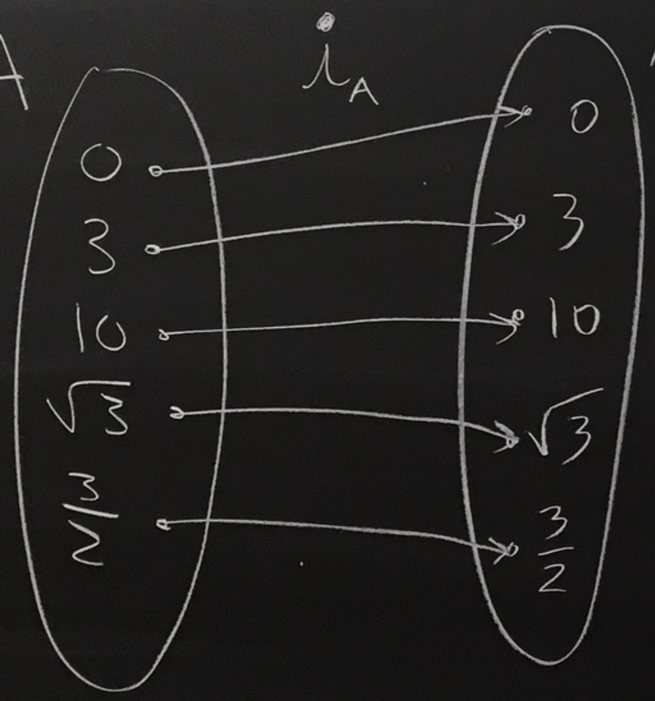
Move test 2 to
Weds - Nov 13

Functions continued...

Ex: Let A be any set.
The identity function on A
is the function $i_A : A \to A$
where $i_A(x) = x$ for all $x \in A$.

Sometimes we just use i
instead of i_A.

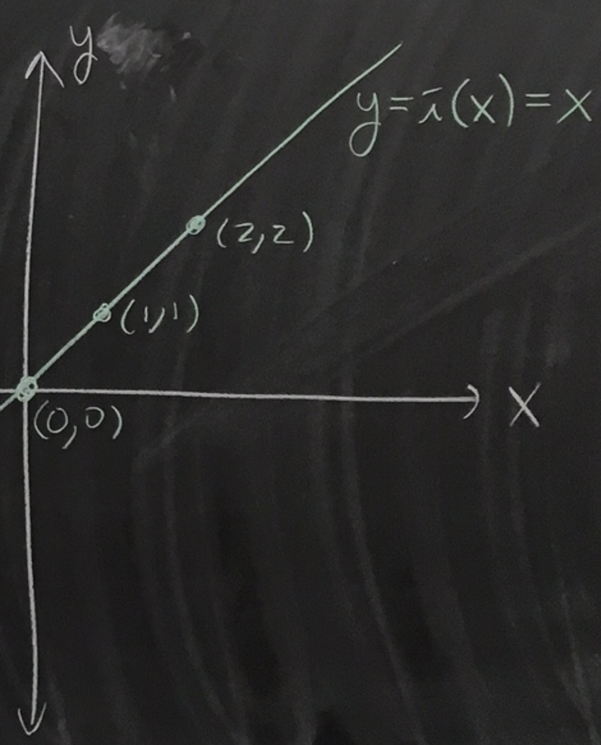
Ex: $A = \{0, 3, 10, \sqrt{3}, \frac{3}{2}\}$



Ex: $A = \mathbb{R}$

$i : \mathbb{R} \to \mathbb{R}$ ← $i = i_{\mathbb{R}}$

$i(x) = x$



Ex: Let $n \in \mathbb{Z}$, $n \geq 2$.

Define the reduction modulo n map

to be $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$

where $\pi_n(x) = \overline{x}$.

map means function

mapping is also used

Ex: $n=3$, $\pi_3 : \mathbb{Z} \to \mathbb{Z}_3$ where $\pi_3(x) = \overline{x}$

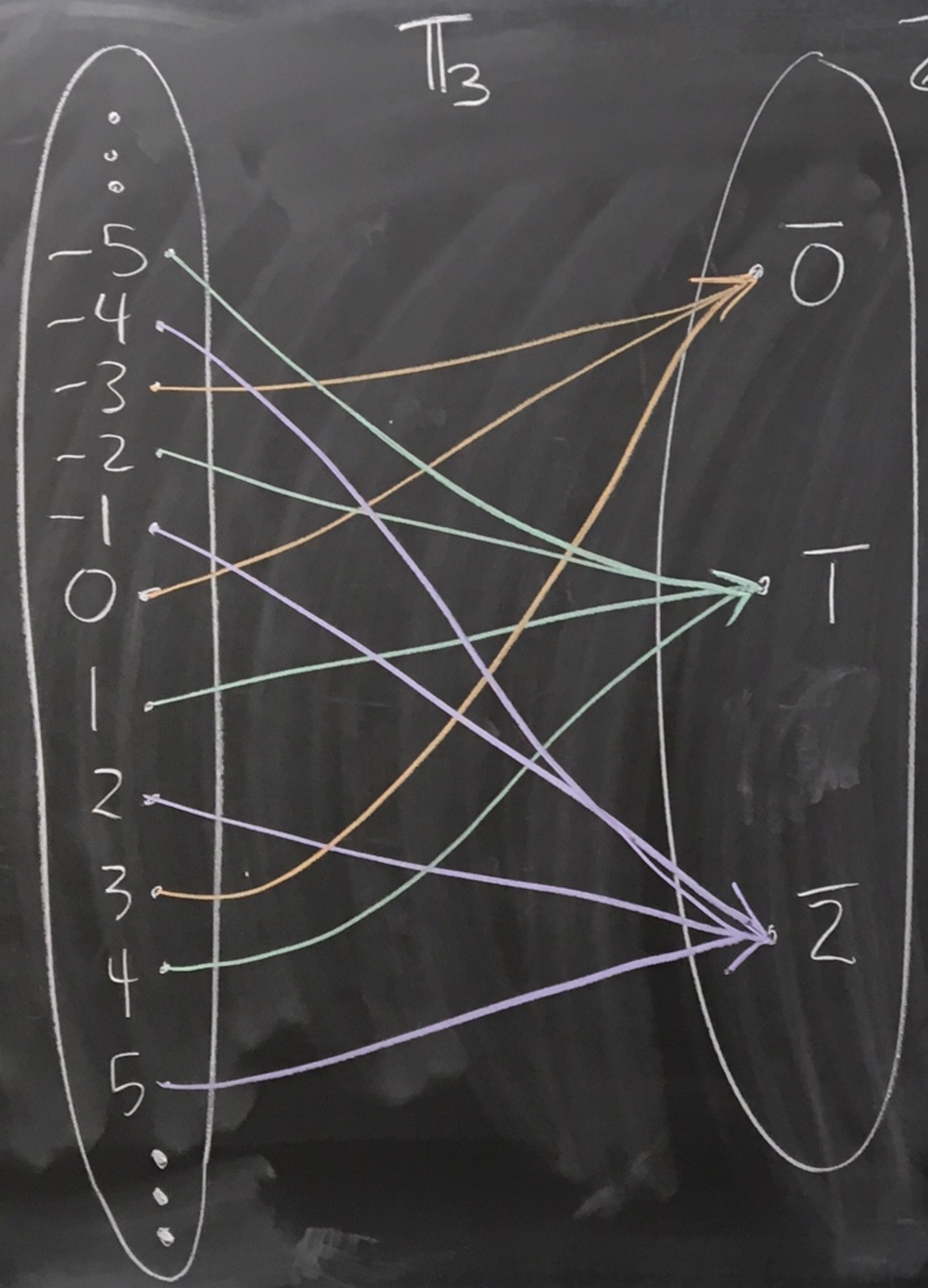
$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$

$\pi_3(1) = \overline{1}$

$\pi_3(4) = \overline{4} = \overline{1}$

$\pi_3(-10) = \overline{-10} = \overline{2}$

$-10 - 2 = -12 + 3$ | (-12)



$\text{domain}(\pi_3) = \mathbb{Z}$

$\text{codomain}(\pi_3) = \mathbb{Z}_3$

$\text{range}(\pi_3) = \mathbb{Z}_3$

$\mathbb{Q}$ ← rational numbers ie fractions

Ex: Suppose you and your friend Peter want to define a function.

You say "what about the function $f: \mathbb{Q} \to \mathbb{Q}$ given by $f\left(\frac{a}{b}\right) = \frac{b}{a}$."

Peter says: "I don't know if that function is ok. what about $f\left(\frac{0}{3}\right) = \frac{3}{0}$? Isn't that undefined?"

You say "Oh, you're right. Good call."

Ex: Then you say, "ok, I've got it.
what about $g: \mathbb{Q} \to \mathbb{Q}$ where $g(\frac{a}{b}) = a$?
That totally works. For example,
$g(\frac{7}{11}) = 7$ and $g(\frac{0}{3}) = 0$.
See everything's ok."
Peter says: "Hey, $g(\frac{14}{22}) = 14$
and $g(\frac{7}{11}) = 7$ but $\frac{14}{22} = \frac{7}{11}$ 111 000
That still is no good."
You say, "Ah man, too bad."

How to show that $f: A \to B$ is well-defined

Check the following:

① If $a \in A$, then $f(a) \in B$.

② If some or all of the elements in A can be expressed in more than one way then we must check that if $a_1, a_2 \in A$ and $a_1 = a_2$ then $f(a_1) = f(a_2)$.

Ex: Is $f: \mathbb{Q} \to \mathbb{Q}$ given by $f\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)^2$ well-defined?

Recall

$\frac{a}{b} = \frac{c}{d}$ in $\mathbb{Q}$

iff

$ad = bc$

Yes, f is well-defined

① Let $\frac{a}{b} \in \mathbb{Q}$. So, $a, b \in \mathbb{Z}$, $b \neq 0$.

Then $f\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$.

And, $a^2 \in \mathbb{Z}$, $b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ (since $b \neq 0$).

So, $\frac{a^2}{b^2} \in \mathbb{Q}$.

② Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ where $\frac{a}{b} = \frac{c}{d}$.

We need to show that $f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right)$.

Since $\frac{a}{b} = \frac{c}{d}$ we have that $ad = bc$.

Thus, $(ad)^2 = (bc)^2$.

So, $a^2d^2 = b^2c^2$.

Hence, $\frac{a^2}{b^2} = \frac{c^2}{d^2}$.

So, $f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right)$.

Ex: Let $n \in \mathbb{Z}$, $n \geq 2$.
Pick $a \in \mathbb{Z}$.
Define

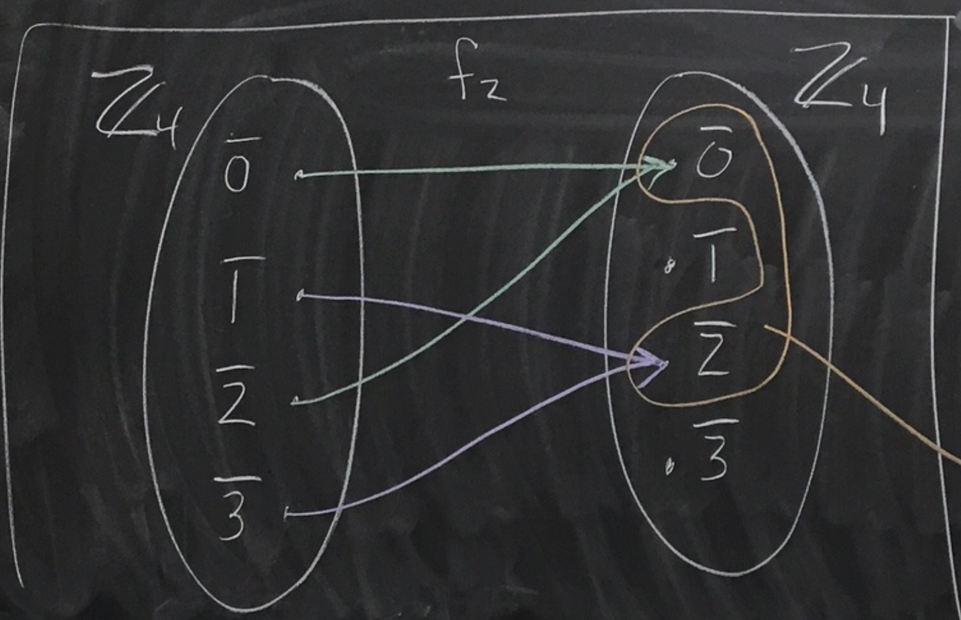
$$f_a : \mathbb{Z}_n \to \mathbb{Z}_n$$

by

$$f_a(\bar{x}) = \bar{a} \cdot \bar{x}$$

For example,
let $n = 4$ and $a = 2$.

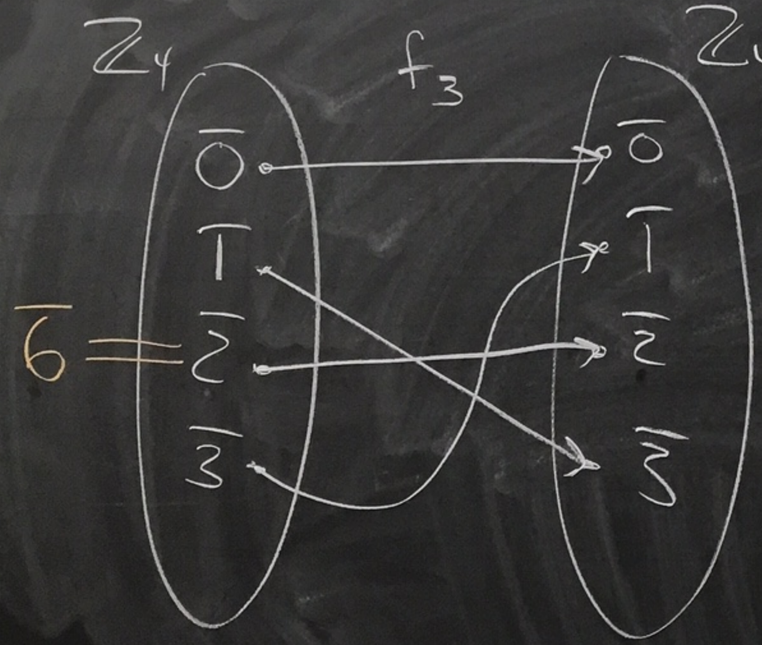
$$f_2 : \mathbb{Z}_4 \to \mathbb{Z}_4 \text{ where } f_2(\bar{x}) = \bar{2} \cdot \bar{x}$$



$f_2(\bar{0}) = \bar{2} \cdot \bar{0} = \bar{0}$
$f_2(\bar{1}) = \bar{2} \cdot \bar{1} = \bar{2}$
$f_2(\bar{2}) = \bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$
$f_2(\bar{3}) = \bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$
$\text{range}(f_2) = \{\bar{0}, \bar{2}\}$

$f_3 : \mathbb{Z} \to \mathbb{Z}_4$

$f_3(\bar{x}) = \bar{3} \cdot \bar{x}$



$f_3(\bar{0}) = \bar{3} \cdot \bar{0} = \bar{0}$

$f_3(\bar{1}) = \bar{3} \cdot \bar{1} = \bar{3}$

$f_3(\bar{2}) = \bar{3} \cdot \bar{2} = \bar{6} = \bar{2}$

$f_3(\bar{3}) = \bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$

$\text{range}(f_3) = \mathbb{Z}_4$

$f_3(\bar{6}) = \bar{3} \cdot \bar{6}$
$= \bar{18} = \bar{2}$

Proposition: Let $n, a \in \mathbb{Z}$ with $n \geq 2$.
Then $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f_a(\bar{x}) = \bar{a} \cdot \bar{x}$ is well-defined.

Proof:

① Let $\bar{x} \in \mathbb{Z}_n$ where $x \in \mathbb{Z}$.

Since $a \in \mathbb{Z}$, we know $\bar{a} \in \mathbb{Z}_n$.
And $ax \in \mathbb{Z}$ so $\overline{ax} \in \mathbb{Z}_n$.
Thus, $f_a(\bar{x}) = \bar{a} \cdot \bar{x} = \overline{ax} \in \mathbb{Z}_n$.

② Suppose $x, y \in \mathbb{Z}$ and $\bar{x} = \bar{y}$ in $\mathbb{Z}_n$. Is $f_a(\bar{x}) = f_a(\bar{y})$?

Since $\bar{a} = \bar{a}$ and $\bar{x} = \bar{y}$ we know $\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{y}$ (from an earlier theorem in class.)
So, $f_a(\bar{x}) = f_a(\bar{y})$. ▨

Weds
10/16

HW 3

#④ Define $\bar{a} \oplus \bar{b} = \bar{a}^2 + \bar{b}^2$ on $\mathbb{Z}_n$.

Prove $\oplus$ is a well-defined operation on $\mathbb{Z}_n$.

$$\begin{array}{r} 3 \\ 4\overline{)13} \\ -12 \\ \hline 1 \end{array}$$

remainder

$\bar{13} = \bar{4} \cdot \bar{3} + \bar{1}$

$= \bar{0} \cdot \bar{3} + \bar{1}$

$= \bar{1}$

Ex: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{2} \oplus \bar{3} = \bar{2}^2 + \bar{3}^2 = \bar{4} + \bar{9} = \bar{13} = \bar{1}$

$\bar{4} = \bar{0}$

$\bar{13} = \bar{13} + \bar{4} + \bar{4} + \bar{4}$

$= \bar{1}$

Proof that $\oplus$ is well-defined on $\mathbb{Z}_n$

① Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$ where $a, b \in \mathbb{Z}$.

Then,

$$\bar{a} \oplus \bar{b} = \bar{a}^2 + \bar{b}^2 = \bar{a} \cdot \bar{a} + \bar{b} \cdot \bar{b}$$
$$= \overline{a^2 + b^2}$$
$$= \overline{a^2 + b^2}$$

And $a^2 + b^2 \in \mathbb{Z}$.

So, $\bar{a} \oplus \bar{b} = \overline{a^2 + b^2} \in \mathbb{Z}_n$.

Thm from class / In $\mathbb{Z}_n$:

If $\bar{x} = \bar{y}$ and $\bar{w} = \bar{z}$ then

$\bar{x} + \bar{w} = \bar{y} + \bar{z}$

$\bar{x} \cdot \bar{w} = \bar{y} \cdot \bar{z}$

② Let $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n$ where $\bar{a} = \bar{c}$ and $\bar{b} = \bar{d}$.

We need to show that $\bar{a} \oplus \bar{b} = \bar{c} \oplus \bar{d}$.

From a theorem in class, since $\bar{a} = \bar{c}$ we know $\bar{a}^2 = \bar{c}^2$.

Also since $\bar{b} = \bar{d}$ we get $\bar{b}^2 = \bar{d}^2$.

Since $\bar{a}^2 = \bar{c}^2$ and $\bar{b}^2 = \bar{d}^2$ we get

$\bar{a}^2 + \bar{b}^2 = \bar{c}^2 + \bar{d}^2$.

So, $\bar{a} \oplus \bar{b} = \bar{c} \oplus \bar{d}$. $\square$

Def: Let A and B be sets and $f: A \to B$.

We say that f is <u>one-to-one</u> or <u>injective</u> if

for every $a_1, a_2 \in A$ we have that the following is true:

If $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

<u>Contrapositive:</u> If $f(a_1) = f(a_2)$, then $a_1 = a_2$.

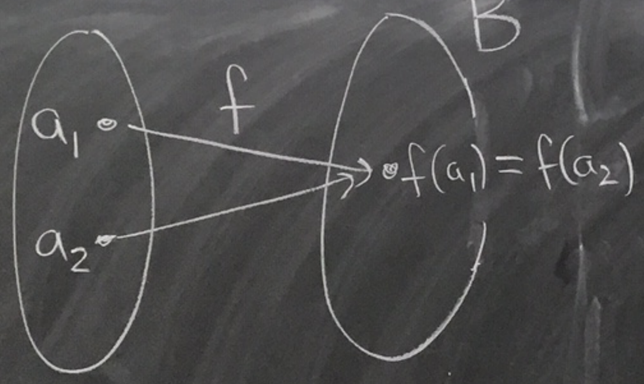
this means:
f is a function with
domain$(f) = A$
codomain$(f) = B$

input →
output →

If P, then Q

<u>Contrapositive:</u> If $\neg Q$, then $\neg P$.

A



not one-to-one
if $a_1 \neq a_2$

How to prove $f: A \to B$ is one-to-one

Let $a_1, a_2 \in A$.
Suppose $f(a_1) = f(a_2)$.

⋮ (proof stuff)

Conclude that $a_1 = a_2$.

Ex: Let $f: \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 10x + 1$.

Then f is one-to-one.

pf: Let $a, b \in \mathbb{R}$.

Suppose $f(a) = f(b)$.

Then $10a + 1 = 10b + 1$

So, $10a = 10b$.

Thus, $a = b$.

Therefore, f is one-to-one. ☐

Note that f is well-defined since $f(x) = 10x + 1 \in \mathbb{R}$ for every $x \in \mathbb{R}$

Ex:

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

$f(x) = \frac{1}{x}$

f is not well-defined since $0 \in \mathbb{R}$ ← domain

but $f(0) = \frac{1}{0} \notin \mathbb{R}$ ← codomain

Ex: Let $n \in \mathbb{Z}$ with $n \geq 2$.

Define $f: \mathbb{Z}_n \to \mathbb{Z}_n$ by

$f(\bar{x}) = \bar{x}^2$.

f is well-defined

① Let $\bar{x} \in \mathbb{Z}_n$ where $x \in \mathbb{Z}$.

Then,

$f(\bar{x}) = \bar{x}^2 = \bar{x} \cdot \bar{x} \in \mathbb{Z}_n$.

② Suppose $\bar{x}_1 = \bar{x}_2$ where $x_1, x_2 \in \mathbb{Z}$.

Then,

$f(\bar{x}_1) = \bar{x}_1^2 = \bar{x}_2^2 = f(\bar{x}_2)$. ▨

Thm from class.
Multiply $\bar{x}_1 = \bar{x}_2$ and $\bar{x}_1 = \bar{x}_2$

f(6)

Ex: $f : \mathbb{Z}_7 \to \mathbb{Z}_7$ $\quad f(\bar{x}) = \bar{x}^2$

calculations

$f(\bar{3}) = \bar{3}^2 = \bar{9} = \bar{2}$

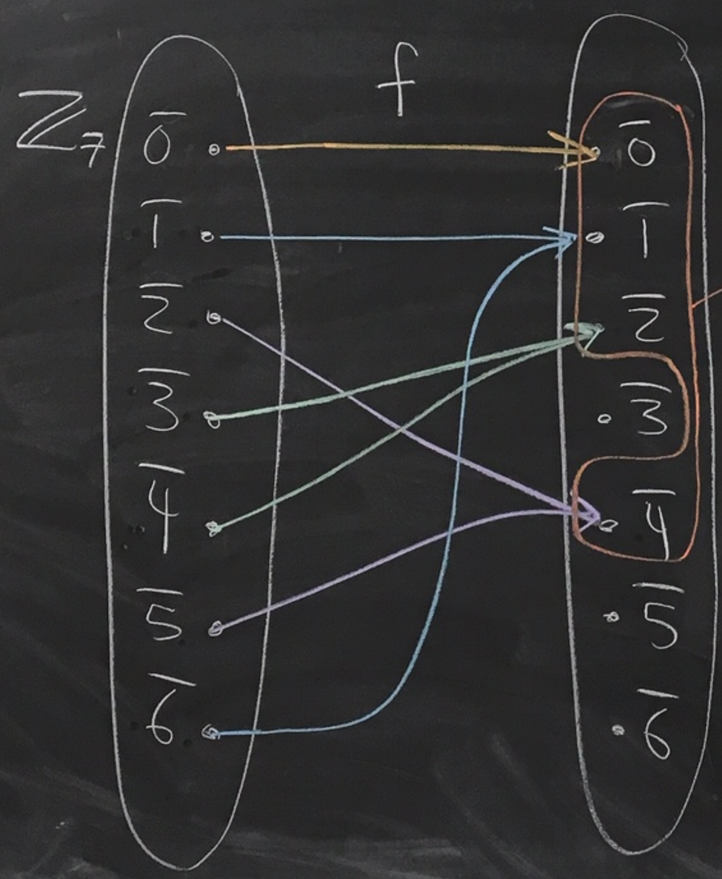
$f(\bar{4}) = \overline{16} = \bar{2}$

$\bar{5} = \overline{-2}$

$f(\bar{5}) = f(\overline{-2}) = \bar{4}$

$\bar{6} = \overline{-1}$

$f(\bar{6}) = f(\overline{-1}) = \bar{1}$



these are called quadratic residues

range$(f) = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$

f is not one-to-one

for example, $\bar{1} \neq \bar{6}$ but $f(\bar{1}) = f(\bar{6})$

$\bar{6} = \overline{-1}$

Ex: $f: \mathbb{Z}_n \to \mathbb{Z}_n$, $f(\bar{x}) = \bar{x}^2$

f is <u>not</u> one-to-one if $n > 2$.

pf: If $n > 2$, then $\bar{1} \neq \overline{-1}$ in $\mathbb{Z}_n$. ←

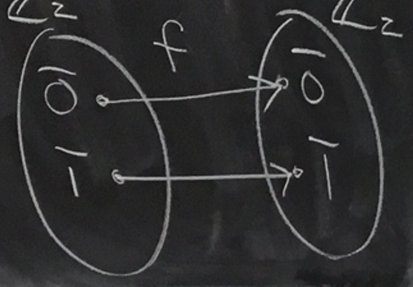
And, $f(\bar{1}) = \bar{1}^2 = \bar{1}$ and $f(\overline{-1}) = (\overline{-1})^2 = \bar{1}$.

So, f is not one-to-one if $n > 2$. ▨

Why is $\bar{1} \neq \overline{-1}$ when $n > 2$?

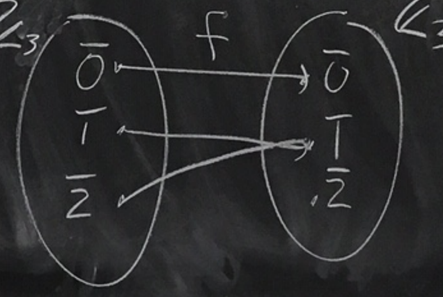
If $\bar{1} = \overline{-1}$ then
$1 \equiv -1 \pmod{n}$ and so
$n \mid (1-(-1))$ or $n \mid 2$.
So, $n = \pm 1, \pm 2$

Ex: $\mathbb{Z}_2$



$f: \mathbb{Z}_2 \to \mathbb{Z}_2$
$f(\bar{x}) = \bar{x}^2$
f is one-to-one

Ex: $\mathbb{Z}_3$



$f: \mathbb{Z}_3 \to \mathbb{Z}_3$
$f(\bar{x}) = \bar{x}^2$
f is <u>not</u> one-to-one

Oct 21
Monday

HW 3

⑧ $S = \mathbb{N} \times \mathbb{N}$

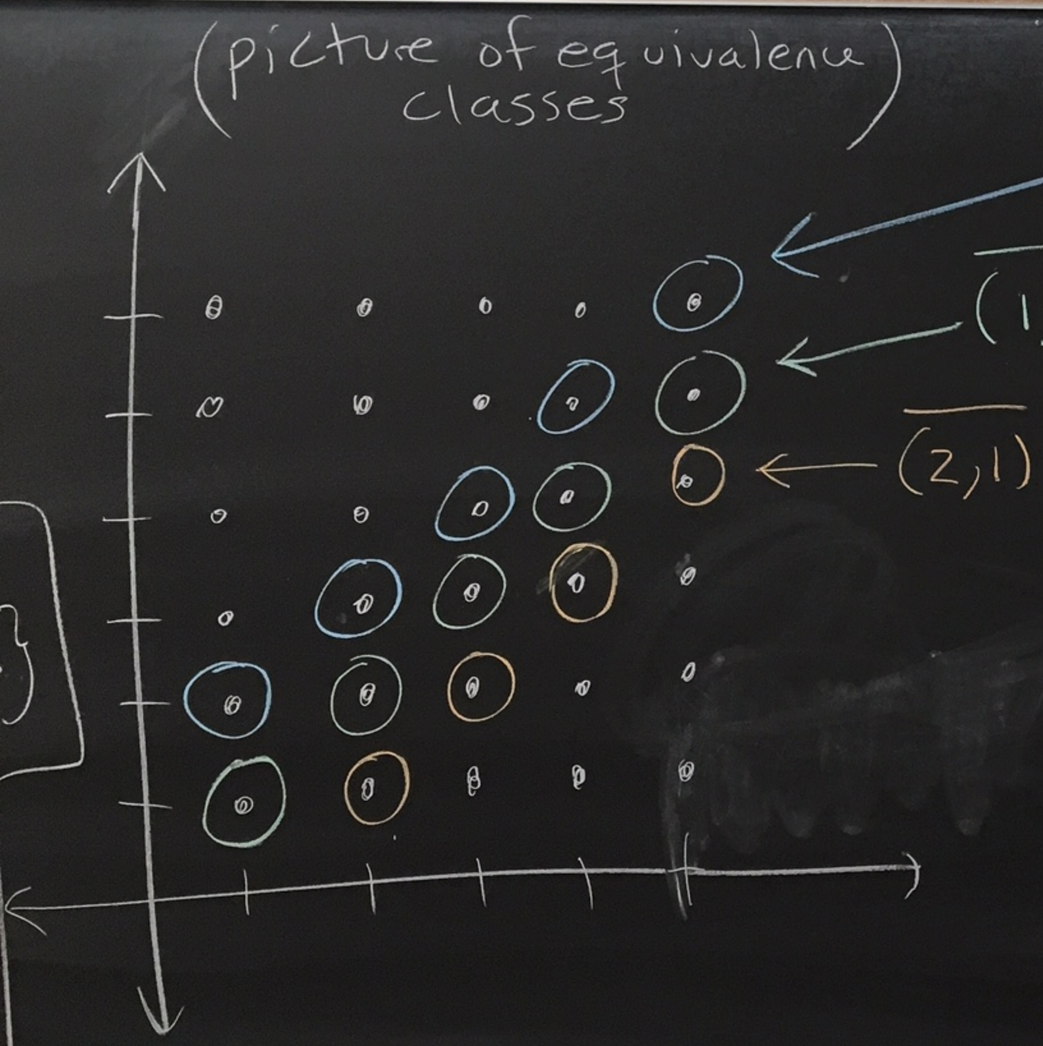
$(a,b) \sim (c,d)$ iff $a+d = b+c$

This is an equivalence relation by part (c). We proved this in class.

$(2,1) \sim (4,3)$
since
$2+3 = 1+4$

$\overline{(2,1)} = \{(2,1), (3,2), (4,3), \ldots\}$

(picture of equivalence classes)



(e) Define

$$\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$$

We want to prove that $\oplus$ is well-defined on the set of equivalence classes $\mathbb{N}\times\mathbb{N}/\sim$

Ex: $\overline{(1,2)} \oplus \overline{(1,1)} = \overline{(1+1, 2+1)} = \overline{(2,3)}$

(1,2) ↕ equal $\overline{(1,2)}$; (1,1) ↕ equal $\overline{(1,1)}$; (2,3) ↕ equal $\overline{(2,3)}$

$\overline{(4,5)} \oplus \overline{(3,3)} = \overline{(4+3, 5+3)} = \overline{(7,8)}$

(2)

Proof of (e):

① Pick $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{N}\times\mathbb{N}/\sim$ where $a,b,c,d \in \mathbb{N} = \{1,2,3,4,\dots\}$

Then $a+c \in \mathbb{N}$ and $b+d \in \mathbb{N}$.

So, $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)} \in \mathbb{N}\times\mathbb{N}/\sim$.

② Let $\overline{(a_1,b_1)}, \overline{(a_2,b_2)}, \overline{(c_1,d_1)}, \overline{(c_2,d_2)} \in \mathbb{N}\times\mathbb{N}/\sim$

and $\overline{(a_1,b_1)} = \overline{(a_2,b_2)}$ and $\overline{(c_1,d_1)} = \overline{(c_2,d_2)}$.

We need to show that

$$\overline{(a_1,b_1)} \oplus \overline{(c_1,d_1)} = \overline{(a_2,b_2)} \oplus \overline{(c_2,d_2)}.$$

Since $\overline{(a_1,b_1)} = \overline{(a_2,b_2)}$ we have that $a_1+b_2 = b_1+a_2$.

Since $\overline{(c_1,d_1)} = \overline{(c_2,d_2)}$ we have that $c_1+d_2 = d_1+c_2$.

Adding the above (two equations) gives $a_1+c_1+b_2+d_2 = b_1+d_1+a_2+c_2$.

Scratchwork

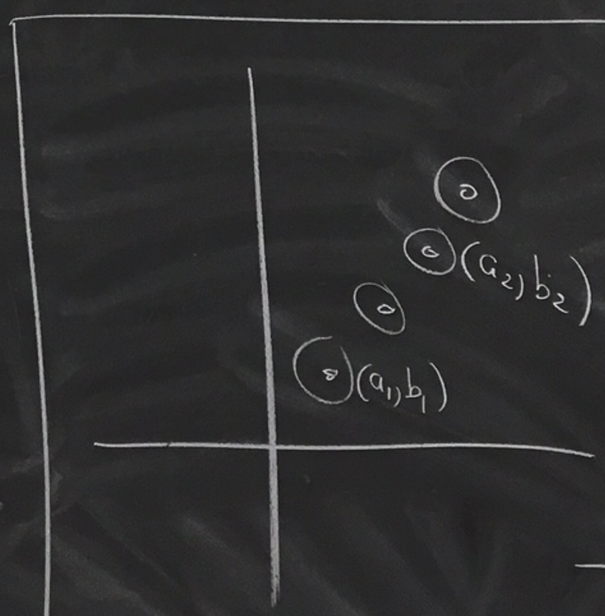
Want to show:

$\overline{(a_1+c_1, b_1+d_1)} = \overline{(a_2+c_2, b_2+d_2)}$

$a_1+c_1+b_2+d_2 = b_1+d_1+a_2+c_2$

So, $\overline{(a_1+c_1,\ b_1+d_1)} = \overline{(a_2+c_2,\ b_2+d_2)}$.

That is, $\overline{(a_1, b_1)} \oplus \overline{(c_1, d_1)} = \overline{(a_2, b_2)} \oplus \overline{(c_2, d_2)}$.



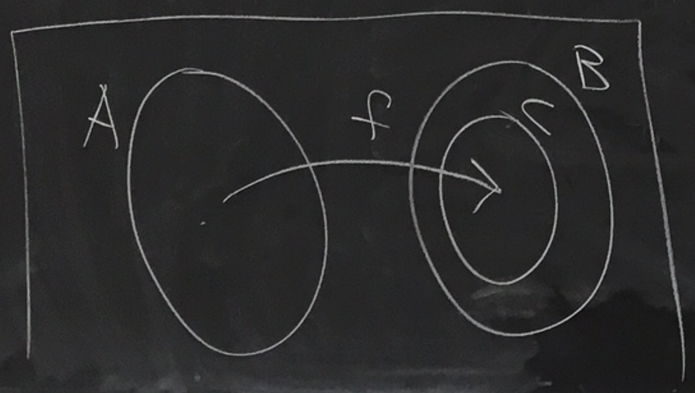
$\overline{x} = \overline{y}$ iff $x \sim y$

$\overline{(a_1, b_1)} = \overline{(a_2, b_2)}$

$\longrightarrow (a_1, b_1) \sim (a_2, b_2)$

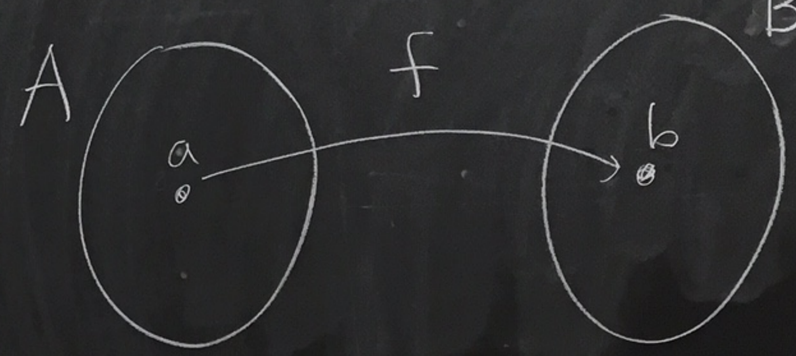
$\longrightarrow a_1 + b_2 = b_1 + a_2$

Def: Let A and B be sets and $f: A \to B$. Let C be the range of f. We say that f is <u>surjective</u> or <u>onto B</u> if $C = B$.



Another way to say this:

f is <u>onto B</u> if for every $b \in B$ there exists $a \in A$ with $f(a) = b$



There can be more than one a with $f(a) = b$.

How to prove $f: A \to B$ is onto

Pick/Let $b \in B$.

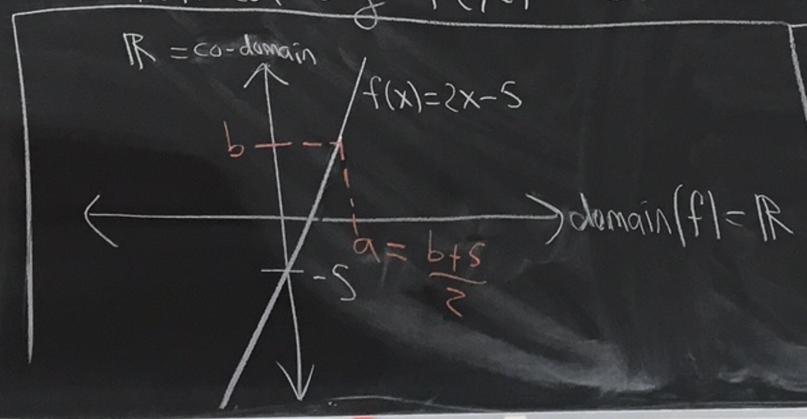
Find $a \in A$ with $f(a) = b$.

Scratchwork

$b = f(a) = 2a - 5$

$\frac{b+5}{2} = a$

Ex: Let $f: \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x - 5$.



Proof that f is onto

Let $b \in \mathbb{R}$.

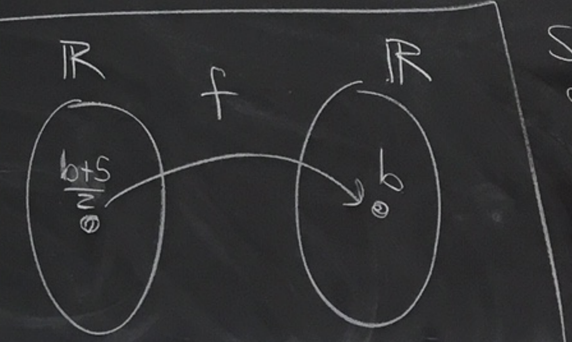
Set $a = \frac{b+5}{2}$.

Then $a \in \mathbb{R}$ and

$f(a) = 2a - 5$

$= 2\left(\frac{b+5}{2}\right) - 5 = b$.

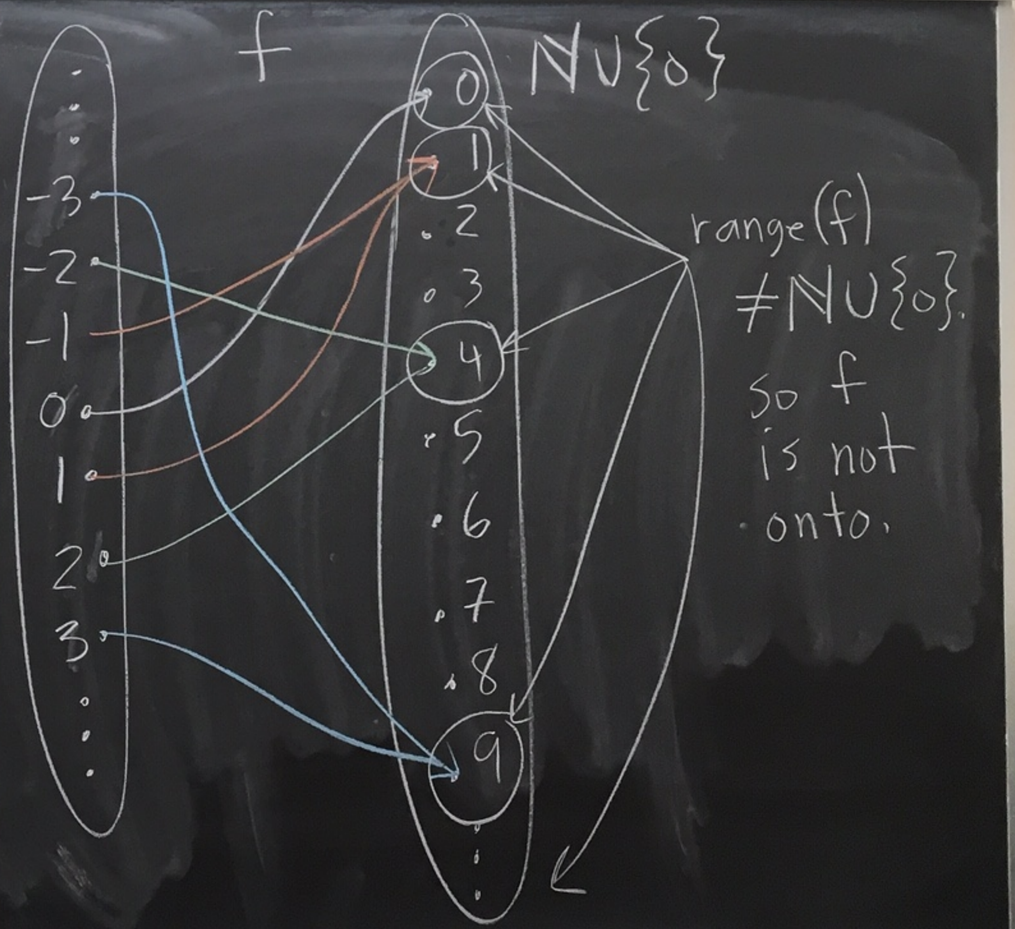
Since b was arbitary, f is onto.



D

How to show $f: A \to B$ is not onto

Find some $b \in B$ where there does not exist $a \in A$ with $f(a) = b$.



Ex: Let $f: \mathbb{Z} \to \mathbb{N} \cup \{0\}$ be given by $f(x) = x^2$.

pf that f is not onto:

Consider $2 \in \mathbb{N} \cup \{0\}$.

There is no $x \in \mathbb{Z}$ with $f(x) = 2$.

Why?

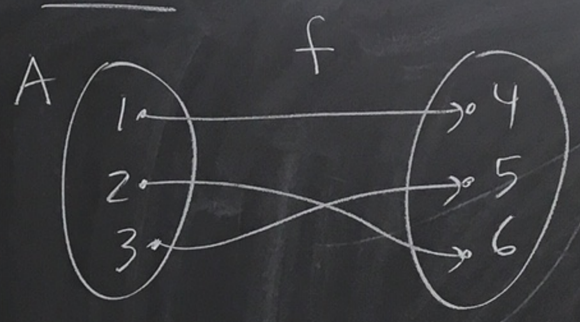
If $x^2 = 2$, then $x = \pm\sqrt{2} \notin \mathbb{Z}$.

That's why. ∎

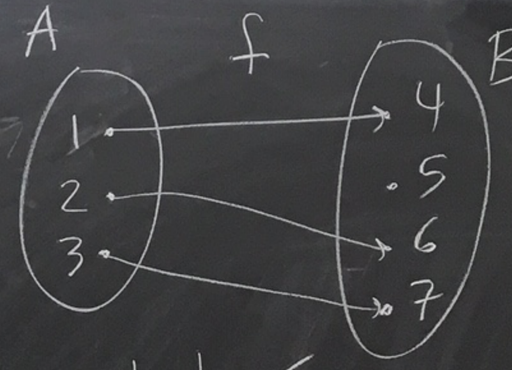
$a = \frac{b+5}{2}$

Def: Let A and B be sets and $f: A \to B$. We say that f is a bijection if f is one-to-one and onto.

Ex:



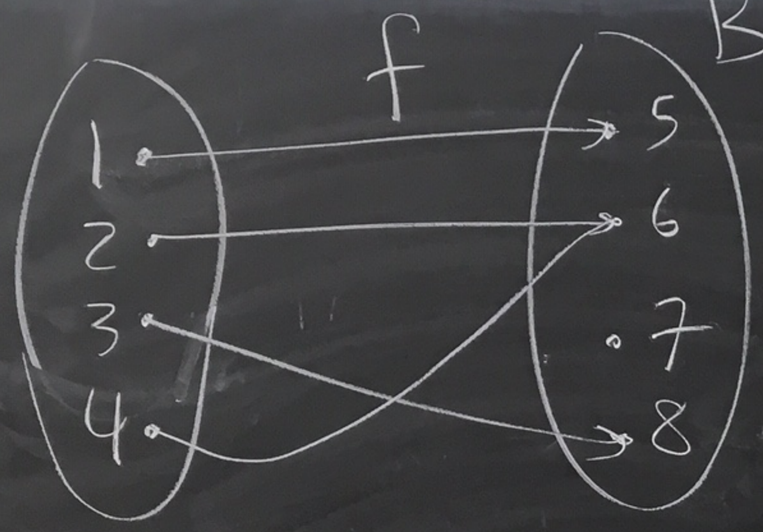
1-1 and onto
bijection



1-1 ✓

onto ✗ ← $5 \notin$ range(f)

not a bijection

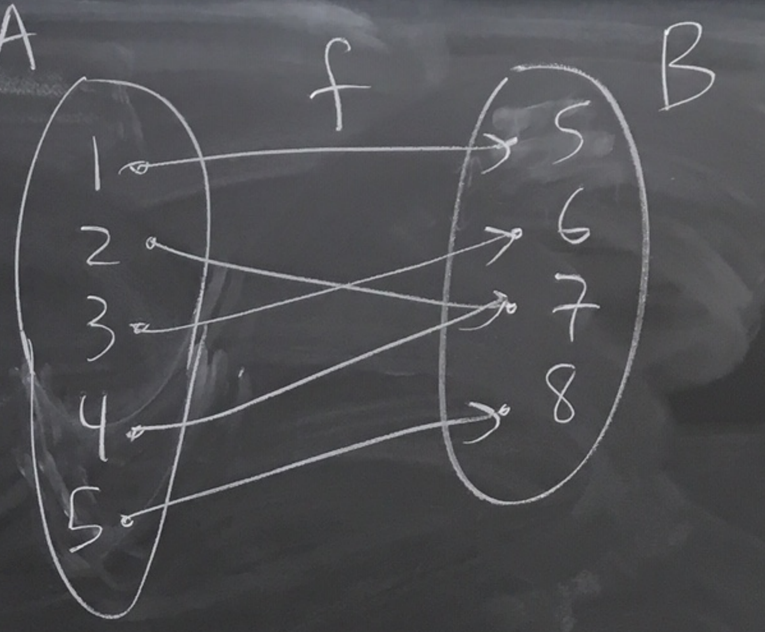


1-1 X $f(2)=f(4)$

onto X $7 \notin \text{range}(f)$

bijection X

$a = \frac{b+5}{2}$

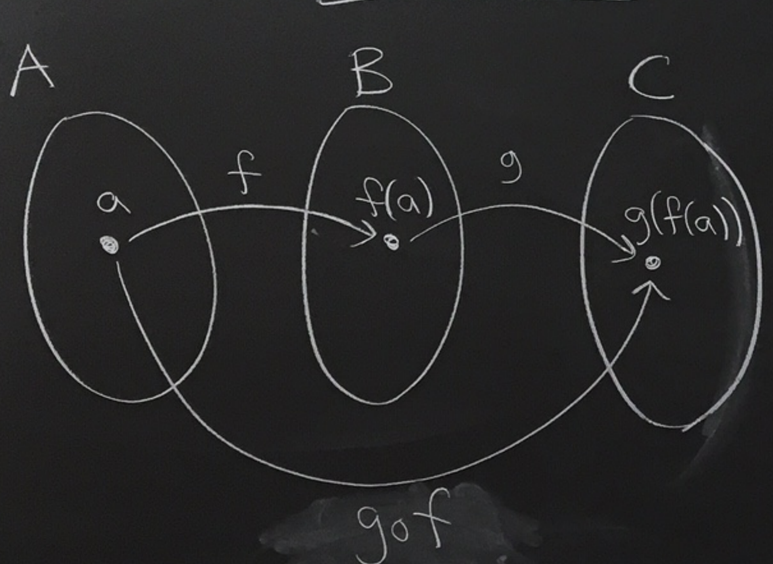


1-1 X $\leftarrow (f(2)=f(4))$

onto ✓

bijection X

Weds
10/23

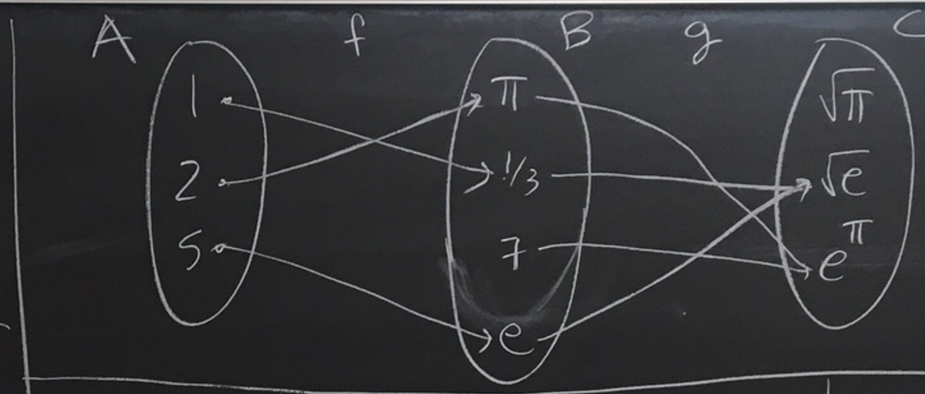


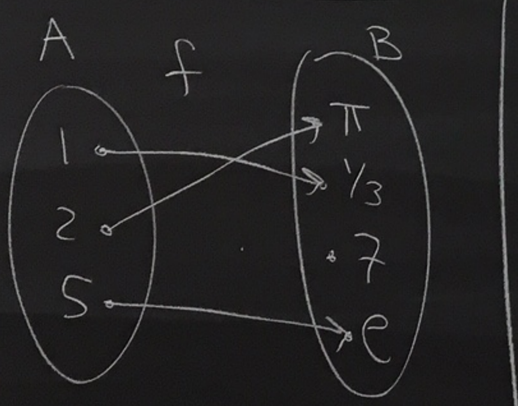
Def: Let A, B, and C be sets.
Let $f: A \to B$ and $g: B \to C$.
Define the composition of f and g
to be the function $g \circ f : A \to C$
where $(g \circ f)(a) = g(f(a))$.

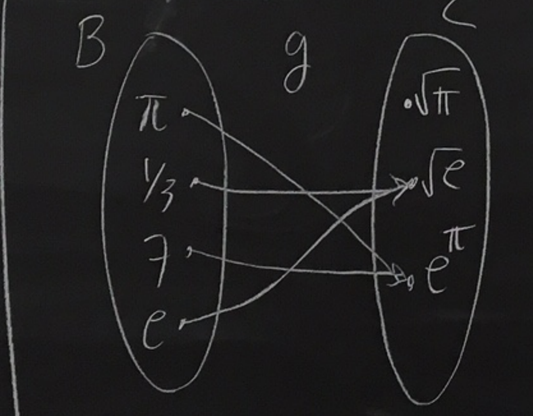
Ex: $A = \{1, 2, 5\}$

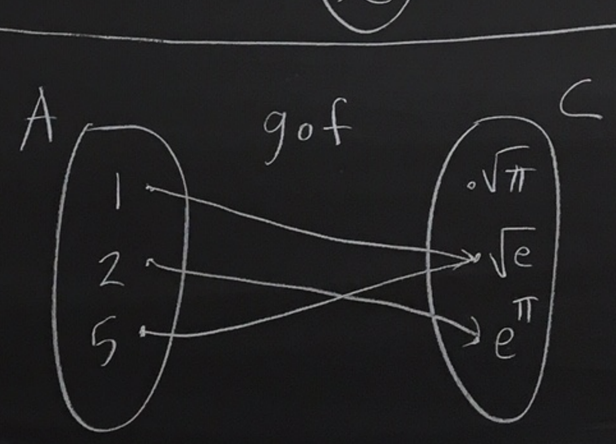
$B = \{\pi, \frac{1}{3}, 7, e\}$

$C = \{\sqrt{\pi}, \sqrt{e}, e^{\pi}\}$









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

$= g(\frac{1}{3}) = \sqrt{e}$

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

$= g(\pi) = e^{\pi}$

$(g \circ f)(5) = g(f(5)) = g(e) = \sqrt{e}$

Theorem: Let A, B, C be sets.

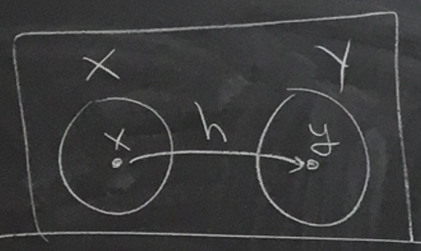
Let $f: A \to B$ and $g: B \to C$.

① If f and g are both onto, then $g \circ f$ is onto.

② If f and g are both one-to-one, then $g \circ f$ is one-to-one.

③ If f and g are both bijections then $g \circ f$ is a bijection.

bijection means one-to-one and onto



$h: X \to Y$.

prove h is onto

pf: Let $y \in Y$.

⋮

Find $x \in X$ with $h(x) = y$

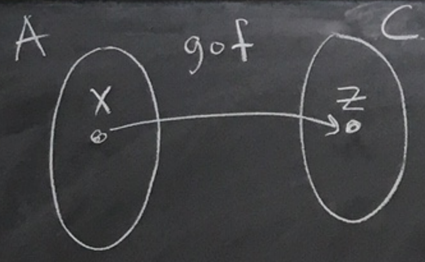
pf:

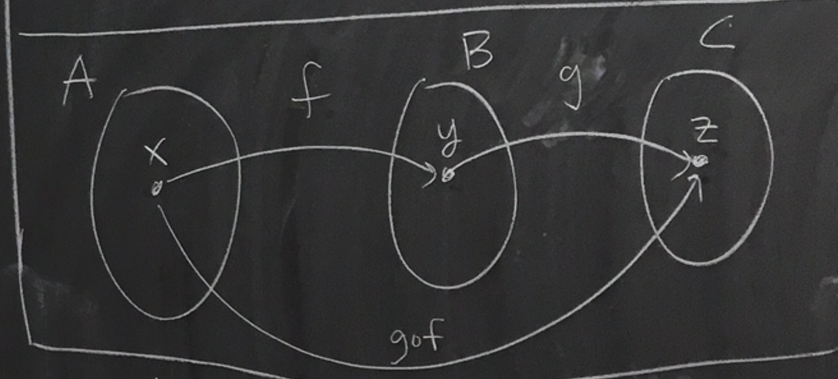
① Assume that f and g are onto.
We want to show that $g \circ f$ is onto.

Let $z \in C$.

Since $g: B \to C$ is onto,
there exists $y \in B$
with $g(y) = z$.

Since $f: A \to B$ is onto,
there exists $x \in A$
with $f(x) = y$.





Then, $x \in A$ and $(g \circ f)(x) = g(f(x))$
$= g(y) = z$.

So, $g \circ f$ is onto.

② Assume f and g are both one-to-one
We want to prove that $g \circ f$ is one-to-one.
Suppose $a_1, a_2 \in A$ with $(g \circ f)(a_1) = (g \circ f)(a_2)$.
So, $g(f(a_1)) = g(f(a_2))$.
Since g is one-to-one and
$g(\boxed{f(a_1)}) = g(\boxed{f(a_2)})$
we know $f(a_1) = f(a_2)$.
Since f is one-to-one and $f(\boxed{a_1}) = f(\boxed{a_2})$
we know $a_1 = a_2$.
Therefore, $g \circ f$ is one-to-one.

$h: X \to Y$
How to prove h is one-to-one
pf: Let $x_1, x_2 \in X$ Assume $h(x_1) = h(x_2)$. ⋮ Show $x_1 = x_2$.

pf:
① Assu
We
Let
Sinc
Sinc

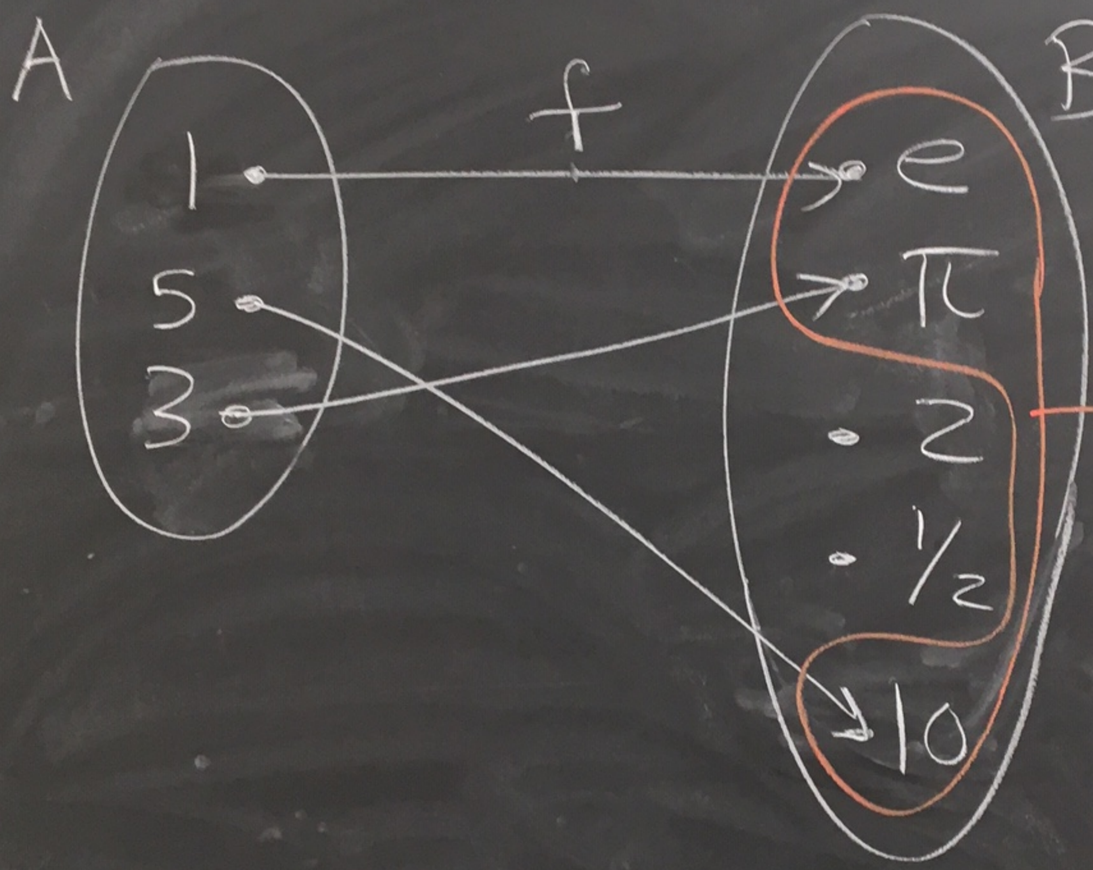
(3) Suppose f and g are both bijections (1-1 and onto).

By part 1, since f and g are both onto, we have $g \circ f$ is onto.

By part 2, since f and g are both 1-1, we have $g \circ f$ is 1-1.

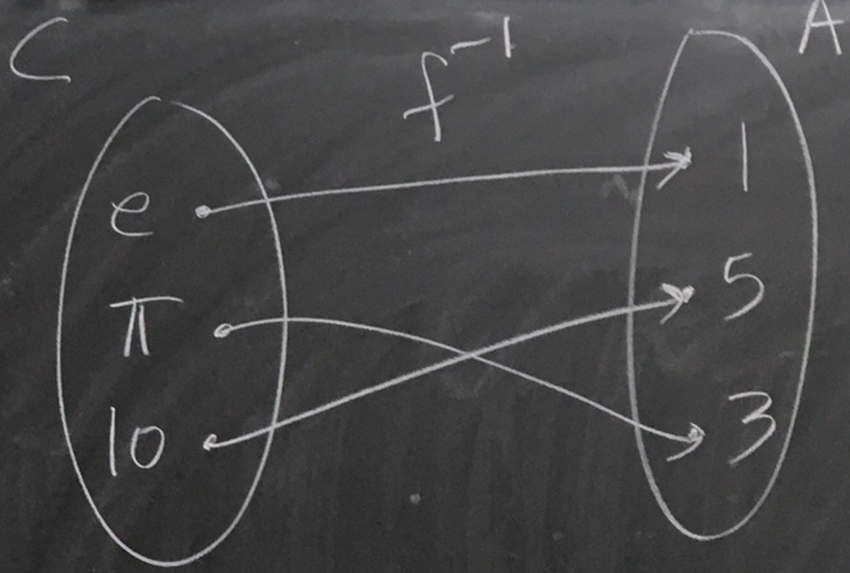
So, $g \circ f$ is a bijection.

Ex: Consider this function f.

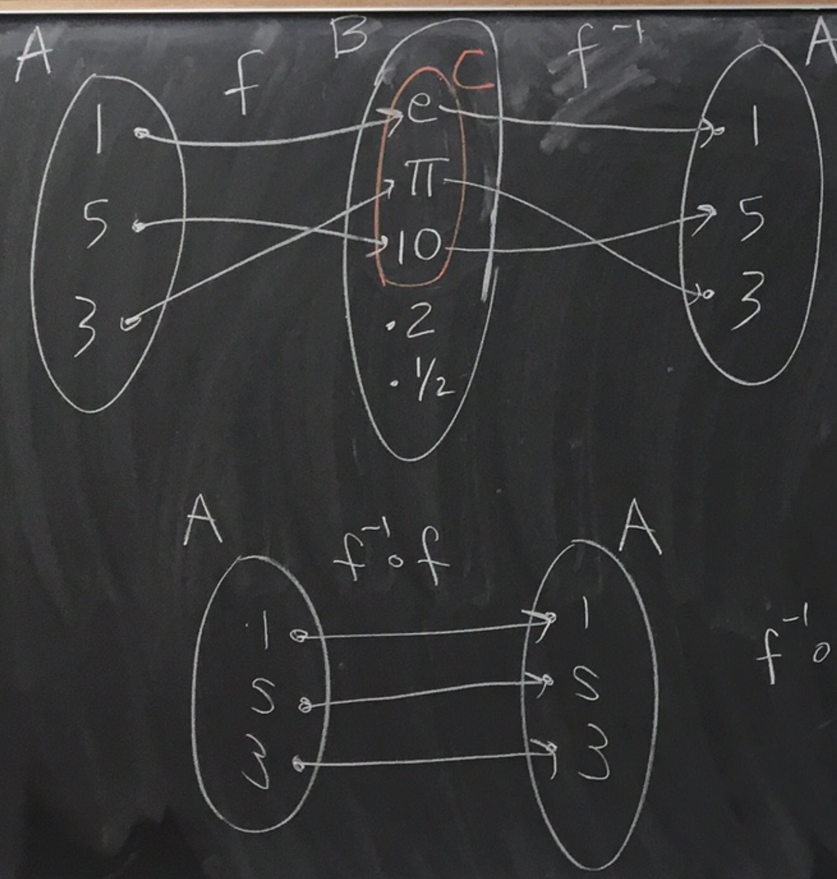


C = range(f)
= {e, π, 10}

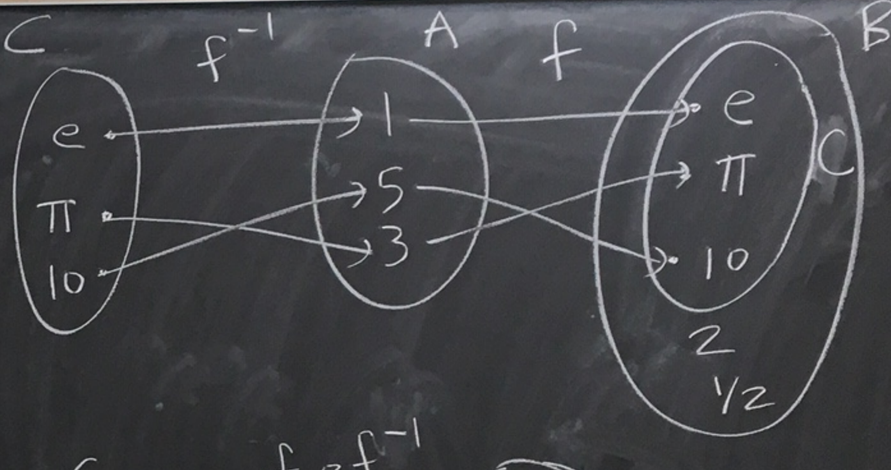
f is one-to-one.
So we can make $f^{-1}: C \to A$
by reversing the arrows.
f^{-1} will be a well-defined function because f is one-to-one
So there is only one arrow to reverse at each element of C.

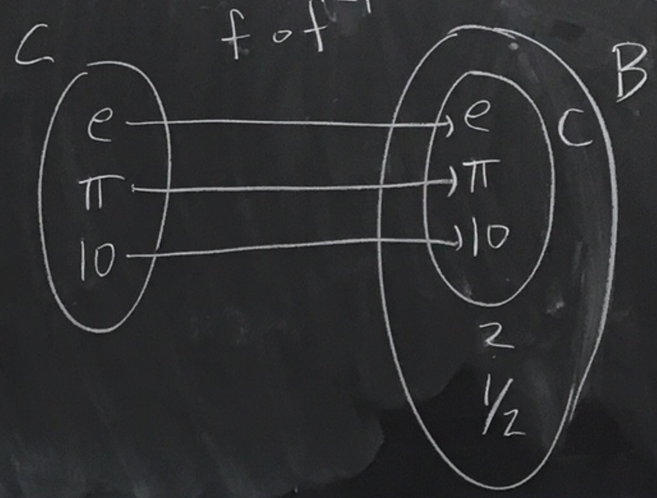


$\text{domain}(f^{-1}) = C = \text{range}(f)$
$\text{range}(f^{-1}) = A = \text{domain}(f)$



$f^{-1}\circ f = i_A$





$(f\circ f^{-1})(z) = z$
for all $z \in C$
$(f\circ f^{-1})(z) = i(z)$
for all $z \in C$.

Def: Let A and B be sets.
Let $f: A \to B$ be a one-to-one function. Let $C = \text{range}(f)$.
Define the inverse function of f to be $f^{-1}: C \to A$
where $f^{-1}(c) = a$ iff $f(a) = c$.

f^{-1} is well-defined since f is one-to-one $\left\{\right.$ (that is, there is a unique a with $f(a)=c$ for all $c \in C = \text{range}(f)$)

C for range(f)
$= \{e, \pi, 10\}$

M W

f^{-1} $f(x)$ $f^{-1}(y)$

HW review

M W

cardinality

review F

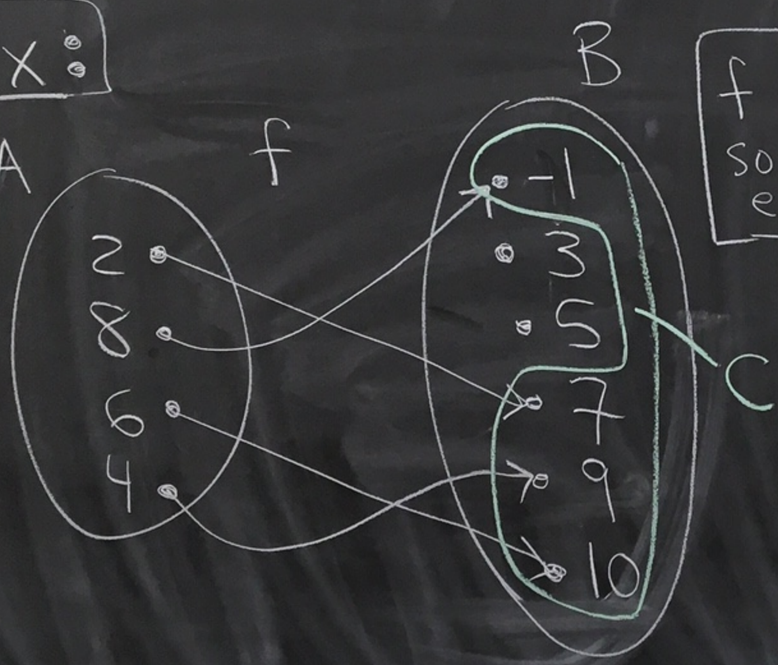
M +2

Mon
10/28

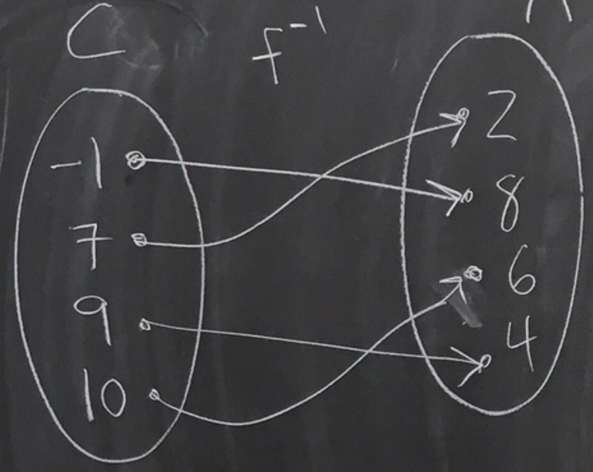
Last time recap:

$f: A \to B$ is one-to-one with $C = \text{range}(f)$.
Define $f^{-1}: C \to A$ where $f^{-1}(c) = a$ iff $f(a) = c$

Ex:



f is 1-1 so f^{-1} exists



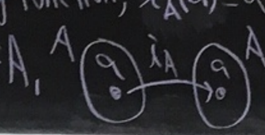
Theorem: Let A, B be sets.
Let $f: A \to B$ be one-to-one.
Let $C = \text{range}(f)$ and $f^{-1}: C \to A$
be the inverse function of f.
Then the following are true;

① $\text{domain}(f^{-1}) = \text{range}(f)$

② $\text{range}(f^{-1}) = \text{domain}(f)$.
In particular, $f^{-1}: C \to A$ is onto A.

③ f^{-1} is one-to-one

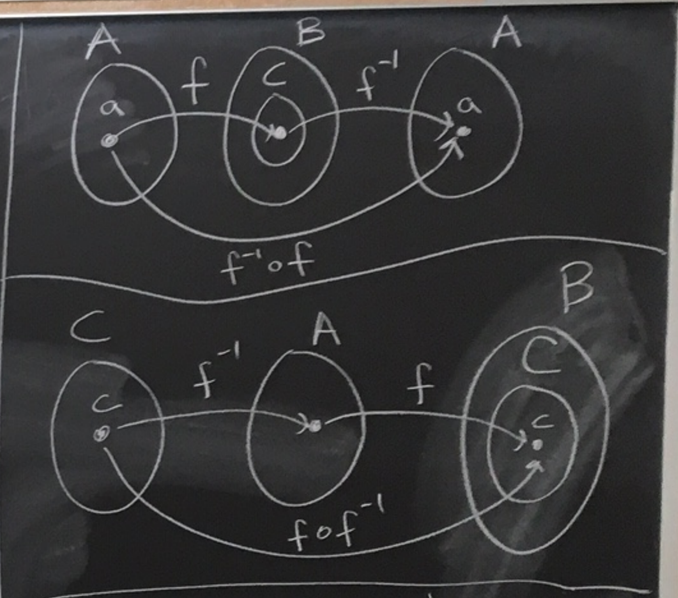
Here $i_A: A \to A$ is the identity function, $i_A(a) = a$ for all $a \in A$,



④ $(f^{-1} \circ f)(a) = a$
for all $a \in A$.
So, $f^{-1} \circ f = i_A$.

⑤ $(f \circ f^{-1})(c) = c$
for all $c \in C$.

⑥ If $g: C \to A$
and $g \circ f = i_A$,
then $g = f^{-1}$.



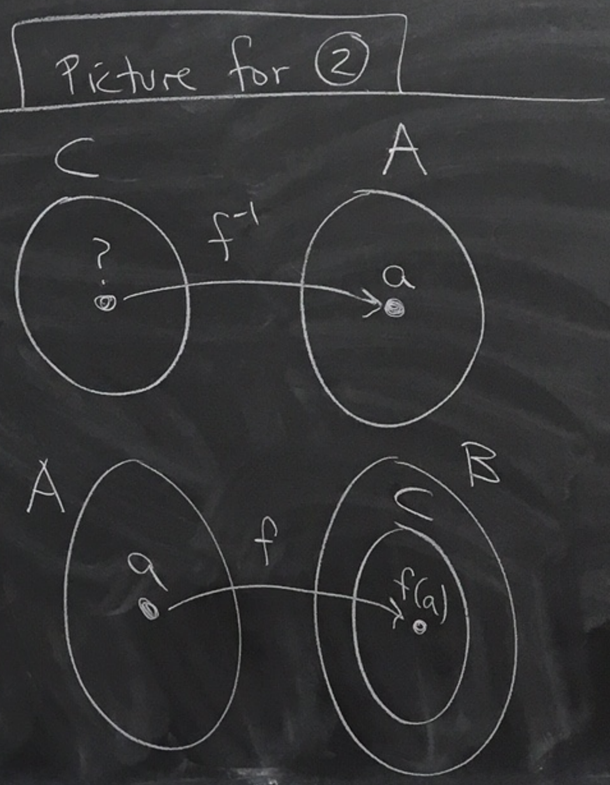
⑥ is a way to verify that some function is f^{-1}

pf:

① This is by def of f^{-1}.
That is, $\text{domain}(f^{-1}) = C = \text{range}(f)$.

② Let's show that $\text{range}(f^{-1}) = A$.
Pick some $a \in A$.
We want $c \in C$ with $f^{-1}(c) = a$.
Set $c = f(a)$.
Then by def of f^{-1}, $f^{-1}(c) = a$.
So, $a \in \text{range}(f^{-1})$.
Thus, f^{-1} is onto A and $\text{range}(f^{-1}) = A$.

Picture for ②



(3) Suppose $f^{-1}(c_1) = f^{-1}(c_2)$ where $c_1, c_2 \in C$.

We need to show that $c_1 = c_2$.

Let $a = f^{-1}(c_1) = f^{-1}(c_2)$.

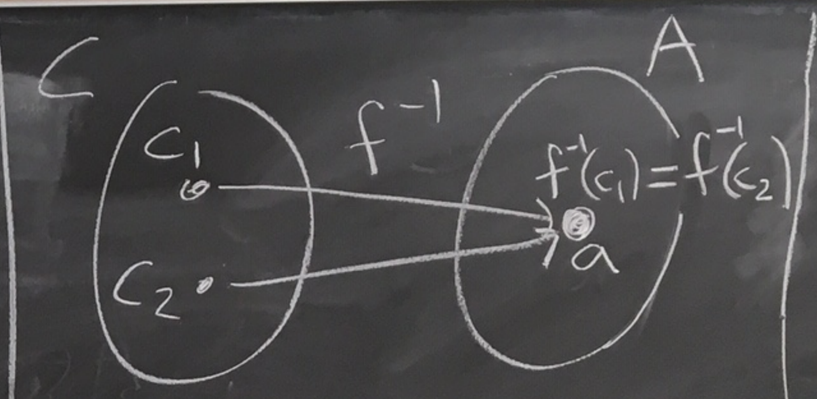
Since $a = f^{-1}(c_1)$ we have

$f(a) = c_1$.

Since $a = f^{-1}(c_2)$ we have,

$f(a) = c_2$.

So, $c_1 = f(a) = c_2$,



If $c_1 \neq c_2$, then f^{-1} would not be 1-1. We want to show that this doesn't happen.

→ Thus, f^{-1} is one-to-one.

(4) Let's show that $f^{-1} \circ f = i_A$.

Let $a \in A$.

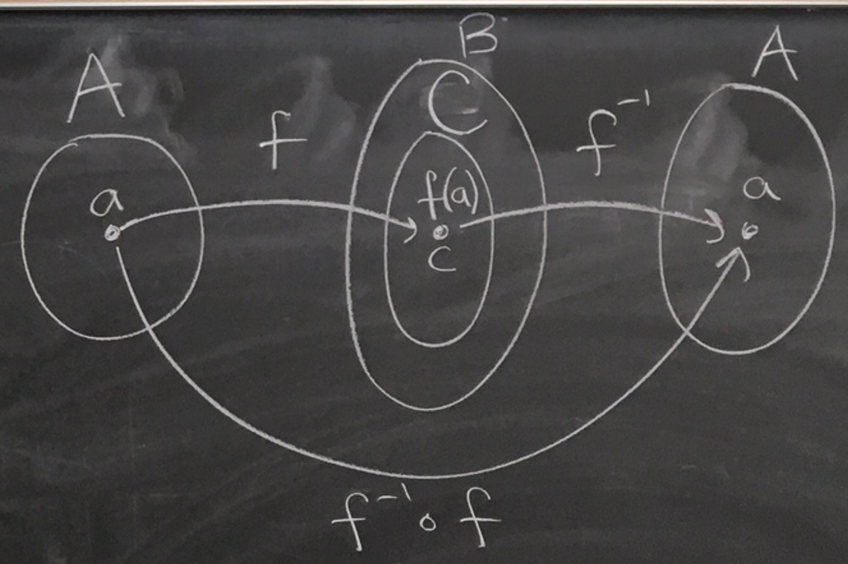
Set $c = f(a)$.

Then, $f^{-1}(c) = a$ by def of f^{-1}.

So,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a))$$
$$= f^{-1}(c)$$
$$= a = i_A(a)$$

Since, $(f^{-1} \circ f)(a) = i_A(a)$ for all $a \in A$, we have $f^{-1} \circ f = i_A$.



To show that two functions $g: X \to Y$ and $h: X \to Y$ are equal, you show $g(x) = h(x)$ for all $x \in X$.

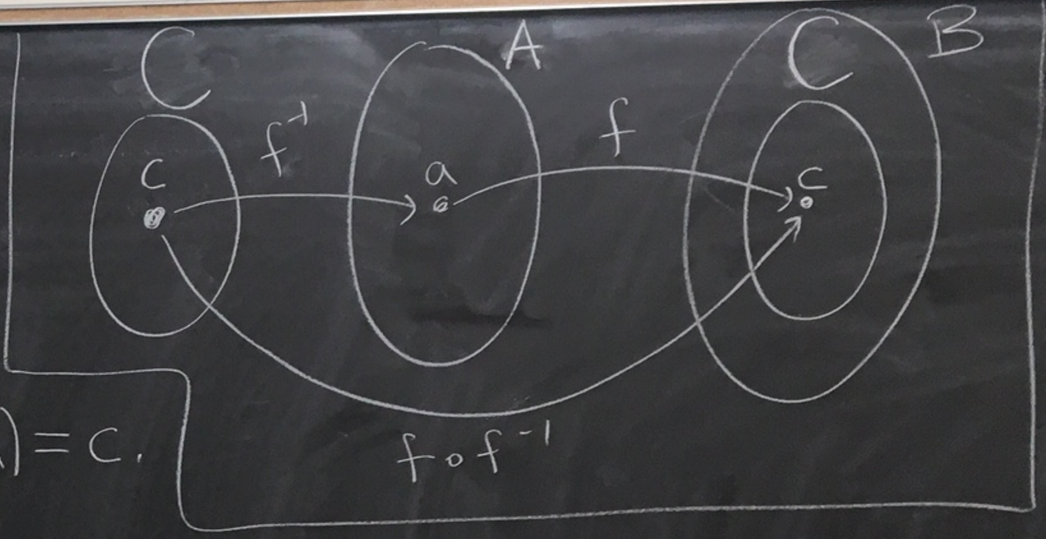
⑤ Let's show

$(f \circ f^{-1})(c) = c$ for all $c \in C$.

Pick $c \in C$.

Then $f^{-1}(c) = a$ where $a \in A$ and $f(a) = c$.

So, $(f \circ f^{-1})(c) = f(f^{-1}(c)) = f(a) = c$.



⑥ Let $g: C \to A$.

Suppose $g \circ f = i_A$.

We need to show that $g = f^{-1}$. ⟵ **Need to show** $g(c) = f^{-1}(c)$ for all $c \in C$

Pick some $c \in C$.

Then $f^{-1}(c) = a$ where $a \in A$ and $f(a) = c$.

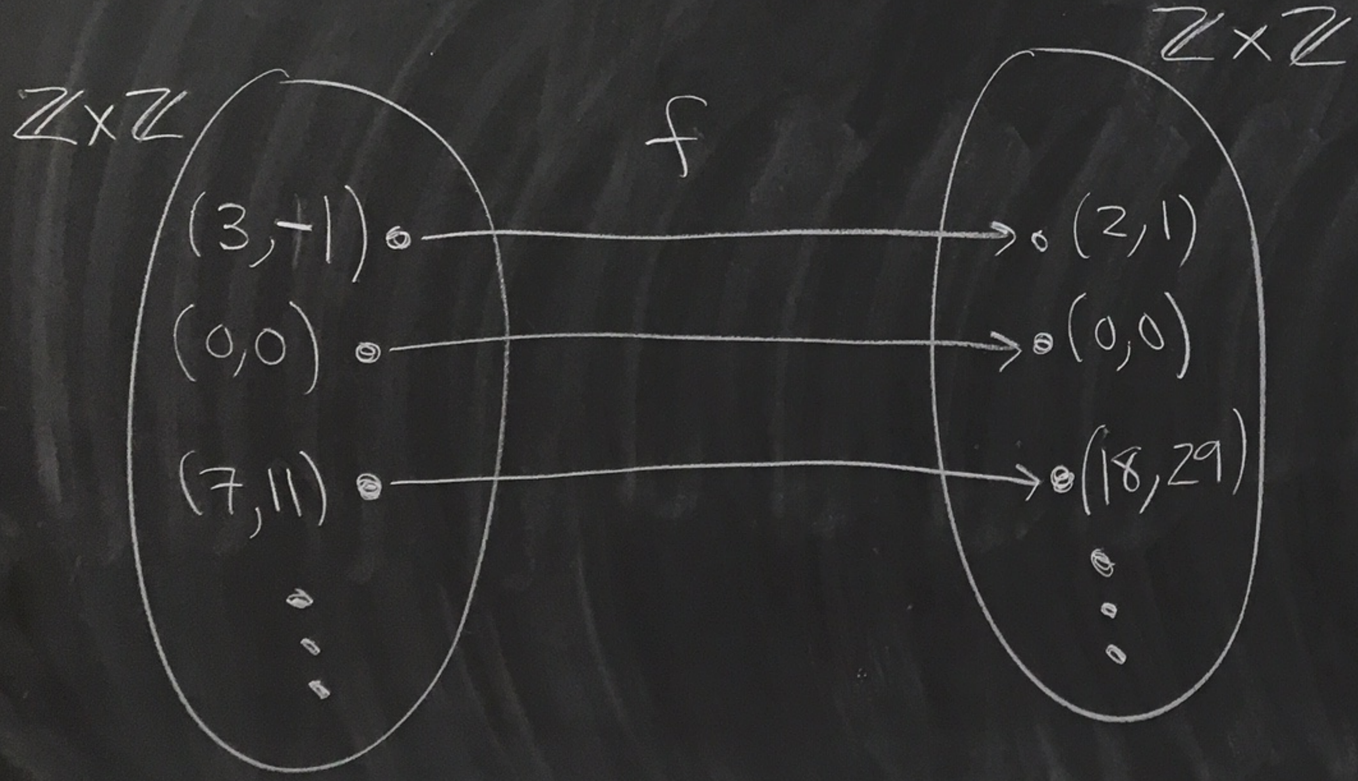
So,

$$g(c) = g(f(a)) = (g \circ f)(a) = i_A(a) = a = f^{-1}(c).$$

That is, $g(c) = f^{-1}(c)$.

Since c was arbitrary we have $g = f^{-1}$. ▨

Ex: Consider $f: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ given by $f(m,n) = (m+n, m+2n)$



$f(7,11) = (7+11, 7+2\cdot 11)$

$= (18, 29)$

$f(3,-1) = (3-1, 3+(2)(-1))$

$= (2, 1)$

f is one-to-one

pf: Suppose $f(m_1, n_1) = f(m_2, n_2)$
for some $(m_1, n_1), (m_2, n_2) \in \mathbb{Z} \times \mathbb{Z}$.
We need to show that $(m_1, n_1) = (m_2, n_2)$.
Since $f(m_1, n_1) = f(m_2, n_2)$ we know that

$$(m_1 + n_1, m_1 + 2n_1) = (m_2 + n_2, m_2 + 2n_2).$$

So,

$$\begin{cases} m_1 + n_1 = m_2 + n_2 & \text{eq } ① \\ m_1 + 2n_1 = m_2 + 2n_2 & \text{eq } ② \end{cases}$$

Add $-(\text{eq}①)$ to eq② to get $n_1 = n_2$.

Replace $n_1 = n_2$ into eq① to get

$m_1 + n_1 = m_2 + n_1$.

So, $m_1 = m_2$.

Thus, $(m_1, n_1) = (m_2, n_2)$.

So, f is one-to-one. ∎

$$-(m_1 + n_1) = -(m_2 + n_2)$$
$$+ \quad (m_1 + 2n_1) = (m_2 + 2n_2)$$
$$n_1 = n_2$$

Weds
10/30

$g(5,-7) = (5-7, 5+2(-7))$

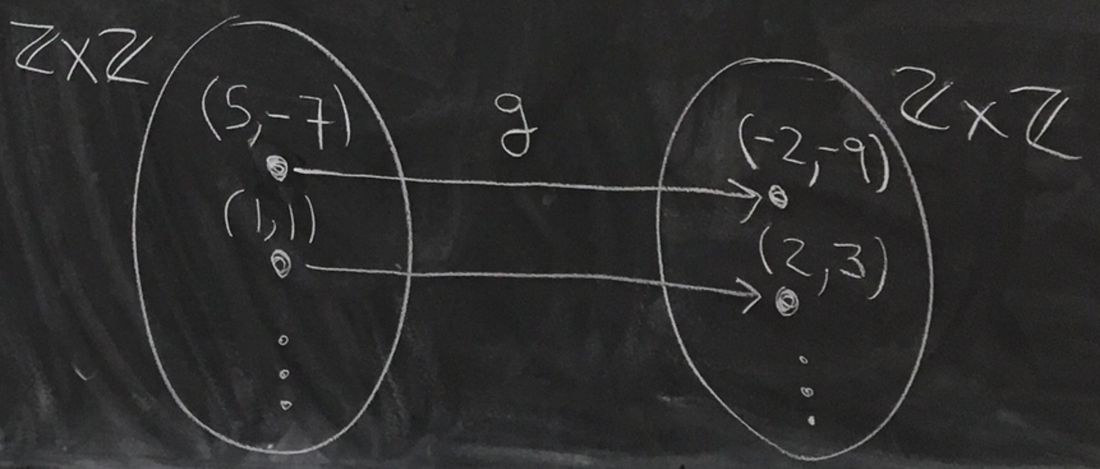
$= (-2, -9)$

Last time

$g: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$

$g(m,n) = (m+n, m+2n)$

We showed that g is one-to-one.



Claim: g is onto.

Proof:

Pick some $(b,c) \in \mathbb{Z} \times \mathbb{Z}$.

We need to find

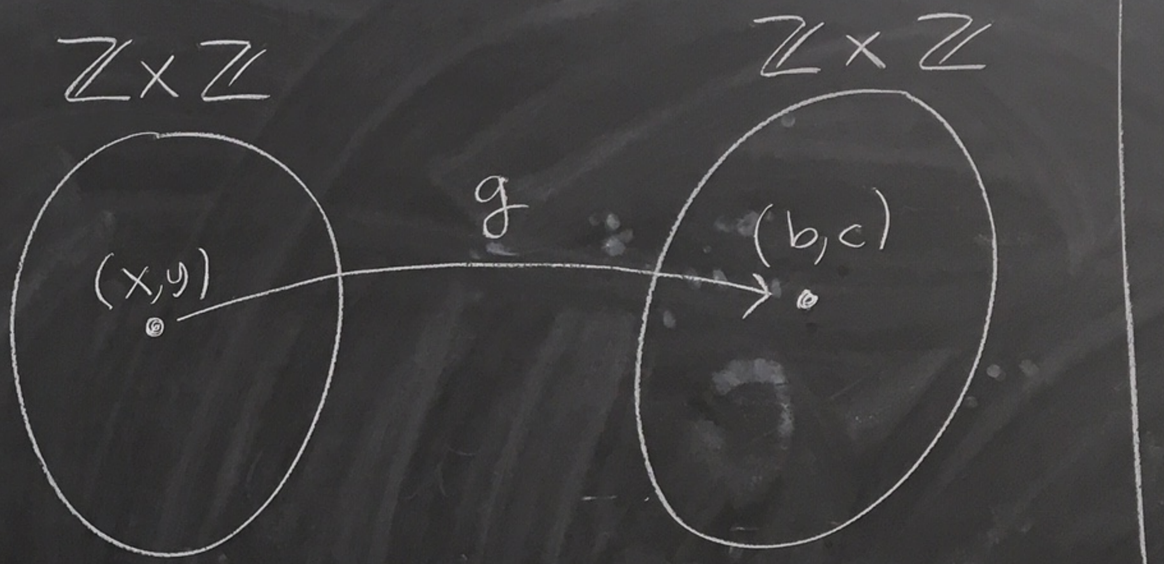
$(x,y) \in \mathbb{Z} \times \mathbb{Z}$ where

$g(x,y) = (b,c)$.

That is we need to solve

$$(x+y, x+2y) = (b,c)$$

for x and y.



So we need to solve

$$\begin{cases} x+y=b & (1) \\ x+2y=c & (2) \end{cases}$$

$-①+②$ gives $y = c-b$.

Plugging this back into ①

gives $x = b-y = b-(c-b)$

$= 2b-c$.

Note that $(x,y) = (2b-c, c-b)$

is in $\mathbb{Z}\times\mathbb{Z}$ and

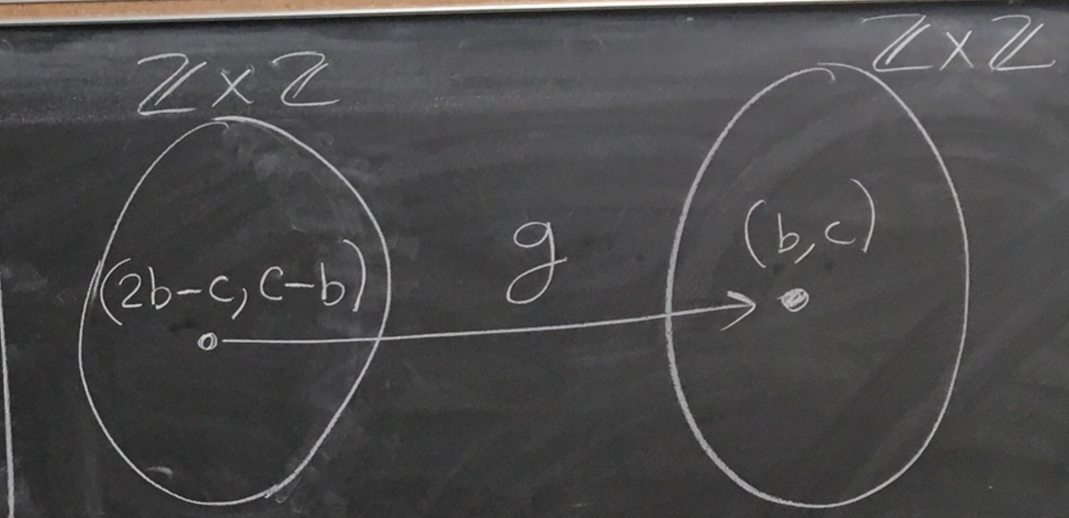
$g(x,y) = g(2b-c, c-b)$

$= ((2b-c)+(c-b),\ g(2b-c)+2(c-b))$

$= (b,c)$.

Summary: Given $(b,c)\in\mathbb{Z}\times\mathbb{Z}$ we have that $(2b-c, c-b)\in\mathbb{Z}\times\mathbb{Z}$

and $g(2b-c, c-b) = (b,c)$. So, g is onto.



So, $g: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$
given by $g(m,n) = (m+n, m+2n)$
is a bijection (one-to-one & onto).

Since g is one-to-one, g^{-1} exists.
And domain(g^{-1}) = range(g) = $\mathbb{Z}\times\mathbb{Z}$.
So, $g^{-1}: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$.

(g is onto)

Claim: $g^{-1}(b,c) = (2b-c, c-b)$

pf: Let $h: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$
with $h(b,c) = (2b-c, c-b)$.

Thm from last time (part 6)

$f: A \to B$, f is 1-1
C = range(f)
If $h: C \to A$ and
$h \circ f = i_A$ then $h = f^{-1}$.

Let's show $h \circ g = i$.
Let $(m,n) \in \mathbb{Z}\times\mathbb{Z}$.
Then,
$(h \circ g)(m,n) = h(g(m,n)) = h(m+n, m+2n)$
$= (2(m+n) - (m+2n), (m+2n) - (m+n))$
$= (m, n) = i(m,n)$.

By thm part 6 from last time $g^{-1} = h$.

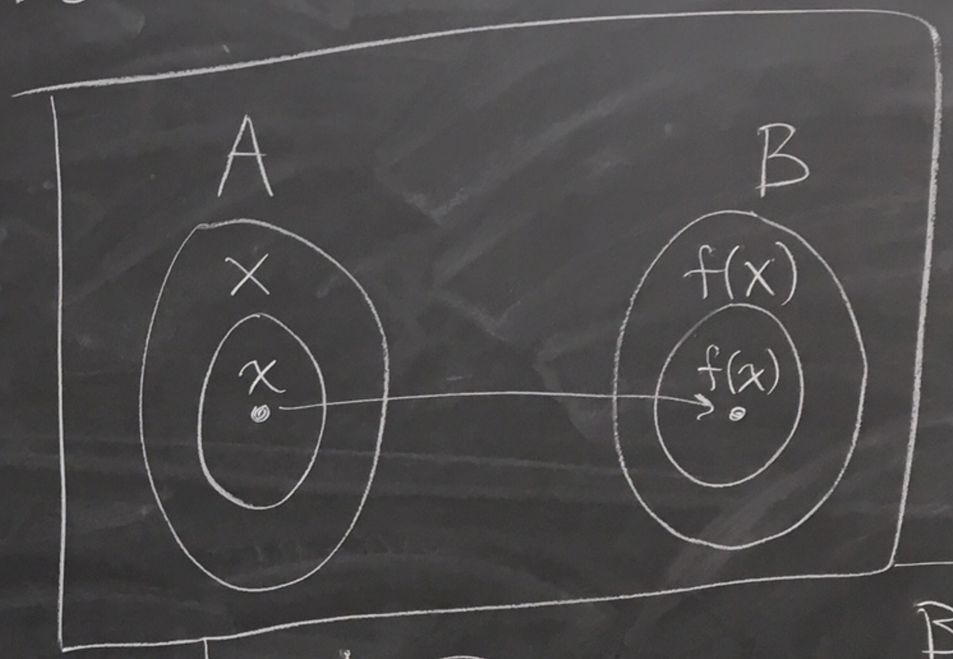
Def: Let A and B be sets.

Let $f: A \to B$.

① Let $X \subseteq A$.

The image of X under f is

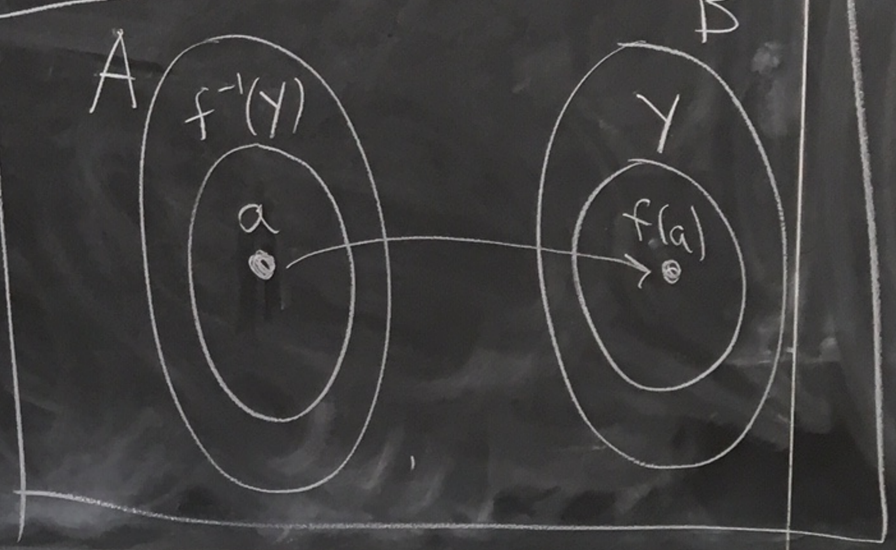
$$f(X) = \{ f(x) \mid x \in X \}$$



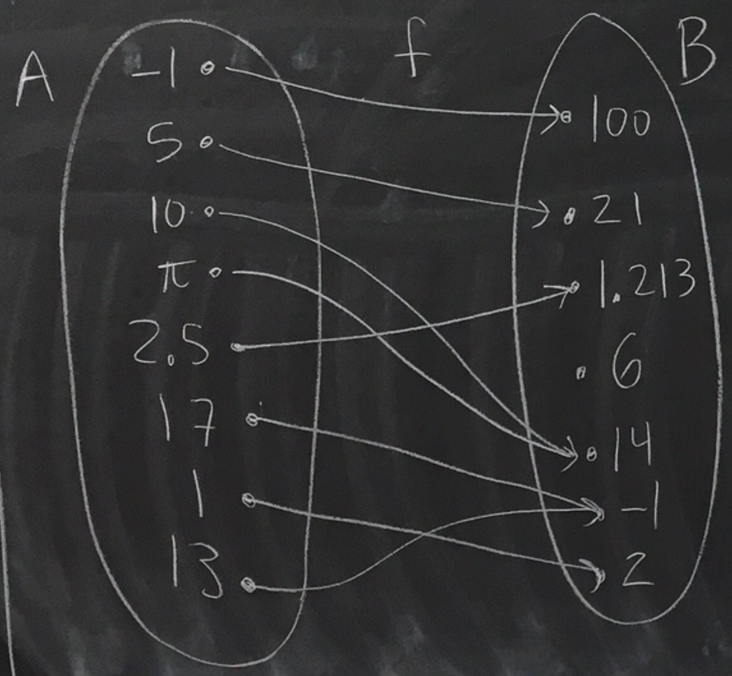
② Let $Y \subseteq B$.

The inverse image of Y under f is

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



Ex: Consider the following function.

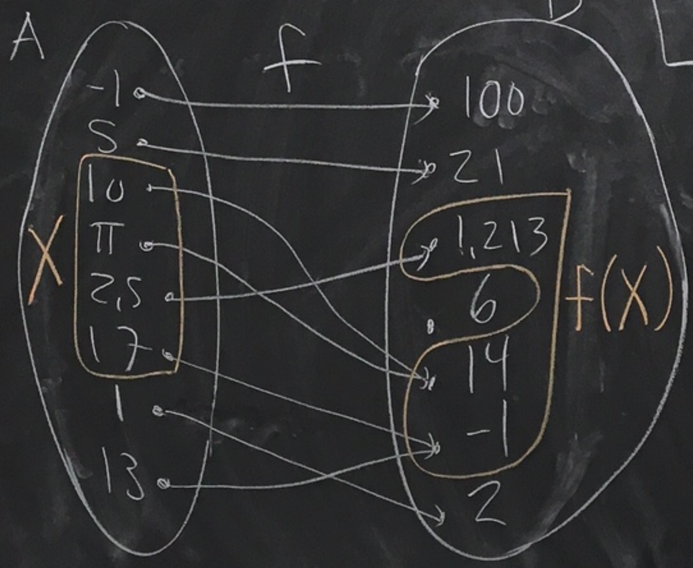


Calculate $f(X)$ where

$X = \{10, \pi, 2.5, 17\}$

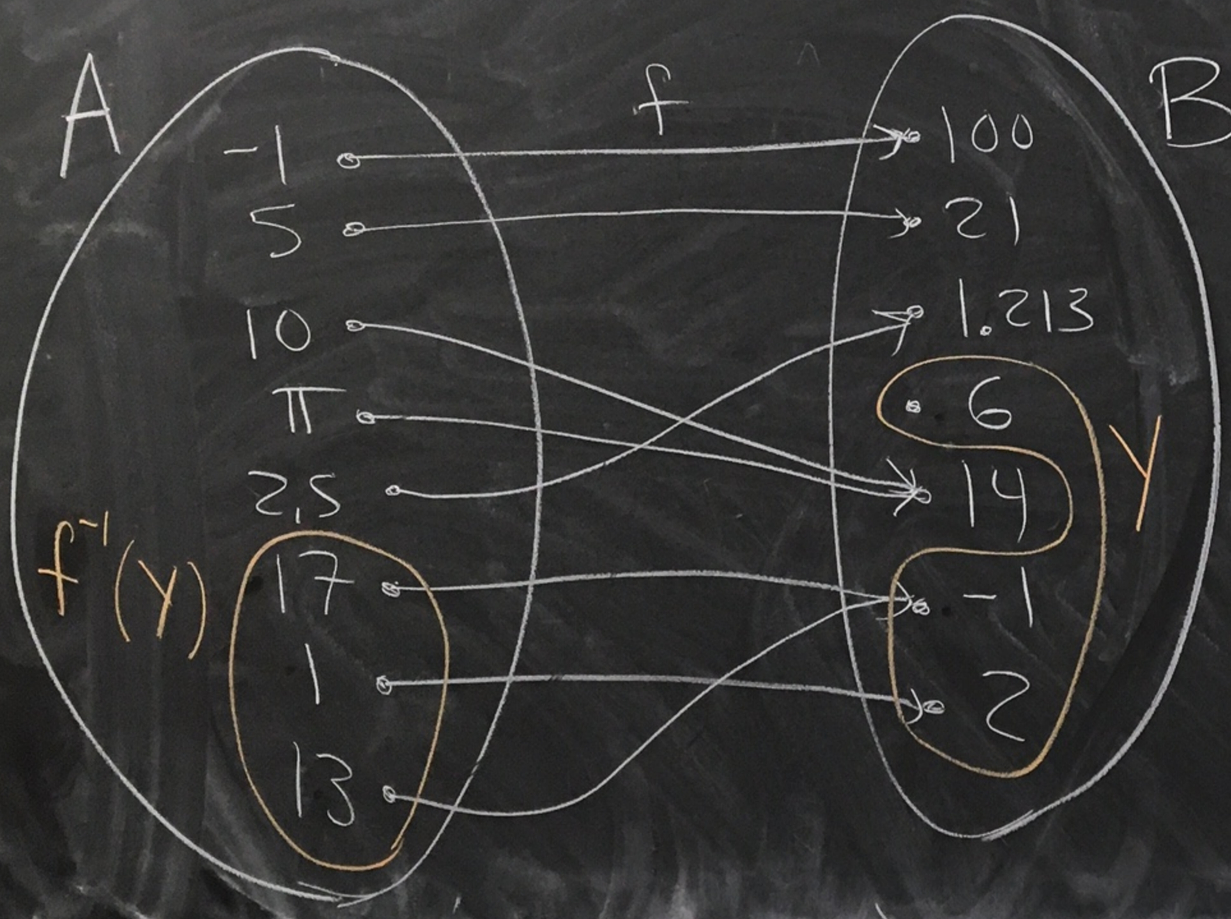
$f(X) = \{f(10), f(\pi), f(2.5), f(17)\} = \{14, 14, 1.213, -1\}$

$= \{14, 1.213, -1\}$



Let $Y = \{6, -1, 2\}$.

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



$f(17) = -1 \in Y$

$f(1) = 2 \in Y$

$f(13) = -1 \in Y$

$f^{-1}(Y) = \{17, 1, 13\}$

note: This does not mean the inverse function

Thm: Let A, B, W, Z be sets where $W \subseteq A$ and $Z \subseteq A$. Let $f: A \to B$. Then

① $f(W \cap Z) \subseteq f(W) \cap f(Z)$ ← Hammack 12.6 #7

② Give an example to show that $f(W \cap Z) = f(W) \cap f(Z)$ is not always true. ← Hammack 12.6 #8

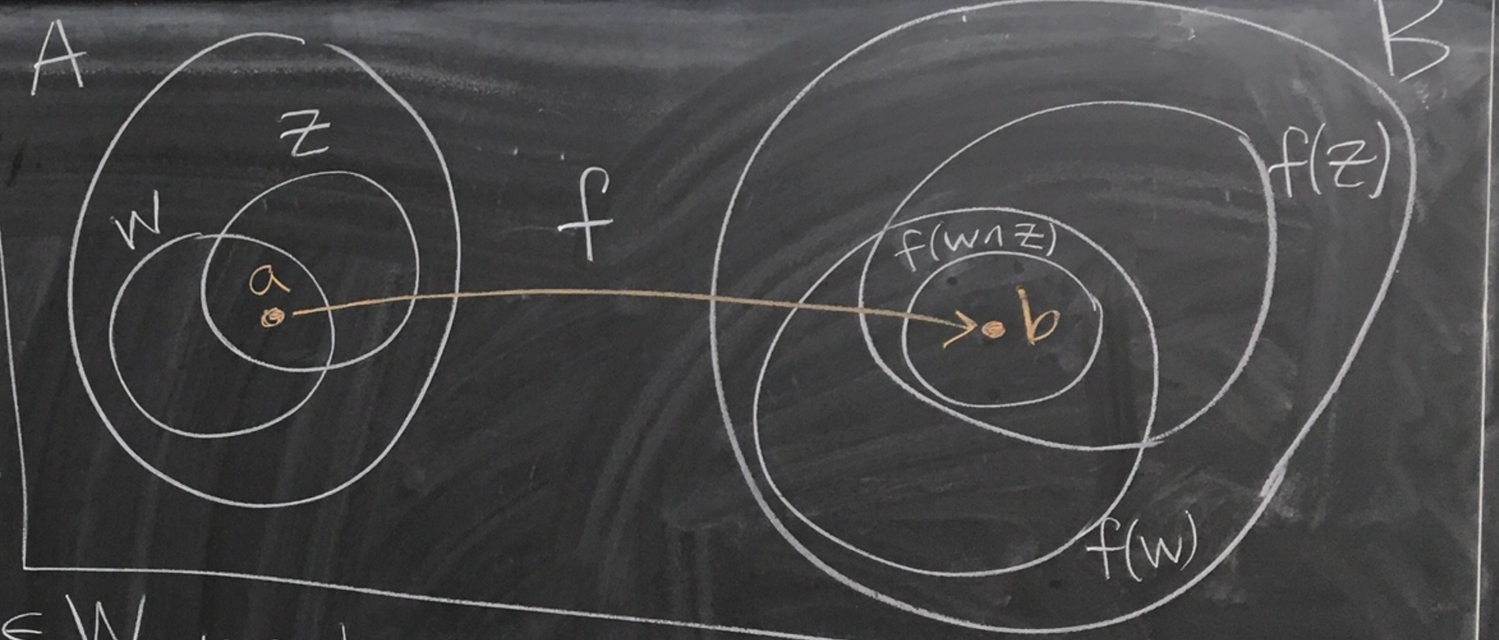
③ $f(W \cup Z) = f(W) \cup f(Z)$ ← HW 4 #14

① Let $b \in f(W \cap Z)$.

So, $b = f(a)$

where $a \in W \cap Z$.

So, $a \in W$ and $a \in Z$.



Since $b = f(a)$ and $a \in W$ we know $b \in f(W)$.

Since $b = f(a)$ and $a \in Z$ we know $b \in f(Z)$.

Thus, $b \in f(W) \cap f(Z)$.

Therefore, $f(W \cap Z) \subseteq f(W) \cap f(Z)$.

Nov 4
Monday

Last time

① $f(W \cap Z) \subseteq f(W) \cap f(Z)$

Hammock 12.6 #7

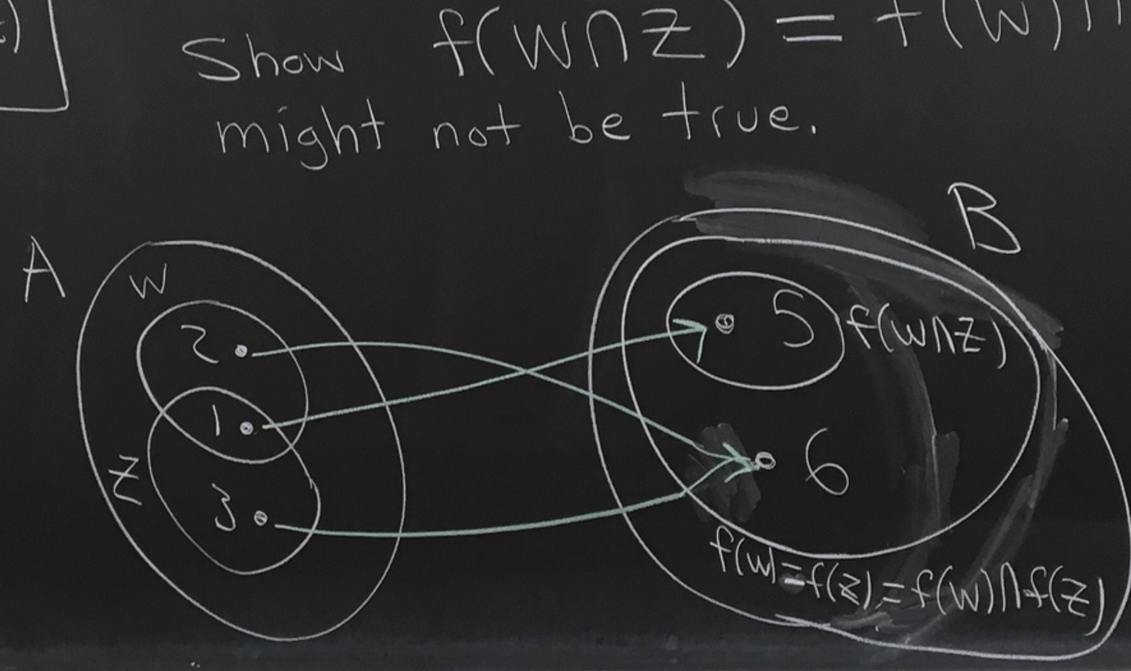
continued from last time ...

② $f : A \to B$

$W \subseteq A$ and $Z \subseteq A$

Show $f(W \cap Z) = f(W) \cap f(Z)$ might not be true.

Hammock 12.6 #8



$W = \{1,2\}$

$Z = \{1,3\}$

$f(W) = \{5,6\}$

$f(Z) = \{5,6\}$

$f(W \cap Z) = \{5\}$

$f(W) \cap f(Z) = \{5,6\}$

③ $f(W \cup Z) = f(W) \cup f(Z)$

HW 4 #14

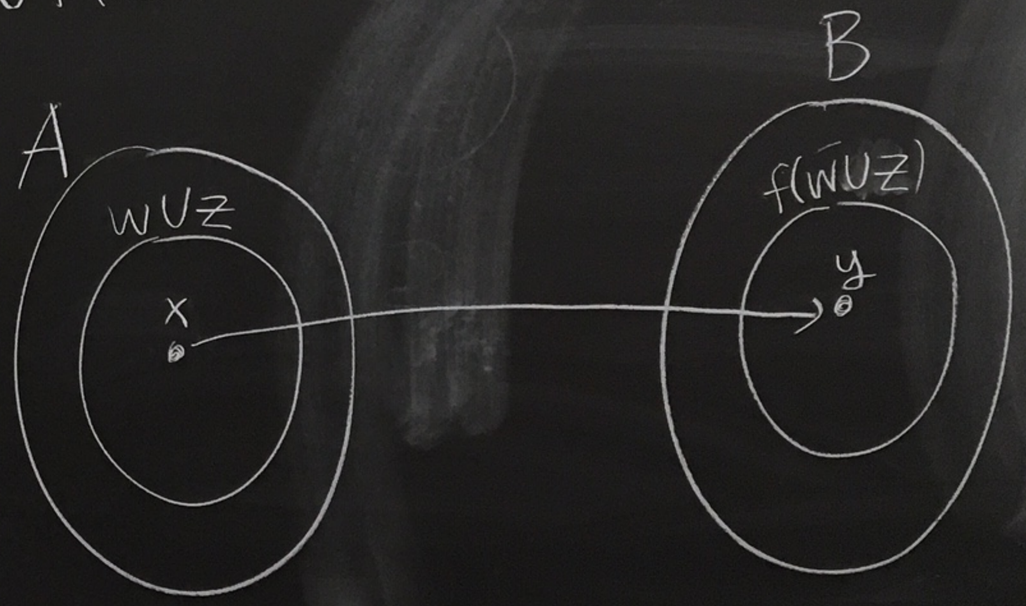
Proof:

$\subseteq$: We will show $f(W \cup Z) \subseteq f(W) \cup f(Z)$.

Let $y \in f(W \cup Z)$.

So there exists $x \in W \cup Z$ with $f(x) = y$.

Note this implies $x \in W$ or $x \in Z$.

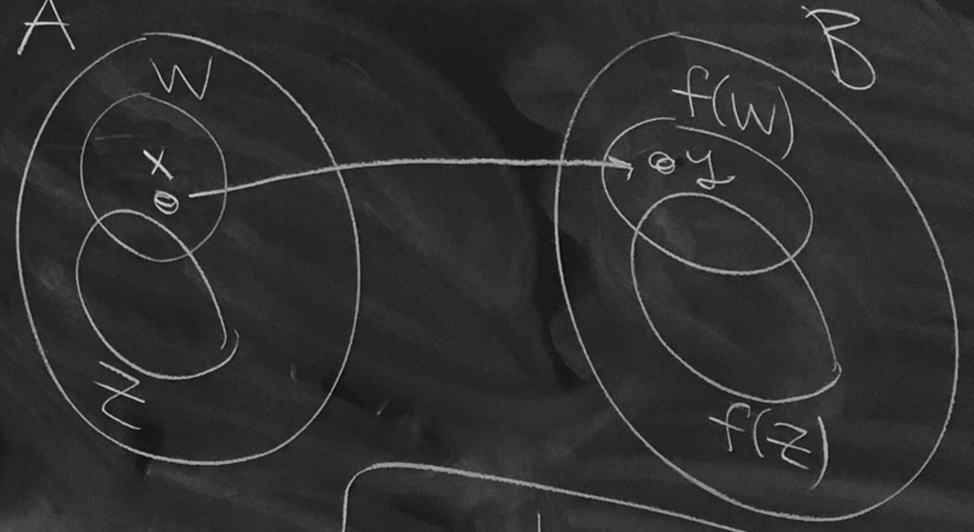


case 1: If $x \in W$, then $y = f(x)$ is in $f(W)$.
case 2: If $x \in Z$, then $y = f(x)$ is in $f(Z)$.

Thus, $y \in f(W)$ or $y \in f(Z)$.

So, $y \in f(W) \cup f(Z)$. Therefore, $f(W \cup Z) \subseteq f(W) \cup f(Z)$.

⊇: We will show
$f(W) \cup f(Z) \subseteq f(W \cup Z)$.
Let $y \in f(W) \cup f(Z)$.
So, $y \in f(W)$ or $y \in f(Z)$.



case 1 picture

Case 1: Suppose $y \in f(W)$.

Then there exists $x \in W$ with $y = f(x)$.

Since $x \in W$ we know $x \in W \cup Z$.

Since $x \in W \cup Z$ and $y = f(x)$ we know $y \in f(W \cup Z)$.

Case 2: Suppose $y \in f(Z)$.

Then there exists $x \in Z$ with $y = f(x)$.

Since $x \in Z$ we know $x \in W \cup Z$.

Since $x \in W \cup Z$ and $y = f(x)$ we know $y \in f(W \cup Z)$.

In either case, $y \in f(W \cup Z)$.

Therefore, $f(W) \cup f(Z) \subseteq f(W \cup Z)$. ▨

Hw 4

(14) $f: A \to B$

(b) If $W \subseteq B$ and $Z \subseteq B$
then $f^{-1}(W \cap Z) = f^{-1}(W) \cap f^{-1}(Z)$.

(c) If $Y \subseteq B$, then
$A - f^{-1}(Y) \subseteq f^{-1}(B - Y)$

Proof of (b)

$\subseteq$: We will show $f^{-1}(W \cap Z) \subseteq f^{-1}(W) \cap f^{-1}(Z)$

Let $a \in f^{-1}(W \cap Z)$.

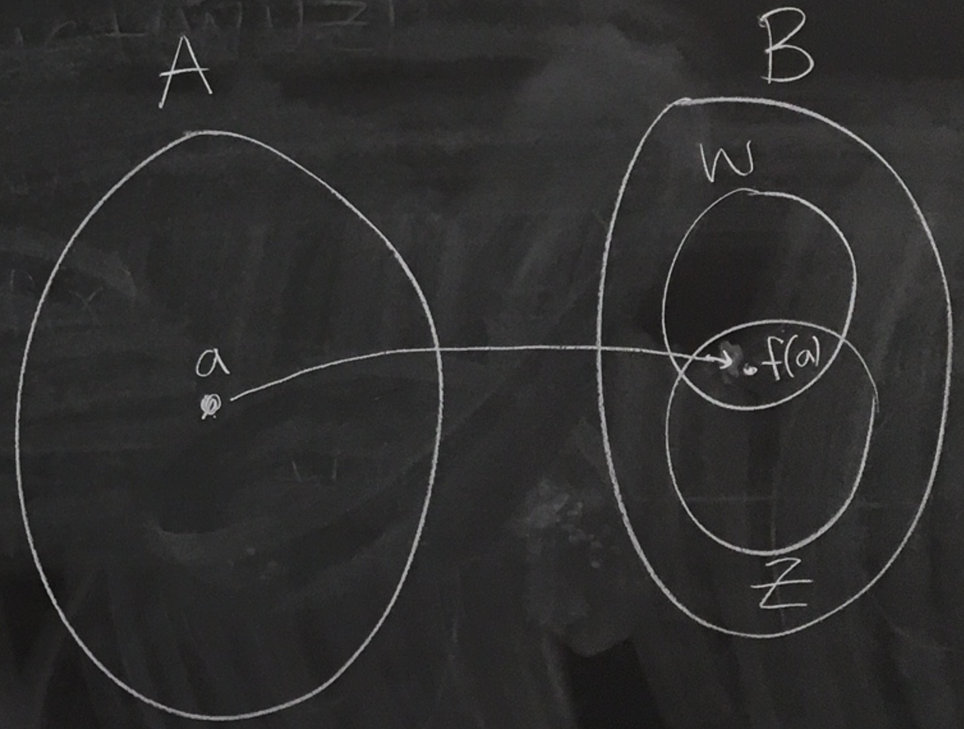
Then $f(a) \in W \cap Z$.

So, $f(a) \in W$ and $f(a) \in Z$.

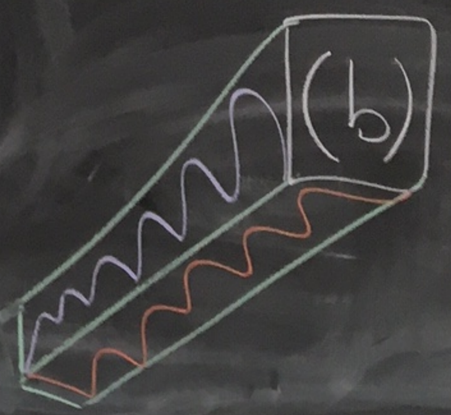
Since $f(a) \in W$ we have $a \in f^{-1}(W)$.

Since $f(a) \in Z$ we have $a \in f^{-1}(Z)$.

Thus, $a \in f^{-1}(W) \cap f^{-1}(Z)$.



(2): Let $a \in f^{-1}(W) \cap f^{-1}(Z)$.
So, $a \in f^{-1}(W)$ and $a \in f^{-1}(Z)$.
Thus, $f(a) \in W$ and $f(a) \in Z$.
Hence, $f(a) \in W \cap Z$.
Therefore, $a \in f^{-1}(W \cap Z)$.
So, $f^{-1}(W) \cap f^{-1}(Z) \subseteq f^{-1}(W \cap Z)$.



(c) $Y \subseteq B$, $A - f^{-1}(Y) \subseteq f^{-1}(B-Y)$.

Let $a \in A - f^{-1}(Y)$.

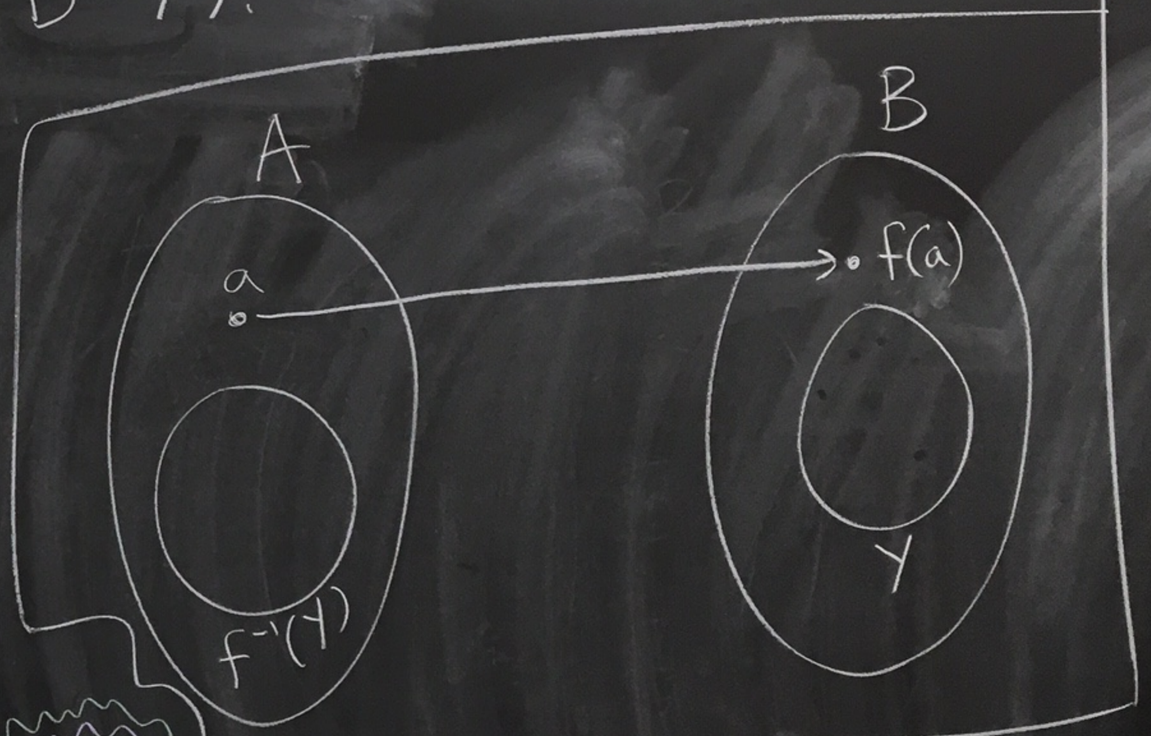
So, $a \in A$ and $a \notin f^{-1}(Y)$.

Thus, $f(a) \in B$ and $f(a) \notin Y$.

So, $f(a) \in B - Y$.

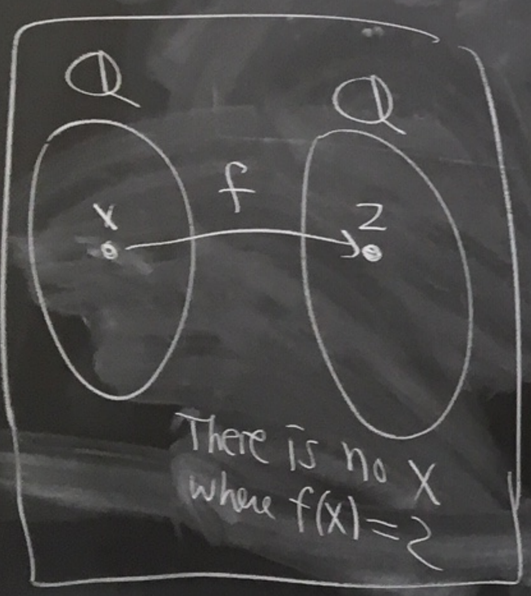
Thus, $a \in f^{-1}(B-Y)$.

Therefore, $A - f^{-1}(Y) \subseteq f^{-1}(B-Y)$. (a)



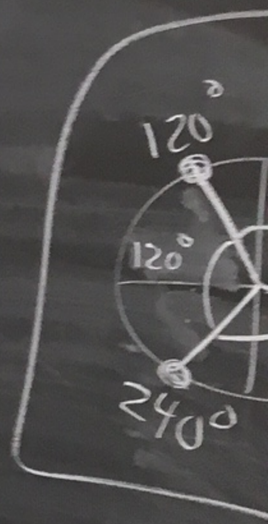
Hw 4

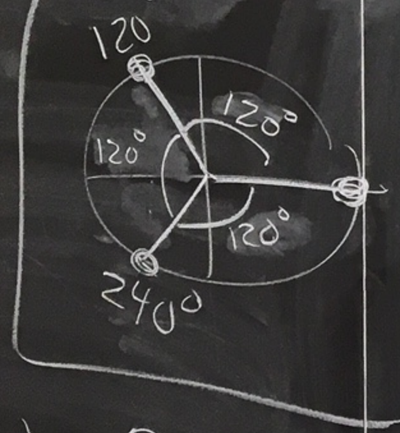
2(b) $f: \mathbb{Q} \to \mathbb{Q}$, $f(x) = x^3$



(1-1 ??) Given $x, y \in \mathbb{Q}$, if $f(x) = f(y)$ then $x^3 = y^3$. So, $x = y$.
So, f is 1-1.

(onto ??) No, f is not onto $\mathbb{Q}$.
For example, there is no $x \in \mathbb{Q}$ with $f(x) = 2$.
If so, there would be $x \in \mathbb{Q}$ with $x^3 = 2$.





$f(x) = 2.$

$h\ x^3 = 2,$

Either use HW technique to show there is no $x \in \mathbb{Q}$ with $x^3 = 2$.

Or say that the only solutions to $x^3 = 2$ are

$x = 2^{1/3}$, $2^{1/3}\left(\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)\right)$, $2^{1/3}\left(\cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right)\right)$

$x = 2^{1/3}$, $2^{1/3}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$, $2^{1/3}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)$

None of these are in $\mathbb{Q}$.

Test 2

- def statements
- computations
- proofs

11/13
Weds

Test 2 – next Weds – 11/20

M	W
	11/13 functions
11/18 Cardinality	11/20 Test 2
12/2 Cardinality	12/4 Cardinality
12/9 Review HW on cardinality	12/11 Final 12-2pm

HW 3 (Constructing $\mathbb{Q}$ out of $\mathbb{Z}$)

(9) $S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$

Define $\sim$ on S where

$(a,b) \sim (c,d)$ iff $ad = bc$.

(a) Is $(1,5) \sim (-3,-15)$?

$(1)(-15) = (5)(-3)$

Yes.

Motivation

We are going to construct $\mathbb{Q}$.

$(1,2) \in S$ think of it as $\frac{1}{2}$

$(a,b) \in S$, $b \neq 0$, think of it as $\frac{a}{b}$

$\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$

$\mathbb{N}$ → problem 8

$\mathbb{Z}$ → problem 9

$\mathbb{Q}$

(b) Is $(1,1) \sim (3,5)$?

No because $(1)(5) \neq (1)(3)$.

(c) Show $\sim$ is an equivalence relation

Pf: See solutions.

(d) List five elements from

$\overline{(1,1)} = \{(1,1), (2,2), (5,5), (-2,-2), (-8,-8), \ldots\} = \overline{(2,2)}$

$\overline{(2,3)} = \{(2,3), (4,6), (-2,-3), (-4,-6), (8,12), \ldots\} = \overline{(8,12)}$

(f) Define $\overline{(a,b)} \odot \overline{(c,d)} = \overline{(ac, bd)}$

Show $\odot$ is well-defined.

Step 1: Pick $(a,b),(c,d) \in S$.

So, $a,b,c,d \in \mathbb{Z}$ and $b \neq 0$ and $d \neq 0$.

$\mathbb{Z}$ is closed under multiplication so

$ac, bd \in \mathbb{Z}$.

Since $b \neq 0$ and $d \neq 0$, we know $bd \neq 0$.

So, $(ac, bd) \in S$.

Thus, $\overline{(a,b)} \odot \overline{(c,d)} = \overline{(ac,bd)} \in S/\sim$.

Recall $S/\sim$ means the set of equivalence classes

Motivation

(f) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

(e) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

$S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$

Step 2 Suppose $(a,b),(c,d),(e,f),(g,h) \in S$
and $\overline{(a,b)} = \overline{(e,f)}$ and $\overline{(c,d)} = \overline{(g,h)}$.
We need to show $\overline{(a,b)} \odot \overline{(c,d)} = \overline{(e,f)} \odot \overline{(g,h)}$

Since $\overline{(a,b)} = \overline{(e,f)}$ and $\overline{(c,d)} = \overline{(g,h)}$
we know $(a,b) \sim (e,f)$ and $(c,d) \sim (g,h)$.

Thus, $af = be$ and $ch = dg$.
Multiplying these equations gives $afch = bedg$.
So, $(ac)(fh) = (bd)(eg)$.

Side-work

NTS:

$\overline{(ac,bd)} = \overline{(eg,fh)}$

$(ac,bd) \sim (eg,fh)$

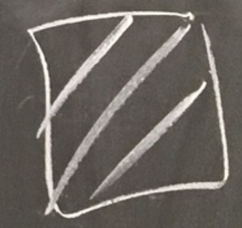
$acfh = bdeg$

Thus, $(ac, bd) \sim (eg, fh)$.

Hence, $\overline{(ac, bd)} = \overline{(eg, fh)}$.

Therefore,

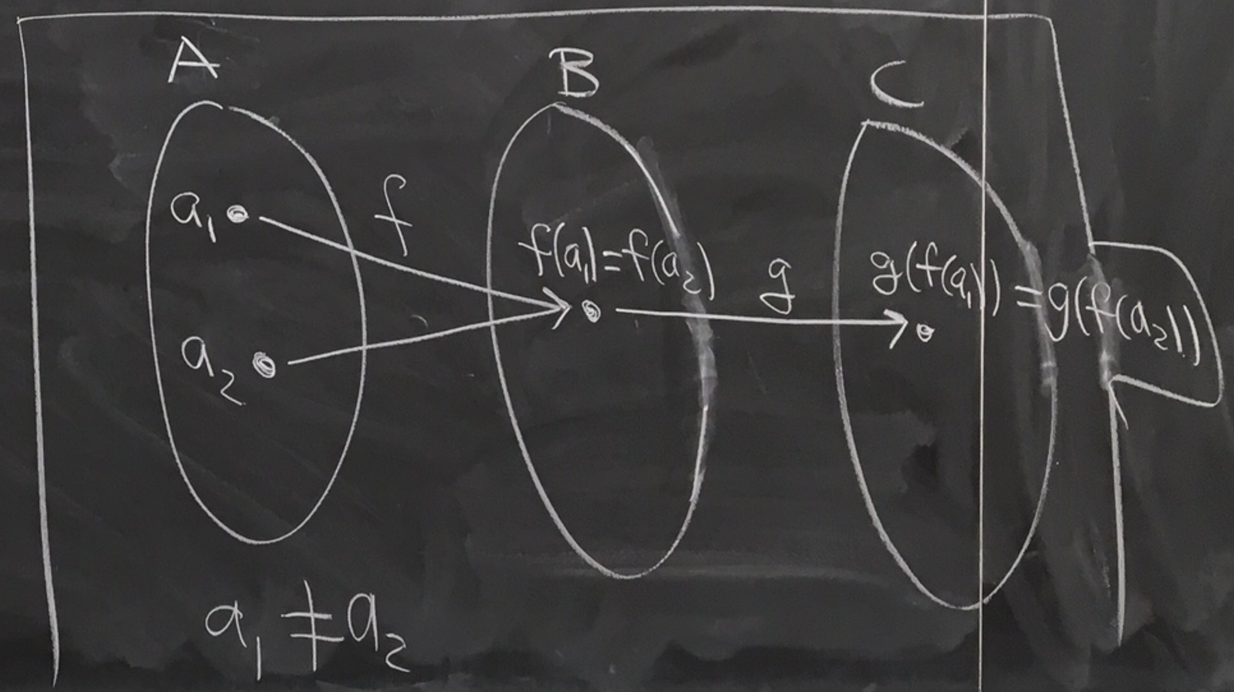
$$\overline{(a,b)} \odot \overline{(c,d)} = \overline{(e,f)} \odot \overline{(g,h)}.$$



HW 4

⑨ Suppose $f: A \to B$ and $g: B \to C$.
Prove: If f is not one-to-one
then $g \circ f$ is not one-to-one.

Pf: Since f is not one-to-one there exist $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$ and $a_1 \neq a_2$.



Then, $g(f(a_1)) = g(f(a_2))$.

Hence $(g \circ f)(a_1) = (g \circ f)(a_2)$ and $a_1 \neq a_2$.

Therefore, $g \circ f$ is not one-to-one. ▨

Then, $g(f(a_1)) = g(f(a_2))$.

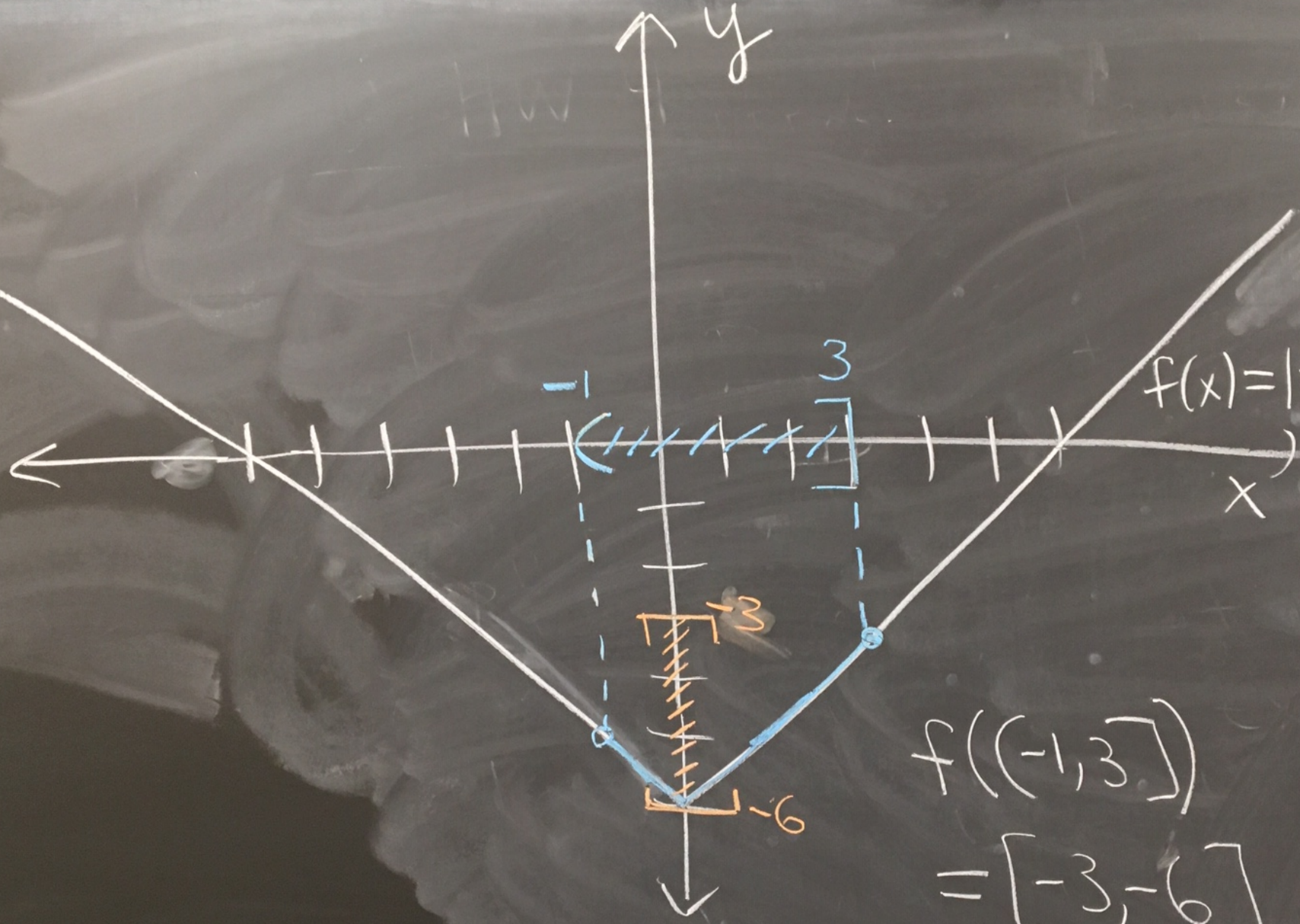
Hence $(g \circ f)(a_1) = (g \circ f)(a_2)$ and $a_1 \neq a_2$.

Therefore, $g \circ f$ is not one-to-one. ▨

Ex: $f(x) = |x| - 6$

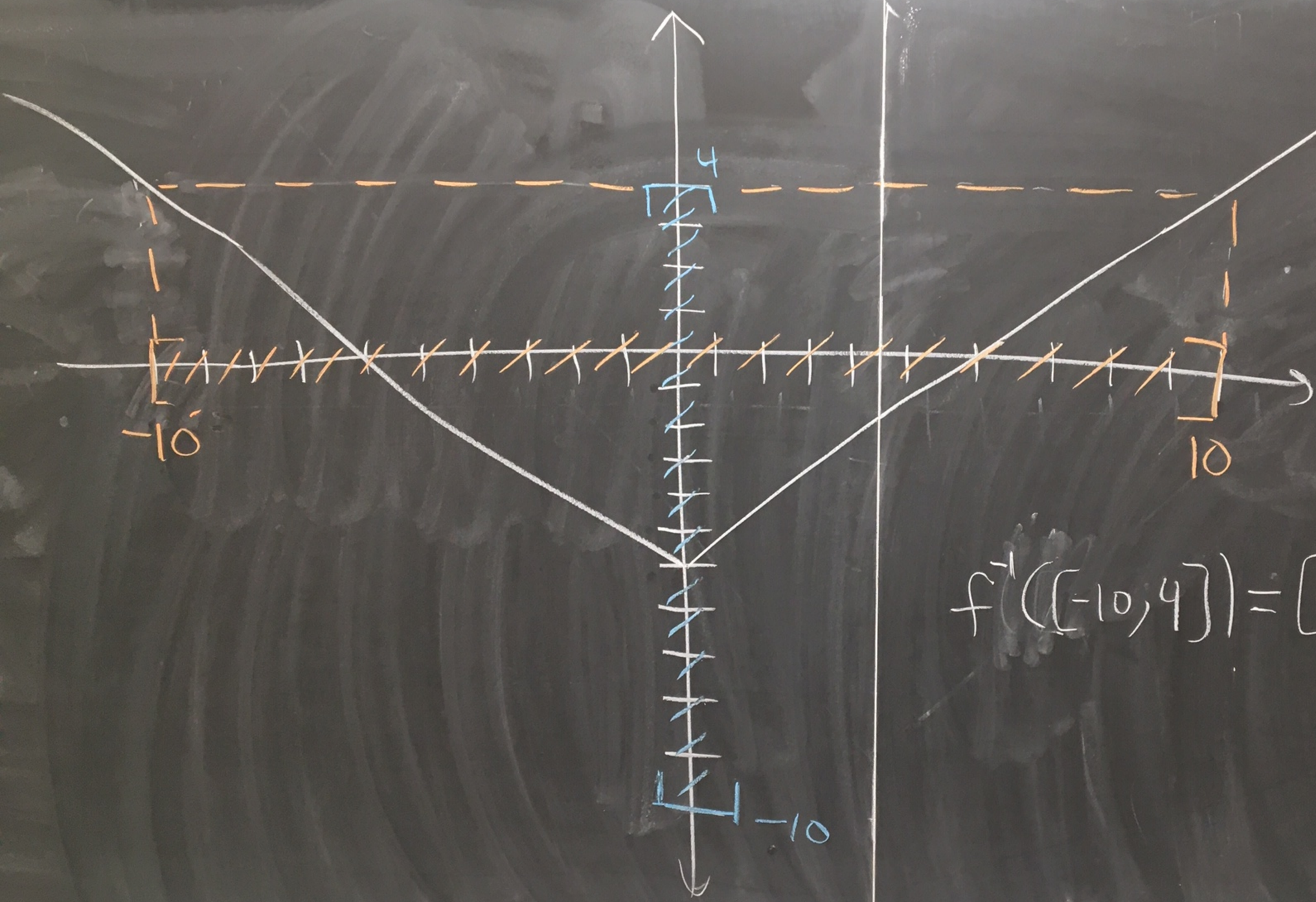
(a) $f((-1, 3])$

(b) $f^{-1}([-10, 4])$



$f((-1,3])$

$=[-3,-6]$



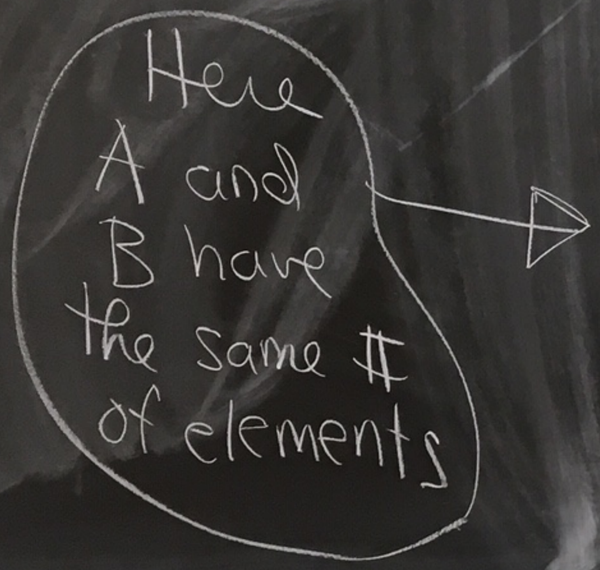
$f(x) = |x| - 6$

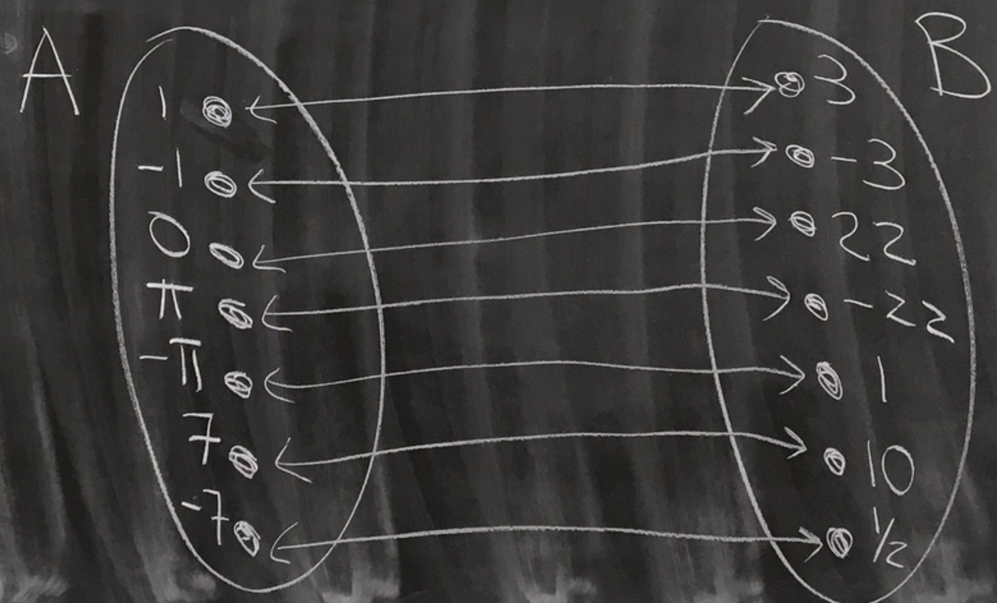
$f^{-1}([-10, 4]) = [-10, 10]$

Monday
11/18

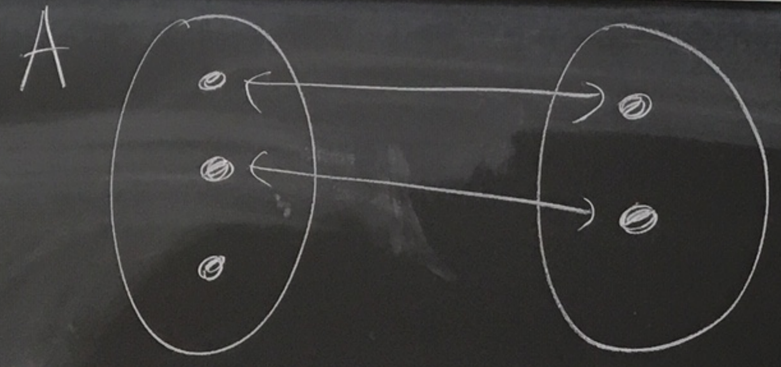
Cardinality

How can we tell if two finite sets have the same number of elements?





You see if you can pair up the elements in a 1-1 and onto way.



there is no way to pair up the elements of A and B in a 1-1 and onto way.

So, A and B have different sizes.

Def: Let A and B be sets. We say that A and B have the same cardinality if there exists a bijection between them. And if such a bijection exists we write $|A| = |B|$.

If no such bijection exists we say that A and B have unequal cardinality and we write $|A| \neq |B|$.

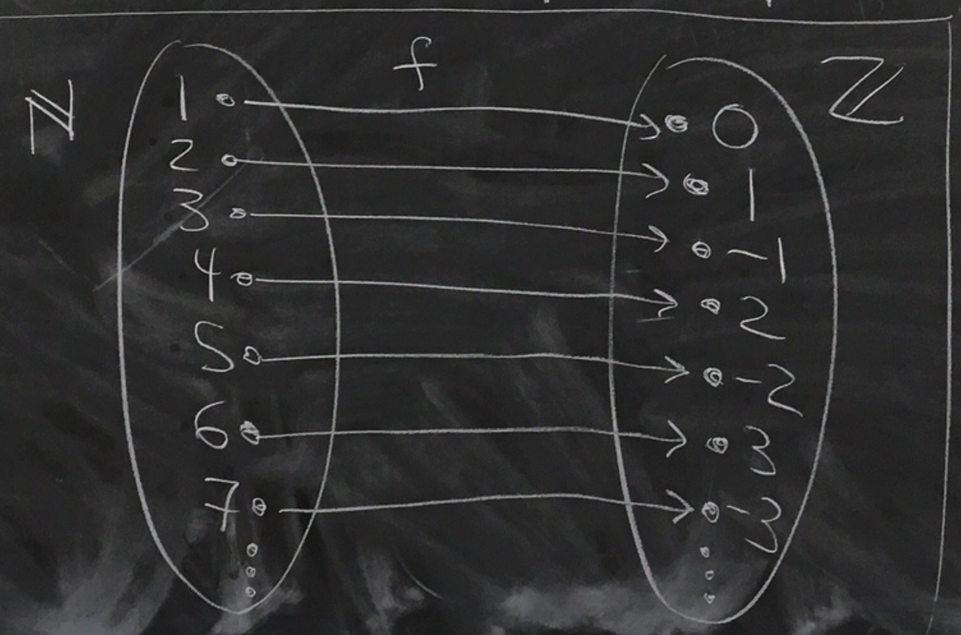
Ex: $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Q: Is $|\mathbb{N}| = |\mathbb{Z}|$ or $|\mathbb{N}| \neq |\mathbb{Z}|$??

Formula for f

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\left(\frac{n-1}{2}\right) & \text{if } n \text{ is odd} \end{cases}$$

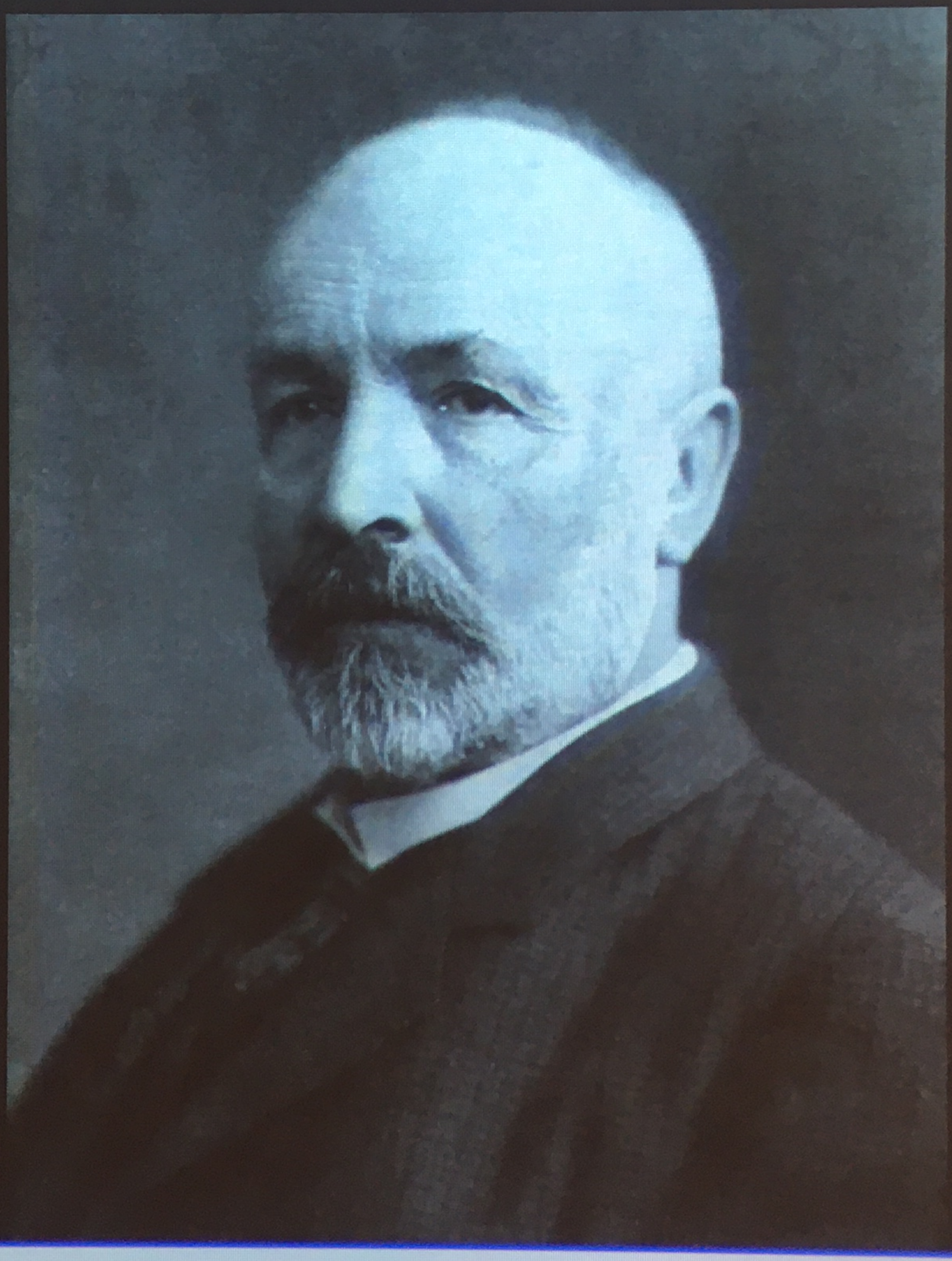


Define $f: \mathbb{N} \to \mathbb{Z}$ as in the picture (and keep going with the same pattern).

Then $f: \mathbb{N} \to \mathbb{Z}$ is a bije

So, $|\mathbb{N}| = |\mathbb{Z}|$

ecure https://www.bing.com/search?q=cantor+math&form=EDGEAR&qs=HS&cvid=f



the fast, new browser built for Windows

Ex: $|\mathbb{N}| \neq |\mathbb{R}|$.

(Cantor's Diagonalization Argument)

We will show that there is no bijection $f: \mathbb{N} \to \mathbb{R}$.

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

We prove that f can't be onto.

Let's make a table.
Suppose f has the following outputs.

n	$f(n)$
1	$X_1 \cdot \mathbf{b_{11}} b_{12} b_{13} b_{14} b_{15} \cdots$
2	$X_2 \cdot b_{21} \mathbf{b_{22}} b_{23} b_{24} b_{25} \cdots$
3	$X_3 \cdot b_{31} b_{32} \mathbf{b_{33}} b_{34} b_{35} \cdots$
4	$X_4 \cdot b_{41} b_{42} b_{43} \mathbf{b_{44}} b_{45} \cdots$
5	$X_5 \cdot b_{51} b_{52} b_{53} b_{54} \mathbf{b_{55}} \cdots$
⋮	⋮

here $X_i \in \mathbb{Z}$

$b_{ij} \in \{0,1,2,3,4,5,6,7,8,9\}$

If the decimal expansion terminates, just add 0's forever.

Define $b = 0.b_1 b_2 b_3 b_4 b_5 \cdots$

where $b_{\bar{\imath}} = \begin{cases} 0 & \text{if } b_{\bar{\imath}\bar{\imath}} \neq 0 \\ 1 & \text{if } b_{\bar{\imath}\bar{\imath}} = 0 \end{cases}$

By construction $b \neq f(n)$ for all $n \in \mathbb{N}$.

So, b is not in the range of f.

But $b \in \mathbb{R}$. So, f is not onto. ∎

Concrete example

n	f(n)
1	1.32547...
2	5.00000000...
3	-17.3317325...
4	0.50000000...
5	3.14159926...
6	-100.10057892...
⋮	⋮

$b_{11}=3$ $b_{33}=1$ $b_{55}=9$

$b = 0.0\,1\,0\,1\,0\,0\,\ldots$

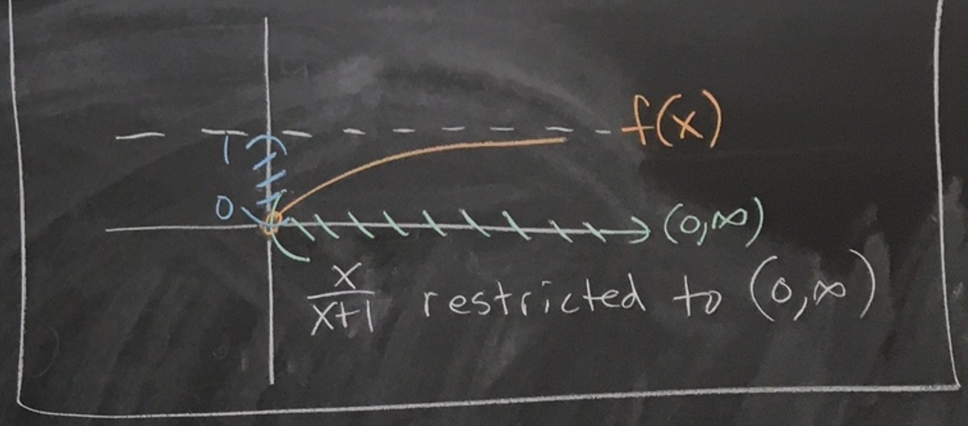
$b_{22}=0$ $b_{44}=0$ $b_{66}=8$

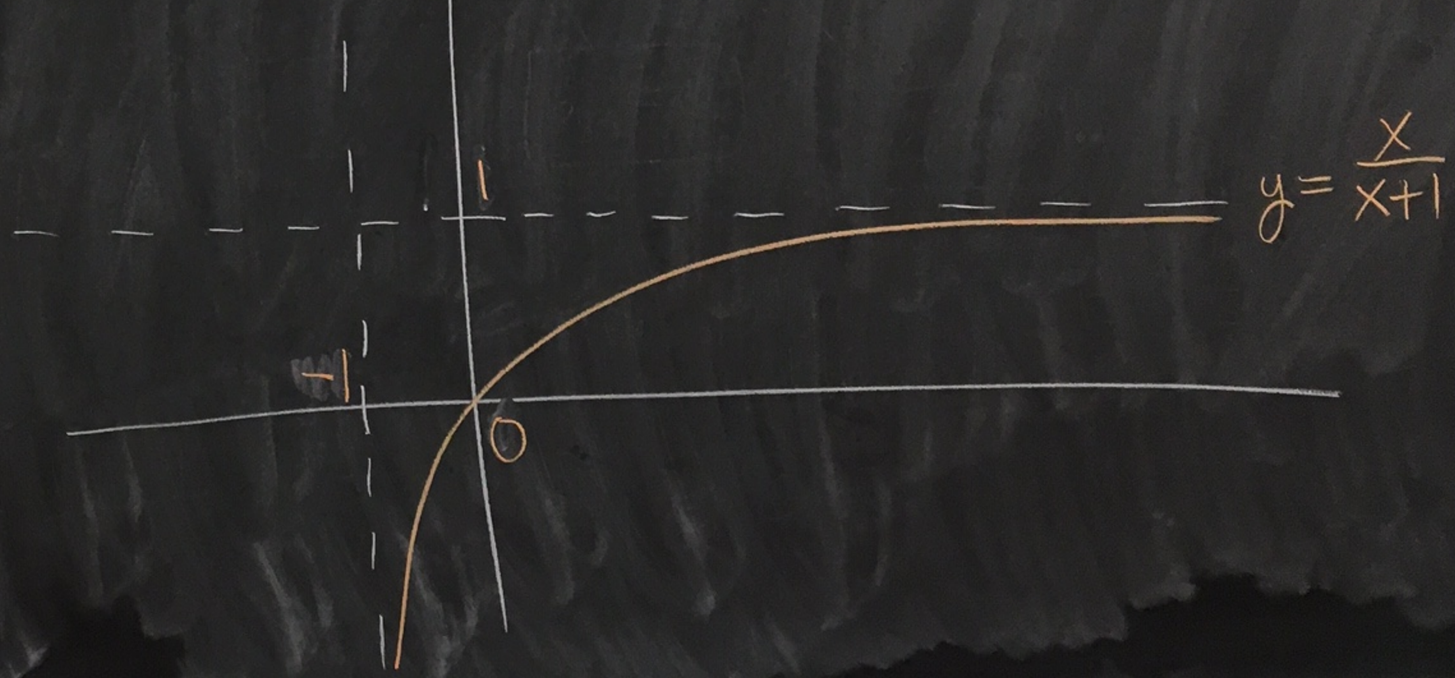
Ex: $|(0,\infty)| = |(0,1)|$

Let $f:(0,\infty) \longrightarrow (0,1)$

be defined by

$$f(x) = \frac{x}{x+1}$$





f is 1–1

Suppose $f(x_1) = f(x_2)$ where $x_1, x_2 \in (0, \infty)$.

Then $\frac{x_1}{x_1+1} = \frac{x_2}{x_2+1}$.

So, $x_1x_2 + x_1 = x_1x_2 + x_2$.

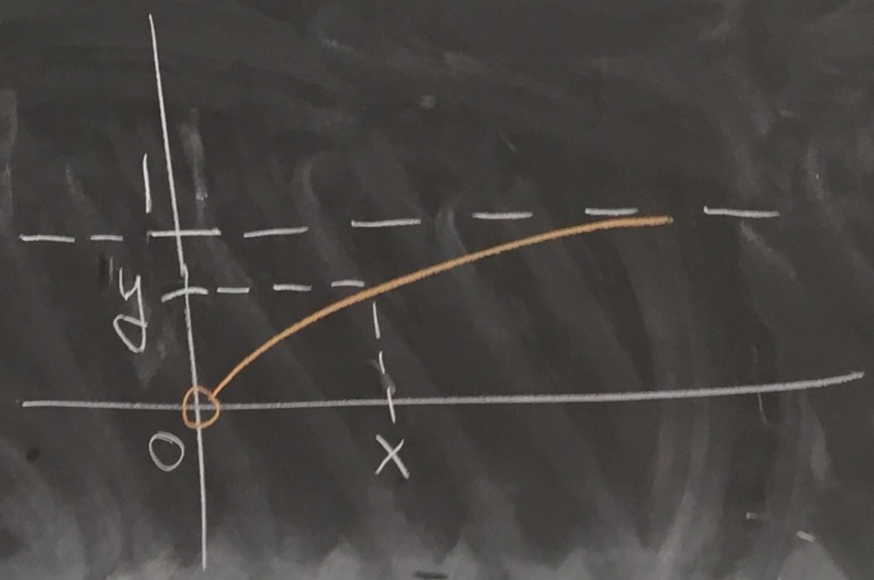
Thus, by adding $-x_1x_2$ to both sides,

we get $x_1 = x_2$.

f is onto

Let $y \in (0,1)$.

We want to find $x \in (0, \infty)$ where $f(x) = y$.



Let's solve $\frac{x}{x+1} = y$.

We want $x = xy + y$,

ie $x - xy = y$,

ie $x(1-y) = y$.

ie $\boxed{x = \frac{y}{1-y}}$

Check: $f\left(\frac{\frac{y}{1-y}}{\frac{y}{1-y}+1}\right) = \frac{\left(\frac{y}{1-y}\right)}{\left(\frac{y+(1-y)}{1-y}\right)} = \frac{y}{1} = y.$

Is $x \in (0,\infty)$?

We know $0 < y < 1$.

So, $-1 < -y < 0$.

Thus, $0 < 1-y < 1$.

Thus, $\boxed{0 < \frac{y}{1-y} = x}$.

So, $\boxed{|(0,\infty)| = |(0,1)|}$

Summary: Given $y \in (0,1)$, set $x = \frac{y}{1-y}$. Then $f(x) = y$ and $0 < x < \infty$. So, f is onto. ▨

Monday
12/2

Recall from last time

We say that two sets A and B have the same cardinality if there exists a bijection between them. If so, we write $|A| = |B|$.

If no such bijection exists we write $|A| \neq |B|$.

Ex:

$|\mathbb{N}| = |\mathbb{Z}|$

$|\mathbb{N}| \neq |\mathbb{R}|$

$|(0,1)| = |(0,\infty)|$

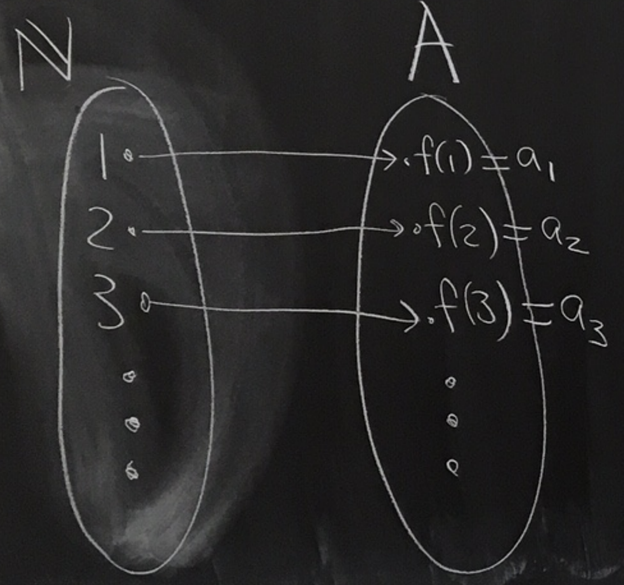
Def: Let A be a set.

- We say that A is <u>countably infinite</u> if $|A| = |\mathbb{N}|$
- We say that A is <u>countable</u> if either A is finite or A is countably infinite.
- We say that A is <u>uncountable</u> if A is not countable, that is A is infinite and $|A| \neq |\mathbb{N}|$.

Ex: $\mathbb{Z}$ is countably infinite. $\mathbb{Z}$ is countable.

$\{1,2,4\}$ is countable. $\mathbb{R}$ is uncountable.

Theorem: A set A is countably infinite iff its elements can be arranged in an infinite list $a_1, a_2, a_3, \ldots$ with no repeats.



proof:

($\Rightarrow$) Suppose A is countably infinite. Then there exists $f: \mathbb{N} \to A$ that is a bijection. Define $a_i = f(i)$.

Then consider the list $a_1, a_2, a_3, \ldots$

Since f is onto, our list gives all of A.

Since f is 1-1, the list has no repeats.

($\Leftarrow$) Suppose the elements of A can be arranged in an infinite list $a_1, a_2, a_3, \ldots$ with no repeats.

Define $f: \mathbb{N} \to A$ by $f(i) = a_i$.

Since the list has no repeats, f is 1-1.

Since the list contains all the elements of A, f is onto.

So f is a bijection and $|\mathbb{N}| = |A|$.

So, A is countably infinite. $\square$

Theorem: $\mathbb{Q}$ is countably infinite.

0 1 −1 2 −2 3 −3 ...

Start here

$\frac{0}{1}$ → $\frac{1}{1}$ → $\frac{-1}{1}$ → $\frac{2}{1}$ → $\frac{-2}{1}$ → $\frac{3}{1}$ → $\frac{-3}{1}$ ...

$\frac{1}{2}$ → $\frac{-1}{2}$ → ~~$\frac{2}{2}$~~ → ~~$\frac{-2}{2}$~~ → $\frac{3}{2}$ → $\frac{-3}{2}$ ...

$\frac{1}{3}$ → $\frac{-1}{3}$ → $\frac{2}{3}$ → $\frac{-2}{3}$ → ~~$\frac{3}{3}$~~ → ~~$\frac{-3}{3}$~~ ...

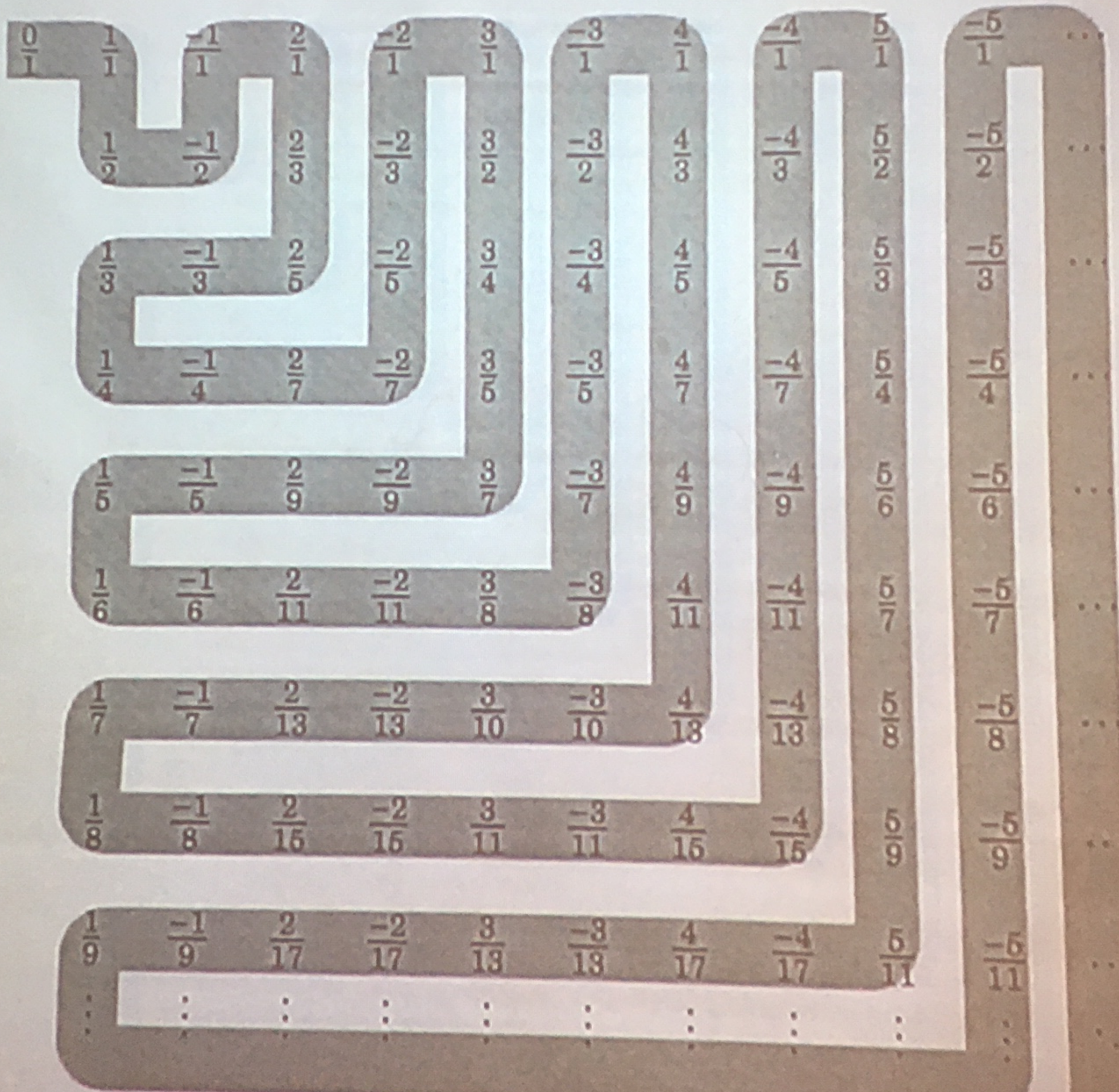
$\frac{1}{4}$ → $\frac{-1}{4}$ → ~~$\frac{2}{4}$~~ → ~~$\frac{-2}{4}$~~ → $\frac{3}{4}$ → $\frac{-3}{4}$ ...

$\frac{1}{5}$ → $\frac{-1}{5}$ → $\frac{2}{5}$ → $\frac{-2}{5}$ → $\frac{3}{5}$ → $\frac{-3}{5}$ ...

$\frac{1}{6}$ → $\frac{-1}{6}$ → ~~$\frac{2}{6}$~~ → ~~$\frac{-2}{6}$~~ → ~~$\frac{3}{6}$~~ → ~~$\frac{-3}{6}$~~ ...

...

0 1 −1 2 −2 3 −3 4 −4 5 −5 ⋯



We put $\mathbb{Q}$ into an infinite list
with no repeats by weaving through
the infinite table as indicated
and removing repeats as we encounter
them. Here are the first entries in the list:

$$0, 1, \frac{1}{2}, -\frac{1}{2}, -1, 2, \frac{2}{3}, -\frac{1}{3}, \frac{1}{3}, \cdots$$

This will give an arrangement of $\mathbb{Q}$ into
an infinite list with no repeats. So, $\mathbb{Q}$ is
countably infinite. ▨

sets in each column have same cardinality

Countably infinite

$\mathbb{N}$

$\mathbb{Z}$

$\mathbb{Q}$

Uncountable

$\mathbb{R}$ $\quad \mathcal{P}(\mathbb{R})$ $\quad \mathcal{P}(\mathcal{P}(\mathbb{R}))$ $\quad \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))$ ...

$\mathcal{P}(\mathbb{N})$

We will show $\mathcal{P}(A)$ is "bigger" than A for all A.

You can keep getting "bigger" and "bigger" infinite sets by continually taking the power set of each set.

$\aleph$ is the first letter in the Hebrew alphabet

aleph

this cardinality is called $\aleph_0$ aleph naught

is there any set "in between" in cardinality between $\mathbb{N}$ and $\mathbb{R}$?

Unknown.

Continuum hypothesis

Some more theorems (see Hammack)

Thm: If A and B are countably infinite, then $A \times B$ is countably infinite. [Similar proof as $\mathbb{Q}$ is countably infinite.]

Thm: If A and B are countably infinite, then $A \cup B$ is countably infinite.

Thm: An infinite subset of a countably infinite set is countably infinite.

Thm: If $U \subseteq A$ and U is uncountable, then A is uncountable.

Thm:

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$$

Final

Test 1 topics

Test 2 topics

little bit of cardinality

At least one proof
will be exactly one
from test 1 | test 2
without any changes

12/4
Weds

Def: Let A and B be sets.

① $|A| = |B|$ means there exists a bijection $f: A \to B$.

② $|A| \leq |B|$ means there exists a one-to-one function $f: A \to B$

③ $|A| < |B|$ means there exists a one-to-one function $f: A \to B$, but there is no bijection $g: A \to B$

Ex: $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$

$|\mathbb{N}| < |\mathbb{R}|$

The next theorem will show that

$$|\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))| < \cdots$$

So there is no "biggest" set.

Theorem: Let A be a set. Then $|A| < |\mathcal{P}(A)|$.

pf:

If A is finite then $|A| < 2^{|A|} = |\mathcal{P}(A)|$.

Now assume A is infinite.

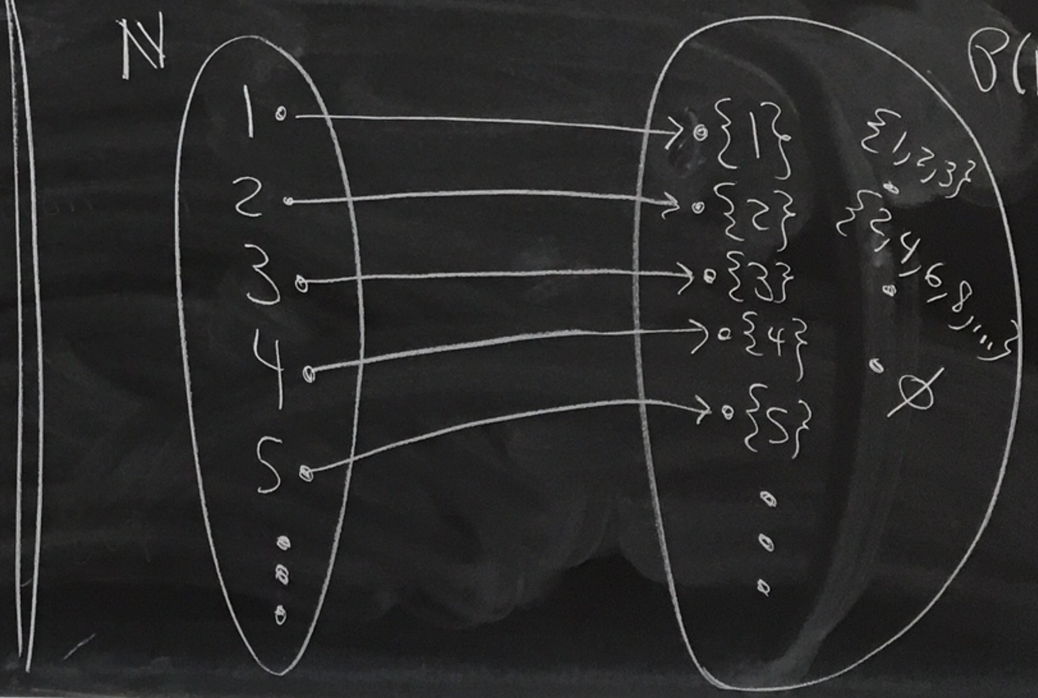
Step 1: Create $f: A \to \mathcal{P}(A)$ that is 1-1

Define $f: A \to \mathcal{P}(A)$ by $f(a) = \{a\}$.

Let's show f is 1-1.

Suppose $f(x) = f(y)$ where $x, y \in A$.

Side example of $f: \mathbb{N} \to \mathcal{P}(\mathbb{N})$ that is 1-1.



Then $\{x\}=\{y\}$. ⟸ $x\in\{y\}$, so $x=y$.

So, $x=y$.

So, $|A|\leq|\mathcal{P}(A)|$.

Step 2: Show there is no bijection $g: A\to\mathcal{P}(A)$.

Suppose $g: A\to\mathcal{P}(A)$.
We will show g cannot be onto.
We do this by constructing

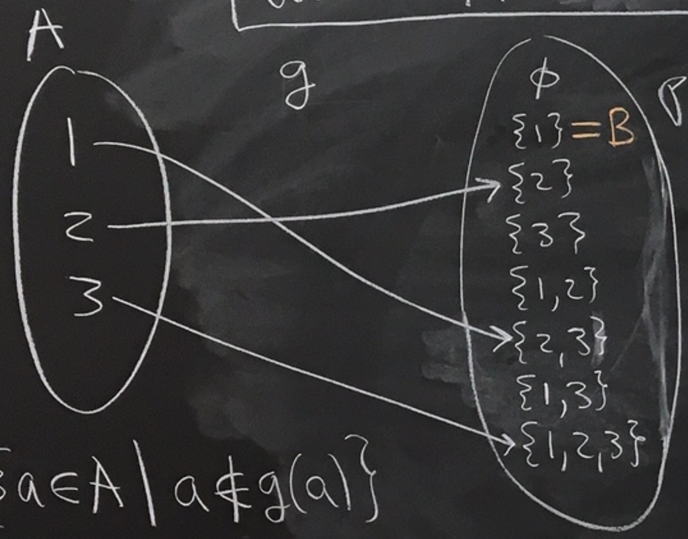
↳ an element $B\in\mathcal{P}(A)$ that isn't in the range of g.

Let

$$B=\{a\in A \mid a\notin g(a)\}.$$

Note $B\subseteq A$, so $B\in\mathcal{P}(A)$.
Let's show $B\notin$ range(g).

Example of B where $A = \{1,2,3\}$



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

$1 \notin g(1)$? Yes. $1 \notin \{2,3\}$

$2 \notin g(2)$? No. $2 \in \{2\}$

$3 \notin g(3)$? No, $3 \in \{1,2,3\}$

$B = \{1\}$

$B \notin \text{range}(g)$

(proof continued...)

Let $a \in A$.

We will show $g(a) \neq B$.

One we've shown this then we know there is no element of A that maps to B.

Case 1: Suppose $a \in g(a)$.

Thus, by the def. of B, $a \notin B$.

Why can't we have $g(a) = B$?

Suppose $g(a) = B$.

By assumption, $a \in g(a)$. So if $g(a) = B$, then $a \in B$.

B.

$a \in B$.

→ Then we would have both $a \notin B$ and $a \in B$, which can't happen.

So in this case, $g(a) \neq B$.

Case 2: Suppose $a \notin g(a)$

Since $a \notin g(a)$ we have $a \in B$.

Why can't $g(a) = B$?

If $g(a) = B$, then since $a \notin g(a)$ we would get $a \notin B$.

We can't have $a \in B$ and $a \notin B$.

→ So in this case, $g(a) \neq B$.

In both cases $g(a) \neq B$.

Since a was an arbitrary element of A, we have shown $B \notin \text{range}(g)$.

So, g isn't onto. ▨

Cantor-Bernstein-Schröder Theorem

Let A and B be sets.

If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

That is, if there exist one-to-one functions $f: A \to B$ and $g: B \to A$, then there exists a bijection $h: A \to B$.

Thm: $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

$$|\mathbb{Q}| = |\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < \cdots$$

$$|\mathbb{N}| = |\mathbb{Z}|$$

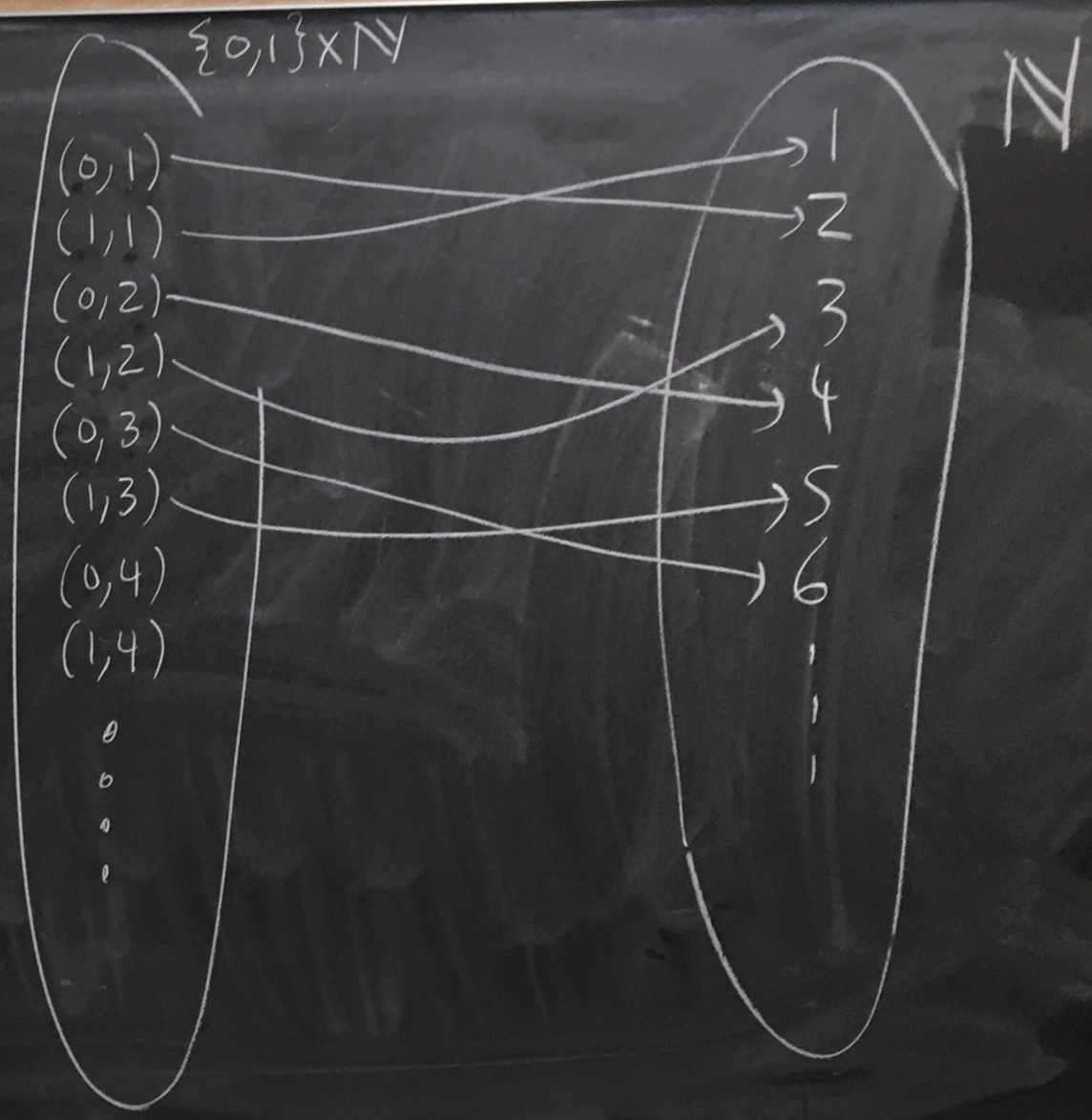
$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$$

14.1

(9) Show $|\{0,1\} \times \mathbb{N}| = |\mathbb{N}|$

$$f(a,n) = \begin{cases} 2n, & \text{if } a=0 \\ 2n-1, & \text{if } a=1 \end{cases}$$

$f(a,n) = 2n - a$



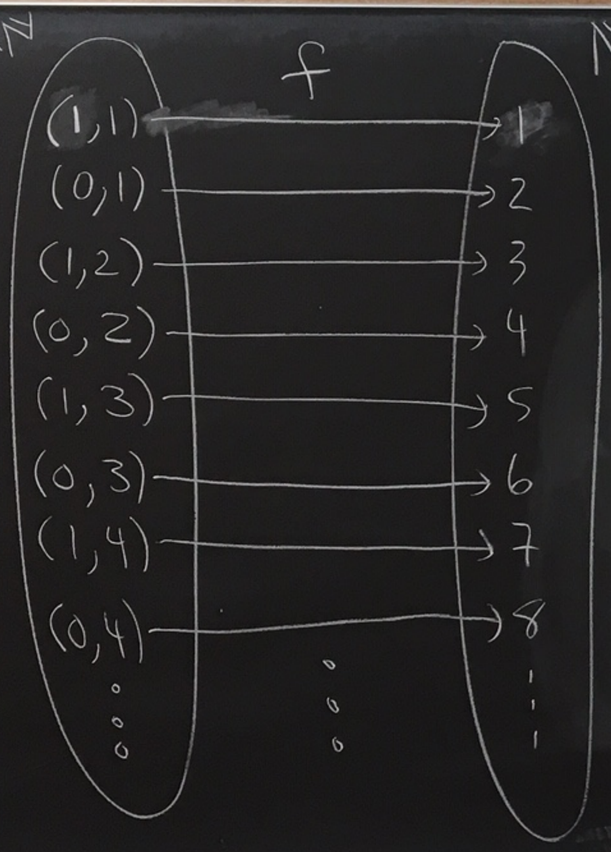
Mon
12/9

14.1

#9 Show that $\{0,1\} \times \mathbb{N}$ has the same cardinality as $\mathbb{N}$ by constructing a bijection between the two sets.

a_2.

$n_2 - a_2 = 2n_2$
be even.



$$f(a,n) = \begin{cases} 2n, & \text{if } a=0 \\ 2n-1, & \text{if } a=1 \end{cases}$$

$f(a,n) = 2n - a$

f is a bijection

① f is one-to-one

Suppose $f(a_1,n_1) = f(a_2,n_2)$ for some $a_1, a_2 \in \{0,1\}$ and $n_1, n_2 \in \mathbb{N}$.

Since $f(a_1,n_1)=f(a_2,n_2)$ we have $2n_1-a_1=2n_2-a_2$.

<u>case 1: Suppose $a_1=0$.</u>

Then, $2n_2-a_2=2n_1-a_1=2n_1$

So, $2n_2-a_2$ is even.

Since $a_2=0$ or $a_2=1$ we must have $a_2=0$ to <u>have $2n_2-a_2=2n_2$ be even.</u>

<u>case 2: Suppose $a_1=1$.</u>

Then, $2n_2-a_2=2n_1-a_1=2n_1-1$ is odd.

So, $a_2\neq 0$, because then $2n_2-a_2=2n_2$ would be even.

So, $a_2=1$.

So, if $a_1=0$ then $a_2=0$,
and if $a_1=1$ then $a_2=1$.

So, $a_1=a_2$.

Since $2n_1-a_1=2n_2-a_2$ and $a_1=a_2$
we get $2n_1=2n_2$.

Thus, $n_1=n_2$.

Therefore, $(a_1,n_1)=(a_2,n_2)$.

So, f is 1-1.

$f(a,n)=2n-a$

f is onto

Let $b\in\mathbb{N}$.

case 1: Suppose b is even.

Then $b=2n$ for some $n\in\mathbb{N}$.

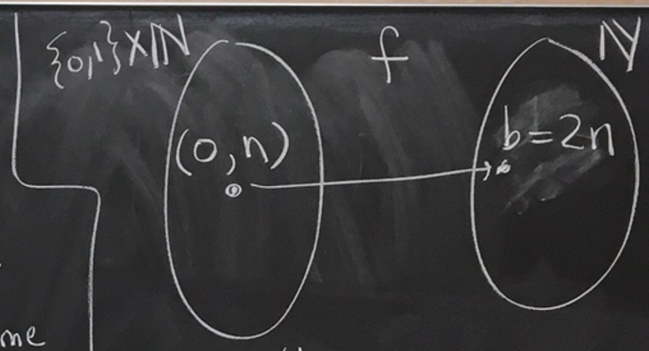
And $f(0,n)=2n-0=b$.

case 2: Suppose b is odd.

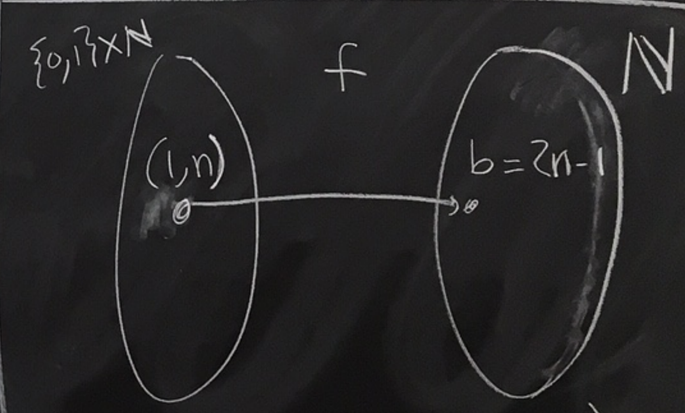
Then $b=2n-1$ for some $n\in\mathbb{N}$.

And $f(1,n)=2n-1=b$.

Therefore f is onto. ▨



(b even picture)



(b is odd picture)

$f: A \longrightarrow B$
$3k \longmapsto 5k$

14.1

⑤ Same question with

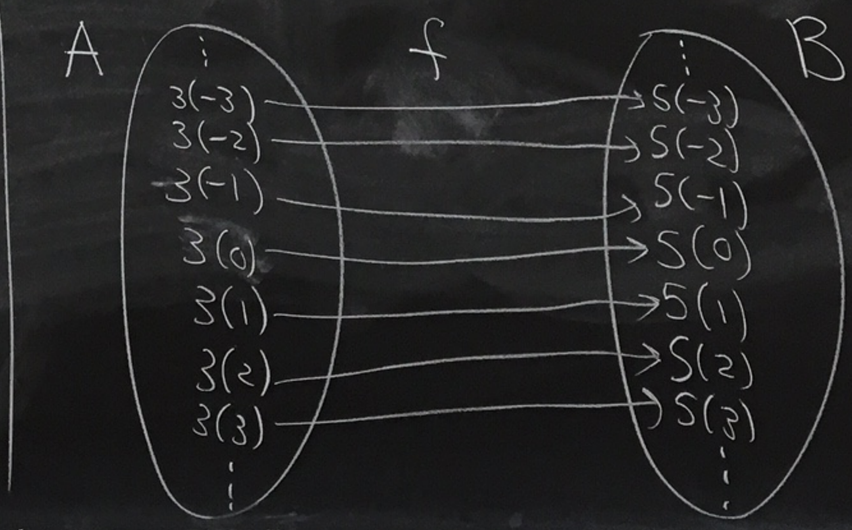
$$A = \{3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

and $B = \{5k \mid k \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

Scratchwork

$3k \longmapsto 5k$

$x \longmapsto \frac{5}{3}x$



Define
$f: A \to B$
by $f(x) = \frac{5}{3}x$

f is well-defined

Let $x \in A$.

Then $x = 3k$ for some $k \in \mathbb{Z}$.

And $f(x) = \frac{5}{3}x = \frac{5}{3}(3k)$

$= 5k \in B$.

f is 1-1

Suppose $f(x_1) = f(x_2)$ where $x_1, x_2 \in A$.

Then, $\frac{5}{3}x_1 = \frac{5}{3}x_2$.

Cancelling the $\frac{5}{3}$ gives $x_1 = x_2$.

f is onto

Let $b \in B$.

Then,

$b = 5k$

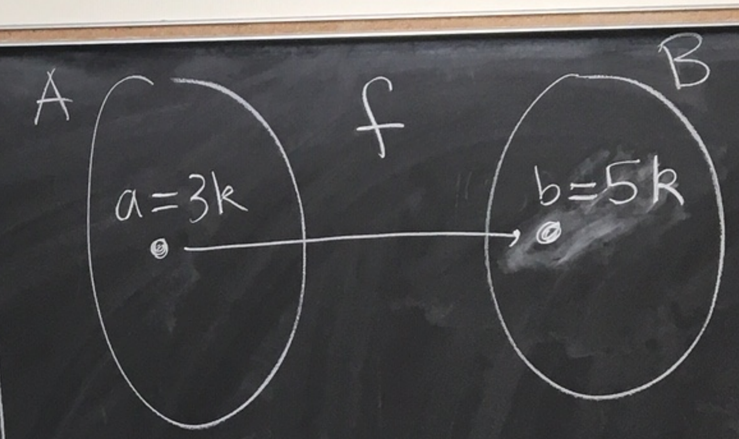
for some $k \in \mathbb{Z}$.

Consider $a = 3k$.

Then $a \in A$ and

$f(a) = f(3k) = \frac{5}{3}(3k) = 5k = b$.

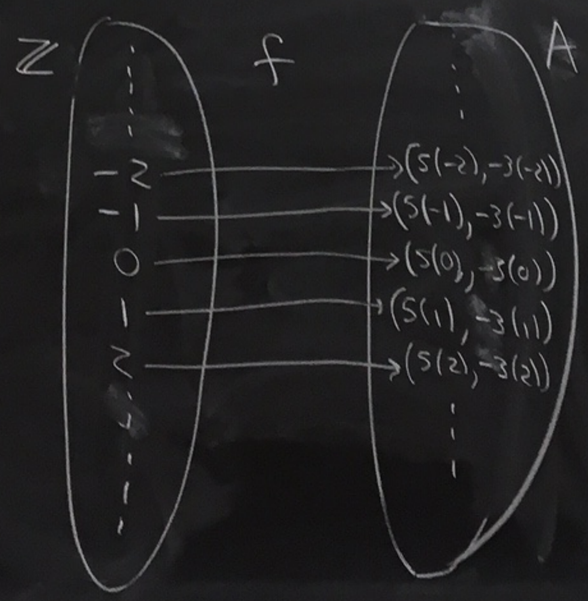
So, f is onto. ▨



14.2

(3) Prove that $A=\{(5n,-3n) \mid n\in\mathbb{Z}\}=\{\ldots(5(-2),-3(-2)),(5(-1),-3(-1)),(5(0),-3(0)),(5(1),-3(1)),\ldots\}$ $\quad (-10,6)\quad (-5,3)\quad (0,0)\quad (5,-3)$
is countably infinite.

Define $f:\mathbb{Z}\longrightarrow A$
by $f(n)=(5n,-3n)$



f is 1-1

Suppose $f(n_1)=f(n_2)$ where $n_1,n_2\in\mathbb{Z}$
Then $(5n_1,-3n_1)=(5n_2,-3n_2)$.

So, $5n_1=5n_2$ and $-3n_1=-3n_2$.
Dividing $5n_1=5n_2$ by 5 gives $n_1=n_2$.
So, f is 1-1.

f

Let

Then

And

f

So,

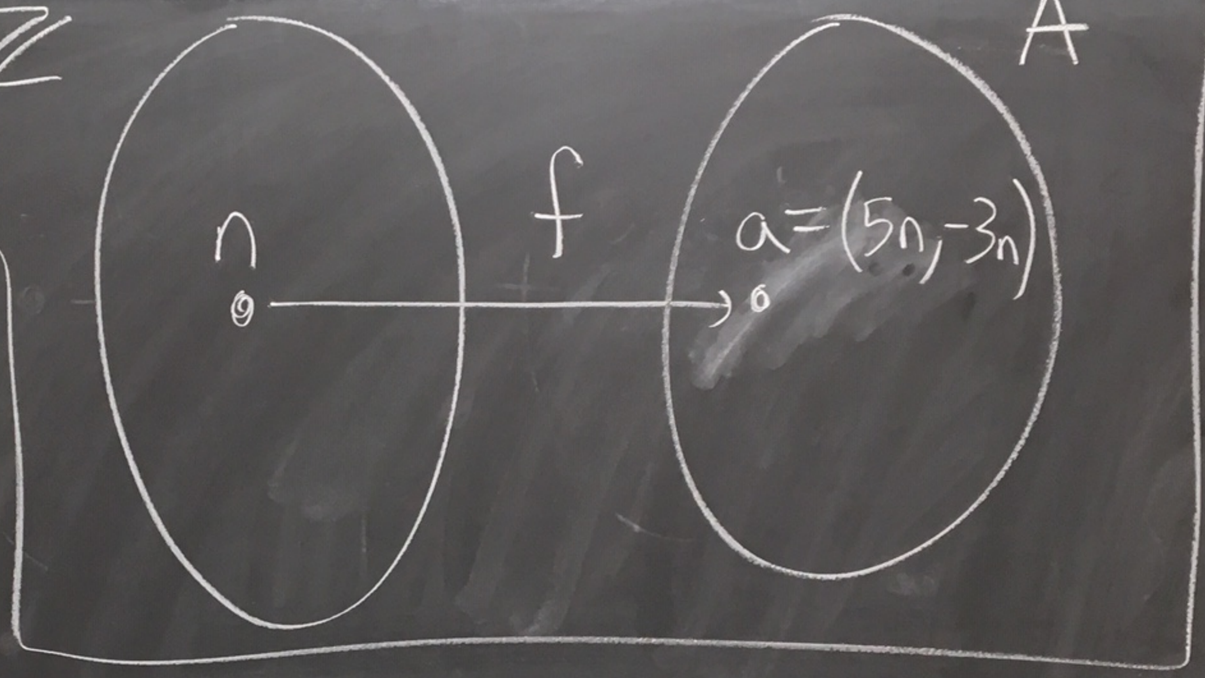
The

f is onto.

Let $a \in A$.
Then $a = (5n, -3n)$
for some $n \in \mathbb{Z}$.

And,
$f(n) = (5n, -3n) = a$.

So, f is onto.



Therefore, f is a bijection. So, $|\mathbb{Z}| = |A|$.

Thus, $|\mathbb{N}| = |\mathbb{Z}| = |A|$.

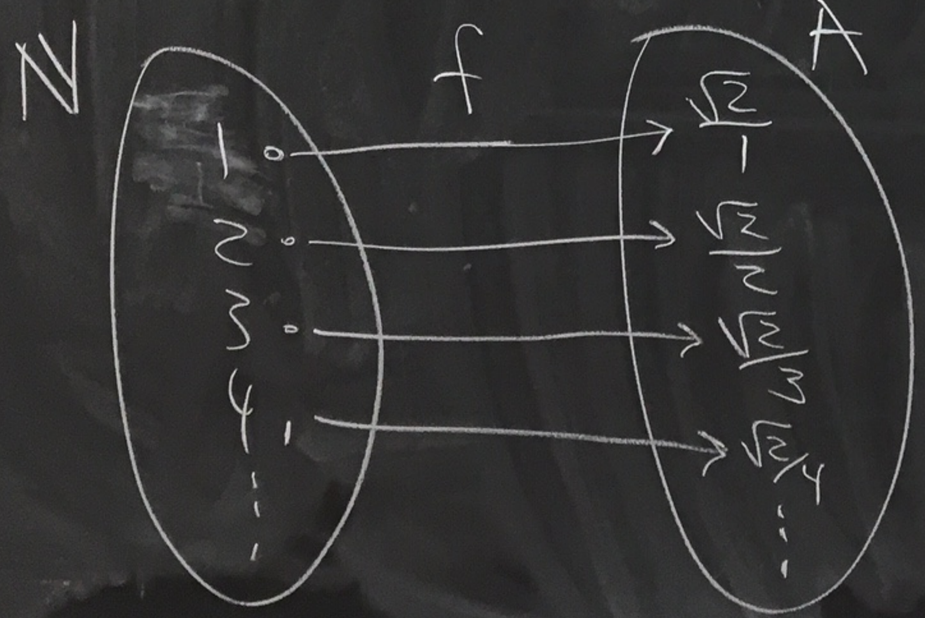
So, A is infinitely countable.

∎

14.2

(10) $A = \left\{ \frac{\sqrt{2}}{n} \mid n \in \mathbb{N} \right\} = \left\{ \frac{\sqrt{2}}{1}, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{3}, \frac{\sqrt{2}}{4}, \ldots \right\}$

Is A countably infinite?



Define $f: \mathbb{N} \to A$ by $f(n) = \frac{\sqrt{2}}{n}$

f is 1-1

Suppose $f(n_1)=f(n_2)$ where $n_1, n_2 \in \mathbb{N}$

Then, $\frac{\sqrt{2}}{n_1} = \frac{\sqrt{2}}{n_2}$.

So, $(\sqrt{2})n_2 = (\sqrt{2})n_1$

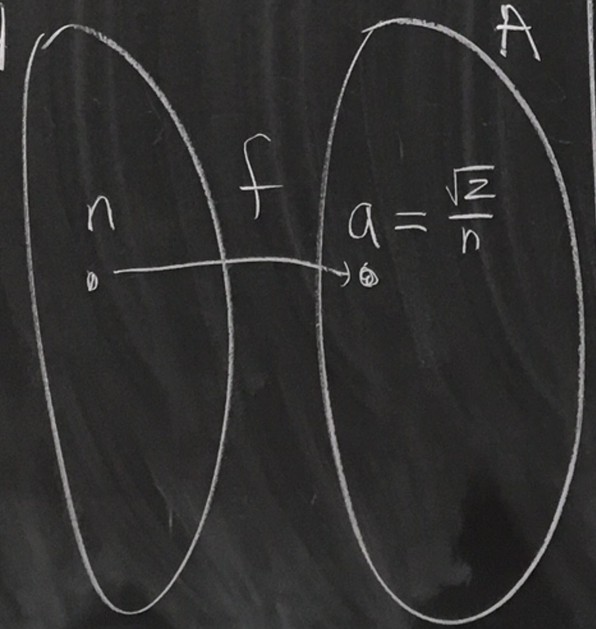
Thus, $n_2 = n_1$.

f is onto

Let $a \in A$

Then, $a = \frac{\sqrt{2}}{n}$ where $n \in \mathbb{N}$

And $f(n) = \frac{\sqrt{2}}{n} = a$.



So, f is a bijection.

Therefore, $|\mathbb{N}| = |A|$

And A is countably infinite