MAT 108

Winter 2021
LEFT BOARD

Elem → Adv math.

Reading and writing proofs.

Like essay – structure
 \ ideas

Eng is not precise enough.

So use predicate logic

And some set theory.

Def: A proposition is a sentence which is true (T) or false (F) (or has a truth value).

Examples:	Prop
$1+1=3$	Y it is F

	Prop?
① This sentence is not a prop.	Y F
② I am liar.	N paradox

(3) Lysol can kill viruses. 1Y

(1) If F then ~~the sent~~ is a prop. ✓
If T then not a prop x

(1) Call the sentence P:
If P is True then P is not a prop so not T or F] Is T
If P is False then P is a prop so either T or F]. Not F

Using steps from Thm 1.1.1:

$\sim P \wedge Q$

by (h) $\quad \sim(A \wedge B)$ is eq. $\sim A \vee \sim B$

(a) $\quad \sim(\sim A)$ is eq to A

$\sim P \wedge Q$ is eq to $\sim[\sim(\sim P \wedge Q)]$

(a)

which is eq to

(h) $\sim[\sim(\sim P) \vee \sim Q]$

which is eq to

(a) $\sim[P \vee \sim Q]$

210106

Building new props from old:

$\sim Q \qquad (\sim Q) \qquad$ same.

$Q \wedge (P \vee R)$

Truth tables

equivalent

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

Note: $P \Rightarrow Q$ and $\underbrace{(\sim Q) \Rightarrow (\sim P)}_{\text{the contrapositive.}}$ are equivalent, as is $\sim P \vee Q$

Eng Ex:

P: My dog is hungry.

Q: My dog is inside.

$P \Rightarrow Q$: If my dog is hungry then it is inside.

$Q \Rightarrow P$: If my dog is inside then it is hungry.

$\sim Q \Rightarrow \sim P$: If my dog is outside then it is full.

$\sim P \vee Q$: Either my dog is full or it is inside.

1, 3, 4 have the same meaning.

2 is different.

$\overline{210108}|$

Today quantifiers;
Complete. first order logic notation,

Ex:
Everyone I know likes chocolate

or dislikes coffee.

Rewriting this in logic:
$P(x)$ is x likes chocolate.

$Q(x)$ is x likes coffee.

Notation: A sentence like $P(x)$ is an <u>open sentence with variable x</u>.

The above becomes:

$$(\underbrace{\forall}_{\text{for all}} x \underbrace{\in}_{\text{in}} \underbrace{\{\text{people I know}\}}_{\text{the set of people I know.}})\, P(\underbrace{x}_{\text{person I know.}}) \vee \sim Q(x)$$

or: In the universe (of discourse)

{people I know}.

$(\forall x)\ P(x) \vee \sim Q(x)$

Everyone I know who likes chocolate also likes coffee.

equiv.

For everyone I know if they like chocolate then they ~~also~~ like coffee

$(\forall x \in \{\text{ppl I know}\})\ P(x) \Rightarrow Q(x)$

Compare $(\forall x \in \{\text{ppl I know with } P(x) \text{ true}\})$ $(Q(x))$.

(equivalent) ✓

Thm 1.3.1: If $P(x)$ is an open sentence then in any universe

ⓐ $\sim(\forall x)\, P(x)$ is eq. to $(\exists x) \sim P(x)$

ⓑ $\sim(\exists x)\, P(x)$ is eq to $(\forall x) \sim P(x)$

Check example:

$\sim(\forall x \in \{\text{ppl I know}\})(P(x) \vee \sim Q(x))$ eq by 1.3.1

$(\exists x \in \{\text{" "}\}) \sim(P(x) \vee \sim Q(x))$ eq by DeMorgan

$(\exists x \in \text{" "})(\sim P(x) \wedge Q(x))$

Def: The truth set in a universe $\mathcal{U}$ for an open sentence $P(x)$ is all x in $\mathcal{U}$ for which $P(x)$ is true

2/6/11

Proofs: See §1.7 pgs 64, 65, 66, 67

Examples:

Def: An integer $a \in \mathbb{Z}$ is <u>even</u> if there is an integer n with $a = 2n$.

$(\exists n \in \mathbb{Z})(a = 2n)$

An integer $a \in \mathbb{Z}$ is **odd** if $(\exists n \in \mathbb{Z})\ (a = 2n+1)$

Thm: If x is a real number with $x^2 \leq 1$ then $x^2 - 7x > -10$

Proof: Assume x is a real number with $x^2 \leq 1$.

Hence $x \leq |x| = \sqrt{x^2} \leq \sqrt{1} = 1 < 2$.

Hence $x < 5$.

Hence $(x-2) < 0$ and $(x-5) < 0$

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

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

There for $x^2 - 7x > -10$. q.e.d.

Approach: $x^2+6>5x$

$$(x-2)(x-3) = x^2-5x+6>0$$

$$\underbrace{x>3}_{\text{both pos}} \text{ or } \underbrace{x<2}_{\text{both neg}}$$

$$x<1$$

Proofs to grade: (bad example)

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

"Proof": Let a. ②

① Then by squaring an odd we get an odd.

③ An odd plus an odd is even.

So a^2+1 is even.

Problems: 1 why is this true?

2 This is not a sendence.

should be

Let a be an odd integer.

3 is also not clear.

210113 Proof Structures:

Recall: §1.7 64–67 should be reread.

From pg 67:

To start working out a proof consider:

Understand the statement

Logical form.

Assumptions and Conclusion.

Ideas

Step 9: Understand:

Try an example: eg $a=3$ and $b=6$ and $c=9$ claim is that 3 divides $6-9$
$= -3$

Logic: $P \wedge Q \implies R$

If... then...

P is a div b

Q is a div c

R is a div $b-c$

with quantifiers:

$(\forall a,b,c \in \mathbb{Z})$

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})$

Ass & Concl:

Ass: P, Q

a div b or $(\exists n)$ $n \cdot a = b$ Ass

a div c or $(\exists m)$ $m \cdot a = c$ Ass

Concl: R

a div b-c

Ideas: With a, b, c as above

have $b - c = n \cdot a - m \cdot a = \underbrace{(n-m)}_{\text{this is an integer.}} \cdot a$

last.

Contra position proof:

Claim: Assume ~~that~~ m is an integer
If m^2 is an odd integer
then m is an odd integer.

Proof: Assume m is an integer.

Assume m is even.

Hence $\exists t \in \mathbb{Z}$ with $2 \cdot t = m$.

Hence $2t^2$ is also an integer.

Hence $m^2 = (2t)^2 = 4t^2 = 2(2t^2)$.

Hence m^2 is even.

Therefore: If m^2 is odd then m is odd.

qed.

Example with cases and proof by contradiction:

Idea of proof by contradiction:

To prove P, assume $\sim P$ and show Q and $\sim Q$.

U: understand.

eg $a=1$ $\quad a^2-2=-1$ ✓

$a=2$ $\quad a^2-2=2$ ✓

$a=4$ $\quad a^2-2=14$ ✓

✓

L: Logic:

Right now: $(\forall a)\ P$

Plan: $(\forall a)\ \underbrace{\sim P \Rightarrow (Q \wedge \sim Q)}$

(to see these are equivalent:

$P \vee \underbrace{(Q \wedge \sim Q)}$ or P

contrapositive

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

eq. ~~or~~ $\underbrace{\sim Q \vee Q}_{T} \Rightarrow P$

Ass: $\sim P$

Concl: Q and $\sim Q$

Ideas: $\sim P$ is $(4$ divides $a^2-2)$

or $(\exists t)$ with $4t = a^2-2$

Cases: e a is even

(b) a is odd

even: $a = 2s$ so $4t = (2s)^2 - 2 = 4s^2 - 2$

so $2t = 2s^2 - 1$

or $1 = 2s^2 - 2t = 2(s^2 - t)$

Q: 1 is even.

$\sim Q$ is clearly true.

Need to show Q

210115 Mon. No Lect.
HW due Wed.

Recall: Claim 1: If a is an integer and a^2 is even then a is even.
Pf: Earlier.

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

Proof: Note that 1 is not even.

Assume a is an integer and 4 divides a^2-2

Hence there is an int t with $4t = a^2-2$

Hence $a^2 = 2(2t-1)$ so $2t-1$ is an integ.

so a^2 is even

and by Claim 1 a is even.

Hence there is an integr s with $a=2s$

and s^2-t is an integer.

Hence $4t = (2s)^2-2$ so $1 = 2(s^2-t)$ is even.

Therefore 1 is even and 1 is not even

which is a contradiction. qed.

$\cancel{A}$: ~Q or p is even so $p = 2s$
~R or q is even or $q = 2 \cdot k$ ①

Concl: ~P or q is not the smallest possible denominator.

I: $a = \frac{p}{q} = \frac{2s}{2k} = \frac{s}{k}$ ②

and $k < q$ and hence a smaller denom. so ~P. ✓

Proof: Assume $a = \frac{p}{q}$ with p and q both even integers.

Hence there are integers s and k with $p = 2s$, $q = 2k$ so $a = \frac{p}{q} = \frac{2s}{2k} = \frac{s}{k}$

Therefore q is not the smallest possible denominator. qed.

U: eg $1^2+15=16$

$8\cdot 1 = 8$ $\quad 16 \not< 8$ oops.

maybe search else

L: $(\exists n \in \mathbb{Z})\ (n^2+15 < 8n)$.

A: No ass. want

Concl: $n^2+15<8n$

I: $n^2+15-8n<0$

or $(n-5)(n-3)<0$

need $\overline{n-5}$ & $n-3$ to have different signs,

so take $n=4$

2/01/20

Pythagorean's Thm

Thm: $\sqrt{2}$ is irrational.

Plan Proof:

U: try $\left(\frac{7}{5}\right)^2 = 1.96$

$\left(\frac{10}{7}\right)^2 = 2.040816\ldots$

L: $\sim P$

P is $\sqrt{2}$ is rational

or (contradiction approach)

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

Ass: $\sim P$ $\sqrt{2} = \frac{p}{q}$

Concl: Q and $\sim Q$.

Still have not had to choose Q.

I: If $\sqrt{2} = \frac{p}{q}$. ③

Recall: If q is as small as possible ① Recall

Tidy.

p is odd or q is odd.

Compute $2 = \frac{p^2}{q^2}$ or $2q^2 = p^2$ ④

so p^2 is even also showed before this ② Recall.

means: p even. $\Rightarrow$ q is odd.

and (4) $p = 2k$ and $q = 2m+1$ (5)

Proof: Note that 1 is not even.

Say that if a is rational, $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $a = \frac{p}{q}$ and q as small as possible then $a = \frac{p}{q}$ is in reduced form.

Recall we proved last time that if $a = \frac{p}{q}$, is a rat. number in reduced form then p or q is odd,

Recall we proved before that if n is an int. and n^2 is even then n is even,

For contradiction assume $\sqrt{2}$ is rational and $\sqrt{2} = \frac{p}{q}$ is in reduced form.

Hence $2 = \frac{p^2}{q^2}$ so $2q^2 = p^2$ so p^2 is even so p is even so $p = 2k$ for some int. k.

Hence q must be odd so $q = 2m+1$ for some int. m.

Hence $k^2 - 2m^2 - 2m$ is an integer and

$4k^2 = (2k)^2 = p^2 = 2q^2 = 2(2m+1)^2 = 8m^2 + 8m + 2$

Hence $2[k^2 - 2m^2 - 2m] = 1$ and 1 is even.

Therefore 1 is even and 1 is not even a contradiction

so $\sqrt{2}$ is irrational.

good

Recall $(\exists!\, x)(P(x))$

is equiv to:

$$\underbrace{(\exists x)(P(x))}_{\text{find an example.}} \wedge (\forall u, v)\left[(P(u) \wedge P(v)) \Rightarrow (u = v)\right]$$

Ans:

A ③ has more than 1] false

(4) $(x-2)^2=0$ true

(5) $\dfrac{4 \pm \sqrt{-4}}{2}$ not $\mathbb{R}$ false

no answers

(c) (3) Find a different example and done.

(4) Example for $\exists$

More work for $\forall$.

Claim: $(\exists!\, x \in \mathbb{R})\ x^2 - 4x + 4 = 0$.

Proof: First show $(\exists x \in \mathbb{R})\ x^2 - 4x + 4 = 0$

by taking $x = 2$ so $2^2 - 4 \cdot 2 + 4 = 0$ ✓.

Uniqueness: Assume $u^2 - 4u + 4 = 0$

and $v^2 - 4v + 4 = 0$.

Hence $(u-2)^2 = 0$ and $(v-2)^2 = 0$

so $u - 2 = 0$ and $v - 2 = 0$

so $u = 2$ and $v = 2$ so $u = v$.

∎

If P then Q.

or

$$P \Rightarrow Q$$

By contr. eq.

$$[\sim (P \Rightarrow Q)] \Rightarrow (R \wedge \sim R)$$

~~Possibly can choose $R = Q$~~

eq: $[\sim(\sim P \vee Q)] \Rightarrow (R \wedge \sim R)$

eg: $(P \land \sim Q) \Rightarrow (R \land \sim R)$

~~eg:~~ $\cancel{(P \land \sim Q) \Rightarrow (Q \land \sim Q)}$

~~eg:~~ $\cancel{P \land \sim Q \Rightarrow Q}$

or maybe choose $R = P$

$$(P \land \sim Q) \Rightarrow (P \land \sim P)$$

or $P \land \sim Q \Rightarrow \sim P$

enough to show $\sim Q \Rightarrow \sim P$

210122 §1.8 Number Theory (for proofs).

Next week Set Theory (" ").

Recall: If a and b are integers then a divides b iff there is an integer c with $a \cdot c = b$.

If p is an integer then p is prime iff the only positive integers dividing p are 1 and p.

Def (pg77): If a, b and d are nonzero integers

then $\gcd(a,b) = d$ iff

(i) d divides both a and b
(say d is a common divisor of a and b)

(ii) every common divisor of a and b
is at most d.

In first order logic:

$(\forall a, b, d \in \mathbb{Z}_{\neq 0})\ [\gcd(a,b) = d] \iff$

$$\underbrace{\left[(\exists s,t\in\mathbb{Z})\ (d\cdot s=a)\wedge(d\cdot t=b)\right]}_{d\ \text{is a common div.}} \wedge \left[(\forall e\in\mathbb{Z})\underbrace{\left[(\exists u,v\in\mathbb{Z})\ (e\cdot u=a)\wedge(e\cdot v=b)\right]}_{e\ \text{is a common div of}\ a\ \&\ b}\Longrightarrow(e\le d)\right]$$

Brk Rm: Translate lcm def. into logic.

Claims:

ⓐ $(\forall a \in \overbrace{\mathbb{N}_{\geq 10}}^{\{10,11,12,\dots\}})(\exists b \in \mathbb{N})\ (\gcd(a,b)=1) \wedge (a \leq b)$

ⓑ $(\exists a \in \mathbb{N}_{\geq 10})(\forall b \in \mathbb{N})\ (\gcd(a,b)=1) \vee (a \leq b)$

Proof sketch for a:

Assume $a \geq 10$ is an integer.

Choose $b = a+1$.

Note that 1 and -1 are the only divisors of 1.

Assume that d is a common div. of a

and $b = a+1$.

Hence there are integers s and t.

with $d \cdot t = a+1$ and $d \cdot s = a$

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

so d is 1 or -1.

Hence $(a, b) = 1$.

qed.

2/10/25 More number theory from §1.8.

Division and Euclid's Alg.

Def: If a, b, x, y, n are integers and $n = a \cdot x + b \cdot y$ then n is a <u>linear combination</u> of a and b

Thm 1.8.1 (Prove later by induction)

If a and b are nonzero integers, then $\gcd(a,b)$ is equal to the smallest positive linear combin. of a and b.

Thm 2.5.1 (Division Alg).
If a and b are nonzero integers, there is a unique pair of integers q and r with

$$b = a \cdot q + r$$

and $0 \le r < |a|$.

Notation for Euclid's Alg:

$$b = a \cdot q_1 + r_1$$

$$a = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

$$\vdots$$

$$r_{k-2} = r_{k-1} \cdot q_k + r_k$$

$$r_{k-1} = r_k \cdot q_{k+1}$$

Thm: 1.8.2: If $b \geq a > 0$ are integers then $\gcd(a,b) = r_k$ from Euclid's algorithm.

Brk. Rm: Apply Euclid's Alg to

$$b = 256 \geq a = 81 > 0$$

Find $r_k = 1$ and k, and the q_i's.

$k = 3$ $\qquad$ $r_1 = 13$ $\quad$ $r_2 = 3$ $\quad$ $r_3 = 1$

Claim: (1.8.3):

If a, b and p are integers with p prime and p divides ab then p divides a or p divides b.

Proof: Assume a, b and p are integers with p prime, p dividing ab but not a. Hence the only pos. divisors of p are 1 and p so $\gcd(p, a) = 1$. Hence by Thm 1.8.1 there are integers x and y with $1 = x \cdot p + y \cdot a$.

210127

Also there is an int. n with

$ab = np$ and $b = b \cdot x \cdot p + y \cdot a \cdot b$

so $b = b \cdot x \cdot p + y \cdot n \cdot p$

$= [bx + yn] \cdot p$ and $bx+yn$ is an integer.

Therefore p divides b. q.e.d.

Set Notation examples:

$\{3, 4, 5, 6\} = \{x \in \mathbb{Z} \mid x \geq 3, \ x \leq 6\}$

$= \{ \text{" "} : \text{"} \quad \text{"} \}$

$= \{x \mid x \in \mathbb{Z},\ 3 \le x \le 6\}$

has 4 elements.

Write $3 \in \{3, 4, 5, 6\}$

is an element of

$2 \notin$ " "

is not " " .

$\{3, 4\} \subseteq \{3, 4, 5, 6\}$

is a subset of

$\{3\} \not\in \{3, 4, 5, 6\}$

$3 \notin \{3, 4, 5, 6\}$

$\{3\} \in \{\{3\}, \{1,5,6\}\}$ has 2 elts

Power sets:

$\mathcal{P}(\{2,3\}) = \{\underbrace{\{\}}_{=\ \phi}, \{2\}, \{3\}, \{2,3\}\}$

The set of subsets.

ϕ = the empty set

Which are true:

$\exists$ A, B, C sets with

0. $B \boxed{\subsetneq} A$, $B \subseteq C$, ~~and~~ $A \not\subseteq C$ and $C \not\subseteq A$

True

subset but not equal to] proper subset.

1. True $A \subseteq B$, $B \not\subseteq C$, $A \subseteq C$

2. $A \subseteq B$, $B \subseteq C$, $C \subseteq A$

True

$A=B=C$

3. $A \subsetneq B$, $B \subsetneq C$, $C \subsetneq A$

False

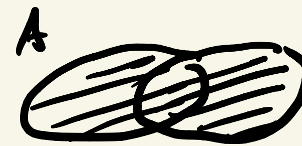
4. $B \subseteq A$, $B \not\subseteq C$, $A \subseteq C$

False

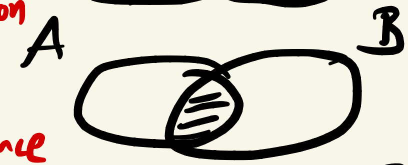
210129 | Set operations.

Related to operations on predicates.

Notation: If A and B are sets write



① $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$ union



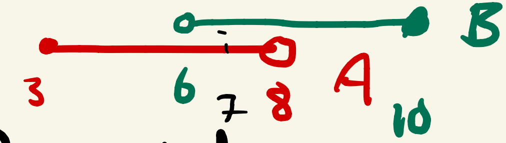
② $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$ intersection

③ $A - B = \{x \mid (x \in A) \wedge (x \notin B)\}$ difference

If A is a subset of a universe U write:

④ $A^c = U - A$ complement

$= \{x \in U \mid x \notin A\}$



Example: $A = [3, 8) \subseteq \mathbb{R} = U$

$B = (6, 10] \subseteq \mathbb{R}$

Find
1. $A \cup B$
2. $A \cap B$
3. $A - B$
4. A^c
5. $A \cap B^c$

Ans:
1. $[3, 10]$
2. $(6, 8)$
3. $[3, 6]$
4. $(-\infty, 3) \cup [8, \infty)$
5. this just $A - B$ which is $[3, 6]$.

Dictionary: If $P(x)$ and $Q(x)$ are open propositions with variable x in $\mathcal{U}$ (a universe)

take $A = \text{Truth}(P) = \{x \in \mathcal{U} \mid P(x) \text{ (is true)}\}$

$B = \text{Truth}(Q) = \{x \in \mathcal{U} \mid Q(x) \text{ (is true)}\}$,

---

$\text{Truth}(P \wedge Q) = A \cap B$

$\text{Truth}(P \vee Q) = A \cup B$

$\text{Truth}(\sim P) = A^c$

$\text{Truth}(P \wedge \sim Q) = A - B$

Truth $(P \Rightarrow Q)$ $=$ $A^c \cup B$

$= (A - B)^c$

Truth Table simln. Venn Daiagram

210201 More set notation:

Products then Families:

Def: If A and B are sets then

$$\underbrace{A \times B}_{\text{the product set}} = \{(a,b) \mid a \in A \text{ and } b \in B\}.$$

Ex: $\{1,2\} \times \{2,3\} = \{(1,2), (1,3), (2,2), (2,3)\}$

Ex: Which one is true?

Prove one and find a counterexample.

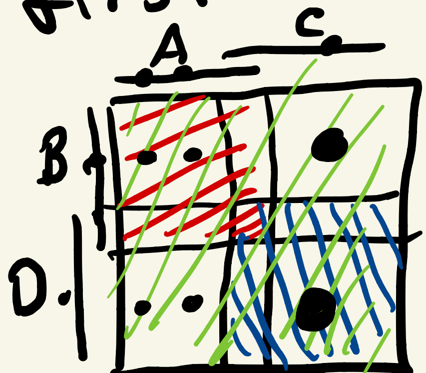
for the other.

$(\forall A, B, C, D \text{ sets})\ (A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

" " " $\supseteq$ " ".

Ans: The first is true.

$\mathcal{U}$:



$A \times B$

$C \times D$

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

For a counterexample to $\supseteq$

L: If $\underbrace{(x,y) \in (A \times B)}_{P}$ or $\underbrace{(x,y) \in (C \times D)}_{Q}$ then $\underbrace{(x,y) \in (A \cup C) \times (B \cup D)}_{R}$.

C: Assume: P and conclude R.
and Assm Q and conclud R.

Sets or families or collections of sets.

Ex: 1 $\mathbb{Q} = \{\underbrace{\{1,2,3\}}_{A_a}, \underbrace{\{2,3,4\}}_{A_b}, \underbrace{\{3,4,5\}}_{A_c}\} = \{A_\alpha \mid \alpha \in \Delta\}$

$\Delta = \{a, b, c\}$] indexing set.

② $\mathcal{B} = \{ [x, x+3] \mid 0 \leq x < 2 \}$

$= \{ B_\alpha \mid \alpha \in \Delta \}$

if $B_\alpha = [\alpha, \alpha+3]$

and $\Delta = [0, 2)$] indexing set

Ex ①

$$\bigcap_{A \in \mathcal{Q}} A = \bigcap_{\alpha \in \{a,b,c\}} A = \{3\}$$

②

$$\bigcap_{B \in \mathcal{B}} B = \bigcap_{\alpha \in [0,2)} B_\alpha = [2,3]$$

210203 Last proof technique: Induction

Example:

Claim: For every $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$ it is true that
$$n^2 = 1 + 3 + 5 + \cdots + (2n-1)$$

Proof: Check the base case of $n=1$ which is $1^2 = 1$ which is true.

Assume for induction that

$n^2 = 1+3+5+ \cdots + (2n-1)$.

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

$= [1+3+ \cdots + (2n-1)] + [2n+1]$

$= 1+3 \cdots\cdots\cdots + [2(n+1)-1]$.

Therefore by PMI the claim holds.

qed.

principle of mathematical induction

could add [since $2n+1$ is the odd number following $2n-1$.

Proof Plan:

U: $n=1$ $\quad 1+3 < 5\cdot 1$ ✓

$n=3$ $\quad 3+3 < 5\cdot 9$ ✓

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

use induction.

C: • Prove $P(1)$ (base case).

• Assume $P(n)$] inductio

Show $P(n+1)$ ↓ step:

I: base case $n=1$ see above

ind. step:

Assume: $n+3 < 5n^2$

Check: $(n+1)+3 = (n+3)+1 < 5n^2+1$

$5n^2+1 < 5n^2+10n+5 = 5(n+1)^2$

Generalized Prin. of Math. Ind:

Show $(\forall n \in \mathbb{N})$ $P(n)$.

by:

- Show $P(1)$ (base case).
- Assume for every $n \leq m$ have $P(n)$.

  Show $P(m+1)$.

Example:

Claim: $\sqrt{2}$ is irrational.

$\frac{a}{1}$ $\times$

$\frac{a}{2}$ $\cdots\cdots$ $\frac{r}{1}$ $\times$

$\frac{a}{3}$ $\cdots\cdots$ $\times$ $\times$

$\frac{a}{4}$ $\cdots\cdots$ $\frac{r}{2}$

$\frac{3}{2} = 6$

$\frac{4}{4} = \sqrt{2}$

210205 Miderm next Wednesday:
On web is an old exam,
Covers Ch 1 & Ch 2 (except 2.6).

More induction proofs:

Def: (Fibonacci numbers):
Inductive definition:
$$f_1 = 1, \ f_2 = 1 \text{ and } f_{n+2} = f_{n+1} + f_n$$
if $n > 0$.

Ex: $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, $f_7 = 13$ ...

Claim 1: If f_n are the Fibonacci numbers then for every $n \geq 1$ have $\gcd(f_n, f_{n+1}) = 1$

Claim 2 If f_n are the Fibonacci numbers then for every $n \geq 1$ have that 3 divides f_{4n}.

$\stackrel{?}{=}$ follows from: $\boxed{\gcd(b,a) \stackrel{?}{=} \gcd(b-a,a)}$

$\gcd(b,a)$: $b = f_{n+1}+f_n$, $a = f_{n+1}$

Call This a Lemma and prove it.

Focus on the Lemma:

1 Check: $\{d \mid d|b \text{ and } d|a\}$
$= \{e \mid e|b-a \text{ and } e|a\}$.

check: $\subseteq$: If $d|b$ and $d|a$
want to show $d|b-a$ and $d|a$,
but if $b = sd$ and $a = td$
then $b-a = sd - td = (s-t)d$.

So $d \mid b-a$ ✓.

$\supseteq$: similar.

Claim: If f_n are the Fibonacci numbers then for every natural number n we have
$\gcd(f_n, f_{n+1}) = 1$.

Proof: Use the following Lemma:

Lemma: If $b \geq a > 0$ then $\gcd(b,a) = \gcd(b-a, a)$.

Proof of Lemma: It suffices to show that that b and a have the same common divisors as $b-a$ and a.

If d divides b and a then $b = sd$ and $a = td$ so $b - a = (s-t)d$.

If d divides $b-a$ and a then $b-a = ud$ and $a = vd$ so $b = (b-a)+a = (u+v)d$.

hence the lemma holds.

Prove the claim by induction.

For the $n=1$ base case need $\gcd(1,1)=1$ which is true.

For induction assume $\gcd(f_n, f_{n+1}) = 1$

Hence $\gcd(f_{n+2}, f_{n+1}) = \gcd(f_{n+1}+f_n, f_{n+1})$.

Hence by the lemma $\gcd(f_{n+2}, f_{n+1}) = \gcd(f_n, f_{n+1})$

which is 1 by the ind. hyp.
qed.

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

Proof: For induction consider the base case $n=1$ which is $f_4 = 3$ is div. by 3.

For ind. assume f_{4n} is div. by 3.

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

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

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

which is divisible by 3 since f_{4n} is.

Therefore by PMI. the claim holds.

End.

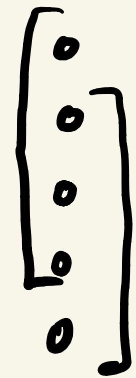
$f_{4n} = 3 \cdot s$ ~~so~~

$f_{4(n+1)} = 3 \cdot f_{4n+1} + 2 \cdot 3 \cdot s = 3\left[f_{4n+1} + 2 \cdot s\right]$

Horses are all the same color:

case 1

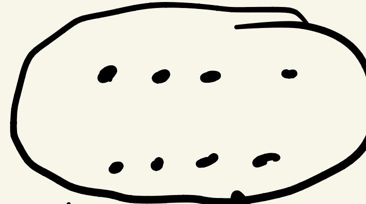
color.



same color

Problem!
The induction proof is wrong for case $n+1=2$

Example: Nim:



move: remove any number of coins from one pile.

Start with 2 equal piles;

2^{nd} player has a winning strategy.

win: take last coin.

Proof: by Gen. ind:

Base case: one coin in each pile

For ind. assume there is a winning 2nd plyr strat. for any number of coins at most n in 2 equal piles —

Show: if there are 2 piles with n+1 each. then after plyr takes r from one pile. The second can take r from both and by the ind. hyp. there is a winning strat. for 2 piles of $(n+1-r)$, G Ind: Assume $\forall k \leq n$ have $P(k)$.

Prove $P(n+1)$

210208 | Wednesday; Midterm

1 sheet notes, (both sides).

Chapt 1, 2 (except 2.6).

Regular zoom location.

Instructions up this afternoon,

Cameras: Point at your work

Try out during quiz tomorrow.

Uploading similar to Homework

Arrive ~10 min early to check ID...

Exam: Both on screen
and vice chat box link.

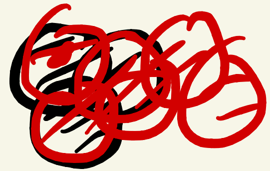
50 min exam.
Old exam and practice exam on
web page. (answers today).

Upload <u>after</u> 50 min.

gcd proofs set proofs. families proofs.	induction.

Proof sketch:

Und:



$\bigcup_{\alpha\in\Gamma} A_\alpha$ $\qquad$ $\bigcup_{\alpha\in\Delta} A_\alpha$

Logic: $\left(a \in \bigcup_{\alpha\in\Gamma} A_\alpha\right) \Rightarrow \left(a \in \bigcup_{\alpha\in\Delta} A_\alpha\right)$.

Ass/Ccld: Assume $a \in \bigcup_{\alpha\in\Gamma} A_\alpha$

or $(\exists \alpha\in\Gamma)(a\in A_\alpha)$.

$\bigcup_{\alpha\in\Delta} \leftrightarrow \exists\alpha$

$\bigcap \leftrightarrow \forall\alpha$

$\alpha\in\Delta$

Concl: $a \in \bigcup_{\alpha\in\Delta} A_\alpha$

or $(\exists \alpha\in\Delta)\ (a\in A_\alpha)$.

Ideas: If $\alpha\in\Gamma$ and $a\in A_\alpha$

then since $\Gamma\subseteq\Delta$ also $\alpha\in\Delta$.

as needed.

Proof sketch:

Und: eg $m=5, \quad n=13$

$$13 = \underbrace{2}_{q} \cdot 5 + \underbrace{3}_{r}$$

Logic: Want $\exists!$

which requires: ① $\exists r, q$ with ...

② ceng 2 solns are the same (!)

$$\underbrace{(\forall n \in \mathbb{N})\ (\forall m,\ 0 < m \leq n)\ (\exists!\ q, r)\ [(n = q \cdot m + r) \wedge (0 \leq r < m)]}_{P(n)}$$

Might use induction: $[\forall n \in \mathbb{N}]\ P(n)$

Ass/Concl: Assume $\underbrace{P(m) \text{ for every } m < n}_{\text{Generalized induction}}$

Conclude $P(n)$.

Ideas: Uniqueness :

Assume there are two solns

Show the same:

$$n = q \cdot m + r \qquad 0 \le r < m$$

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

Hence: $0 = n - n = q \cdot m + r - \tilde{q} \cdot m - \tilde{r}$

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

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

Also $-m < \tilde{r} - r < m$

so

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

$-m < m \cdot s < m$

$-1 < s < 1$

Hence $\tilde{r} - r = 0$ so $\tilde{r} = r$.

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

so $0 = q - \tilde{q}$ so $q = \tilde{q}$.

210212 Set Theory and the rest of math!

300 BC on (Euclid). Geometry as foundation.

1800's shift to set theory.

Next:

$$
\begin{tikzcd}
 & \text{Relations } 3.1 \arrow[r] \arrow[d] & \text{functions } 4 \\
\text{Set Products. } (2.2) \arrow[ur] & \text{Equivalences } 3.2 \arrow[r] & \text{Modular Arithmetic, Related to gcd. } 3.4
\end{tikzcd}
$$

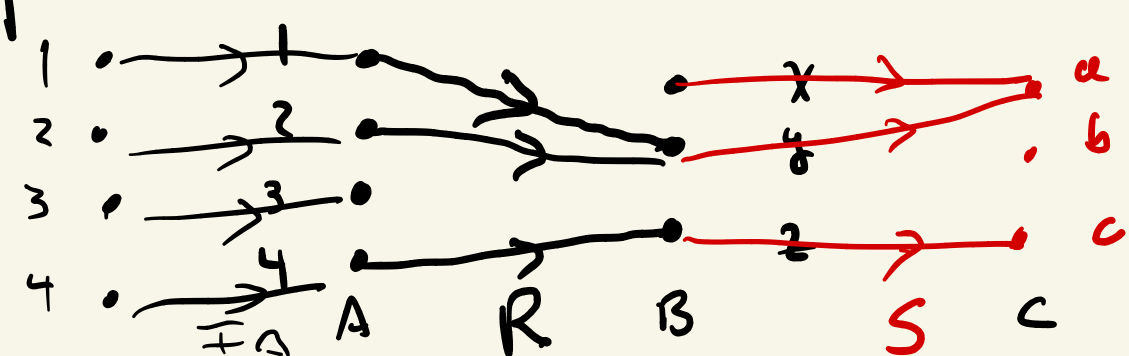
Example: $A = \{1, 2, 3, 4\}$

$B = \{x, y, z\}$,

$R = \{(1,y), (2,y), (4,z)\}$ just one example

eg: $2 R y$ and $2 \not{R} x$

Digraph associated to R (like truth table or venn diag)



eg: $\mathrm{Dom}(R) = \{1, 2, 4\}$

$\mathrm{Rng}(R) = \{y, z\}$

Ex: $I_{\{1,2,3,4\}} = \{(1,1), (2,2), (3,3), (4,4)\}$

with digraph:

$$
\begin{array}{ccc}
1 \bullet & \longrightarrow & \bullet\ 1 \\
2 \bullet & \longrightarrow & \bullet\ 2 \\
3 \bullet & \longrightarrow & \bullet\ 3 \\
4 \bullet & \longrightarrow & \bullet\ 4
\end{array}
$$

$R^{-1} = \{(y, 1), (y, 2), (z, 4)\}$

Ex: R as above and S a reln. from B to $C = \{a, b, c\}$.

eg $S = \{(x, a), (y, a), (z, c)\}$

then $S \circ R = \{(2, a), (1, a), (4, c)\}$

Claim: If A and B are sets and R is a relation from A to B then $I_B \circ R = R$. Here I_B is the identity relation on B.

Proof: Assume $(a,b) \in I_B \circ R$.

Hence there is $\tilde{b} \in B$ with $a R \tilde{b}$ and $\tilde{b} \, I_B \, b$. Hence $b = \tilde{b}$ and $a R b$.

Hence $(a,b) \in R$.

Assume $(a,b) \in R$. Hence if $\tilde{b} = b$ then $a R \tilde{b}$ and $\tilde{b} \, I_B \, b$ so $(a,b) \in I_B \circ R$.

qed

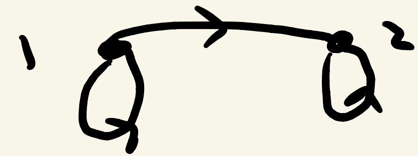
210217 Equivalence Relations.

Recall: A <u>relation</u> from A to B is a subset $R \subseteq A \times B$.

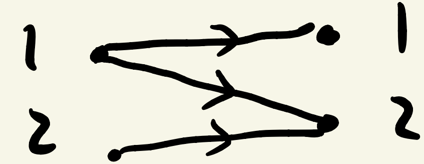
Example: $I_A = \{(x,x) \mid x \in A\}$

directed graphs

Ex: $R = \{(1,1), (1,2), (2,2)\}$



for a relation on $\{1,2\}$.

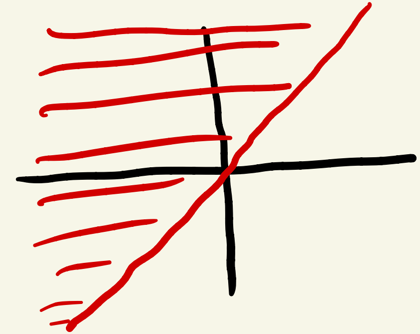


same relnR

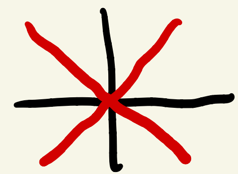
Ex: Relations on $\mathbb{R}$ = real numbers.

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

$$U = \{(x,y) \mid x \leq y\} \quad \longleftrightarrow$$



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



Sketch:

Logic: $R = \{(x,y) \mid xRy\}$.

$R^{-1} = \{(x,y) \mid yRx\}$,

$\mathrm{Dom}(R^{-1})$ and $\mathrm{Rng}(R)$ are sets so $\subseteq$ are $\supseteq$.

try together:

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

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

$$\|$$

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

Properties of some relations:

Def: If R is a relation on a set A.

① R is reflexive if $(\forall x \in A)$ xRx

② R is symmetric if $(\forall x, y \in A)$ $xRy \Rightarrow yRx$

③ R is transitive if $(\forall x, y, z \in A)$

$$(xRy) \wedge (yRz) \Rightarrow xRz$$

④ R is an equivalence relation if it is reflexive, symmetric and transitive.

Claim: A relation R on A is symmetric iff $R = R^{-1}$.

$\boxed{210219}$ Proof: Assume R is a symmetric relation on A and $(a,b) \in R$. Hence aRb so bRa by symmetry of R so $aR^{-1}b$ so $(a,b) \in R^{-1}$.

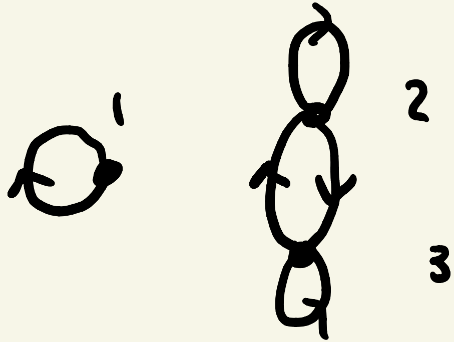
Therefore $R \subseteq R^{-1}$.

Assume R is sym on A and $(a,b) \in R^{-1}$.

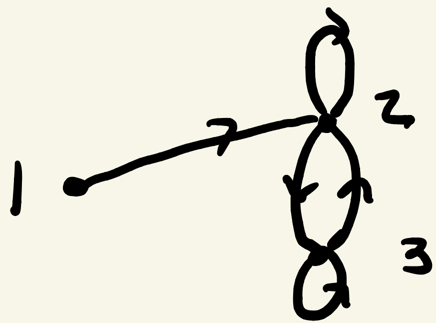
Hence $aR^{-1}b$ so bRa so aRb
so $(a,b) \in R$. Therefore $R^{-1} = R$.

For $\Leftarrow$ assume $R = R^{-1}$ and
aRb. Hence $(a,b) \in R = R^{-1}$ so
$(a,b) \in R^{-1}$ so $aR^{-1}b$ so bRa.
Therefore R is symmetric. q.e.d.

Examples:

$R =$  a relation on $A = \{1,2,3\}$

(equiv)

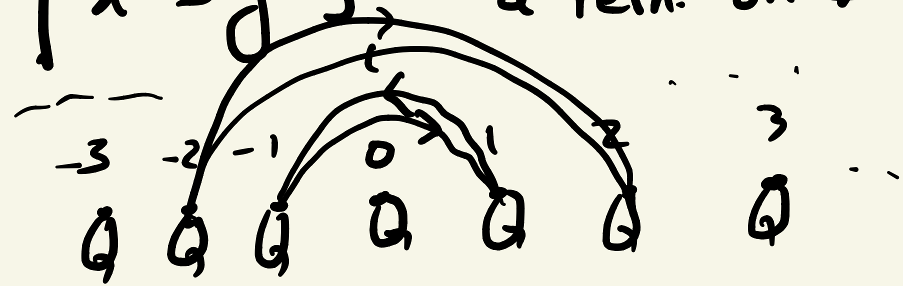
$S =$  " "

(not equiv)

$$A/R = \Big\{ \underset{\overline{1}}{\underset{\shortparallel}{\{1\}}},\ \ \{\underset{\overline{2}}{\underset{\shortparallel}{2}}, \underset{\overline{3}}{\underset{\shortparallel}{3}}\} \Big\}$$

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

$$V = \{ (x,y) \in \mathbb{Z}^2 \mid x^2 = y^2 \}$$ a reln. on $\mathbb{Z}$.



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

$$\{0\} = \overline{0}, \quad \{1,-1\} = \overline{1} = \overline{-1}, \quad \{2,-2\} = \overline{2} = \overline{-2}$$

$$= \{ \{n,-n\} \mid n \in \mathbb{Z} \}$$

$$= \{\{0\}\} \cup \{\{n,-n\} \mid n \in \mathbb{N}\}$$

$$U = \{(x,y) \in \mathbb{Z}^2 \mid 3 \text{ divides } x-y\}$$

a reln on $\mathbb{Z}$

$$\mathbb{Z}/U = \Big\{ \underbrace{\{3,0,6,9,12,-3\ldots\}}_{=\,\overline{-3}\,=\,\overline{3}\,=\,\overline{0}\,=\,\overline{6}},\ \underbrace{\{1,4,7,10,-2,-5,\ldots\}}_{=\,\overline{1}\,=\,\overline{4}\,=\,\overline{-2}},\ \underbrace{\{2,5,8,-1,-4,\ldots\}}_{=\,\overline{2}\,=\,\overline{-1}\,=\,\overline{5}\,=\,\ldots} \Big\}$$

$3U3$

$3U0$

$3U6$

$3U9$

$3U-3$ ⋮

$$\mathbb{Z}/\mathcal{U} = \{\bar{0}, \bar{1}, \bar{2}\}$$

$$= \{\{3n \mid n \in \mathbb{Z}\}, \{3n+1 \mid n \in \mathbb{Z}\}, \{3n+2 \mid n \in \mathbb{Z}\}\}.$$

$$= \{\{3n+s \mid n \in \mathbb{Z}\} \mid s \in \{0,1,2\}\}.$$

Note: $\mathcal{U}$ and V are both equiv. relns.

Proof sketch:

Uni: See above examples.

Logic: ~~If~~ (R is eq.) $\Longrightarrow$ (A/R a part).

$(P_{refl} \wedge P_{sym} \wedge P_{trans}) \Longrightarrow (Q_1 \wedge Q_2 \wedge Q_3)$

$P_{refl}, P_{sym}, P_{trans}$ $\quad$ Q_i, Q_{ii}, Q_{iii}

I: Q_i: $\emptyset \overset{?}{\notin} A/R$.

if $\bar{x} \in A/R$ then: need $\bar{x} \neq \emptyset$.

but xRx since R refl.

so $x \in \bar{x} \neq \emptyset$.

Qiii: If $x \in A$ then

$x \in \bigcup_{\bar{y} \in F} \bar{y}$ since $x \in \bar{x}$ ✓

Qii: $\forall$ $\bar{x}, \bar{y} \in A/R$ have $(\bar{x} = \bar{y}) \vee (\bar{x} \cap \bar{y} = \phi)$

equiv: $(\bar{x} \cap \bar{y} \neq \phi) \Longrightarrow (\bar{x} = \bar{y})$

Assume $z \in \bar{x} \cap \bar{y}$

show $\bar{x} \subseteq \bar{y}$ (also need $\bar{x} \supseteq \bar{y}$).

so assume $u \in \bar{x}$ and show $u \in \bar{y}$.

Assume $z \in \bar{x}$, $z \in \bar{y}$, $u \in \bar{x}$ and show $u \in \bar{y}$.

$$\begin{array}{cccc} \Downarrow & \Downarrow & \Downarrow & \Uparrow \\ xRz & yRz & xRu & yRu \end{array}$$

by sym: zRx

so by trans have yRx and yRu

so done and $\bar{x} \subseteq \bar{y}$.

210227 Next § 3.4: Modular Arithmetic.

Proof of Thm 3.3.1

Assume R is an equivalence relation on a nonempty set A.

If $x \in A$ then $\bar{x} \in A/R$ and since R is reflexive have xRx so $x \in \bar{x}$.

Hence if $x \in A$ then $x \in \bar{x} \subseteq \bigcup_{\bar{y} \in A/R} \bar{y}$ hence
$$\bigcup_{\bar{y} \in A/R} \bar{y} = A.$$

Also if $\bar{x} \in A/R$ then $x \in \bar{x}$ so $\bar{x} \neq \emptyset$.

If $z \in \bar{y} \cap \bar{x}$ and $w \in \bar{x}$

then yRz, xRz and xRw

so by symmetry zRx and using transitivity

twice have yRx and yRw

so $w \in \bar{y}$. Therefore $\bar{x} \subseteq \bar{y}$.

Similarly $\bar{y} \subseteq \bar{x}$ so $\bar{y} = \bar{x}$. qed.

Examples: In $\mathbb{Z}_7$:

Find: or find the remainder after div by 7 of:

Ans:

ⓐ $3+5 = \overline{8} = \overline{1}$ — 1

ⓑ $3 \cdot 5 = \overline{15} = \overline{1}$ — 1

ⓒ $5^3 = (\overline{-2})^3 = \overline{-8} = \overline{-1} = \overline{6}$ — 6

ⓓ $216 + 698 = \overline{5} + \overline{-2} = \overline{3}$ — 3

ⓔ $216 \cdot 698 = \overline{5} \cdot \overline{-2} = \overline{-10} = \overline{4}$ — 4

$\overline{-3}$

(f) $215^{698} = \overline{5}^{698} = \overline{(-2)}^{698} = \overline{(-2)}^{6(116)+2}$

$\overline{5} \xleftrightarrow{-7} \overline{(-2)}$

$\overline{(-2)}^2 = \overline{4}$

$\overline{(-2)}^3 = \overline{-8} = \overline{-1}$

$\overline{(-2)}^6 = \overline{(-1)} \cdot \overline{(-1)} = \overline{1}$

$= \overline{1}^{115} \cdot \overline{(-2)}^2 = \overline{4}$

(4)

Try the same (d), (e), (f) in $\mathbb{Z}_9$

Ans: (d) $\overline{8} + \overline{5} = \overline{13} = \overline{4}$ $\quad$ ($\overline{4}$)

(e) $\overline{-1} \cdot \overline{5} = \overline{-5} = \overline{4}$ $\quad$ ($\overline{4}$)

(f) $\overline{(-1)}^{698} = \overline{1}$ $\quad$ ($\overline{1}$)

RSA is the main public key cryptosystem,

encrypt: publish 698

encode: data $215 \to 215^{698}$

$= 4$

hide 5

decode: $4^5 \to$

Sketch: Examples above: $m=7$

$$8 \equiv 1 \pmod 7$$

$$-2 \equiv 5 \pmod 7$$

$$6 \equiv 6 \pmod 7$$

Logic: $P \wedge Q \Rightarrow R$.

Assume P, Q show R.

$a \equiv_m c$ or $a-c$ is div. by m.

or there is k with $mk = a-c$

and $\quad m\underline{l} = b - d$

so $\quad m\underline{k} + m\underline{l} = (a - c) + (b - d)$

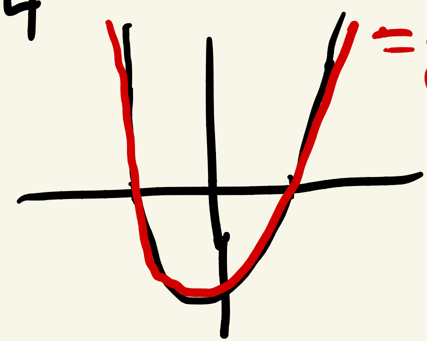
$$= (a + b) - (c + d)$$

210224 Function: in a set theory framework.

Ex: formula for a function from $\mathbb{R}$ to $\mathbb{R}$.

① $f(x) = x^2 - 4$

graph:



$= \text{graph}(f)$

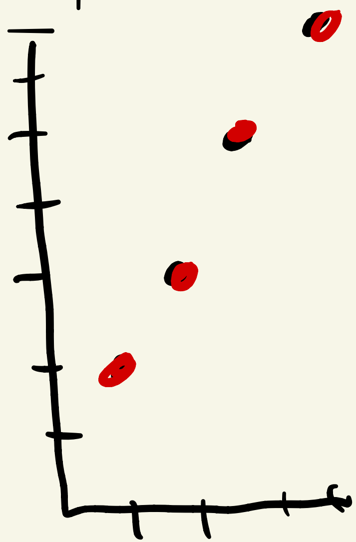
$= \{(x,y) \in \mathbb{R}^2 \mid y = x^2 - 4\}$

Ex: A <u>sequence</u> is a function from $\mathbb{N}$

② to some set.

eg: from $\mathbb{N}$ to $\mathbb{N}$ might be:

p(n) = the n^{th} prime number.
(so p(1) = 2, p(2) = 3, p(3) = 5 ...).



= graph = $\{(n, m) \in \mathbb{N}^2 \mid m \text{ is the } n^{th} \text{ prime}\}$

Vertical line test:
The graph of a relation is the graph of a function if it meets every vertical

line in exactly one point.

Proof: Assyme $x \in \mathbb{R}$. Hence $y = x^2 - 4 \in \mathbb{R}$.
and $f(x) = y$ so $\mathrm{domain}(f) = \mathbb{R}$.
Assume $f(x) = y$ and $f(x) = z$.
Hence $y = x^2 - 4 = z$. qed.

Claim: The inverse to 1 is not a function.
$g = \{(y, x) \in \mathbb{R}^2 \mid y = x^2 - 4\}$.

Sketch: either show $(-12, *)$ has no solns so $-12 \notin \mathrm{Dom}(g)$.

or show there are two solns. $(0, 2)$ & $(0, -2)$, looks easier.

Proof: $(0,2)$ and $(0,-2)$ are both in g.

(since $0 = 2^2 - 4$ and $0 = (-2)^2 - 4$) qed.

Claim: If f is a function from A to A and f is an equivalence relation on A then $f = I_A$.

Proof: Assume A is a set, f is a function from A to A and f is an equivalence relation.

If $a \in A$ then since f is reflexive $(a, a) \in f$ so $I_A \subseteq f$.

If $(b, c) \in f$ with $b \neq c$

then $(b,b) \in f$ also so

by property (ii) of functions.

$c = b$ a contradiction

hence $f \subseteq I_A$.

qed.

Examples:

① $\mathbb{Z}_3 \xrightarrow{f} \mathbb{Z}_6$

$f(\bar{x}) = [2x]$

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

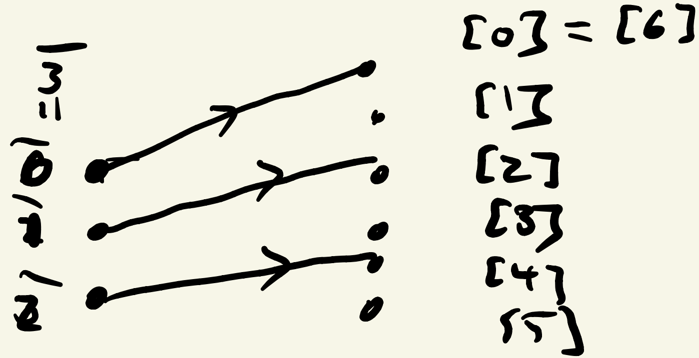
$[x] \in \mathbb{Z}_6$ $\{[0],[1],[2],$
$[3],[4],[5]\}$

$f = \{(\bar{x}, [2x]) \mid x \in \mathbb{Z}\}$.

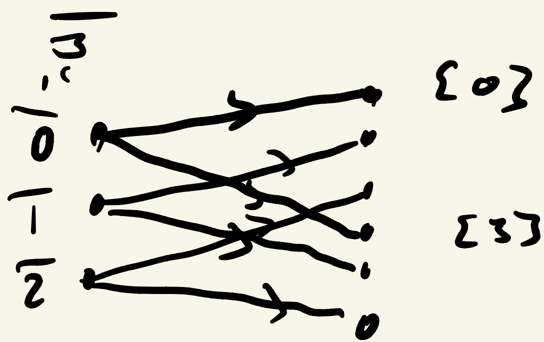
② $\mathbb{Z}_3 \xrightarrow{g} \mathbb{Z}_6$ $\quad g = \{(\bar{x},[x]) \mid x\in\mathbb{Z}\}$.

$$g(\bar{x}) = [x]$$

①



②



210226

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

$$\bar{0} = \bar{3} \quad \cdots$$

$[x] \in \mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

$$[0] = [6] \quad \cdots$$

Claim: The relation $f(\bar{x}) = [x]$ is not a well defined function from $\mathbb{Z}_3$ to $\mathbb{Z}_6$.

Proof: From the definition
$(\bar{0}, [0])$ and $(\bar{3}, [3])$ are in f
but $\bar{0} = \bar{3}$ and $[0] \neq [3]$. q.e.d.

Claim: The relation $g([x]) = \bar{x}$
is a (well defined) function from
$\mathbb{Z}_6$ to $\mathbb{Z}_3$.

Proof:
(i) If $[n] \in \mathbb{Z}_6$ then $([n], \bar{n}) \in g$.
(ii) If $([k], \bar{k})$ and $([l], \bar{l})$ are in g

and $[k]=[l]$ then there is t with

$$k-l = 6t = 3\cdot 2t$$

so $\bar{k}=\bar{l}$. q.e.d.

Inverse function:

If f is a function from A to B then sometimes $f^{-1}=\{(f(a),a) \mid a\in A)$ is a function from B to A.

Composition function:

If g is a function from B to C

and f " " " " A to B

then $g \circ f = \{(a, c) \mid (\exists b \in B)$ with $f(a) = b$ and $g(b) = c\}$.

210301) More conditions on functions.

Sketch: U: $g \circ f = \{(a,c) \in A \times C \mid (\exists b \in B)$

$\underbrace{[(a,b) \in f]}_{f(a)=b} \wedge \underbrace{[(b,c) \in g]}_{g(b)=c}\}$ since both are functions!

L: Want: $(\forall a \in A)(\exists! c \in C)$

$(a,c) \in g \circ f$

equivalently, $\exists c$ and

$!$: $\forall (a,c), (a,\tilde{c}) \in g \circ f$

need $c = \tilde{c}$.

I Try $\exists$ first:

$\forall a \in A$ have $f(a) = b \in B$

and $g(b) = c \in C$.

so $(a, c) \in g \circ f$ ✓

For ! if $(a, c), (a, \tilde{c})$ are in $g \circ f$.

then $\exists\, b, \tilde{b}$ with $(a, b), (a, \tilde{b})$ in f

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

but since f is a function:

have $b = \tilde{b}$

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

so since g is a function:

have $c = \tilde{c}$ similarly.

Ans:

① Not onto since $\text{range}(x^2) = \mathbb{R}_{\geq 0} \neq \mathbb{R}$.

Not one to one since $(-2)^2 = (2)^2 = 4$.

(2) Not onto since range$(e^x) = \mathbb{R}_{>0} \neq \mathbb{R}$.

Is one to one since

if $e^x = e^y$

then $\underset{x}{\underset{\shortparallel}{\ln(e^x)}} = \underset{y}{\underset{\shortparallel}{\ln(e^y)}}$

Another proof. Since e^x is increasing if $x<y$ then $e^x < e^y$ so $e^x \neq e^y$.

(3) Is onto since range$(x^3) = \mathbb{R}$.

IS one to one since

if $x^3 = y^3$

then $x = \sqrt[3]{x^3} = \sqrt[3]{y^3} = y$

Def: If f is a function from A to B which is both one to one and onto call f <u>bijective</u> or a <u>bijection</u>.

Ex: 3 above $h(x) = x^3$ is bijective

from $\mathbb{R}$ to $\mathbb{R}$.

Claim 4.3.2:

If g a fn. from B to C

and f " " A to B

and $g \circ f$ is an onto fn from A to C

then g is also onto C.

Proof: If c is in C then

$c = (g \circ f)(a)$ for some a in A since $g \circ f$ is onto

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

q.e.d.

Claim: If $g : B \to C$ and $f : A \to B$ and $g \circ f : A \to C$ is onto.

then $f : A \to B$ might not be onto.

Proof: Consider the example:

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

$f(1) = 3$, $g(2) = g(3) = 4$

Check: $(g \circ f)(1) = 4$ so $g \circ f$ is onto but $f(1,1) = 3 \neq 2$

so f is not onto.

210303 §4.4

Def: A function f from A to B is a <u>bijection</u> or <u>bijective</u> or a <u>one to one correspondence</u>

if f is both $\underbrace{\text{one to one}}_{\text{injective}}$ and $\underbrace{\text{onto}}_{\text{surjective}}$.

and if $A = B$ f is called a <u>permutation</u>.

(§5.1) will use bijections:

Def: If A and B are sets then $A \approx B$ or A is equivalent to B if there is a bijection from A to B.

Sketch:

L: A reln f from A to B is a function:

if ① $(\forall a \in A)(\exists b \in B)\ (a,b) \in f$

and (ii) $(\forall a \in A)\ (\forall b, \tilde{b} \in B)\ \big(((a,b) \in f) \wedge ((a,\tilde{b}) \in f)\big) \Rightarrow b = \tilde{b}$

or equiv: $(\forall a \in A)(\exists!\, b \in B)\ (a,b) \in f$

A function f from A to B is a bijection:

if (i) (onto) $(\forall b \in B)(\exists a \in A)\ (a,b) \in f$

and (ii) (1-1) $(\forall b \in B)(\forall a, \tilde{a} \in A)\ \big(((a,b) \in f) \wedge ((\tilde{a},b) \in f)\big) \Rightarrow a = \tilde{a}$

or equivalently: $(\forall b \in B)(\exists!\, a \in A)\ (a,b) \in f$

I: If f has

fn: $(\forall a)(\exists! b)$ $(a,b) \in f$

bij: $(\forall b)(\exists! a)$ $(a,b) \in f$.

then: f^{-1} has:

bij: since f is a fn so $(\forall a)(\exists! b)$ $(a,b) \in f$ so $(b,a) \in f^{-1}$

Fn: since f is a bij so $(\forall b)(\exists! a)$ $(a,b) \in f$ so $(b,a) \in f^{-1}$.

Thm 4.4.4. a:

If f is a fn. from A to B

and g " " , B to A

then $f = g^{-1}$ iff

$$g \circ f = I_A \quad \text{and} \quad f \circ g = I_B$$

$$\begin{tikzcd} A \arrow[d, "f"] \arrow[dd, bend right, "g \circ f"'] \\ B \arrow[d, "g"] \\ A \end{tikzcd}$$

Claim: There are fns:

f from A to B

ang g from B to A

with $g \circ f = I_A$ but $f \circ g \neq I_B$.

$f \nmid$ $f \circ g$

B

Proof of Claim: Take $A = \{1\}$, $B = \{2, 3\}$.

and $f(1) = 2$, $g(2) = g(3) = 1$.

Hence $g \circ f(1) = g(2) = 1$ so $g \circ f = I_A$.

But $f \circ g(3) = f(1) = 2 \neq 3$ so $f \circ g \neq I_B$.

qed.

Proof of Thm:

$\Rightarrow$ Show $g \circ f \subseteq I_A$.

Assume $(a, \tilde{a}) \in g \circ f$ so there is $b \in B$ with $(a,b) \in f$ so $(b,a) \in g$. and $(b,\tilde{a}) \in g$ so $a = \tilde{a}$ so $g \circ f \subseteq I_A$.

Show $g \circ f \supseteq I_A$.

Assume a is in A hence there is b in B with (a,b) in f so (b,a) is in g. and (a,a) is in $g \circ f$.

Similarly $f \circ g = I_B$.

Remains to check $\Leftarrow$. (Leave to you)

Sketch

① Compute:

$$\begin{aligned}
\bar{0} &\xmapsto{f} (\bar{0})^2 = \bar{0} \\
\bar{1} &\xmapsto{f} (\bar{1})^2 = \bar{1} \\
(\bar{2}) &\xmapsto{f} (\bar{2})^2 = \bar{4} \\
\bar{3} &\longmapsto (\bar{3})^2 = \bar{9} = \bar{4}
\end{aligned}$$

Proof of ①: $f(\bar{2}) = \bar{4} = f(\bar{3})$

so f is not one to one.

qed.

② Compute:

$$f$$

$$\bar{0} \longmapsto \bar{0}$$

$$\bar{1} \longmapsto \bar{1}$$

$$\bar{2} \longmapsto \bar{8} = \bar{3}$$

$$\bar{3} \longmapsto \overline{27} = \bar{2}$$

$$\overline{-1} = \bar{4} \longmapsto \overline{-1} = \bar{4}$$

210305

Sketch for claim 3:

U_i $\qquad$ $\mathbb{N} \times \mathbb{N}$

$\mathbb{N}/\mathbb{N}$	1	2	3	4	5	6
5	9					
4	7	14	28			
3	5	10	20	40		
2	3	6	12	24		
1	1	2	4	8	16	32

f

f is a bijection if every number in $\mathbb{N}$

appears exactly once in the grid.

L: Is a function:

so need: bijection:

- $\forall \cancel{b}^{\,n} \in \mathbb{N} \quad \exists!\, (\cancel{c,d}^{\,a,b}) \in \mathbb{N}\times\mathbb{N}$

with $f((\cancel{c,d}_{\,a,b})) = \cancel{b}\ n$

or

- exists: (onto)! $\forall n \in \mathbb{N}$ there is (a,b) with $f((a,b)) = n$

unique (1-1): If $f((a,b)) = f((\tilde{a},\tilde{b}))$ then $a = \tilde{a}$ and $b = \tilde{b}$.

I: (onto): If $n \in \mathbb{N}$

then $n = 2^{\alpha}\beta$

with $\alpha \geq 0$ and ($\beta \geq 1$ and odd),

eg $12 = 2^2 \cdot 3$

so $\alpha+1 \geq 1$ is in $\mathbb{N}$

and $\frac{\beta+1}{2}$ is in $\mathbb{N}$

and $n = f(\alpha+1, \frac{\beta+1}{2}) = 2^{\alpha+1-1}(2\frac{\beta+1}{2}-1)$

$a \qquad b \qquad 2^{\alpha}\beta$ ✓.

(1-1): If $f((a,b)) = f((\tilde{a},\tilde{b}))$

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

For contradiction assume $a \neq \tilde{a}$

may assume $a > \tilde{a}$

divide both sides by $2^{\tilde{a}-1}$

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

so even = odd $\times$.

Hence ~~If~~ $a = \tilde{a}$ ~~and~~ then

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

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

so $$b = \tilde{b}$$ ✓

Notes:

$f: A \to B$ is a bijection

iff ~~(Thm. 4.4)~~ (HW 4.4.6)

$\exists\, g: B \to A$ with $f \circ g = I_B$ and $g \circ f = I_A$

iff (Thm 4.4.4)

$\exists\, g : B \to A$ with $g = f^{-1}$

iff ((Cor 4.4.3)

$\exists\, g : B \to A$ with $g = f^{-1}$

and g is a bijection.

Ans:

$$
\begin{tikzcd}
{[1,\infty)} \arrow[r, "e"] & (1,\infty) \arrow[r, "b^{-1}"] & (0,1) \\
{(0,1]} \arrow[u, "c"] \arrow[urr, bend right, "f = b^{-1}\circ e \circ c"'] & &
\end{tikzcd}
$$

$$
f\left(\tfrac{1}{2}\right) = \underbrace{b^{-1}\Big(\underbrace{e\big(\underbrace{c\left(\tfrac{1}{2}\right)}_{2}\big)}_{3}\Big)}_{\frac{1}{3}} = \frac{1}{3}
$$

$$f\left(\frac{1}{\pi}\right) = \frac{1}{\pi}$$

$$f(1) = \frac{1}{2}$$

$$f(x) = \begin{cases} \dfrac{1}{\frac{1}{x} + 1} = \dfrac{x}{1+x} & \text{if } \frac{1}{x} \in \mathbb{N} \\ \dfrac{1}{\frac{1}{x}} = x & \text{else} \end{cases}$$

210308 Ch5: Counting and set cardinality:

Def: If A and B are sets then A is equivalent to B

$A \approx B$ or

if $\exists\, A \xrightarrow{f} B$ with f a bijective function

Ex: $\underset{\mathbb{N}_3}{\{1,2,3\}} \approx \{a,b,c\} \neq \{1,2,3\}$

Def: $\mathbb{N}_k = \{1, 2, \dots, k\}$

$\mathbb{N}_0 = \varphi$

Def: If $A \approx \mathbb{N}_k$ write $\overline{\overline{A}} = k = \overline{\overline{\{a,b,c\}}}$

and say A has cardinality k.

eg $\overline{\overline{\varphi}} = 0$, $\overline{\overline{\{a, b, c\}}} = 3$

If $A \approx \mathbb{N}$ write $\overline{\overline{A}} = \aleph_0$

aleph not

If $A \approx (0,1)$ write $\overline{\overline{A}} = c$

and say A is denumerable or countably infinite.

and say A has the cardinality of the continuum.

If $\bar{\bar{A}} = k$ or $\aleph_0$ call A <u>countable</u>.

If $\bar{\bar{A}} = k$ call a <u>finite</u> and otherwise <u>infinite</u>.

210310 Inequivalence of sets:

Inductive step in proof that

$P(n)$: $\forall r < n$ $\nexists$ $f : \mathbb{N}_n \longrightarrow \mathbb{N}_r$ which is injective.

Use: HW problem:

If $x \in \mathbb{N}_k$ $\exists$ $g : \mathbb{N}_k - \{x\} \longrightarrow \mathbb{N}_{k-1}$ a bijection.

Assume $P(n)$

Use contradiction to show $P(n+1)$.

Assume for contradiction $\sim P(n+1)$.

so $\exists\ f : \mathbb{N}_{n+1} \longrightarrow \mathbb{N}_r$ injective
with $r < n+1$

hence: $f|_{\mathbb{N}_n} : \mathbb{N}_n \longrightarrow \mathbb{N}_r - \{x\}$

if $x = f(n+1)$ since f is injective,

and $f|_{\mathbb{N}_n}$ is injective.

and by HW $\exists\ g : \mathbb{N}_r - \{x\} \longrightarrow \mathbb{N}_{r-1}$
injective.

so $g \circ f|_{\mathbb{N}_n} : \mathbb{N}_n \longrightarrow \mathbb{N}_{r-1}$ injective.

and $r-1 < n$ so

$\exists\ g \circ f|_{\mathbb{N}_n} : \mathbb{N}_n \to \mathbb{N}_{r-1}$ inj. and $r-1 < n$

contradicting $P(n)$. q.e.d.

Thm 5.2.4: $\mathbb{N} \not\approx (0,1)$

Proof Plan: Show $\nexists f: \mathbb{N} \to (0,1)$ surjective.

Assume $f: \mathbb{N} \to (0,1)$ and find $x \in (0,1)$ with $x \notin \operatorname{Im}(f)$,

Clever diagonalization trick.

consider decimal expansions of each $f(n)$ and write a_n for the n^{th} digit of the decimal exp of $f(n)$ diagonal eg:

$f(1) = .\mathbf{3}2154\ldots$ $\qquad a_n \qquad a_1 = 3 \quad b_1 = 5$

$f(2) = .5\mathbf{5}51122\ldots$ $\qquad a_2 = 5 \quad b_2 = 3$

$f(3) = .35\mathbf{6}13\ldots$ $\qquad a_3 = 6 \quad b_3 = 5$

$f(4) = .333\mathbf{5}1111$ $\qquad a_4 = 5 \quad b_4 = 3$

$f(5) = .9987\mathbf{5}443\ldots$ $\qquad a_5 = 5 \quad b_5 = 3$

$\vdots$

choose $b_n \neq a_n$ eg $b_n = \begin{cases} 5 & \text{if } a_n \neq 5 \\ 3 & \text{if } a_n = 5 \end{cases}$

Check $B = .b_1 b_2 b_3 \ldots \notin \mathrm{Im}(f)$.

eg: $= .53533\ldots$

Thm 5.4.3: If A is a set then $A \not\approx \mathcal{P}(A)$

Proof sketch

u! for A finite:

if $\overline{\overline{A}} = n$ then $\overline{\overline{\mathcal{P}(A)}} = 2^n \neq n$

eg $\overline{\overline{\emptyset}} = 0$ and $\overline{\overline{\mathcal{P}(\emptyset)}} = 2^0 = 1 \neq 0$

$\overline{\overline{\{1\}}} = 1$ and $\overline{\overline{\mathcal{P}(\{1\})}} = 2^1 = 2 \neq 1$

L: for any $f: A \longrightarrow \mathcal{P}(A)$ show f is not onto and so not bijective.

Trick/Idea: Given f build.

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

eg: $f : \{1,2,3\} \to \mathcal{P}(\{1,2,3\})$.

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

$$B = \{2\}$$

Key: $B \notin \mathrm{Im}(f)$

Note: $(0,1) \not\approx \mathcal{P}((0,1)) \not\approx \mathcal{P}(\mathcal{P}((0,1)))$

$\not\approx \mathcal{P}(\mathcal{P}(\mathcal{P}((0,1)))) \; \ldots$

210312

First order Predicate Logic:

Propositions: Truth Tables] inside back cover

$\wedge, \vee, \sim, \Rightarrow, \Leftrightarrow$

universe $\exists \quad \forall \quad \exists!$

Sets: Venn Diagrams

$\cap, \cup, \underbrace{A^c}_{\text{in a universe}}, \in, \underset{\text{family}}{\bigcap}, \underset{\text{family}}{\bigcup}, \times, -,$

$\emptyset, \mathcal{P}(A), \overline{\overline{A}}, \approx$

Relations: $R \subseteq A \times B$

xRy or $(x,y) \in R$

R^{-1}, $R \circ S$, $\mathrm{dom}(R)$, $\mathrm{rang}(R)$.

Equivalence relations: 3 properties, $\overline{x}$, A/R (set of sets).

eg $\mathbb{Z}_n = \mathbb{Z}/R$ for the right R.

Functions: $\forall x \ \exists! \, y$ with $(x,y) \in f$ write $f(x) = y$

bijective functions: $\forall y \ \exists! \, x$ with $(x,y) \in f$.
2 properties

Example Problems:

Find $\gcd(182, 21)$

Ans: Two approaches:

① Euclid's Alg:

$$182 = 8 \cdot 21 + 14$$

$$21 = 1 \cdot 14 + \boxed{7} = \gcd$$

$$14 = 2 \cdot 7$$

② Factor both: $2 \cdot \boxed{7} \cdot 13 = 182$ ⇐ gcd.

$3 \cdot \boxed{7} = 21$

Problem:

(a) Prove that $\underbrace{S = \{(x,y) \in \mathbb{R}^2 \mid x-y \in \mathbb{Q}\}}_{\text{relation on } \mathbb{R}}$

is an equivalence relation.

(b) Find $x, y, z \in \mathbb{R}$ with $\overline{x} = \overline{y} \neq \overline{z}$

(c) Show that $\overline{\pi}$ is denumerable.

(b) $\bar{x} = \{ y \mid (x,y) \in S \}$

eg $\bar{x} = \bar{y}$ if $x = y$

eg $\bar{0} = \overline{\tfrac{1}{2}}$

Proof: $\subseteq$ if $a \in \bar{0}$ then $(0,a) \in S$ so $0 - a \in \mathbb{Q}$ so $\tfrac{1}{2} - a \in \mathbb{Q}$

so $(\tfrac{1}{2}, a) \in S$ so $a \in \overline{\tfrac{1}{2}}$.

$\supseteq$ similarly.

and $\quad \overline{0} \neq \overline{\pi}$

since: $\quad \pi \in \overline{\pi}$ since $(\pi, \pi) \in S$

since S is reflexive

(or $\pi - \pi = 0 \in \mathbb{Q}$).

but $\quad \pi \notin \overline{0}$ since

for contradiction assume $\pi \in \overline{0}$

so $(0, \pi) \in S$ so $0 - \pi \in \mathbb{Q}$.

but $-\pi \notin \mathbb{Q}$. a contradiction.

q.e.d.