Lecture 11
10/19/21

Exam 1 Solutions posted
- graded EoW
- HW 2 this week

Ex, R_1 =
R_1 <

Today: Relations,
Equivalence Classes

We'll look at the notion of relations on a set, a way of comparing two elements of a set

Def The Cartesian product of two sets A and B denoted $A \times B$ is the set of all ordered pairs where a is in A and b is in B

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

Ex $A = \{1,2,3\}$

$B = \{2,3\}$

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

Ex $A = \{x,y,z\}$, $B = \{1,2,3\}$

	1	2	3
x	(x,1)	(x,2)	(x,3)
y	(y,1)	(y,2)	(y,3)
z	(z,1)	(z,2)	(z,3)

Def A relation on a set S is a subset $R \subseteq S \times S$. Generally we write

$$x R y \iff (x,y) \in R$$

$$x \not R y \iff (x,y) \notin R$$

$R = \{(x,y) \in A \times A \mid x < y\}$

Ex $A = \{1,2,3\}$, $R = \{(1,2),(1,3),(2,3)\} \Rightarrow$ $1R2, 1R3, 2R3$
$1 \not R 1, 3 \not R 1, \ldots$

Suppose we have a set A, and a set R which is a subset of $A \times A$.
Does this represent anything we are familiar with?

Ex $A = \{1,2,3,4,5,6\}$

$R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6)$
$(2,2), (2,4), (2,6),$
$(3,3), (3,6),$
$(4,4)$
$(5,5)$
$(6,6)\}$

What about R here?

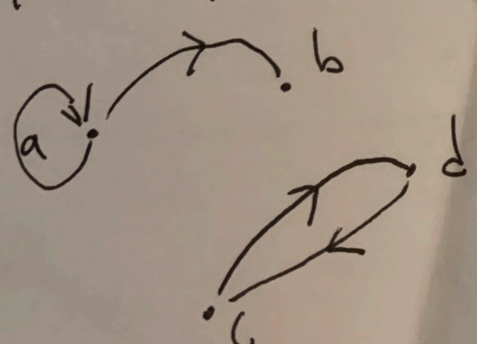
~~$R = \{(x,y) \mid x$~~ $R = \{(x,y) \in A \times A \mid x \mid y\}$

Def A directed graph is an ordered pair $G = (V, E)$
where V is a set of vertices (or nodes)
and E is a set of ordered pairs of vertices (directed edges)

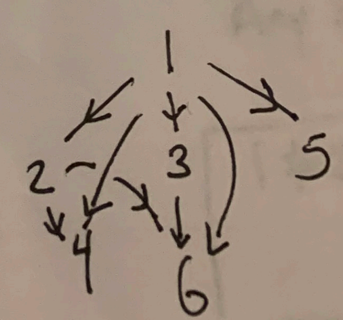
Digraphs and Relations

Can use digraphs to express relations

Ex $A = \{a,b,c,d\}$, $R = \{(a,a), (a,b), (c,d), (d,c)\}$



$xRy \iff (x \mid y \wedge x \neq y)$



Ex $A = \{1,2,3,4,5,6\}$

Properties of Relations

Two $n \times n$ Matrices are Similar if $\exists$ invertible matrix P s.t $B = P^{-1}AP$

$R \subseteq A \times A$

R is reflexive if $\forall x \in A,\ xRx$ (x is related to itself)

Examples

any set $=$ (equality)

$\mathbb{R}, \leq, \geq$ $(2 \leq 2,\ 2 \geq 2)$

$M_{n \times n} \in \mathbb{R}, \sim$

Non Examples

any set $\neq$ non equality

$\mathbb{R}, <, >$ $(2 \not< 2)$

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

s.t xRy we have yRx

Examples

Any set, $=$, $\neq$

$M_{n \times n}(\mathbb{R})$; $\sim$

Non Examples

$<, \leq$ $\boxed{2<3 \text{ but } 3 \not< 2}$

$\mathbb{N} : |$ (divisibility) $\boxed{2|4 \text{ but } 4 \nmid 2}$

R is transitive if $\forall x,y,z \in R,\ (xRy \wedge yRz) \to xRz$

Examples

$=$

$\mathbb{R} : <, \leq$

$\mathbb{N} : |$

$\boxed{2|4 \wedge 4|8 \to 2|8}$

Non Examples

Any set with $\neq$

$\boxed{1 \neq 2 \wedge 2 \neq 1 \text{ but } 1 = 1}$

$1 \neq \neq 1$

Recall: A relation on a set A is a subset $R \subseteq A \times A$

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

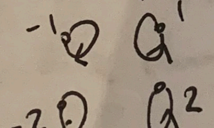
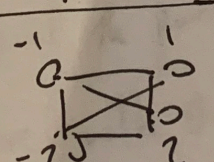
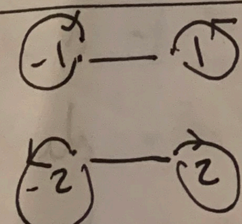
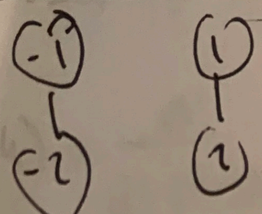
Def^n A relation R is called an equivalence relation if

1) $\forall x \in A,\ xRx$ (reflexive)
2) $\forall x,y \in A\ \ xRy \to yRx$ (symmetric)
3) $\forall x,y,z \in A\ \ (xRy \wedge yRz) \to xRz$ (transitive)

The equivalence class of $x \in A$ (equivalence class is attached to an element)

is $[x] = \{y \in A \mid xRy\} \subseteq A$

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

Relation	Graph	Equivalence Classes
equal		$\{-2\}, \{-1\}, \{1\}, \{2\}$
nothing		$\{-2,-1,1,2\} = [1] = [2] =$ Here $[x]$ is the equivalence class represented
parity (evenness/oddness)		$\{-2,2\} = [2], [-2]$ $\{-1,1\} = [-1], [1]$
Same Sign		$\{-1,-2\} = [-1] = [-2]$ $\{1,2\} = [2] = [1]$

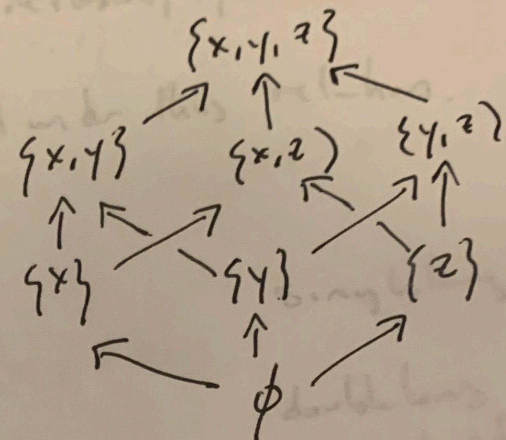
Ex

$A = \mathcal{P}(\{1,2,3\})$ where $\mathcal{P}(S)$ is the power set of S

Def The power set of a set S is the set of all subsets of S, including the empty set and S itself

Ex $S = \{x, y, z\}$

We can write the elements of the power set ordered with respect to inclusion as a digraph



Remark The binomial theorem which we will discuss is closely related to the power set

which we will discuss is closely related to the power set

$\Rightarrow$ A k-element subset of some set is a k-element combination

$\Rightarrow$ # combinations $C(n,k)$ or $_nC_k$, the binomial coefficient is the number of subsets with k elements in a set with n elements.

is the number of subsets with k elements of the power set of a set w/ n elements.

$\Rightarrow$ # of sets w/ k elements of the power set of a set w/ n elements.

$C(3,0) = 1$ subset with 0 elements (empty set)

$C(3,1) = 3$ subsets w/ 1 element (singletons)

$C(3,2)$ 3 subsets with 2 elements (complements of singletons)

$C(3,3)$ 1 subset w/ 3 elements (original set)

A combination $_nC_k$ or $C(n,k) = \dfrac{n!}{k!\,(n-k)!}$

$A = P(\{1,2,3\})$ $\qquad A R B \Leftrightarrow |A| = |B|$

Let A be the powerset of the set $S = \{1,2,3\}$

Two subsets are related iff they have the same size (cardinality).

$\Rightarrow$ There is not much to check here, since the relation is built on equality (and equality is reflexive, symmetric, transitive)

Lets look at equivalence classes of A under this relation.

$[0] = \{\emptyset\}$

$[\{1\}] = \{\{1\}, \{2\}, \{3\}\}$ singletons

$[\{1,2\}] = \{\{1,2\}, \{1,3\}, \{2,3\}\}$ doubletons or unordered pairs

All equivalent b/c same # elem

$[\{1,2,3\}] = \{\{1,2,3\}\}$

Prop

Suppose R_1, R_2 are both equivalence relations (i.e. $R_1, R_2 \subseteq A \times A$)

Then $R = R_1 \cap R_2$ is an equivalence relation.

(we define a new relation)

Since $R_1, R_2 \subseteq A \times A$, we know $R_1 \cap R_2 \subseteq A \times A$ so this is a relation.

Proof Reflexivity. Suppose $x \in A$, want to show xRx i.e. $(x,x) \in R$

We know xR_1x, xR_2x $\Rightarrow (x,x) \in R_1 \wedge (x,x) \in R_2 \Rightarrow (x,x) \in R_1 \cap R$

$\Rightarrow xRx$ ✓

Transitivity: Suppose $xRy \wedge yRz$ (want to show xRz)

$\Rightarrow (x,y) \in R = R_1 \cap R_2$ $\quad (y,z) \in R = R_1 \cap R_2 \Rightarrow$ $x,y \in R_1$, $x,y \in R_2$, $y,z \in R_1$ & $y \in$

Transitive Suppose xRy and yRz (want to show xRz)

$\Rightarrow (x,y) \in R = R_1 \wedge R_2 \Rightarrow (x,y) \in R_1$ and $(x,y) \in R_2$

$(y,z) \in R = R_1 \wedge R_2 \Rightarrow (y,z) \in R_1$ and $(y,z) \in R_2$

$\Rightarrow xR_1y$ and $yR_1z \Rightarrow xR_1z \Rightarrow (x,z) \in R_1$ $\Rightarrow (x,z) \in R_1 \wedge R_2$

xR_2y and $yR_2z \Rightarrow xR_2z \Rightarrow ((x,z) \in R_2$

$\Rightarrow xRz$ $\square$

Symmetric

$xRy \Rightarrow yRx$

$(x,y) \in R = R_1 \wedge R_2 \Rightarrow (x,y) \in R_1$ and $(x,y) \in R_2$

both R_1 and R_2 symmetric so

$(y,x) \in R_1$ and $(y,x) \in R_2$

$\Rightarrow (y,x) \in R_1 \wedge R_2 \Rightarrow y, x \in R$ $\square$

~~Prop Def we say that a is congruent to b mod n if $n|(a-b)$~~

~~$a \equiv b \pmod n \iff n|(a-b)$~~ ~~$\exists k \in \mathbb{Z}$ s.t. $n \cdot k = a$~~

Def Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo n and write $a \equiv b \pmod n$ if $n|(a-b)$

(or a and b have the same remainder when divided by n)

n is called the modulus

Ex ~~8|~~ $8 \equiv 3 \bmod 5 \iff 5 | 8-3$

$20 \equiv 4 \bmod 8 \iff 8 | 20-4$

$13 \equiv -1 \bmod 7 \iff 7 | 13-(-1)$

Proposition $\equiv (\text{mod } n)$ is an equivalence relation

That is:

1) $\forall a \in \mathbb{Z}$, $a \equiv a (\text{mod } n)$ (reflexivity)

2) $\forall a, b \in \mathbb{Z}$, if $a \equiv b (\text{mod } n) \rightarrow b \equiv a (\text{mod } n)$
(symmetric)

3) $\forall a, b, c \in \mathbb{Z}$, if $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$
then $a \equiv c (\text{mod } n)$ (transitivity)

<u>Thm</u> The following statements are equivalent

i) $a \equiv b (\text{mod } n)$

ii) $n | (a-b)$

iii) $a - b = nt$ for some $t \in \mathbb{Z}$

iv) $a = b + nt$ for some $t \in \mathbb{Z}$

) Reflexive: since $a - a = 0t$ $\forall t \in \mathbb{Z}$ then $a \equiv a (\text{mod } n)$ ✓

Symmetric: Let $a, b \in \mathbb{Z}$ s.t. $a \equiv b (\text{mod } n)$. Then $a - b = nt$
for some $t \in \mathbb{Z}$.
$\Rightarrow$ Multiply both sides by -1 $\Rightarrow b - a = n(-t)$
Since $(\mathbb{Z}, +)$ a group then $-t \in \mathbb{Z}$ and so $b \equiv a (\text{mod } n)$

ransitive. Suppose $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$. Then $a - b = nt$ / $b - c = nt'$ for some $t, t' \in \mathbb{Z}$

$\Rightarrow a - c = n(t + t') \Rightarrow t + t' \in \mathbb{Z} \Rightarrow a \equiv c (\text{mod}$

Def The equivalence classes for the equivalence relation $\equiv$ are called congruence ~~sets~~ classes. They form a partition of $\mathbb{Z}$. The set of all congruence classes is denoted $\mathbb{Z}_n$.

Def $a \equiv b \pmod{n} \iff n \mid a-b$

For $x \in \mathbb{Z}$ (fixed x), define the equivalence class of x wrt $\equiv \pmod{n}$

by $[x] = \{a \in \mathbb{Z} \mid a \equiv x \pmod{n}\}$

Ex $n=3$ $\quad x=0$, $\quad [0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{3}\}$

all integers a s.t. a is congruent to 0 mod 3

$\Rightarrow$ ~~a-0 3~~ $\Rightarrow$

$3 \mid a-0 \Rightarrow 3 \mid a$

$\Rightarrow = \{0, \pm 3, \pm 6\}$

Ex

equivalence class of 1 $\quad [1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{3}\}$

$\Rightarrow \{1, 4, 7, 10, \dots, -2, -5\}$

$3 \mid 1-1$, $3 \mid 4-1$, $3 \mid 7-1$

$3 \mid -2-1$, $3 \mid -5-1$

$[2] = \{a \in \mathbb{Z}$ s.t. $a \equiv 2 \pmod{3}\}$

$\Rightarrow \{-4, -1, 2, 5, 8, 11, \dots, -7, \}$

$3 \mid a-2$

We can find all of the integers in one of these three sets. None of these sets overlap

$\Rightarrow$ these sets partition the integers

Fact: There are exactly n equivalence classes modulo n

$$[0], [1], [2], \ldots, [n-1]$$

Every integer is in one of these equivalence classes

Def^n Fix n, the set of least residues is given by

$$\{0, 1, \ldots, n-1\}$$

Every element in this set of least residues is attached to one of these equivalence classes.

Claim For all $a \in \mathbb{Z}$, ~~[illegible]~~ a is congruent to exactly one of the least residues modulo n

$\Rightarrow$ If you are talking about arithmetic modulo n, you only need to talk about the numbers $0, \ldots, n-1$

Proof: Use division algorithm w/ ~~[illegible]~~ a, n

$$a = n \cdot q + r \quad \text{with } \cancel{q}\ 0 \leq r \leq n-1$$

$$\Rightarrow a - r = n \cdot q$$

$$\Rightarrow n \mid (a-r)$$

$$\Rightarrow a \equiv r \pmod n$$

$\Rightarrow a \equiv$ to a number between 0 and $n-1$

in other words one of these least residues. Note q, r in division algorithm is unique $\Rightarrow \equiv$ to exactly 1 of these residues