Math 2001 . Lecture 20.

06. 28. 2022.

Last time: . more inductive proofs : the fundamental thm of arithmetic

Fibonacci numbers

Today: . relations (on sets)

1. Motivation, notation and definitions

Many mathematical statements assert some relationship between two objects:

(1, 2) $1 < 2$, $4 \leq 4$ → (4, 4), $6 = \frac{30}{5}$, $3 \in \{1, 2, 3\}$,

$a \equiv b \pmod{n}$, $X \subseteq Y$, $\mathbb{R} \nsubseteq \mathbb{Z}$, $3 \mid 18$, $3 \nmid 19$.

Notation: All the above statements can be expressed as xRy where R describes a relationship between x and y.

$3 \mid 18$ → $3 R 18$ where $R =$ "divides" → notation: $(3, 18)$

Def: A <u>relation</u> (formally) on a set A is a subset $R \subseteq A \times A$.

We often abbreviate (identify) the statement $(x,y) \in R$ as xRy.

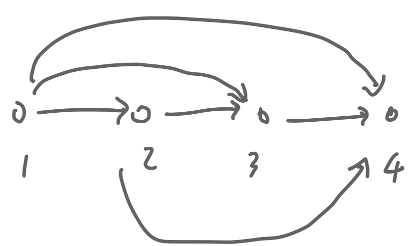
(e.g. $(3,18) \in R \leftrightarrow 3R18$, or $3 \mid 18$)
divides

The statement $(x,y) \notin R$ is abbreviated $x \not R y$.

Sometimes, especially when A is finite, we can capture the relation R via a directed graph $G=(V,E)$ where $V=A$ and $E=\{(a,b) \mid a,b \in A : aRb\}$

$a \to b$

E.g. $A = \{1,2,3,4\}$ $R =$ "$<$" $= \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$.



The following natural (potential) properties of relations are interesting to study:

Def: Suppose R is a relation on a set A. We say that

(1) R is <u>reflexive</u> if xRx $\forall x \in A$.

e.g. The usual rel $<$ on $A = \mathbb{R}$ is not reflexive;

- - - $=$ - - - is reflexive.

(2) R is <u>symmetric</u> if $\forall x, y \in A$, $xRy \Rightarrow yRx$. (equivalently, $(x,y) \in R$ iff $(y,x) \in R$)

e.g. $<$ on $\mathbb{R}$: not symm, "$|$" on $\mathbb{Z}$: not symm

$=$: symm, "$\equiv \pmod n$" : symm. $3 \mid 18$, $18 \nmid 3$.

(3) R is <u>transitive</u> if $\forall x, y, z \in A$, xRy and $yRz \Rightarrow xRz$.

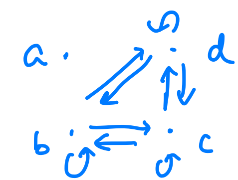
e.g. $<$, $=$ on $\mathbb{R}$ are transitive, $|$ on $\mathbb{Z}$ is transitive.

A quick chart:

Relation on $A := \mathbb{Z}$	$<$	$\leq$	$=$	$\mid$	$\nmid$	$\neq$
Reflexive?	N	Y	Y	Y	$n \nmid n \ \forall n \in \mathbb{Z}$ N	N
Symmetric?	N	N	Y	N	$a \nmid b \Rightarrow b \nmid a$? N	Y
transitive?	Y	Y	Y	Y	$a \nmid b,\ b \nmid c \Rightarrow a \nmid c$? N	N

Example: Consider the following relation R on the set $A = \{a, b, c, d\}$.

$$R = \{(b,b), (b,c), (c,b), (c,c), (d,d), (b,d), (d,b), (c,d), (d,c)\}.$$



- Is R reflexive? No, since $a \not R a$.
- Is R symm? Yes, since $xRy \Rightarrow yRx$ by inspection.
- Is R transitive? Yes, by careful, exhaustive checks.

2. Equivalence relations

Def: A relation R on a set A is called an <u>equivalence relation</u> if it is reflexive, symmetric, and transitive.

Def: Suppose R is an equiv. rel. on a set A. For each elt $a \in A$, we define the <u>equivalence class</u> of A to be the set

$$[a] := \{x \in A : x R a\} \overset{\text{symm.}}{=} \{x \in A : a R x\}.$$

Q: Why are equivalence relations interesting?

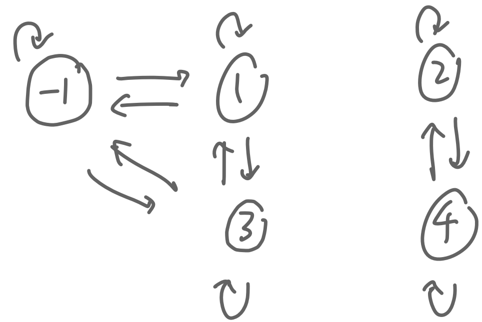
Eventual answer: If R is an equiv. rel on A, then

- $\forall x, y \in A$, $xRy \Longleftrightarrow [x] = [y]$
- The equiv. classes of R partition A.

$\Big\} \rightarrow$ formal proofs tomorrow.

Example: Consider the rel. R on $A = \{-1, 1, 3, 2, 4\}$ given by

the graph



Note: The rel. R is an equiv. rel.

pf: Either check reflexivity, symmetry and transitivity by inspection,

Or note that R coincides with the relation "having the same parity".

By the def. on equiv. classes, $[a] = \{x \in A : xRa\}$ which is an equiv. rel. on A.

$= \{$the neighbors of a in the graph$\}$.

so $[-1] = \{-1, 1, 3\}$, $[1] = \{-1, 1, 3\}$, $[3] = \{-1, 1, 3\}$;

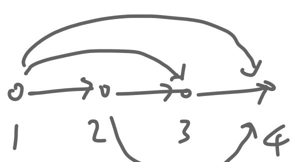
$[2] = \{2, 4\}$, $[4] = \{2, 4\}$. $\to$ two classes: $[-1] = [1] = [3] = \{-1, 1, 3\}$

$[2] = [4] = \{2, 4\}$.

Observation: While there are 5 elts in A, there are only 2 distinct equiv. classes for R; we have $[x]=[y] \iff xRy \ \forall x,y \in A$, and the distinct equiv. classes partition A. $(A = \underbrace{[-1]}_{C_1} \sqcup \underbrace{[2]}_{C_2})$

Note: Given any rel R on a set A (not necessarily an equiv. rel), we can still define the set $[a] = \{x \in A : aRx\}$ - but the sets $[a]$ $(a \in A)$ don't always behave as nicely as when R is an equiv. rel.

e.g. $\{1,2,3,4\}$, $<$



as many distinct sets $[a]$ as $|A|$.

$[1] = \{x \in A : 1Rx\} = \{2,3,4\}$

$[2] = \{3,4\}$,

$[3] = \{4\}$,

$[4] = \phi$.

3. Verifying a rel. is an equiv. rel.

Eg. (congruence) Let $A=\mathbb{Z}$, let $n\in\mathbb{Z}_{>0}$, and define xRy for $x,y\in\mathbb{Z}$ if $x\equiv y \pmod n$. Then R is an equivalence rel.

Pf: We check that R is reflexive, symm, and transitive.

(ref.) we need to show that xRx $\forall x\in A=\mathbb{Z}$. ie, that $x\equiv x \pmod n$ for all $x\in\mathbb{Z}$. This is true because $n \mid 0 = x-x$ $\forall x\in\mathbb{Z}$.

(symm.) We need to show that $\forall x,y\in\mathbb{Z}$, $xRy \Rightarrow yRx$, ie., that $\forall x,y\in\mathbb{Z}$, $x\equiv y \pmod n \Rightarrow y\equiv x \pmod n$. Suppose $x\equiv y \pmod n$, then $n \mid x-y$. So $(x-y)=nk$ for some $k\in\mathbb{Z}$. But then $y-x = -(x-y) = -nk = n(-k)$, so $n \mid y-x$. so $y\equiv x \pmod n$, as desired.

(transitivity): E.x.

By the above, it follows that R is an equiv. rel. $\square$

What are the equivalence classes?

e.g. $n=2$. $\{\ldots, -4, -2, 0, 2, 4, 6, \ldots\} = [0]$

$[1] = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$

$n=3$. $[0] = \{\ldots, -6, -3, 0, 3, \ldots\}$

$[1] = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$

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

There are n equivalence classes, the usual "residue classes".

Example. (P. 213) Let $A = \left\{ \frac{m}{n} \,\middle|\, m, n \in \mathbb{Z},\ n \neq 0 \right\}$. Consider the rel. R

(fractions) on A defined by " $\frac{a}{b} \, R \, \frac{c}{d}$ if $ad = bc$ " $\forall \frac{a}{b}, \frac{c}{d} \in A$.

$\swarrow (m,n)$

Prove that R is an equivalence rel on A.

Eg: $\frac{2}{5} \, R \, \frac{6}{15}$ since $2 \cdot 15 = 5 \cdot 6$, $\frac{1}{3} \, R \, \frac{7}{21}$ since $1 \cdot 21 = 3 \cdot 7$

$\frac{0}{4} \, R \, \frac{0}{17}$ since $0 \cdot 17 = 0 \cdot 4$.

In fact, R is just "being equal as rational numbers".

(and hence the equivalence classes of A are just the rational numbers.)

Pf: We check that R is ref., symm, and transitive.

(1) Take $x \in A$. Then $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$.

We have $\frac{a}{b} R \frac{a}{b}$ since $a \cdot b = b \cdot a$, i.e., we have xRx.

It follows that R is reflexive.

(2) Symm. E.x.

(3) transitivity: Suppose xRy and yRz for some $x, y, z \in A$, say

$x = \frac{a}{b}$, $y = \frac{c}{d}$, $z = \frac{e}{f}$ for some $a, b, c, d, e, f \in \mathbb{Z}$ with

$b, d, f \neq 0$. We hope to show that xRz. i.e., $\frac{a}{b} R \frac{e}{f}$. i.e. $\underbrace{af = be}_{\text{want}}$.

Now, since xRy and yRz, we have

$$(*) \quad \underbrace{ad = bc \quad \text{and} \quad cf = de}_{\text{have}}. \quad (\Rightarrow adcf = bcde)$$

By (*), we have $adcf = bcde$. $(\triangle)$

We discuss cases:

(i) if $dc \neq 0$, then dividing both sides of $(\triangle)$ by dc, we get

$af = be$, so $\frac{a}{b} R \frac{e}{f}$, i.e. xRz, as desired.

(ii) if $dc = 0$, then $c = 0$ since $d \neq 0$.

Thus, we have $ad = bc = b \cdot 0 = 0$ and $0 = c \cdot f = de$ by (*).

Since $d \neq 0$, it follows that $a = 0 = e$, so $af = be = 0$, as desired.

By (1), (2) and (3), we conclude that R is an equiv. rel. $\square$