PLP - 27

TOPIC 27—PROPERTIES & CONGRUENCE

Demirbaş & Rechnitzer

PROPERTIES OF RELATIONS

TOO GENERAL

- Definiton of relation is too(?) general
- Usually require additional properties to be interesting
- Consider “is divisible by” on integers. Has useful properties
    - For all $n \in \mathbb{Z}$, we know $n \mid n$
    - For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$ then $a \mid c$
- Notice that $\leq$ on reals has *similar* properties
    - For all $x \in \mathbb{R}$, we know $x \leq x$
    - For all $x, y, z \in \mathbb{R}$, $x \leq y$ and $y \leq z$ then $x \leq z$

Such additional *structure* make those relations more interesting and useful

3 USEFUL PROPERTIES

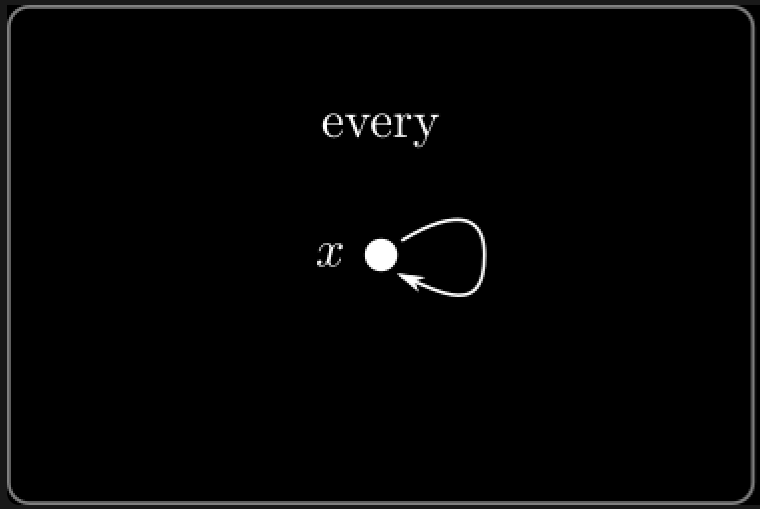
DEFINITION:

Let R be a relation on a set A. Then R is

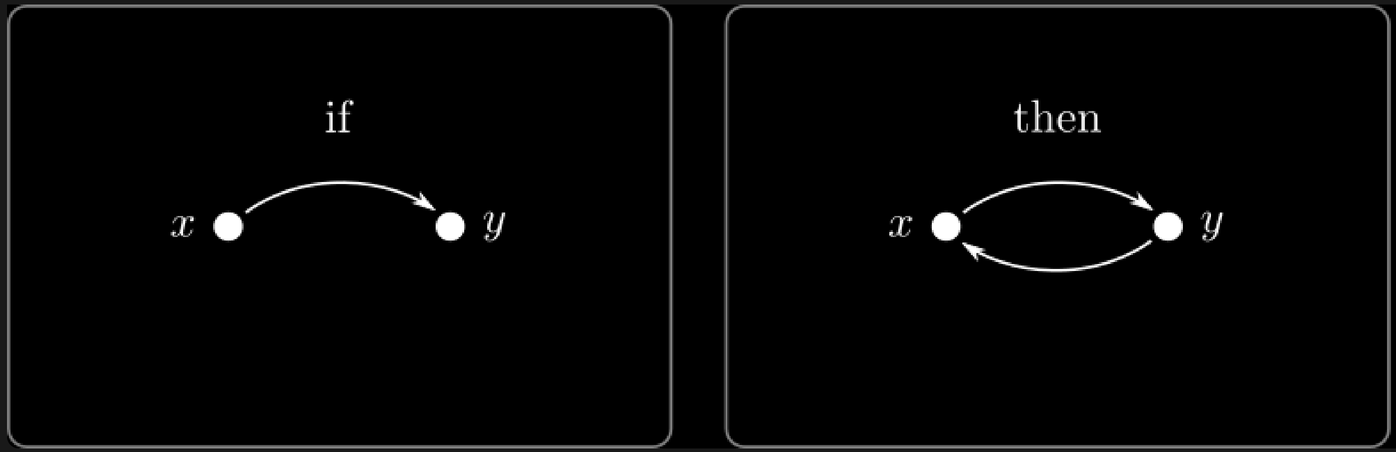
- reflexive when $\forall a \in A, a \ R \ a$
- symmetric when $\forall a, b, a \ R \ b \implies b \ R \ a$
- transitive when $\forall a, b, c, (a \ R \ b) \wedge (b \ R \ c) \implies a \ R \ c$

Relations on $\mathbb{Z}$	$<$	$\leq$	$=$	$\neq$	$\mid$	$\nmid$
reflexive	F	T	T	F	T	F
symmetric	F	F	T	T	F	F
transitive	T	T	T	F	T	F

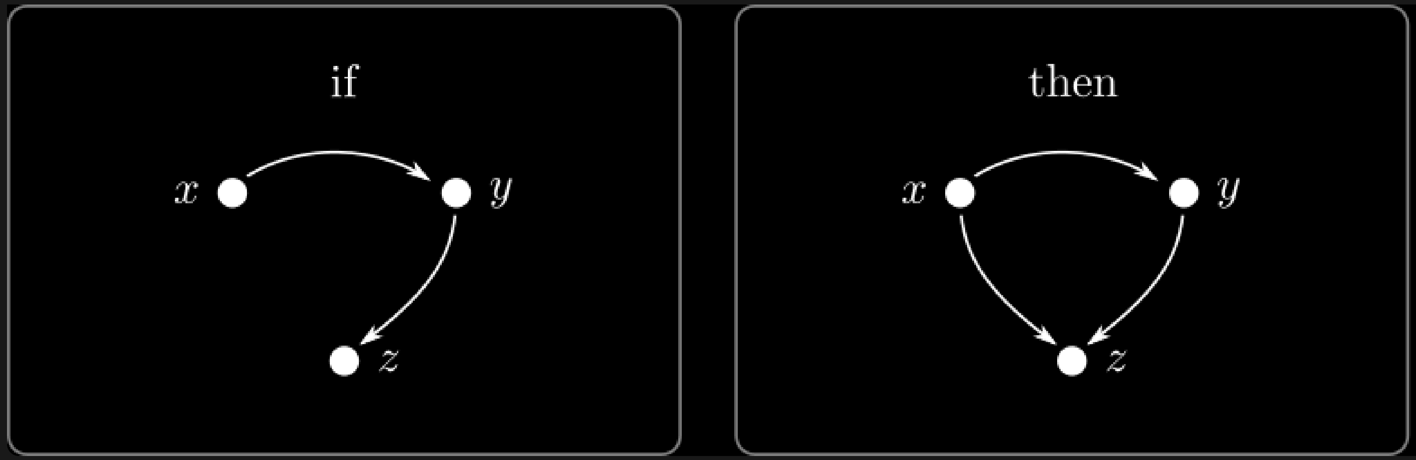
PICTURES



reflexive



symmetric



transitive

EXAMPLES — GOOD FOR CLASS

Let R be the relation “is a subset of” on $\mathcal{P}\left(\mathbb{Z}\right)$

Let R be the relation “lives within 10km of” on the set of people watching now.

CONGRUENCE

CONGRUENCE MODULO n

THEOREM:

Let $n \in \mathbb{N}$ then the relation of congruence modulo n is reflexive, symmetric and transitive.

Scratch work

- Let n be a fixed real number.
- Recall that $a \equiv b \pmod{n}$ when $n \mid (a-b)$ — *must* know definitions
- Three things to prove, so three sub-proofs
- This uses

$$P \implies (Q \wedge R \wedge S) \equiv (P \implies Q) \wedge (P \implies R) \wedge (P \implies S)$$

REFLEXIVE

congruence modulo n is reflexive

Scratch work

- Need to show $\forall a \in \mathbb{Z}, n \mid (a - a)$
- So let a be any integer, then $a - a = 0 = n \cdot 0$
- Hence $n \mid (a - a)$.

PROOF.

Fix $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. Then since $(a - a) = n \cdot 0$, it follows that $n \mid (a - a)$. Hence $a \equiv a \pmod{n}$ as required.

SYMMETRIC

congruence modulo n is symmetric

Scratch work

- Need to show $\forall a, b \in \mathbb{Z}, (n \mid (a-b)) \implies (n \mid (b-a))$
- So let a, b be any integers, and assume that $n \mid (a-b)$
- Hence $a - b = n \cdot k$ and thus $b - a = n(-k)$

PROOF.

Fix $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. Assume that $a \equiv b \pmod{n}$, and so $(a-b) = n \cdot k$ for some $k \in \mathbb{Z}$.

This tells us that $(b-a) = n(-k)$ and so $n \mid (b-a)$ and thus $b \equiv a \pmod{n}$ as we needed.

TRANSITIVE

congruence modulo n is transitive

Scratch work

- Need to show $\forall a, b, c \in \mathbb{Z}, (n \mid (a-b)) \wedge (n \mid (b-c)) \implies (n \mid (a-c))$
- So let a, b, c be any integers, and assume that $n \mid (a-b)$ and $n \mid (b-c)$
- Hence $a-b = n \cdot k$ and $b-c = n \cdot \ell$
- We need to say something about $a-c$ — easy! $a-c = n(k+\ell)$

PROOF.

Fix $n \in \mathbb{N}$, and let $a, b, c \in \mathbb{Z}$. Assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. So $a-b = nk, b-c = n\ell$ for some $k, \ell \in \mathbb{Z}$

Hence $(a-c) = n(k+\ell)$ and so $n \mid (a-c)$ and thus $a \equiv c \pmod{n}$ as we needed.