Lecture 10

Tuesday, September 29, 2020 12:05 PM

Lecture 10 : Equivalence Relations

← crucial for MODULAR ARITHMETIC ! (also in any algebra class)

Def: Let X be a set ($X = \mathbb{Z}$), an equivalence relation is a relation on X (given $a, b \in X$, a relation tells you whether $a \sim b$ or not. "a relates to b") such that

(1) REFLEXIVE : $a \sim a$, $\forall a \in X$ (for all elts in X)

(2) SYMMETRIC : if $a \sim b$, then $b \sim a$.

(3) TRANSITIVE : if $a \sim b$, $b \sim c$, then $a \sim c$.

Example: $X = \mathbb{Z}$, the relation is $a \sim b$ iff $a - b$ is even, i.e. divisible by 2.

$1 \not\sim 2$, $41 \sim 70$, $11 \sim 13$. In general, $a \sim b$ iff a, b same parity, i.e. both odd or both even.

$5 \sim 7$, $48 \sim 52$, $-71 \not\sim 122$ $\Longrightarrow$ we check this an $\boxed{\text{EQUIVALENCE RELATIONS}}$

Non-example: $X = \mathbb{Z}$, relation is $a \sim b$ iff $a \leq b$. This is NOT an equivalence relation.

(1) REFLEXIVE ? ($a \leq a$? true ✓)

(2) SYMMETRIC ? $3 \sim 5$ bc $3 \leq 5$ but $5 \not\sim 3$ bc $5 \not\leq 3$. No!

(3) TRANSITIVE ? Yes.

§2. Modular arithmetic : "INTEGERS MODULO n"

Let $X = \mathbb{Z}$ and $n \in \mathbb{N}$ a natural number. (for each n we define)

Def: (Relation modulo n) We say $a \sim b$ modulo n, and write $a \equiv b \mod n$, (can also write $a \equiv b \ (n)$) if $a - b$ is divisible by $n \in \mathbb{N}$. ← "people in same team if the remainder by n are same"

Examples: (the same example as previous slide!)

1. $\boxed{n=3}$

$0 \overset{?}{\sim} 4$ ✗	$11 \overset{?}{\sim} 27$ ✗	$19 \overset{?}{\sim} -1$ ✗
$1 \sim 4$ ✓	$-1 \overset{?}{\sim} 4$ ✗	$-3 \overset{?}{\sim} -4$ ✗
$5 \sim 7$ ✗	$-2 \overset{?}{\sim} -5$ ✓	$0 \overset{?}{\sim} 120$ ✓

2. $\boxed{n=5}$

$0 \overset{?}{\sim} 4$ ✗	$11 \overset{?}{\sim} 27$ ✗	$19 \overset{?}{\sim} -1$ ✓
$1 \overset{?}{\sim} 4$ ✗	$-1 \overset{?}{\sim} 4$ ✓	$-3 \overset{?}{\sim} -4$ ✗
$5 \sim 7$ ✗	$-2 \overset{?}{\sim} -5$ ✗	$0 \sim 120$ ✓

3. $\boxed{n=2}$

$0 \overset{?}{\sim} 4$ ✓	$11 \overset{?}{\sim} 27$ ✓	$19 \sim -1$ ✓
$1 \overset{?}{\sim} 4$ ✗	$-1 \overset{?}{\sim} 4$ ✗	$-3 \overset{?}{\sim} -4$ ✗
$5 \overset{?}{\sim} 7$ ✓	$-2 \overset{?}{\sim} -5$ ✗	$0 \sim 120$ ✓

Prop. 6.24: (modulo n is an equivalence) Let $X = \mathbb{Z}$, $n \in \mathbb{N}$ and "$\equiv \mod n$" the relation $a \equiv b \mod n$ iff $a - b$ divisible by n. Then:

(1) It is REFLEXIVE : $a \equiv a \mod n$? Yes, $a - a = 0$ is divisible by n. ✓

(2) It is SYMMETRIC : $a \equiv b \mod n$ imply $b \equiv a \mod n$? Yes, $n \mid a - b$ iff $n \mid b - a$. ✓

(3) It is TRANSITIVE : if $a \equiv b \mod n$, $b \equiv c \mod n$, is it true $a \equiv c \mod n$?

$$\left.\begin{aligned} a \equiv b \mod n &\Leftrightarrow n \mid a-b \\ b \equiv c \mod n &\Leftrightarrow n \mid b-c \end{aligned}\right\} \Rightarrow n \mid (a-b)+(b-c) \Rightarrow a \equiv c \mod n \text{ i.e. } n \mid a-c.$$

→ this shows modulo n is an equivalence relation!