MATH 2301

03 August 2022

* Last time : Equivalence classes

Let R be an equivalence relation on a set S

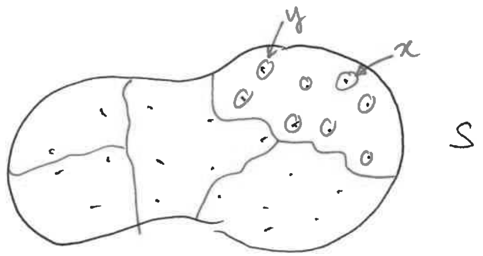
Let $x \in S$.

The equivalence class of x, denoted $[x]_R = [x]$

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

Proposition

1) If $y, z \in [x]$, then $y \sim_R z$, i.e. $(y,z) \in R$.
2) If $y \notin [x]$, and $z \in [x]$, then $y \nsim_R z$, i.e, $(y,z) \notin R$.
3) If $y \in [x]$, then $x \in [y]$, and in fact, $[x] = [y]$
4) If E_1 and E_2 are two equivalence classes, then either $E_1 = E_2$, or $E_1 \cap E_2 = \emptyset$.



Pf sketch:

1) If $y, z \in [x]$, then $(x,y) \in R$ & $(x,z) \in R$
   By symmetry + transitivity, $(y,z) \in R$

2) $y \notin [x]$, $z \in [x]$ Want to show that $y \nsim z$.

   If $y \sim z$, we'd have $(y,z) \in R \Leftrightarrow (z,y) \in R$.
   Since $z \in [x]$, we have $(x,z) \in R$
   $\Rightarrow (x,y) \in R$ by transitivity ← definitely false, because $y \notin [x]$

   $\Rightarrow y \nsim z$.

3) If $y \in [x] \Rightarrow (x,y) \in R$
   By symmetry, $(y,x) \in R \Rightarrow y \in [x]$
   Exercise : Use properties of R to show that $[x] = [y]$

4) Let E_1 & E_2 be equivalence classes.
   If $E_1 \cap E_2 = \emptyset$ then we're done.
   If $x \in E_1$ and $x \in E_2$, then ?
   Suppose $E_1 = [y]$, $E_2 = [z]$
   $\Rightarrow (y,x) \in R$ and $(z,x) \in R$
   $\Rightarrow (y,z) \in R$, and $(z,y) \in R \Rightarrow y \in [z]$,
   $z \in [y] \Rightarrow [y] = [z]$

Notation

Let E be an equivalence class.
If $a \in E$, then a is called a representative of E, and $E = [a]$

Modular arithmetic

Example $S = \mathbb{Z}$ integers.

1) $R_2 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y$ is divisible by $2\}$
(an equivalence relation).

2) $R_{15} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y$ is divisible by $15\}$

Question

Equivalence classes of R_2?

Note: If x, y are ~~ev~~ both even then $x \sim y$
If x, y are both odd, then ~~...~~ $x \sim y$
If one even & the ~~od~~ other is odd, then $x \not\sim y$

$\Rightarrow$ $[2] = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$
$\| $
$[-56] = [6] = [0] \ldots$

$[17] = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$
$\|$
$[-57] = [1] = [13] = \ldots$

The set of equivalence classes of R_2 is $\{[5], [22]\}$

odds evens

Equivalence classes of R_5?

(rem. 4) $[9] = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\} = [4]$

(rem. 0) $[0] = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} = [0]$

(rem. 1) $[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\} = [1]$

(rem. 2) $[7] = \{\ldots, -8, -3, 2, 7, 12, \ldots\} = [2]$

(rem. 3) $[3] = \{\ldots -7, -2, 3, 8, 13, \ldots\} = [3]$

In general, you can write R_d for any positive integer d:
$\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid (x-y)$ is divisible by $d\}$

R_d will have exactly d equivalence classes.
The standard labelling is:
$[0]_d, \quad [1]_d, \quad [2]_d, \quad [3]_d, \quad \ldots \quad [d-1]_d.$

$[0]_d = [-5d]_d$, $[3]_d = [3d+3]_d$

* **Modular addition.**

Consider R_d.

Set $\mathbb{Z}_d :=$ set of equivalence classes of R_d

$$\mathbb{Z}_d = \{[0], [1], \ldots, [d-1]\}$$

We'll define an operation $+_d$ or $+$ on $\mathbb{Z}_d$

as follows:

$[r] +_d [s] := [r+s]$

Is this well-defined? $\to$ Next time.