Typed-up notes for Week 2
& Week 3
have been uploaded onto
the Week 2 tab!

I'll edit them a bit more
next week though.

Office hours Friday 11-12
MB-B21

Wednesdays 1-2
Learning Cafe

Last Monday

Equivalence relation R on a set S.

We write

$$[a] = [a]_R$$

for $a \in S$

to mean

$$\{b \in S \mid aRb\}.$$

In particular, if R is an equivalence relation.

then $[a] = [b]$

for any $b \in S$

aRb.

equivalence class represented by a.

[Key issue: (6)

n, m positive integers.

Q: $\boxed{n^2 \mid m^2 \Rightarrow n \mid m\ ?}$

To prove this we use

the fundamental theorem of arithmetic

$$n = \prod_{p} p^{r_p} \qquad r_p \geq 0 \quad \forall p$$

product

$$= p_1^{r_1} \cdot p_2^{r_2} \cdots\cdots$$

p_i's are distinct primes.

Def S a set.

A partion $\mathcal{P}$ of S

is a set of subsets of S

satisfying the conditions

- $\emptyset \notin \mathcal{P}$

- If A & $B \in \mathcal{P}$

  (i.e. A & B are subsets of S in $\mathcal{P}$)

  & distinct,

then $A \cap B = \emptyset$

- The union of all $A \in P$ is S.

Theorem 9

$$\left\{ \begin{array}{c} \text{partions } P \\ \text{of } S \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{equivalence} \\ \text{relations } R \end{array} \right\}$$

on S

$$\{ \underbrace{[a]_R}_{\text{a subset of } S} \}_{a \in S} \longleftarrow\!\shortmid R$$

$P \longmapsto$ Define $a \mathcal{R} b$

if a & b lie

in the same

$A \in P$

Let's prove Theorem 9!

Suppose we are given an equiv. relation $\mathcal{R}$ on S.

We need to check that

$\{ [a]_R \}$

satisfies the conditions for partion.

- No element of $\{[a]_R\}$ is ϕ.

Since R is <u>reflexive</u>,

$$a \in [a]_R$$

Therefore $[a]$ is non-empty.

- If $[a]$ and $[b]$ are distinct,

then $[a] \cap [b] = \phi$

Equivalently,

$$\boxed{\begin{array}{l}\text{if } [a] \cap [b] \neq \phi, \\ \text{then } [a] = [b].\end{array}}$$

By assumption,

$$\exists\ c \in \underbrace{[a] \cap [b]}_{\neq \phi}$$

$\Rightarrow \quad c \in [a]$

$c \in [b]$

$\Rightarrow \quad aRc$ ... (*)

i.e. bRc hold.

That means cRb also holds ... (**)

(because R is symmetric)

Since R is transitive

(*) (**) $\Rightarrow aRb$

$\Rightarrow \quad [a] = [b].$

- The union T of $[a]$'s $a \in S'$ equals S'.

We need to check

① $S' \subseteq T$

② $T \subseteq S'$.

① By definition

$\forall a \in S'$, $\quad [a] \subseteq S'$

$$[a] = \{ b \in S' \mid aRb \}$$

Therefore

$$T \subseteq S'.$$

(I've used the fact that

$$U \subseteq S'$$

$$V \subseteq S'$$

then $\quad U \cup V \subseteq S'$)

② $S \subseteq T$?

Let a be an element in S.

(GOAL: $a \in T$)

The equivalence

$$[a] \subseteq T$$

OTOH,

$$a \in [a]$$

Therefore, $a \in T$. $\square$.

We've just proved that

equiv. relation R $\Longrightarrow$ partion P.

Conversely, suppose we are given a partion P,

we need to check that the relation R

(defined s.t. aRb $\Leftrightarrow$ a & b lies in a part in P.

satisfies the conditions.

(Exercise! Do it!)

Also check that

R so defined is

unique.

3.2 Congruences mod n.

Let n be a positive integer

Def We define a relation

$$\equiv$$

on $S = \mathbb{Z}$ (the integers)

by: $a, b \in \mathbb{Z}$

$$a \equiv b \pmod{n}$$

(a is congrent to b mod n)

if and only if n divides

$b - a$

$(\text{or } a - b)$

<u>Prop 10</u> $\equiv$ is an equivalence relation on $\mathbb{Z}$.

(congruence mod n relation)

According to Theorem 9, this defines a partion on $\mathbb{Z}$.

What is it?

$$\{[0],\ [1],\ \cdots\cdots,\ [n-1]\}$$

$$[0] = [n] = [2n] = \cdots$$

$$[1] = [n+1] = [-n+1] = [-3n+1]$$

By Theorem 9, we know that every integer belongs to exactly one [ ] above.