CSE 16 8-9-22

- SETs : response ≥ ~~85%~~ 80% → + 0.1% score

Theorem

Given a partition of set A:

$$P = \{ S_i \subseteq A \mid i = 1, 2, 3, \dots \},$$

there exists a unique equiv. rel. R on A whose eq. classes [a] are exactly the members S_i of P. i.e.

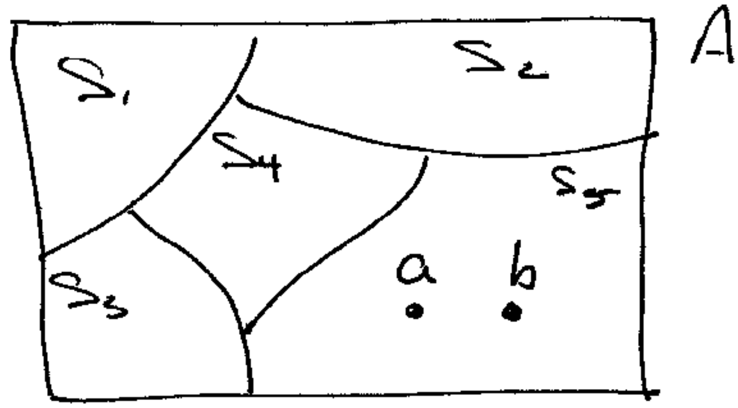
$$P = \{ [a]_R \mid a \in A \}$$

Proof:

Define a relation $R \subseteq A \times A$ by

$$R = \{ (a,b) \mid \exists i : a,b \in S_i \}$$

i.e. aRb iff a and b belong to the same member S_i of P.



We must show R is an eq. relation.

Reflexive ✓

By Part (3) of defn. of Partition, each $a \in A$ lies in some S_i of P. Thus aRa for all $a \in A$.

<u>Symmetric</u> ✓

let $a, b \in A$ and suppose aRb. Then $a, b \in S_i$ for some i. $\therefore$ $b, a \in S_i$.
$\therefore$ bRa.

<u>transitive</u> ✓

let $a, b, c \in A$, and suppose both aRb and bRc. We have

$$\exists i \quad : \quad a, b \in S_i$$

and

$$\exists j \quad : \quad b, c \in S_j .$$

But then $b \in S_i \cap S_j$, so $S_i \cap S_j \neq \emptyset$. By part (2), we have $i = j$. Thus $a, c \in S_i$, hence aRc.

We've shown R is an eq. relation. We must show the eq. classes $[a]$ are the members S_i of P.

Let $[a]$ be an eq. class of R. Then $a \in [a]$. By (3) $a \in S_i$ for some i. But if $x \in A$:

$$x \in [a] \text{ iff } xRa \text{ iff } x \in S_i$$

Therefore $[a] = S_i$.

Let $S_i \in P$. By (1), $S_i \neq \emptyset$ so there exists $a \in S_i$. Again

$$x \in [a] \text{ iff } xRa \text{ iff } x \in S_i,$$

whence $S_i = [a]$.

still to show: R is unique.
leave as exercise. ∎

<u>Exercise</u>
Let R_1, R_2 be equiv. relations on a set A, and suppose R_1 and R_2 have exactly the same equiv. classes. Prove $R_1 = R_2$.

(11.5) Integers Modulo n

The eq. classes of $\equiv_n$ $(n \in \mathbb{N})$ are called

- <u>congruence classes</u> mod n

or

- <u>residue classes</u> mod n.

<u>notation</u>: $[a]_n$ or $[a]$

<u>Defn.</u>

Given $n \in \mathbb{N}$, the set of residue classes mod n is denoted $\mathbb{Z}_n$.

Thus

$$\mathbb{Z}_n = \{ [a]_n \mid a \in \mathbb{Z} \}$$
$$= \{ \{ a + kn \mid k \in \mathbb{Z} \} \mid a \in \mathbb{Z} \}$$

we now know: $\mathbb{Z}_n$ forms a Partition of $\mathbb{Z}$.

any $x \in [a]_n$ is called a <u>representative</u> of $[a]_n$, since $[x]_n = [a]_n$

It's common to choose representatives for $[\cdot]_n$ to be

$$\{0, 1, 2, \dots, n-1\}$$

i.e. the possible remainders on division by n. Thus

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

where

$$[0] = \{\dots, -2n, -n, 0, n, 2n, 3n, \dots\}$$

$$[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$$

$$\vdots$$

$$[a] = \{a + kn \mid k \in \mathbb{Z}\}$$

$$\vdots$$

$$[n-1] = \{(n-1) + kn \mid k \in \mathbb{Z}\}.$$

we can define operations

$$+, -, \cdot$$

on $\mathbb{Z}_n$.

Defn

Given $[a], [b] \in \mathbb{Z}_n$, let

$$[a]+[b] = [a+b],$$

$$[a]-[b] = [a-b]$$

and

$$[a]\cdot[b] = [a\cdot b].$$

we must show that these operations are <u>well defined</u>, i.e. if we choose different representatives for $[a]$ and $[b]$, we get same result.

Lemma

If $[a']_n = [a]_n$ and $[b']_n = [b]_n$, then

$$[a+b]_n = [a'+b']_n,$$
$$[a-b]_n = [a'-b']_n$$
and
$$[ab]_n = [a'b']_n$$

Proof:

This follows from:

$a \equiv_n a'$ and $b \equiv_n b'$ imply:

(i) $a+b \equiv_n a'+b'$

(ii) $a-b \equiv_n a'-b'$

(iii) $ab \equiv_n a'b'$

which was previously proved.

we show (iii) only:

$$a \equiv_n a' \rightarrow n \mid a-a' \rightarrow a-a' = k_1 n \quad (k_1 \in \mathbb{Z})$$

and

$$b \equiv_n b' \rightarrow n \mid b-b' \rightarrow b-b' = k_2 n \quad (k_2 \in \mathbb{Z}).$$

Then

$$\begin{aligned} ab - a'b' &= (ab - a'b) + (a'b - a'b') \\ &= (a-a')b + (b-b')a' \\ &= k_1 n \cdot b + k_2 n \cdot a' \\ &= (k_1 b + k_2 a') n \end{aligned}$$

$\therefore \quad n \mid (ab - a'b')$

$\therefore \quad ab \equiv_n a'b'.$ $\blacksquare$

Ex. $+$ and $\cdot$ for $\mathbb{Z}_2 = \{[0], [1]\}$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Ex. $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Ex $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

← exercise

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exercise: $\mathbb{Z}_3$, $\mathbb{Z}_6$, $\mathbb{Z}_7$

"hw8": do not turn in

(11.4) # 2, 6

(11.5) # 2, 4, 6

12.1 Functions

<u>Defn</u>

Let A, B be sets. A <u>function</u> f from A to B is a relation

$$f \subseteq A \times B$$

from A to B with the property:

For all $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

we call A the <u>domain</u> of f

$$A = \mathrm{dom}(f)$$

and B the <u>codomain</u> of f

$$B = \mathrm{codom}(f).$$

<u>Notation</u>

write $f: A \to B$ to mean f is a function with domain A and codomain B.

Given $a \in A$, write $f(a)$ for the unique $b \in B$ s.t. $(a,b) \in f$, i.e.

$$b = f(a)$$

As a set:

$$f = \{ (a, f(a)) \mid a \in A \} \subseteq A \times B$$

sometimes called graph(f).