Let $m \in \mathbb{Z}^+$, then eq. class of a (with respect to $\equiv_m$) is

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

Ex. $m = 2$

$x \in [0]$ iff $x = 2k$
iff x is even

$x \in [1]$ iff $x = 2k+1$
iff x = odd

so

$[0] = [2] = [4] = \dots = \{\text{even \#s}\}$

$[1] = [3] = [5] = \dots = \{\text{odd \#s}\}$.

Ex. $m = 3$

$x \in [0]$ iff $x = 3k$ (some k)

$x \in [1]$ iff $x = 3k+1$ "

$x = [2]$ iff $x = 3k+2$ "

For general $m \in \mathbb{Z}^+$, we can divide any $x \in \mathbb{Z}$ by m:

$$x = km + r \quad (0 \le r < m)$$

$\therefore$ $x \in [r]$.

So the classes $[0], [1], [2], \ldots, [m-1]$ are <u>all</u> the eq. classes of $\equiv_m$.

Problems (11.3) 2, 4, 6, 8, 10, 12

11.4 Eq. Classes and Partition

Recall a <u>Partition</u> of A is a set of subsets $S_i \subseteq A$ (for $1 \le i \le k$)

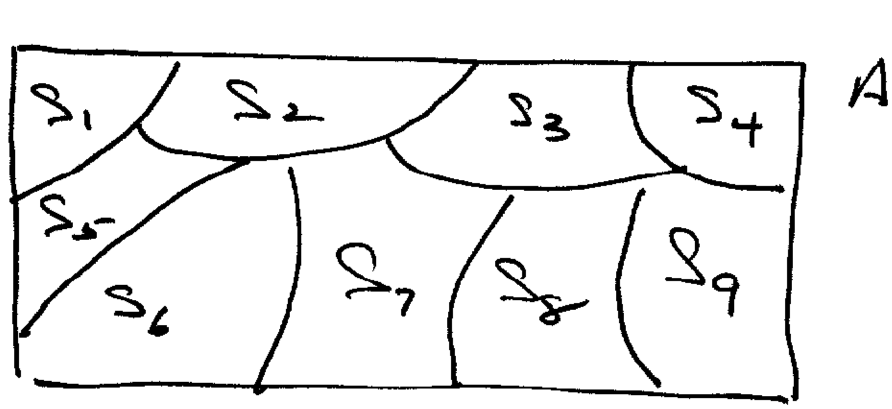
$$P = \{ S_i \mid 1 \le i \le k \} \subseteq \mathbb{P}(A)$$

such that

(i) $S_i \neq \emptyset$

(ii) $S_i \cap S_j = \emptyset \quad (1 \le i < j \le k)$

(iii) $\bigcup_{i=1}^{k} S_i = A$



Theorem

Let R be an eq. relation on A. Then the set of eq. classes of R

$$\{[a] \mid a \in A\} \subseteq \mathbb{P}(A)$$

forms a partition of A.

Proof.

for any $a \in A$, we have $a \in [a]$ since aRa (by reflexive). This shows

$$[a] \neq \emptyset$$

proving (i).

Similarly $\{a\} \subseteq [a]$, so

$$A = \bigcup_{a \in A} \{a\} \subseteq \bigcup_{a \in A} [a] \subseteq A$$

$$\therefore \quad A = \bigcup_{a \in A} [a]$$

Proving part (iii) (defn of Partition).

Finally we show $[a] \neq [b] \Rightarrow [a] \cap [b] = \phi$, for any $a, b \in A$, establishing (ii). We prove this by contraposition, i.e.

$$[a] \cap [b] \neq \phi \Rightarrow [a] = [b]$$

Assume $[a] \cap [b] \neq \phi$, say $c \in [a] \cap [b]$.

Then

$c \in [a] \Rightarrow c R a \Rightarrow a R c$ (symmetric)

$c \in [b] \Rightarrow c R b$

$\therefore$ aRb (transitive)

It follows that $[a] = [b]$, proving (ii). $\blacksquare$

<u>Theorem</u>

Given a Partition

$$P = \{S_i \mid 1 \le i \le k\}$$

of the set A, there exists a unique eq. relation R on A, whose eq. classes are exactly the members S_i of P, i.e.

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

Proof.

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

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

In other words: aRb iff both a and b lie in the same member of the Partition P. We must show that R is an eq. relation.

Reflexive

By part (iii), each $a \in A$ lies in some member S_i of P. Therefore aRa, for all $a \in A$. $\therefore$ R is reflexive.

<u>symmetric</u>

Let $a, b \in A$ and suppose aRb.

Then $a, b \in S_i$ for some i $(1 \le i \le k)$.

Thus $b, a \in S_i$, whence bRa,

and therefore R is symmetric.

<u>transitive</u>

Let $a, b, c \in A$ and suppose both

aRb and bRc. Then we have

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

and

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

But then $b \in S_i \cap S_j$, so $S_i \cap S_j \neq \emptyset$.

By Part (ii), we have $i = j$.

So $a, c \in S_i$ and aRc.

This proves R is transitive

we've shown R is an eq. rel. on A, It remains to show the eq. classes of R are exactly the members of P.

Let [a] be such an eq. class, where $a \in A$. Then, by (iii) $a \in S_i$ for some i $(1 \le i \le k)$. But

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

therefore $[a] = S_i$.

Let S_i be a member of P. By Part (i), $S_i \neq \phi$ so $a \in S_i$ for some $a \in A$.

But again

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

so $\therefore$ $S_i = [a]$.

leave as exercise: show R is unique.

Exercise

Let R_1, R_2 be eq. relations on A, and suppose R_1 and R_2 have the same eq. classes. Then prove that $R_1 = R_2$.

Problems (11.4): 2, 6

11.5 Integers modulo n

The eq. classes of $\equiv_n$ (for $n \in \mathbb{Z}^+$) are usually called

- congruence classes mod n

or

- residue classes mod n

notation write $[a]_n$ if necessary to specify n.

Defn

Given $n \in \mathbb{Z}^+$, the set of residue classes mod n is denoted: $\mathbb{Z}_n$

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

As we've seen, $\mathbb{Z}_n$ forms a partition of $\mathbb{Z}$.

Any $x \in [a]$ is called a <u>representative</u> of the class $[a]$ since

$$[x] = [a]$$

It's common to choose representatives to be

$$0, 1, 2, \ldots, n-1$$

i.e. possible remainders on div. by n. Thus

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

where

$$[0] = \{kn \mid k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \dots\}$$

$$[1] = \{1+kn \mid k \in \mathbb{Z}\} = \{\dots\dots\}$$

$$[2] = \{2+kn \mid k \in \mathbb{Z}\}$$

$$\vdots$$

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

There's a simple way to define arithmetic $(+, -, \cdot)$ on $\mathbb{Z}_n$.

<u>Defn</u>

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

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

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

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

It's necessary to prove these operations are consistent, i.e. they do not depend on particular representatives $a \in [a]$ and $b \in [b]$

suppose

$$a' \in [a] \quad \text{so} \quad [a'] = [a]$$

and

$$b' \in [b] \quad \text{so} \quad [b'] = [b]$$

we must show:

$$[a' + b'] = [a + b]$$

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

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

This follows from

<u>Theorem</u>

If $a' \equiv a \pmod{n}$ and $b' \equiv b \pmod{n}$,

then

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

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

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

<u>Exercise</u>: Prove this thm.

<u>Ex.</u> $+, \cdot$ for $\mathbb{Z}_2$

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

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

<u>Ex.</u> $+, \cdot$ for $\mathbb{Z}_3$

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

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Exercise

write $+, \cdot$ table for:

$$\mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_7$$

book

Problems: (11.5) 2, 4, 6