cse 16 3-10-22

- SETs : due sunday ✓
- quiz 5 : tonight ✓

Theorem

Given a Partition of a set A

$$P = \{ S_i \mid 1 \leq i \leq k \},$$

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

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

Proof.

Define $R \subseteq A \times A$ by

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

In other words aRb iff both a and b belong to the same member of P. We must show R is an equivalence relation.

reflexive

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

Symmetric

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

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

$\therefore$ $b, a \in S_i$, and $\therefore$ bRa. We've shown R is symmetric.

Transitive

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 $S_i \cap S_j \neq \emptyset$. Part (ii) now implies $i = j$. Thus $a, c \in S_i$, and $\therefore$ aRc $\therefore$ R is transitive.

we've shown R is an eq. rel.

we now 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 Part (iii) $a \in S_i$ for some $1 \le i \le k$. But

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

$$\therefore \quad [a] = S_i$$

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

$x \in S_i$ iff xRa iff $x \in [a]$,

so that $S_i = [a]$.

we've shown that the eq. classes of R are exactly the members of $\mathcal{P}$.

exercise! Prove R is unique. $\blacksquare$

<u>Exercise</u>

Let R_1, R_2 be eq. relations on a set A, and suppose R_1 and R_2 have exactly the same eq. classes. Prove that $R_1 = R_2$.

11.5 Integers modulo n

Recall $\equiv_n$ is an eq. relation on $\mathbb{Z}$, for all $n \in \mathbb{N}$. The eq. classes of $\equiv_n$ are called

- congruence classes mod n

or

- residue classes mod n

<u>Notation</u>: $[a]_n$ to specify n, if necessary.

<u>Defn</u>

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

Thus

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

we've seen $\mathbb{Z}_n$ 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 the representatives of classes in $\mathbb{Z}_n$ to be

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

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

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

where

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\}$$
$$[1] = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}$$
$$\vdots$$
$$[r] = \{r + kn \mid k \in \mathbb{Z}\}.$$
$$\vdots$$
$$[n-1] = \{(n-1) + kn \mid k \in \mathbb{Z}\}$$

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

<u>Defn</u>

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

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

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

and

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

we must prove that these ops. are well defined, i.e. if we choose different representatives of $[a]$ and $[b]$ we get the same results.

Lemma

If $a' \in [a]$ (so $[a'] = [a]$) and $b' \in [b]$ (so $[b'] = [b]$), then

$$[a' + b'] = [a + b],$$
$$[a' - b'] = [a - b]$$
and
$$[a' \cdot b'] = [a \cdot b].$$

This follows from a prior theorem

Theorem

If $a' \equiv_n a$ and $b' \equiv_n b$ then

$$a' + b' \equiv_n a + b$$
$$a' - b' \equiv_n a - b$$
$$a' \cdot b' \equiv_n a \cdot b$$

<u>Proof</u> (of $a' \cdot b' \equiv_n a \cdot b$):

we have

$$a' - a = k_1 n \quad (\text{some } k_1 \in \mathbb{Z})$$

and $b' - b = k_2 n \quad (\text{"} \quad k_2 \in \mathbb{Z})$

Then

$$a' \cdot b' - a \cdot b = a' \cdot b' - a \cdot b' + a \cdot b' - a \cdot b$$

$$= (a' - a) \cdot b' + (b' - b) \cdot a$$

$$= k_1 n \cdot b' + k_2 n \cdot a$$

$$= (k_1 b' + k_2 a) n$$

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

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

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

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

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

$[0] = \{2k \mid k \in \mathbb{Z}\} = \{\text{even \#s}\}$

$[1] = \{2k+1 \mid k \in \mathbb{Z}\} = \{\text{odd \#s}\}$

note: $(\equiv_2)$ = "same Parity relation".

Exercise

same thing for $\mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$.

Review Problems

- slight re-statement of 11.3 #16

Define $A = \{(a,b) \mid a,b \in \mathbb{Z},\ b \neq 0\}$

$$= \mathbb{Z} \times (\mathbb{Z} - \{0\})$$

Define R on A by

$(a,b)\,R\,(c,d)$ iff $ad = bc$

i.e.

$$R = \{((a,b),(c,d)) \mid a,b,c,d \in \mathbb{Z},\ b \neq 0,\ c \neq 0,\ ad = bc\}$$

show R is an eq. relation.

Proof:

reflexive

show $(a,b) R (a,b)$

i.e. $a \cdot b = b \cdot a$ ✓

symmetric

show $(a,b) R (c,d) \Rightarrow (c,d) R (a,b)$

i.e. $ad = bc \Rightarrow cb = da$ ✓

Transitive

show: $(a,b) R (c,d)$ and $(c,d) R (e,f)$

$\Rightarrow (a,b) R (e,f)$, i.e.

$ad = bc$ and $cf = de \Rightarrow af = be$.

$\Downarrow$ $\Downarrow$

$adf = bcf$ and $bcf = bde$

$\Rightarrow adf = bde \Rightarrow af = be$ ✓

11.2 # 2

$$A = \{a, b, c\}$$

$$R = \{(a,b), (a,c), (c,c), (b,b), (c,b), (b,c)\}$$

ref. : $\boxed{no}$, since $a \not R a$

symm: $\boxed{no}$, aRb but $b \not R a$

trans: $\boxed{yes}$

anti-sym: $\boxed{no}$ since bRc, cRb but $b \neq c$.

digraph