Lecture 6

Proposition: Let R be an equivalence relation on a set A and $a, b \in A$.

$$aRb \text{ if and only if } [a] = [b]$$

Proof:

($\Rightarrow$) WTS (want to show) $[a] = [b]$, i.e. $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

* $[a] \subseteq [b]$

  Let $x \in [a]$, then xRa. By hypothesis, aRb. Then xRb by transitivity.

* $[b] \subseteq [b]$

  Let $x \in [b]$, then xRb. Since aRb, then bRa by symmetry. Thus, xRa by transitivity.

($\Leftarrow$) By reflexivity, aRa, hence $a \in [a]$. By hypothesis, $a \in [b]$. Then, aRb.

Corollary: Let R be an equivalence relation on A. Then any two equivalence classes are either disjoint or identical.

A, B sets

$A \cap B = \phi$

$A = B$

$A \cap B \neq \phi$

Proof: Let $[a]$ and $[b]$ be equivalence classes.

If $[a] \cap [b] \neq \phi$, $\exists\, c \in [a] \cap [b]$. Then, cRa and cRb.

By symmetry aRc, thus aRb by transitivity. By the previous Proposition $[a] = [b]$.

Question: Do the equivalence classes of R give a partition of A?

Theorem: Let A be a nonempty set.

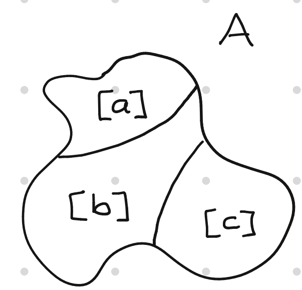
a) Let R be an equivalence relation on A. Then R yields a partition of A, $A/R := \{ [a] \mid a \in A \}$.

b) A partition $\mathcal{P}$ of A gives rise to an equivalence relation on A where $a R_{\mathcal{P}} b$ if and only if a, b are in the same subset.

A/R is called the quotient set of A by R.

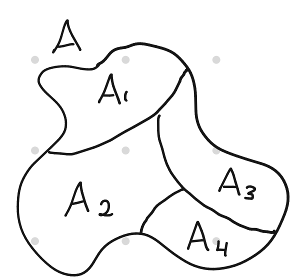
A mod R

$R \subseteq A \times A \rightsquigarrow [a], [b], [c]$ subsets of A $\rightsquigarrow$



$A/R = \{[a], [b], [c]\}$

$\mathcal{P} = \{A_1, A_2, A_3, A_4\}$



$\rightsquigarrow R_{\mathcal{P}} \subseteq A \times A$

Proof:

a) WTS: (1) Elements of $\mathcal{P}$ are mutually disjoint.

It follows from Corollary.

(2) $\bigcup_{a \in A} [a] = A$, i.e., $\bigcup_{a \in A} [a] \subseteq A$ ✓ by def and $A \subseteq \bigcup_{a \in A} [a]$

For all $a \in A$, $a \in [a]$. Thus, $A \subseteq \bigcup_{a \in A} [a]$.

b) See examples.

$$\underset{\text{ER}}{\left\{ \begin{array}{l} \text{Equivalence Relations} \\ \text{on } A \end{array} \right\}} \xleftrightarrow{\text{correspondence}} \underset{\mathcal{P}}{\left\{ \begin{array}{l} \text{Partitions} \\ \text{of } A \end{array} \right\}}$$

$$R \overset{f}{\longmapsto} A/R$$

$$R_{\mathcal{P}} \underset{g}{\longleftarrow\!\!\!\shortmid} \mathcal{P}$$

$g \circ f = id_{ER}$

$f \circ g = id_{\mathcal{P}}$

$\blacksquare$

Ex: For all $x, y \in \mathbb{Z}$ define $x \sim y$ if $|x| = |y|$.

$\sim$ is an equivalence relation.

$$[x] = \{ y \in \mathbb{Z} \mid y \sim x \} = \{ y \in \mathbb{Z} \mid |y| = |x| \} = \{ y \in \mathbb{Z} \mid y = \pm x \} = \{-x, x\}$$

$$[2] = [-2] = \{-2, 2\} \qquad [0] = \{0\}$$

$$\mathbb{Z} = \bigsqcup_{a \in \mathbb{N}} [a] = \bigsqcup_{a \in \mathbb{N}} \{-a, a\}$$

$\bigsqcup$ denotes disjoint union

Ex: See previous example of equiv. rel. on $\mathbb{R}$ $\Longrightarrow$ $\mathbb{R} = \bigsqcup_{0 \leq a \leq \pi} \{ x \in \mathbb{R} \mid \cos x = \cos a \}$

Ex: See previous example of equiv. rel. on $\mathbb{R} \times \mathbb{R}$ $\Longrightarrow$ $\mathbb{R} \times \mathbb{R} = \bigsqcup_{a \in \mathbb{R}} \{ (a, y) \mid y \in \mathbb{R} \}$

Modular Arithmetic

Def: Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say a is congruent to b modulo n if $n \mid (a-b)$.

Notation: $a \equiv_n b$ or $a \equiv b \pmod{n}$ or $a \bmod n = b$

$a - b = nk$ for some $k \in \mathbb{Z}$ or b is the remainder of a divided by n

$$a = nk + b$$

Ex: $10 \equiv_5 0$ because $10 - 0 = 5 \cdot 2$ or because $10 \div 5$ has remainder 0.

$7 \equiv_5 2$ because $7 - 2 = 5 \cdot 1$ or because $7 \div 5$ has remainder 2.

Proposition 12: Congruence module n is an equivalence relation on $\mathbb{Z}$.

The equivalence class of a modulo n is denoted $[a]_n$

(or simply $[a]$ when there is no place for confusion).

Proof:

(1) Let $a \in \mathbb{Z}$. Since $a - a = 0 = n0$, then $a \equiv_n a$.

(2) If $a \equiv_n b$, then $\exists k \in \mathbb{Z}$ s.t. $a - b = nk$. Then $b - a = n(-k)$, i.e. $b \equiv_n a$.

(3) If $a \equiv_n b$ and $b \equiv_n c$, then $\exists k, l \in \mathbb{Z}$ s.t. $a - b = nk$ and $b - c = nl$.

Therefore, $a - c = (a-b) + (b-c) = n(k+l)$, i.e. $a \equiv_n c$.

Equivalence Classes of Congruence Module n

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv_n a\}$$
$$= \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z},\ x - a = nk\}$$
$$= \{\underbrace{a + nk}_{\text{multiples of } n \text{ plus } a} \mid k \in \mathbb{Z}\}$$

> $[a]_n$ is the set of all integers that when divided by n give remainder a.

Ex:

- $[0]_2 = \{2k \mid k \in \mathbb{Z}\}$ even $\qquad [1]_2 = \{1 + 2k \mid k \in \mathbb{Z}\}$ odd

- $[0]_3 = \{3k \mid k \in \mathbb{Z}\} = [3]_3$

  $[1]_3 = \{1 + 3k \mid k \in \mathbb{Z}\} = [4]_3$

  $[2]_3 = \{2 + 3k \mid k \in \mathbb{Z}\} = [5]_3$