READ APPENDICES A–D.

## EQUIVALENCE RELATIONS

Let $S$ be a set.

DEF A relation on $S$ is a subset $R \subseteq S \times S$, where $S \times S := \{(s_1, s_2) : s_1, s_2 \in S\}$

NOTATION If $(s,t) \in R$, we often denote this symbolically by $s \sim t$ or $sRt$ (etc...), w/ a symbol for the relation between the elements of $S$.

DEF An equivalence relation on a set $S$ is a relation $R$ w/ $(x,y) \in R$ denoted by $x \sim y$, satisfying:

(i) (REFLEXIVE) For all $x \in S$, $x \sim x$.

(ii) (SYMMETRIC) For all $x, y \in S$, if $x \sim y$, then $y \sim x$.

(iii) (TRANSITIVE) For all $x, y, z \in S$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

EX "=" on any set $S$

$$R := \{(x,x) : x \in S\} \subseteq S \times S$$

DEF If $\sim$ is an equivalence relation on $S$ and $a \in S$, then the equivalence class containing $a$ is the set

$$[a] := \{x \in S : x \sim a\}$$

(everything related to $a$)

DEF A partition $\mathcal{P}$ of a set $S$ is a collection of subsets of $S$ satisfying:

(i) $\bigcup_{X \in \mathcal{P}} X = S$ (every element of $S$ is in some subset in $\mathcal{P}$)

(ii) If $X, Y$ in $\mathcal{P}$, then either

$$\underbrace{X = Y}_{\text{contain exactly the same elements}} \quad \text{or} \quad \underbrace{X \cap Y = \emptyset}_{\text{no over-lap @ all}}.$$

EX $S = \{1, 2, 3, 4, 5, 6\}$

$$\mathcal{P} = \{\{1, 2, 6\}, \{3, 5\}, \{4\}\}$$

**THM** The equivalence classes of an equivalence relation form a partition of a set; conversely, given a partition $\mathcal{P}$ on a set $S$, one can define an equivalence relation on $S$ defined by $x \sim y$ iff there is $A$ in $\mathcal{P}$ such that $x, y \in A$.

**EX** $S = \{1, 2, 3, 4, 5, 6\}$

$$\mathcal{P} = \{ \{1, 2, 6\}, \{3, 5\}, \{4\} \}$$

Then the equivalence relation $\sim$ induced by the partition $\mathcal{P}$ satisfies:

$1 \sim 1$, $1 \sim 2$, $1 \sim 6$, $2 \sim 1$, $2 \sim 2$, $2 \sim 6$,

$3 \sim 3$, $3 \sim 5$, $4 \sim 4$, $5 \sim 3$, $5 \sim 5$,

$6 \sim 1$, $6 \sim 2$, $6 \sim 6$

(and no other pairs are related)

**IMPORTANT EXAMPLE**

set: $\mathbb{Z}$, the integers; fix $n \in \underbrace{\mathbb{N}}_{\text{positive integers}}$

Then $x \equiv y \pmod{n}$ iff $n \mid (x-y)$

"$x$ is congruent to $y$ modulo $n$"

"$n$ divides $(x-y)$" means: there exists $j \in \mathbb{Z}$ such that $(x-y) = n \cdot j$

<u>THM</u> Congruence modulo $n$ is an equivalence relation.

<u>Q</u>: What are the equivalence classes of this equivalence relation?

When $n = 1$, since $1 \mid (x-y)$ for <u>all</u> $x, y \in \mathbb{Z}$, $x \equiv y \pmod{1}$ for <u>all</u> $x, y \in \mathbb{Z}$

There is only <u>one</u> equivalence class, say $[0]$, and $[0] = \mathbb{Z}$.

<u>RECALL</u> <u>THM</u> (DIVISION ALGORITHM) Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then there exist <u>unique</u> $q, r \in \mathbb{Z}$ such that $a = bq + r$ <u>and</u> $0 \le r < b$.

EX $a = 43, \quad b = 25$

$43 = 25 \cdot 1 + 18$ $\quad q = 1, \ r = 18$
$0 \le 18 < 25$

$a = -5, \quad b = 7$

$-5 = 7 \cdot -1 + 2$ $\quad q = -1, \ r = 2$
$0 \le 2 < 7$

When $n = 2$, by the Division Algorithm, for any $x \in \mathbb{Z}$, $x = 2q + r$, where $r = 0$ or $r = 1$.

This means $2 \mid (x - r)$, and so every integer is related either to 0 or to 1, and the classes don't overlap (uniqueness part of Div. Alg.).

Thus the equivalence classes are:

$[0] = \{ \ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots \}$
(even integers)

$[1] = \{ \ldots, -5, -3, -1, 1, 3, 5, 7, \ldots \}$
(odd integers)

In general, by the Division Algorithm, $x = nq + r$, where $0 \leq r < n$, and $r$ is <u>unique</u>. Hence the equivalence classes of congruence modulo $n$ are $[0], [1], \ldots, [n-1]$.

<u>NOTATION</u> The set of all equivalence classes modulo $n$ is denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$.

Typically, for ease of notation, we will write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, knowing that by "$k$" we mean "$[k]$."