- Just like w/ 3 we'll usually write
$a \equiv b \pmod{n}$ for $a \equiv_n b$.

- Just like with 3, $\equiv_n$ is an equiv. relation for any fixed $n \in \mathbb{N}$.

Non-examples of equiv. relations:

① Consider $\leq$ (e.g. on $\mathbb{R}$): reflexive, symmetric, but not transitive. Hence not an equiv. relation.

② Consider the relation $\neq$ of inequality (e.g. on $\mathbb{Z}$):

symmetric since $n \neq m \Rightarrow m \neq n$
but not reflexive, since never $n \neq n$,
nor transitive (e.g. $2 \neq 4$ and $4 \neq 2$ but $2 = 2$)

Equivalence classes: Def'n: Sps R is an equiv. relation on A. Given $x \in A$, the equivalence class of x, denoted $[x]_R$, is the set of elements in A related to x by R

i.e. $[x]_R = \{y \in A \mid (x,y) \in R\}$

(note: by symmetry could have as well defined $[x]_R$ by $\{y \in A \mid (y,x) \in R\}$)

Warning: overloaded notation: we've used $[\,]$'s when defining $[n] = \{1, \dots, n\}$

↳ this is completely unrelated to meaning of $[x]_R$ for an equiv. relation R so don't get confused!

Ex's ① Consider the equality relation $=$ on $\mathbb{N}$. For any fixed $n \in \mathbb{N}$ we have:

$$[n]_= \text{ is } \{m \in \mathbb{N} \mid n = m\}$$

which is just $\{n\}$

e.g. $[1]_=$ is $\{1\}$, $[2]_=$ is $\{2\}$, etc.

② Let R denote the floor equiv. relation on $\mathbb{R}$: $(x,y) \in R$ iff $\lfloor x \rfloor = \lfloor y \rfloor$

- Now: fix $x \in \mathbb{R}$ and suppose $\lfloor x \rfloor = n$
- What is $[x]_R$?

by defn: $[x]_R = \{y \in \mathbb{R} \mid (x,y) \in R\}$

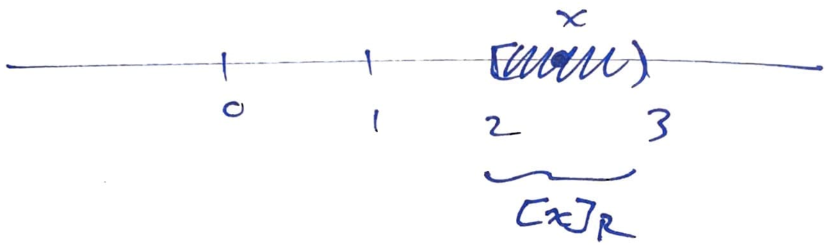
$= \{y \in \mathbb{R} \mid \lfloor x \rfloor = \lfloor y \rfloor\}$

$= \{y \in \mathbb{R} \mid n = \lfloor y \rfloor\}$

$= \{y \in \mathbb{R} \mid n \leq y < n+1\}$

$= [n, n+1)$

e.g. if $x = 2.34$ so that $\lfloor x \rfloor = 2$
then $[x]_R = [2,3)$



Notice: the equiv. classes of R form a partition of $\mathbb{R}$!

we're going to prove later: equiv. classes always partition the underlying set (in this case, $\mathbb{R}$)

③ Consider $\equiv_3$ on $\mathbb{Z}$. What are the equiv. classes? Let's write some down:

$$
\begin{aligned}
[0]_{\equiv_3} \text{ is } & \{n \in \mathbb{Z} \mid 0 \equiv_3 n\} \\
&= \{n \in \mathbb{Z} \mid 3 \mid n - 0\} \\
&= \{n \in \mathbb{Z} \mid 3 \mid n\} \\
&= \{\dots -3, 0, 3, 6, \dots\}.
\end{aligned}
$$

$$
\begin{aligned}
[1]_{\equiv_3} \text{ is } & \{n \in \mathbb{Z} \mid 1 \equiv_3 n\} \\
&= \{n \in \mathbb{Z} \mid 3 \mid n-1\} \\
&= \{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n - 1 = 3k)\} \\
&= \{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n = 3k + 1)\} \\
&= \{\dots -2, 1, 4, 7, \dots\}
\end{aligned}
$$

Similarly $[2]_{\equiv_3}$ is $\{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n = 3k+2)\}$

$$= \{\dots -1, 2, 5, 8, \dots\}$$

<u>Now</u>: $[3]_{\equiv_3}$ is $\{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n = 3k+3)\}$

$$
\begin{aligned}
&= \{\dots -3, 0, 3, 6, \dots\} \\
&= [0]_{\equiv_3}
\end{aligned}
$$

more generally one can prove:

<u>Fact</u>: if R is an equiv. relation on A, and we have $x, y \in A$, then if $y \in [x]_R$, then $[y]_R = [x]_R$.

(we'll prove this later: in course of showing equiv. classes form a partition)

So: we also have:

$$[1]_{\equiv_3} = [4]_{\equiv_3}$$
$$[2]_{\equiv_3} = [5]_{\equiv_3} \quad \text{etc...}$$

So: there are three distinct equiv. classes for $\equiv_3$, each consisting of all $n \in \mathbb{Z}$ of a given remainder when divided by 3 (0, 1, or 2).

- again: the equiv. classes form a <u>partition</u> (of $\mathbb{Z}$ in this case):

$$\mathbb{Z} = \{\dots -3, 0, 3, 6, \dots\} \cup \{\dots -2, 1, 4, 7, \dots\} \cup \{\dots -1, 2, 5, 8, \dots\}$$

$$= [0]_{\equiv_3} \cup [1]_{\equiv_3} \cup [2]_{\equiv_3}$$

pairwise disjoint

Notation for congruence modulo k

we'll write $[n]_k$ instead of $[n]_{\equiv_k}$.

e.g. we'll abbreviate above as:

$$\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$$

Next goal is to see that, in some sense, "equivalence relation" and "partition" are two names for the same concept.

Recall: if A is a set, a partition $\mathbb{P}$ of A is a set of subsets of A (i.e. $\mathbb{P} \subseteq P(A)$) s.t.:

① $(\forall X \in \mathbb{P})\ X \neq \emptyset$

② $(\forall X, Y \in \mathbb{P})\ (X \neq Y \Rightarrow X \cap Y = \emptyset)$

③ $\bigcup\limits_{X \in \mathbb{P}} X = A$

② says the pieces of the partition are pairwise disjoint, can also be written: $(\forall X, Y \in \mathbb{P})\ (X = Y \vee X \cap Y = \emptyset)$

Ex's ① Let $X = \{\ldots -3, 0, 3, 6, \ldots\}$

$Y = \{\ldots -2, 1, 4, 7, \ldots\}$

$Z = \{\ldots -1, 2, 5, 8, \ldots\}$

Then $\mathbb{P} = \{X, Y, Z\}$ is a partition of $\mathbb{Z}$

PF: ① $X, Y, Z \neq \emptyset$

② $X \cap Y = X \cap Z = Y \cap Z = \emptyset$

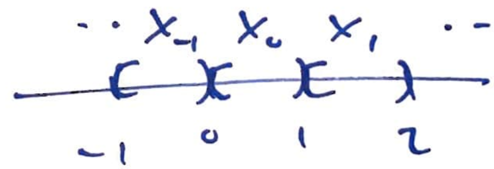
③ $X \cup Y \cup Z = \mathbb{Z}$.

② For every $n \in \mathbb{Z}$ define

$$X_n = \{y \in \mathbb{R} \mid n \leq y < y+1\}$$
$$= [n, n+1)$$

Then $\mathbb{P} = \{X_n : n \in \mathbb{Z}\} = \{\ldots X_{-1}, X_0, X_1, X_2, \ldots\}$ is a partition of $\mathbb{R}$.

PF: you try. Pic:



③ Let $A = \{1, 2, 3, 4\} = [4]$

Then $\mathbb{P} = \{\{1\}, \{2, 3, 4\}\}$ is a partition of A.

Equivalence Classes Partition Sets

Def'n Sps R is an equiv. relation on A. We denote the set of equivalence classes as A/R

i.e. $A/R = \{[x]_R : x \in A\}$

read "A mod R"

Ex's 1. Consider $\equiv_3$ on $\mathbb{Z}$

Then $\mathbb{Z}/\equiv_3 = \{[n]_3 : n \in \mathbb{Z}\}$

$= \{\ldots [-1]_3, [0]_3, [1]_3, [2]_3, \ldots\}$

But we checked

$\ldots [-3]_3 = [0]_3 = [3]_3 = [6]_3 = \ldots$

$\ldots [-2]_3 = [1]_3 = [4]_3 = \ldots$

$\ldots [-1]_3 = [2]_3 = [5]_3 = \ldots$

So really: $\mathbb{Z}/\equiv_3 = \{[0]_3, [1]_3, [2]_3\}$

which we could as well write

$\{[-6]_3, [4]_3, [8]_3\}$

(More) Special Notation: conventional to write $\mathbb{Z}/\equiv_n$ as $\mathbb{Z}/n\mathbb{Z}$.

→ just like with 3, in general we have:

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

② Let R denote the floor equiv. relation on $\mathbb{R}$: $(x,y) \in R$ iff $\lfloor x \rfloor = \lfloor y \rfloor$

– we checked before: for any $x \in [n, n+1)$ we have $[x]_R = [n, n+1)$

e.g. $[0]_R = [.1] = [0,1)$

$[1]_R = [1.99]_R = [1,2)$

So $\mathbb{R}/R = \{[x]_R : x \in \mathbb{R}\}$

$= \{\ldots [-1,0), [0,1), [1,2), \ldots\}$

$= \{\ldots [-1]_R, [0]_R, [1]_R, \ldots\}$

$= \{\ldots [-\frac{1}{2}]_R, [.111\ldots]_R, [1.3]_R, \ldots\}$

<u>Notice</u>: in both ex's 1 and 2 the set of equiv. classes forms a partition of the underlying set ($\mathbb{Z}$ in 1, $\mathbb{R}$ in 2)

- turns out this is always the case:

<u>Theorem</u> If R is an equiv. relation on A, then A/R is a partition of A.

Pf: (HW) For a hint, see 6.7.13 on pg. 449, or go to recitation tomorrow.