(iii) Fix $x, y, z \in \mathbb{R}$. Suppose $(x,y) \in R$ and $(y,z) \in R$. Then $\lfloor x \rfloor = \lfloor y \rfloor$ and $\lfloor y \rfloor = \lfloor z \rfloor$. Hence $\lfloor x \rfloor = \lfloor z \rfloor$. Hence $(x,z) \in R$ ✓. ⑨

③ Define a relation $\equiv_3$ on $\mathbb{Z}$ by $(n,m) \in \equiv_3$ iff $3 \mid (m-n)$ ← $\boxed{\exists k \in \mathbb{Z} \; m-n = 3k}$

i.e. $\equiv_3 = \{(n,m) \in \mathbb{Z}^2 \mid 3 \mid (m-n)\}$

↳ we'll typically write $n \equiv_3 m$ instead of $(n,m) \in \equiv_3$.

e.g. $2 \equiv_3 5$ since $3 \mid (5-2)$

$7 \equiv_3 -2$ since $3 \mid (7-(-2))$

$6 \not\equiv_3 7$ since $3 \nmid (7-6)$

Claim $\equiv_3$ is an equiv. relation on $\mathbb{Z}$.

Pf: (i) Fix $n \in \mathbb{Z}$. Observe $3 \mid n-n$, i.e. $3 \mid 0$ since $0 = 3 \cdot 0$. Hence $n \equiv_3 n$.

(ii) Fix $n, m \in \mathbb{Z}$ and spս $n \equiv_3 m$. We prove $m \equiv_3 n$.

Pf: Since $n \equiv_3 m$ we have $3 \mid m-n$

i.e. $\exists k \in \mathbb{Z}$ s.t. $m-n = 3k$.

but then $n-m = 3(-k)$

hence $3 \mid n-m$ ✓

hence $m \equiv_3 n$ ✓

(iii) Fix $n, m, l \in \mathbb{Z}$. Spse $n \equiv_3 m$ and $m \equiv_3 l$. We prove $n \equiv_3 l$.

Pf: we know $\exists k_1, k_2 \in \mathbb{Z}$ s.t.

$$m - n = 3k_1$$
$$l - m = 3k_2$$

adding these equations gives:

$$(m-n) + (l-m) = 3k_1 + 3k_2$$

$$\Rightarrow l - n = 3(k_1 + k_2)$$

$$\Rightarrow 3 \mid l-n. \checkmark$$

Hence $n \equiv_3 l$ ✓

↳ $\equiv_3$ is called <u>congruence</u> <u>modulo 3</u>.

↳ more convenient to write

$n \equiv m \pmod 3$ instead of $n \equiv_3 m$

(we'll use these notations interchangeably)

→ another way to think about it:
$n \equiv m \pmod 3$ iff n, m have the <u>same</u> <u>remainder</u> when divided by 3.

e.g. $2 \equiv 5 \pmod 3$

since $2 = 3 \cdot 0 + 2$
$5 = 3 \cdot 1 + 2$ same remainder

$7 \equiv 13 \pmod 3$

since $7 = 3 \cdot 2 + 1$
$13 = 3 \cdot 4 + 1$ same

$7 \equiv -2 \pmod 3$

since $7 = 3 \cdot 2 + 1$
$-2 = 3(-1) + 1$

but $7 \not\equiv 11 \pmod 3$

since $7 = 3 \cdot 2 + 1$
$11 = 3 \cdot 3 + 2$ diff.

(4) Nothing special about 3. For any fixed $k \in \mathbb{N}$, can define $\equiv_k$ on $\mathbb{Z}$ by:

$n \equiv_k m$ iff $k \mid m - n$

↳ just like with 3, we'll more usually write: $n \equiv m \pmod{k}$ for $n \equiv_k m$

↳ just like with 3, $\equiv_k$ is an equivalence relation for any $k \in \mathbb{N}$.

Nonexamples of equiv. relations:

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

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

is symmetric, since $n \neq m \Rightarrow m \neq n$

but not reflexive (in fact: never true that $n \neq n$)

nor transitive (e.g. $2 \neq 4$ and $4 \neq 2$ but $2 = 2$)

Equivalence Classes: Def'n: Sps R is an equivalence relation on A. For a fixed $x \in A$, the equivalence class of x, denoted $[x]_R$, is the set of elements 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 $[x]_R$ as $\{y \in A \mid (y,x) \in R\}$.)

Warning: overloaded notation: we've used [ ]'s when defining $[n] = \{1, 2, \ldots, n\}$
- this is completely unrelated to meaning of $[x]_R$ for an equiv. relation R — so don't get confused!

Ex's: ① Let $=$ denote the equality relation on $\mathbb{N}$. Then for any fixed $n \in \mathbb{N}$ we have:

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

e.g. $[1]_= = \{1\}$, $[2]_= = \{2\}$, 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 <u>def'n</u>: $[x]_R = \{y \in \mathbb{R} \mid (x,y) \in R\}$

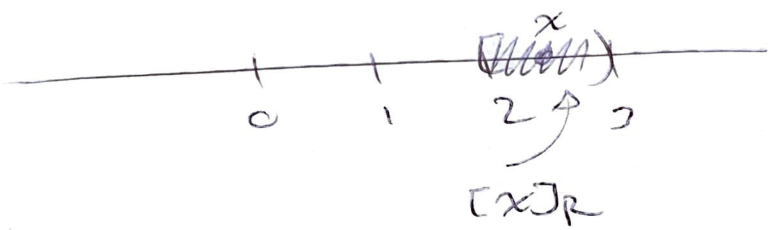
$= \{y \in \mathbb{R} \mid \lfloor x \rfloor = \lfloor y \rfloor\}$

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

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

$= [n, n+1)$

<u>Picture</u>: e.g. if $x = 2.34$ so that $\lfloor x \rfloor = 2$ we have $[x]_R = [2,3)$



<u>Notice</u>: the equiv. classes of R form a <u>partition</u> of $\mathbb{R}$.

we'll prove later: equivalence classes <u>always</u> partition the underlying set (in this case, $\mathbb{R}$).

(3) Consider $\equiv_3$ on $\mathbb{Z}$. What are the equiv. classes of this relation? (15)

Let's write some down:

$[0]_{\equiv_3}$ is $\{n \in \mathbb{Z} \mid 0 \equiv_3 n\}$

$= \{n \in \mathbb{Z} \mid 3 \mid n-0\}$

$= \{n \in \mathbb{Z} \mid 3 \mid n\}$

$= \{\ldots -3, 0, 3, 6, \ldots\}$

$[1]_{\equiv_3}$ is $\{n \in \mathbb{Z} \mid 1 \equiv_3 n\}$

$= \{n \in \mathbb{Z} \mid 3 \mid n-1\}$

$= \{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n-1 = 3k)\}$

$= \{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n = 3k+1)\}$

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

$[2]_{\equiv_3}$ is $\{n \in \mathbb{Z} \mid 2 \equiv_3 n\}$

$=$ (as above) $\{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n = 3k+2)\}$

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

$[3]_{\equiv_3}$ is $\{n \in \mathbb{Z} \mid 3 \equiv_3 n\}$

$= \{n \in \mathbb{Z} \mid 3 \mid n-3\}$

$= \{n \in \mathbb{Z} \mid 3 \mid n\}$

$= \{\ldots, -3, 0, 3, 6, \ldots\} = [0]_{\equiv_3}$.

Sim'ly we can check:

$[4]_{\equiv_3} = [1]_{\equiv_3}$

$[5]_{\equiv_3} = [2]_{\equiv_3}$

$[6]_{\equiv_3} = [3]_{\equiv_3} = [0]_{\equiv_3}$. etc.

<u>Notice</u>: there are three distinct equiv. classes, 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):

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

$\cup \{\ldots, -1, 2, 5, 8, \ldots\}$

pairwise disjoint

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

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 "partition" and "equivalence relation" are, in a sense, 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. $\mathbb{P} \subseteq \mathcal{P}(A)$) 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. $\bigcup_{X \in \mathbb{P}} X = A$

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

Pic:

$\mathbb{P} = \{X, Y, Z\}$ is a partition of A (into 3 pieces)

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

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

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

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:

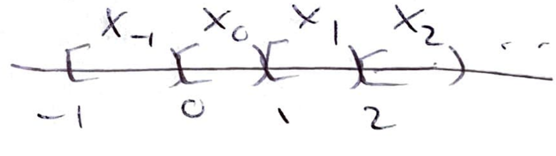
$X_n = \{y \in \mathbb{R} \mid n \leq y < n+1\}$

$= [n, n+1)$

Then $\mathbb{P} = \{X_n : n \in \mathbb{Z}\} = \{\dots, X_{-1}, X_0, X_1, X_2, \dots\}$

is a partition of $\mathbb{R}$.

Pf: you try. Pic:



③ Let $A = \{1, 2, 3, 4\} = [4]$

Define $X = \{1\}$ $Y = \{2, 3, 4\}$

Then $\mathbb{P} = \{X, Y\} = \{\{1\}, \{2, 3, 4\}\}$

is a partition of A.

Equivalence classes partition sets

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

that is: $A/R = \{ [x]_R : x \in A \}$

read "A mod R"

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

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

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

We already 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:

$= \{ [6]_3, [-2]_3, [8]_3 \}$