Math 3200: Day 27

Def: An equivalence relation is a relation on a set which is symmetric, transitive, & reflexive.

If R is an equivalence relation on A & $a \in A$, then the equivalence class of a is the set

$$[a] = \{x \in A : x R a\}.$$

Prop: Let R be the relation on $\mathbb{Z}$ given by aRb if $4 \mid (a+3b)$

Proof: (reflexive) Let $a \in \mathbb{Z}$. Then $a+3a = 4a$ is divisible by 4, so aRa.

(symmetric) Suppose $a, b \in \mathbb{Z}$ so that aRb. Then $4 \mid (a+3b)$, so $a+3b = 4n$ for some $n \in \mathbb{N}$.

Hence, $a = 4n - 3b$, so $b + 3a = b + 3(4n-3b) = b + 12n - 9b = 12n - 8b = 4(3n-2b)$ is divisible by 4, so bRa.

(transitive) Suppose $a, b, c \in \mathbb{Z}$ so that aRb & bRc. Then $a+3b = 4n$ & $b+3c = 4m$ for some $n, m \in \mathbb{Z}$.

Then $a = 4n-3b$ & $3c = 4m - b$, so $a + 3c = (4n-3b) + (4m-b) = 4n + 4m - 4b = 4(n+m-b)$ is divisible by 4, so aRc.

Since R is a reflexive, symmetric, transitive relation, it is an equivalence relation. ∎

Q: What is $[1]$ w.r.t. this R?

A: If $x \in [1]$, then $xR1$, so $4 \mid (x + 3(1)) \Rightarrow x + 3 = 4n$ for some $n \in \mathbb{N}$, meaning that $x = 4n - 3 = 4(n-1) + 1$,

so $x \equiv 1 \pmod 4$. Hence, $[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 4\}$.

More generally, if $a \in \mathbb{Z}$, then $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod 4\}$ b/c $x + 3a = 4n \Rightarrow x = 4n - 3a = 4(n-a) + a$.

Prop: The relation $\equiv \pmod n$ is an equivalence relation on $\mathbb{Z}$ for any $n \in \mathbb{N}$.

Proof: Let $n \in \mathbb{N}$.

(symmetric) Let $a \in \mathbb{Z}$. Then $a - a = 0 = 0 \cdot n$, so $a \equiv a \pmod n$.

(reflexive) Let $a,b \in \mathbb{Z}$ so that $a \equiv b \pmod{n}$. Then $a-b = xn$ for some $x \in \mathbb{Z}$. Then

$$b-a = -(a-b) = -xn = (-x)n, \text{ so } b \equiv a \pmod{n}.$$

(transitive) Let $a,b,c \in \mathbb{Z}$ so that $a \equiv b \pmod{n}$ & $b \equiv c \pmod{n}$, meaning that $a-b = xn$ & $b-c = yn$ for $x,y \in \mathbb{Z}$.

Then $a-c = (a-b)+(b-c) = xn + yn = (x+y)n$, so $a \equiv c \pmod{n}$.

Since it is reflexive, symmetric, & transitive, $\equiv \pmod{n}$ is an equivalence relation. ▨

Thm: Let R be an equivalence relation on a set A & let $a,b \in A$. Then $[a]=[b]$ if & only if aRb.

Proof: ($\Rightarrow$) Suppose $[a]=[b]$. Since R is reflexive, aRa, so $a \in [a] = [b]$, which means that aRb.

($\Leftarrow$) OTOH, suppose aRb. Let $x \in [a]$. Then xRa &, since aRb & R is transitive, xRb, so $x \in [b]$.

Since the choice of x was arbitrary, this implies that $[a] \subseteq [b]$.

Likewise, if $y \in [b]$ then yRb. Since aRb & R is symmetric, bRa and thus, since R is transitive, yRa.

Hence, $y \in [a]$, which implies $[b] \subseteq [a]$. Having proved containment both ways, we see that $[a]=[b]$. ▨

Remark: Notice that we needed all three components of the definition of an equivalence relation. If any one of them were missing we couldn't have arrived at the conclusion.