Equivalence Relations - Informal

Informally a *relation* on a set is basically just a binary predicate R where we interpret:

$$a \; R \; b$$

to mean a *is related to b* in some way.

An **equivalence relation** is then just a type of relation that specifies that

a and b are the same in all the ways that the relation R checks for.

That is, they are **equivalent** as far as R is concerned.

Clearly not all relations are equivalence relations, for example $(a < b)$ says that a and b are different.
Mathematicians often use symbols like:

$$a \sim b \qquad a \cong b \qquad a \simeq b \qquad a \equiv b$$

for our equivalence relations.

Informal Example (that we will **not** make precise)

Let $\mathcal{S}$ be the set of all well formed sentance in first order logic over some well defined grammar and universe of discourse.
Logical equivalence:

$$\mathcal{A} \equiv \mathcal{B}$$

is an equivalence relation on $\mathcal{S}$.
Two sentences might not be identical, but they may well be 'equivalent' in terms of their logical meaning.
The sentences:

if you fail then you try it again

vs

if you do not try it again then you do not fail.

which might become:

$$\mathsf{F} \Rightarrow \mathsf{TA} \quad \equiv \quad \neg\mathsf{TA} \Rightarrow \neg\mathsf{F}$$

May be logically equivalent, they may mean the same thing logically, but they definitely have different implications.

We will not ever work with this, for among other reasons, using one universe of discourse to talk about another tends to create notational challenges (among other philisophical problems)

Equivalence Relations - Formal

We say that a binary predicate R on a set A defines an equivalence relation on A if and only if:

- It is **reflexive**

$$\forall a \in A, a \; R \; a$$

  Everything is equivalent to itself.

- It is **symmetric**

$$\forall a \in A, \forall b \in A \, (a \; R \; b \Rightarrow b \; R \; a)$$

  If a is equivalent to b then b is equivalent to a.

- It is **transitive**

$$\forall a \in A, \forall b \in A, \forall c \in A, ((a \; R \; b) \; \& \; (b \; R \; c)) \Rightarrow (a \; R \; c)$$

  If a is equivalent to b and b is equivalent to c then a is equivalent to c.

Examples - Checking that things are equivalence relations

Is the following an equivalence relation?

On the set of people, $x \sim y$ if x and y have the same first name.

- It is reflexive:
  If x is any person, then x has the same name as x, hence $x \sim x$. This proves
  $$\forall x, x \sim x$$

- It is symmetric:
  If x and y are any two people, if we know that $x \sim y$, then x has the same name as y, but then y has the same name as x, and hence $y \sim x$. This proves
  $$\forall x, \forall y, ((x \sim y) \Rightarrow (y \sim x))$$

- It is transitive:
  If x, y and z are any three people, and if we know that $x \sim y$, so x has the same name as y, and we know $y \sim z$, so y has the same name as z, then we know that x and z have the same first name, and so $x \sim z$ but then y has the same name as x, and hence $y \sim x$. This proves
  $$\forall x, \forall y, \forall z, (((x \sim y) \,\&\, (y \sim z)) \rightarrow (x \sim z))$$

Because it is reflexive, symmetric and transitive, we know that it defines an equivalence

What about:

- On the set of people, $x \sim y$ if x and y have the same age.
- On the set of people, $x \sim y$ if x and y have a common friend.
- If $f : A \to B$ is any function, the relation on A given by $x \sim y$ if $f(x) = f(y)$.
  - For example the function from people to natural numbers which gives someones age.
  - For example the function from people to names which gives someones first name.
  - For example the function from people to natural numbers which gives their blood pressure.
- On the collection of all sets $X \sim Y$ if there exists a bijection $f : X \to Y$. (This is on the assignment)

Equivalence behaves a lot like equality, The properties that characterize equivalence relations are modelled off of those of equality. But equivalence is not equality.

One has to be careful when talking about things being equivalent to always make it clear **In what way you are saying they are equivalent**

Equivalence Classes

Definition

If X is a set with an equivalence relation R then the **equivalence class** of an element x, with respect to an equivalence relation R is the set:

$$[x] = \{y \mid x \; R \; y\}$$

it is a subset of X.
We obtain a map $\text{equiv}_R : X \to \mathcal{P}(X)$ given by $\text{equiv}(x) = [x]$. We call the range of this map the **Set of Equivalence Classes** of R.

The equivalence class of x is just the set of all things that are *equivalent* to x.
We can talk about having equality of equivalence classes, because equivalence classes are sets and those sets can be equal.

It won't be something you need to deal with so much in this course, but if for some reason you have two different equivalence relations R and S that you care about at the same time. Then you might write something like:

$$[x]_R \qquad \text{or} \qquad [x]_S$$

to specify which equivalence class you are considering.

Example - equivalence classes/the set of equivalence classes

Show that congruence modulo n is an equivalence relation.
We define the set:

$$\mathbb{Z}/n\mathbb{Z}$$

to be the set of all equivalence classes under the relation congruence modulo n.
This means that:

- $\mathbb{Z}/n\mathbb{Z}$ is a set.
- The elements of $\mathbb{Z}/n\mathbb{Z}$ are all of the form

$$[a] = \{x \in \mathbb{Z} \mid x \cong a \pmod{n}\},$$

  that is they are equivalence classes modulo n.
- We have that

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-2], [n-1]\}.$$

  gives all the equivalence classes.How can we prove this?
- Some people denote $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}_n$.
- People often write $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ rather than $[0], [1], \ldots, [n-2], [n-1]$ for the equivalence classes in this case.

Theorems about Equivalence Classes

Lemma
If $\sim$ is an equivalence relation then the following are equivalent:

1. $x \sim y$
2. $x \in [y]$
3. $[x] \cap [y] \neq \emptyset$
4. $[x] = [y]$

Theorem
Specifying an equivalence relation is the same as specifying a partitioning of the set X into a collection U_i which satisfty that for all x in X there is a unique i such that $x \in U_i$.

Fun fact that you won't need

Theorem
The equivalence relation on the set X determined by the map $\mathrm{equiv}_R : X \to \mathcal{P}(X)$ is the same as the equivalence relation R which defines it.

Functions on the set of equivalence classes

Theorem
To specify a function f whose domain is the set of equivalence classes of some relation R on a set X it is equivalent to specify a function $\tilde{f}$ on X such that

$$\forall x \in X, \forall y \in X, (x \; R \; y) \Rightarrow (\tilde{f}(x) = \tilde{f}(y))$$

To specify a function

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$$

I need to describe a rule for where to send each of

$$\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

But because it needs to be a function, we need

$$f(\overline{1}) = f(\overline{n+1})$$

so for example a rule like

$$f(\overline{n}) = n + 7$$

Does not describe a function!!!
But something like

$$f(\overline{n}) = \text{ smallest number } k \text{ with } n^k \cong 1 \pmod{n}$$

might (Though that requires a proof).

Example - Working with equivalence classes/sets of equivalence classes

Define modular arithmetic on the set of equivalence classes.
We want to define maps:

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

and

$$* : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

which are supposed to be like 'addition' and 'multiplication'.

Question What do I need to check to show they are actually functions?
Lets check that

$$[a] + [b] = [a + b]$$

defines a function $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$? But

$$[a]^{[b]} = [a^b]$$

does not.

First, what can go wrong?

What would $\overline{5}^{\overline{17}}$ be in $\mathbb{Z}/17\mathbb{Z}$?

Well, $\overline{17} = \overline{0}$ in $\mathbb{Z}/17\mathbb{Z}$. But

$$5^0 \cong 1 \pmod{17} \qquad 5^{17} \cong 5 \pmod{17}$$

So $\overline{5}^{\overline{17}}$ doesn't have a single value in $\mathbb{Z}/17\mathbb{Z}$, in fact, given different choices of representatives for $\overline{17}$ we can get every possible value of $\mathbb{Z}/17\mathbb{Z}$ as the output.
So it fails the vertical line test!

so why is this not a problem for

$$[a] + [b] = [a + b]$$

or

$$[a] \cdot [b] = [ab]$$

Some example Calculations

Calculate

$$(\overline{25} + \overline{27} + \overline{19}) * (\overline{5} + \overline{37} + \overline{29})$$

in $\mathbb{Z}/13\mathbb{Z}$. What about $\mathbb{Z}/7\mathbb{Z}$?

Calculate

$$(\overline{2})^{16} = \overbrace{\overline{2} * \overline{2} * \ldots * \overline{2} * \overline{2}}^{16}$$

in $\mathbb{Z}/17\mathbb{Z}$. What about $\mathbb{Z}/5\mathbb{Z}$?

Calculate

$$(\overline{2})^{1024} = \overbrace{\overline{2} * \overline{2} * \ldots * \overline{2} * \overline{2}}^{1024}$$

in $\mathbb{Z}/17\mathbb{Z}$.

Why equivalence relations and classes

- Equivalence relations give a very useful way of focusing your attention onto particular properties of objects. So by working with equivalence classes rather than all objects separately, it can give a strategy for a proof.
  For example:
  To prove that $\forall n \in \mathbb{N}, n^{17} = n \pmod{17}$ I can prove something about each equivalence class (modulo 17) which gives me a finite number of cases to consider.
  The equivalence class of n modulo 17 is really what determines what n^{17} is congruent to modulo 17.
- One can often prove theorems like:

$$P(x), xRy, \therefore P(y)$$

  (if we know $P(x)$ is true for one element of an equivalence class it is true for all of them!)
  If we have such a theorem, then checking $P(y)$ is the same as checking $P(x)$ for an equivalent object.
  And I can pick the simplest equivalent object. Eg, if I want to prove something about finite sets, I can often just assume my set is looks like:

$$\{1, 2, 3, 4, 5, \ldots, n\}$$

  for some choice n, because every finite set is in some sense 'equivalent' to such a set.