Equivalence relations

A motivating example for equivalence relations is the problem of constructing the rational numbers. A rational number is the same thing as a fraction a/b, $a, b \in \mathbb{Z}$ and $b \neq 0$, and hence specified by the pair $(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$. But different ordered pairs (a, b) can define the same rational number a/b. In fact, a/b and c/d define the same rational number if and only if $ad = bc$. One way to solve this problem is to agree that we shall only look at those pairs (a, b) "in lowest terms," in other words such that $b > 0$ is as small as possible, which happens exactly when a and b have no common factor. But this leads into complicated questions about factoring, and it is more convenient to let (a, b) be any element of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ and then have a framework for treating certain such pairs as equal.

There are many other examples where we would like to treat two objects as the same. For example, we can view an angle as a real number θ, but two the real numbers θ and $\theta + 2k\pi$ define the same angle for every integer k. Equivalence relations are a very general mechanism for identifying certain elements in a set to form a new set.

Let X be a set. A *relation* R is just a subset of $X \times X$. Choose some symbol such as $\sim$ and denote by $x \sim y$ the statement that $(x, y) \in R$. There are three important types of relations in mathematics: functions $f: X \to X$ (we denote by $y = f(x)$ the condition that $(x, y) \in R$), order (we use $x \leq y$ or $x < y$ for $(x, y) \in R$), and equivalence relations for relations that are "like" equality. These are usually denoted by some special symbol such as $\sim$, $\cong$, or $\equiv$. Here is the formal definition:

Definition 1. An *equivalence relation* on a set X is a subset $R \subseteq X \times X$ with the following properties: denoting $(x, y) \in R$ by $x \sim y$, we have

1. For all $x \in X$, $x \sim x$. (We say $\sim$ is *reflexive*.)
2. For all $x, y \in X$, if $x \sim y$ then $y \sim x$. (We say $\sim$ is *symmetric*.)
3. For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$. (We say $\sim$ is *transitive*.)

Here (1) says that the diagonal $\Delta_X = \{(x,x) : x \in X\}$ is a subset of R. (2) says that the set R is symmetric about the diagonal, i.e. that ${}^tR = R$, where ${}^tR$ is the set

$$ {}^tR = \{(y,x) : (x,y) \in R\}, $$

and (3) is not so easy to describe geometrically.

Examples. (1) The graph of a function $f\colon X \to X$ is an equivalence relation only if it is the identity, i.e. the graph is the diagonal. (This follows since we must have (x,x) in the graph for every $x \in X$.)

(2) Order is not an equivalence relation on, say, $X = \mathbb{R}$: $\leq$ is not symmetric and $<$ is neither reflexive nor symmetric.

(3) For $X = \{humans\}$, the relation x loves y is neither reflexive, symmetric nor transitive.

On the other hand, here are some equivalence relations:

1. Equality. In other words, $x \sim y \iff x = y$. Here $R = \Delta_X$.

2. The relation where $x \sim y$ for all $x, y \in X$. Here $R = X \times X$.

3. The relation of congruence on the set of all plane triangles (or all plane figures); likewise similarity of triangles.

4. Let $\ell_1 = \overrightarrow{\mathbf{p}_1\mathbf{q}_1}$ and $\ell_2 = \overrightarrow{\mathbf{p}_2\mathbf{q}_2}$ be two directed line segments in the plane (i.e. ℓ_i is the line segment starting at $\mathbf{p}_i$ and ending at $\mathbf{q}_i$). Then we can define ℓ_1 and ℓ_2 to be *equivalent* if they have the same magnitude and direction, or equivalently if they define the same vectors; this is the same as requiring that $\mathbf{q}_1 - \mathbf{p}_1 = \mathbf{q}_2 - \mathbf{p}_2$. It is straightforward to check that this defines an equivalence relation on the set of directed line segments.

5. We can define when two sets A and B have the same number of elements by saying that there is a bijection from A to B. This is an equivalence relation, provided we restrict to a set of sets (we cannot just define this as an equivalence relation on the "set" of all sets, since this is too big to be a set). For example, we could define this relation on a set such as $\mathcal{P}(\mathbb{R})$, the set of all subsets of the real numbers. The content of this statement is as follows: (1) given a set A, $A \sim A$, i.e. there is a bijection from A to itself (the identity function Id_A); (2) If $A \sim B$, i.e. there is a bijection from A to B, say $f\colon A \to B$, then there is a bijection from B to A, in fact f^{-1} exists since f is a bijection, and $f^{-1}\colon B \to A$ is a bijection from B to A since f is its inverse; (3) If

$A \sim B$ and $B \sim C$, then $A \sim C$. In fact, given a bijection from A to B, say f, and a bijection from B to C, say g, then we have seen that the composition $g \circ f$ is a bijection from A to C.

6. Consider the following equivalence relation on integers: n and m are equivalent (write this as $n \equiv m \pmod 2$) if they are both even or both odd. Another way to say this is to say that $n \equiv m \pmod 2$ if and only if $n - m$ is even, if and only if 2 divides $n - m$. More generally, if n is a fixed positive integer, we define

$$a \equiv b \pmod n \iff n|(b-a),$$

where the notation $d|k$, for integers d, k, means d divides k. Then an argument shows that this is an equivalence relation: clearly $a \equiv a \pmod n$, since n always divides $a - a = 0$. Thus $\equiv \pmod n$ is reflexive. Next, if $a \equiv b \pmod n$, then $n|(b-a)$, and hence $n|(a-b) = -(b-a)$. Hence $\equiv \pmod n$ is symmetric. Finally, to see that $\equiv \pmod n$ is transitive, suppose that $a \equiv b \pmod n$ and that $b \equiv c \pmod n$. Then by definition $n|(b-a)$ and $n|(c-b)$, so that

$$n|((b-a)+(c-b)) = c - a.$$

Then $a \equiv c \pmod n$, so that $\equiv \pmod n$ is transitive and hence an equivalence relation.

7. For a related example, define the following relation $\equiv \pmod{2\pi}$ on $\mathbb{R}$: given two real numbers, which we suggestively write as θ_1 and θ_2, $\theta_1 \equiv \theta_2 \pmod{2\pi} \iff \theta_2 - \theta_1 = 2k\pi$ for some integer k. An argument similar to that above shows that $\equiv \pmod{2\pi}$ is an equivalence relation. Here intuitively $\theta_1 \equiv \theta_2 \pmod{2\pi}$ if θ_1 and θ_2 "define the same angle."

8. Suppose that X is a set and that $f\colon X \to Y$ is a fixed function from X to some set Y. Define $a \sim b$ if $f(a) = f(b)$. The fact that $\sim$ is an equivalence relation follows from the basic properties of equality on Y. For example, $a \sim a$ just says that $f(a) = f(a)$.

Warning: A relation R is a subset of $X \times X$, but equivalence relations say something about elements of X, **not** ordered pairs of elements of X. The ordered pair part comes in because the relation R is the set of all (x, y) such that $x \sim y$. It is accidental (but confusing) that our original example of an equivalence relation involved a set X (namely $\mathbb{Z} \times (\mathbb{Z} - \{0\})$) which itself happened to be a set of ordered pairs.

Equivalence relations are a way to break up a set X into a union of disjoint subsets. Given an equivalence relation $\sim$ and $a \in X$, define $[a]$, the *equivalence class* of a, as follows:

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

Thus we have $a \in [a]$. Given an equivalence class $[a]$, a *representative* for $[a]$ is an element of $[a]$, in other words it is a $b \in X$ such that $b \sim a$. Thus a is always a representative for $[a]$.

For example:

1. If $\sim$ is equality $=$, then $[a] = \{a\}$.

2. If $\sim$ corresponds to $R = X \times X$, in other words $x \sim y$ for all $x, y \in X$, then $[a] = X$ for every $a \in X$.

3. If $\sim$ is congruence $\cong$ of triangles, then the equivalence class of a triangle T is the set of all triangles which are congruent to T. This is sometimes called a *congruence class*.

4. An equivalence class of directed line segments is called (in physics) a *vector*.

5. Here, an equivalence class is called a *cardinal number*.

6. For the equivalence relation on $\mathbb{Z}$, $\equiv \pmod 2$, there are two equivalence classes, $[0]$, which is the set of even integers, and $[1]$, which is the set of odd integers. More generally, given a positive integer n, the equivalence classes for $\equiv \pmod n$ correspond to the possible remainders when we divide by n, in other words there are n equivalence classes which we can write as $[0], [1], \ldots, [n-1]$, and, given $a \in \mathbb{Z}$ with $0 \leq a \leq n-1$, an integer $k \in [a] \iff k$ has remainder a when divided by n, i.e. there exists an integer q such that $k = nq + a$. We shall describe this process in more detail later.

7. As noted before, we think of equivalence classes $\equiv \pmod{2\pi}$ as angles.

8. Given $f : X \to Y$ a function and the equivalence relation $x \sim y$ if $f(x) = f(y)$, the equivalence classes are the sets of preimages $f^{-1}(z)$ for z in the image of f. (Why?) Note that, in this case, $[x] = f^{-1}(f(x))$.

In the above examples, two equivalence classes which are not equal are disjoint. In fact, this is a general property:

Proposition 2. *Let* $\sim$ *be an equivalence relation on a set* X*, and let* $[a]$ *be the equivalence class of* a*. If* $[a] \cap [b] \neq \emptyset$*, then* $[a] = [b]$*. Thus, for every* $a \in X$*,* a *is contained in exactly one equivalence class.*

Proof. Suppose that there is some $c \in [a] \cap [b]$. We first show that $[a] \subseteq [b]$. By definition $c \sim a$ and $c \sim b$. Using symmetry of $\sim$, $a \sim c$ as well. Given $x \in [a]$, by definition $x \sim a$ also. Now $x \sim a$ and $a \sim c$, so by transitivity $x \sim c$. Since $c \sim b$, again by transitivity $x \sim b$. Thus by definition $x \in [b]$, hence $[a] \subseteq [b]$. It then follows by symmetry $[b] \subseteq [a]$ (there is nothing special about either one) so that $[a] = [b]$. □

For an equivalence relation $\sim$, we have the set of all equivalence classes $\{[a] : a \in X\}$. This set is sometimes written $X/\sim$. It is a subset of the power set $\mathcal{P}(X)$ with the following property: two subsets of X which lie in $X/\sim$ are either equal or disjoint (this is the statement of the proposition above) and every element of X lies in some (hence exactly one) set in $X/\sim$. Put another way: X is a **disjoint union** of the equivalence classes.

One can also define an equivalence relation by reversing this procedure: suppose that X is the union of of disjoint subsets, and define $x \sim y$ if x and y are in the same subset. Then one can check that $\sim$ is an equivalence relation whose equivalence classes are exactly the subsets we started with.

Finally, we note that there is a natural surjective function from X to $X/\sim$, often called *projection*, defined by: for all $x \in X$,

$$\pi(x) = [x].$$

Notation: For $X = \mathbb{Z}$ and $\sim$ equal to $\equiv \pmod{n}$, we write $\mathbb{Z}/n\mathbb{Z}$ for $\mathbb{Z}/\sim$. For $X = \mathbb{R}$ and $\sim$ equal to $\equiv \pmod{2\pi}$, we write $\mathbb{R}/2\pi\mathbb{Z}$ for $\mathbb{R}/\sim$.

Sometimes equivalence classes can have a "best" representative. For example, for the rational number example below, a good choice of representative is to take (a, b) with $b > 0$ and as small as possible. For the relation on $\mathbb{Z}$, $\equiv \pmod{2}$, there are two equivalence classes, the even and the odd integers, and an obvious choice is to take [0] for the equivalence class of even integers and [1] for the equivalence class of odd integers. More generally, as we shall see, for $\equiv \pmod{n}$, every equivalence class $[k]$ has a unique representative a with $0 \leq k \leq n-1$. For the equivalence relation $\equiv \pmod{2\pi}$ on $\mathbb{R}$, one often uses the unique representative θ_0 of $[\theta]$ satisfying $0 \leq \theta_0 < 2\pi$. However, for a general equivalence relation, it is not always possible to single out a good representative in a natural way.

We return to the example that comes from trying to construct the rational numbers. Let $\mathbb{Z}$ denote the set of integers, and let $X = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ (the set of ordered pairs (a, b) with $a, b \in \mathbb{Z}$ and $b \neq 0$). Define $(a, b) \sim (c, d)$ if $ad = bc$. Then we have the following:

Proposition 3. *$\sim$ is an equivalence relation on X.*

Proof. First $(a, b) \sim (a, b)$: this is just the statement $ab = ba$, which holds since multiplication is commutative. Also, if $(a, b) \sim (c, d)$, then by definition $ad = bc$. But then $(c, d) \sim (a, b)$ since $cb = da$. Finally to check transitivity, suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then by definition $ad = bc$ and $cf = de$. We must show that $af = be$. Start with $ad = bc$ and multiply by f to get

$$adf = bcf = bde.$$

Since $d \neq 0$, we can cancel it to get $af = be$, as claimed. □

With this notation, we can define addition and multiplication of rational numbers as follows: define, for ordered pairs (a, b),

$$(a, b) + (c, d) = (ad + bc, bd)$$
$$(a, b) \cdot (c, d) = (ac, bd).$$

We would like to define this operation on equivalence classes $[(a, b)]$, as follows: define

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)],$$

and similarly for multiplication. The meaning of this is as follows: given two equivalence classes, pick representatives for each and add according to the formula for adding ordered pairs above. Then take the equivalence class of this sum. The problem is to show that this operation is **well-defined**. In other words, the equivalence class of the sum doesn't depend on which representatives for the equivalence classes you use This amounts to showing for example that if $(a, b) \sim (a', b')$ then $(a, b) + (c, d) \sim (a', b') + (c, d)$. This is a calculation: we have assumed that $ab' = a'b$ and want to show that $(ad + bc, bd) \sim (a'd + b'c, b'd)$. This in turn boils down to checking if

$$(b'd)(ad + bc) = (bd)(a'd + b'c).$$

However the left hand side is $d(b'ad + b'bc) = d(a'bd + b'bc) = (bd)(a'd + b'c)$, so that $(a, b) + (c, d) \sim (a', b') + (c, d)$. An easier calculation shows that, if $(a, b) \sim (a', b')$ then $(a, b) \cdot (c, d) \sim (a', b') \cdot (c, d)$.

We can now define the rational numbers $\mathbb{Q}$ to be the set of all equivalence classes. The integers are "contained" in the natural numbers if we identify $n \in \mathbb{Z}$ with $[(n, 1)]$. Note that $(n, 1) \sim (m, 1)$ means that $n \cdot 1 = 1 \cdot m$, i.e. $n = m$. Thus each equivalence class can contain at most one integer—another way to say this is to say that the function $f \colon \mathbb{Z} \to \mathbb{Q}$ defined by $f(n) = [(n, 1)]$ is injective. Also note that $(n, 1) + (m, 1) = (n + m, 1)$ and that $(n, 1) \cdot (m, 1) = (nm, 1)$. So addition of integers is the same as adding them when viewed as rational numbers. Another way to say this is that the function f has the following properties: $f(n + m) = f(n) + f(m)$ and $f(nm) = f(n) \cdot f(m)$.

Addition and multiplication of rational numbers have all the usual properties (commutative, associative, multiplication distributes over addition). The additive identity is $(0, 1)$ and the additive inverse to (a, b) is $(-a, b)$. The multiplicative identity is $(1, 1)$. Finally, it is easy to see that $(a, b) \sim (0, 1)$ if and only if $a = 0$. Thus if $[(a, b)] \neq [(0, 1)]$, then (b, a) is an element of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ and $(a, b) \cdot (b, a) = (ab, ab) \sim (1, 1)$. So every nonzero element has a multiplicative inverse. In particular, for $b \neq 0$, $[(1, b)]$ is the multiplicative inverse to b.

Of course, we usually write the equivalence class $[(a, b)]$ as a/b. If we identify the integer a with $[(a, 1)]$ as above, then $[(1, b)] = 1/b$ is the multiplicative inverse to b and $a/b = a(1/b)$ in the usual way.

To emphasize: we often want to define functions or operations such as "addition" or "multiplication" on a set $X/\sim$ of equivalence classes. What this means is that we want to define a function $f \colon X/\sim \to Y$ or (in the case of an algebraic operation) a function $f \colon (X/\sim) \times (X/\sim) \to Y$, where in this case Y is often $X/\sim$ as well. There is a general procedure for doing this:

(i) Start with a function $F \colon X \to Y$ and define: $f([x]) = F(x)$. In other words, we choose a representative $x \in [x]$ and define $f([x])$ to be the value of F on x. This is called "defining the function f on representatives."

(ii) To see that the function f is well-defined, we have to show that, if we chose another representative $y \in [x]$, then $F(y) = F(x)$, or equivalently that $x \sim y \implies F(x) = F(y)$. This is called "showing that the function f is well-defined."

In this case, we have: $F = f \circ \pi$.

For example, for $X = \mathbb{R}$ and the equivalence relation $\equiv \pmod{2\pi}$, we can define the cosine of an angle $[\theta]$, i.e. we take the function $F \colon \mathbb{R} \to \mathbb{R}$

defined by $F(x) = \cos x$. Then we define $f([\theta]) = F(\theta)$. If $\theta' \in [\theta]$, i.e. if θ' and θ are two different representatives for $[\theta]$, then $\theta' = \theta + 2k\pi$, and hence $\cos(\theta') = \cos\theta$. Thus f is well-defined. Note that, if we had instead chosen the function $F(x) = x$, or $F(x) = x^2$, or $F(x) = e^x$, then the corresponding function would **not** be well-defined. For example, for $F(x) = x$, the function F has different values on two different representatives θ and $\theta + 2k\pi$ of $[\theta]$, as long as $k \neq 0$, since $F(\theta) = \theta \neq F(\theta + 2k\pi) = \theta + 2k\pi$.

Often, $Y = X'/\approx$ is also a space of equivalence classes, i.e. X' is a set and $\approx$ is an equivalence relation on X'. In many of our examples, in fact, $X' = X$ and $\approx$ is equal to $\sim$. In this case, there is a slight variant of (i) and (ii) above that we use:

(i) Start with a function $F\colon X \to X'$ and define: $f([x]) = [F(x)]$. In other words, we choose a representative $x \in [x]$ and define $f([x])$ to be the equivalence class (for $\approx$) containing $F(x)$.

(ii) To see that the function f is well-defined, we have to show that, if we chose another representative $y \in [x]$, then $[F(y)] = [F(x)]$, or equivalently that $x \sim y \implies F(x) \approx F(y)$.

There are similar variations for functions $f\colon (X/\sim) \times (X/\sim) \to Y$ or $f\colon (X/\sim) \times (X/\sim) \to X'/\approx$; we have already seen examples of this. For example, we have seen that addition and multiplication are well defined functions from $\mathbb{Q} \times \mathbb{Q}$ to $\mathbb{Q}$.

Here are some more examples:

(1) For $\mathbb{Z}/n\mathbb{Z}$, in other words for $X = \mathbb{Z}$ and the equivalence relation $\equiv \pmod{n}$, addition and multiplication are well-defined functions from $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ to $\mathbb{Z}/n\mathbb{Z}$. In fact, suppose that $a_1 \equiv a_2 \pmod{n}$ and that $b_1 \equiv b_2 \pmod{n}$. Then, by definition, there are integers k_1 and k_2 such that $a_1 - a_2 = k_1 n$ and $b_1 - b_2 = k_2 n$. Thus

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = k_1 n + k_2 n = (k_1 + k_2)n,$$

so that $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$. Likewise,

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2) \\ &= a_1 k_2 n + b_2 k_1 n = (a_1 k_2 + b_2 k_1)n. \end{aligned}$$

Hence $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

(2) For $\mathbb{R}/2\pi\mathbb{Z}$, in other words for $X = \mathbb{R}$ and the equivalence relation $\equiv \pmod{2\pi}$, it is not hard to show that addition is a well-defined function

from $(\mathbb{R}/2\pi\mathbb{Z}) \times (\mathbb{R}/2\pi\mathbb{Z})$ to $\mathbb{R}/2\pi\mathbb{Z}$. The argument is very similar to that for addition on $\mathbb{Z}/n\mathbb{Z}$. However, multiplication is **not** well-defined for $\mathbb{R}/2\pi\mathbb{Z}$, in other words one can add angles but it is not in general possible to multiply angles. Concretely, if $t \in \mathbb{R}$ but $t \notin \mathbb{Z}$, then multiplication by t is not well-defined. For example, if $\theta, \theta' \in \mathbb{R}$ are two representatives of $[\theta]$, then $\theta - \theta' = 2k\pi$ with $k \in \mathbb{Z}$. Then $t\theta - t\theta' = 2tk\pi$, and this is of the form $2\ell\pi$ for some integer $\ell \iff tk = \ell$. For multiplication to be well-defined, i.e. independent of the choice of representative, we must have $tk \in \mathbb{Z}$ for all $k \in \mathbb{Z}$. In particular, taking $k = 1$, we see that $t \in \mathbb{Z}$.