Equivalence Relations and Partial Orders

A Non-transitive Joke: \$5 is better than nothing. Nothing is better than perfect happiness.
Therefore, \$5 is better than perfect happiness.

Definition: Let X be a set. If $R \subseteq X \times X$, then R is said to be a *relation* on X. Instead of writing $(a, b) \in R$, we will write $a\,R\,b$ or if $(a, b) \notin R$, we will write $a \not R\, b$.

Relations abound in mathematics and in regular life too. We could speak of relations on the set of people like "A is a brother of B" or "A is B's aunt" or "A and B are neighbors". In mathematics, we have relations on sets of numbers like "$\leq$", "$>$", and "sum to a rational number". Another familiar relation is that of "$\subseteq$" when dealing with sets.

It is quite useful to abstract the concept of equality. Relations which behave like "equals" are called "equivalence relations" (which are defined below). Another important kind of relation abstracts the properties of $\leq$ and $\subseteq$. We call such relations "partial orders". Let us give names to some familiar properties.

Let R be a relation on a set X.

Reflexive: R is *reflexive* iff $x\,R\,x$ for all $x \in X$.

Symmetric: R is *symmetric* iff for all $x, y \in X$, $x\,R\,y$ implies $y\,R\,x$.

Anti-Symmetric: R is *anti-symmetric* iff for all $x, y \in X$, if $x\,R\,y$ and $y\,R\,x$, then $x = y$.

Transitive: R is *transitive* iff for all $x, y, z \in X$, $x\,R\,y$ and $y\,R\,z$ implies $x\,R\,z$.

Here are a few special types of relations:

Equivalence Relation: R is an *equivalence relation* iff it is *reflexive*, *symmetric*, and *transitive*.

Partial Order: X is *partially ordered* by R (or R is a *partial order* on X) iff R is *reflexive*, *anti-symmetric*, and *transitive*.

Total/Simple/Linear Order: X is *totally ordered* by R (or *simply ordered* or *linearly ordered*) iff R is a *partial order* and in addition for each $x, y \in X$ we have $x\,R\,y$ or $y\,R\,x$.

Let me note that partial and total orders have many variant definitions. These differences are either superficial and in the end, logically equivalent to our definition, or sometimes alternate definitions capture orderings more like "$<$" rather than "$\leq$". In such a case, when "$x\,R\,y$" is replaced with "$x\,R\,y$ or $x = y$" our notions of partial order and total order are recovered.

Notice that regular old equality (on some fixed set) is an equivalence relation. We will introduce more interesting equivalence relations below. Next, $\leq$ on the set of real numbers $\mathbb{R}$ is a total ordering (thus also a partial ordering). Finally, given a set X, $\mathcal{P}(X)$ (the power set of X) is partially ordered by $\subseteq$. Note that this is *not* a total order when X has at least 2 elements since in this case we can finds subsets of X, A and B, such that $A \not\subseteq B$ and $B \not\subseteq A$.

Example: Let X be a non-empty set and define $R = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid A \cap B = \emptyset\}$. So in other words, $A\,R\,B$ iff A and B are disjoint subsets of X. This relation is not reflexive: $X \not R\, X$ since $X \cap X = X \neq \emptyset$. This relation is symmetric since A and B are disjoint if and only if B and A are disjoint. This relation fails to be anti-symmetric since just because A and B are disjoint does not mean that $A = B$. Also, this relation fails to be transitive since if A and B are disjoint as well as B and C are disjoint, then it does not follow that A and C are disjoint (consider $A = C$).

Now let us turn our attention more fully to equivalence relations.

Example: $X = \mathbb{Z} \times \mathbb{Z}_{\neq 0}$. Let $(a,b),(c,d) \in X$. Define $(a,b) \sim (c,d)$ iff $ad = bc$.

- $(a,b) \sim (a,b)$ since $ab = ba$. Therefore, $\sim$ is reflexive.
- If $(a,b) \sim (c,d)$, then $ad = bc$. Thus $cb = da$ so $(c,d) \sim (a,b)$. Thus $\sim$ is symmetric.
- Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $ad = bc$ and $cf = de$. Multiplying the first equation by f and the second equation by b, we get that $adf = bcf$ and $bcf = bde$. Thus $afd = bed$. Now recall that $d \neq 0$ (since $(c,d) \in X = \mathbb{Z} \times \mathbb{Z}_{\neq 0}$) so $af = be$. Thus $(a,b) \sim (e,f)$. Therefore, $\sim$ is transitive.

We have just proved that $\sim$ is an equivalence relation. This really isn't that surprising considering that $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. Our relation is merely encoding equality of fractions. No wonder so many elementary and middle school students have troubles with fractions. Equivalence of fractions is many students' first exposure to a non-trivial mathematical equivalence relation.

Definition: Suppose that $\sim$ is an equivalence relation on X. For each $a \in X$, let $[a] = \{x \in X \mid x \sim a\}$. Thus $[a]$ is the set of all the elements of X which are related to a. We call $[a]$ the *equivalence class* of a, and we say that a is a *representative* of this equivalence class.

At this point it is worth mentioning that there is no *standard* notation for equivalence classes. We will use $[a]$ here. Another common notation is $\bar{a}$, but there isn't any accepted standard notation across all textbooks.

Definition: Let $\mathcal{P} \subseteq \mathcal{P}(X)$ and suppose that $\emptyset \notin \mathcal{P}$ ($\mathcal{P}$ is a collection of non-empty subsets of X). Next, suppose that $\cup\mathcal{P} = X$. This means that for each $x \in X$ there exists some $A \in \mathcal{P}$ such that $x \in A$. Finally, suppose that given $A, B \in \mathcal{P}$, either $A \cap B = \emptyset$ or $A = B$. This means that distinct elements of $\mathcal{P}$ are disjoint. In such a case, we call $\mathcal{P}$ a *partition* of X.

Theorem: Let $\sim$ be an equivalence relation on X. Then the equivalence classes of $\sim$ partition X. Conversely, given a partition $\mathcal{P}$ of X, define $a \sim b$ iff there exists some $E \in \mathcal{P}$ such that $a, b \in E$. Then $\sim$ is an equivalence relation on X whose equivalence classes are precisely the elements of $\mathcal{P}$.

proof: Let $\sim$ be an equivalence relation on X. Let $a \in X$. Then $\sim$ is reflexive so $a \sim a$. Thus $a \in [a]$. This means that every equivalence class is non-empty. Also, this shows that every element of X belongs to some equivalence class. Therefore to establish that the equivalence classes of $\sim$ partition X it only remains to show that distinct equivalence classes are disjoint.

Suppose $a, b \in X$ and $[a] \cap [b] \neq \emptyset$. We must show that $[a] = [b]$. Note that since $[a] \cap [b] \neq \emptyset$, there exists some $c \in [a] \cap [b]$. Thus $c \sim a$ and $c \sim b$. Our relation is symmetric so we also have $a \sim c$. Then since $a \sim c$ and $c \sim b$ by transitivity we have $a \sim b$. Again by symmetry we have $b \sim a$.

Suppose that $x \in [a]$. Then, by definition, $x \sim a$. So since $x \sim a$ and $a \sim b$, by transitivity we have $x \sim b$. This means $x \in [b]$ and so $[a] \subseteq [b]$. Likewise, suppose $x \in [b]$. Then $x \sim b$ and $b \sim a$ so $x \sim a$. Thus $x \in [a]$ and so $[b] \subseteq [a]$. Therefore, $[a] = [b]$.

Conversely, suppose $\mathcal{P}$ is a partition of X. Define $a \sim b$ iff there exists some $E \in \mathcal{P}$ such that $a, b \in E$.

First, let $a \in X$. Then since $\mathcal{P}$ is a partition, there exists some $A \in \mathcal{P}$ such that $a \in A$. Thus $a, a \in A$ so $a \sim a$ (our relation is reflexive). Next, suppose $a \sim b$. Then there exists some $E \in \mathcal{P}$ such that $a, b \in E$ so $b, a \in E$ thus $b \sim a$ (our relation is symmetric). Finally, suppose $a \sim b$ and $b \sim c$. Therefore, there exists some $E, E' \in \mathcal{P}$ such that $a, b \in E$ and $b, c \in E'$. Thus $b \in E \cap E'$ so that $E \cap E' \neq \emptyset$. Now distinct sets in a partition are disjoint. Thus $E = E'$ so $a, b, c \in E = E'$. In particular $a, c \in E$. Thus $a \sim c$ (our relation is transitive).

Let $E \in \mathcal{P}$. Then $E \neq \emptyset$ so there exists some $a \in E$. Notice that $x \in E$ implies $a, x \in E$ which implies $x \sim a$. Thus $x \in [a]$, so $E \subseteq [a]$. Suppose that $x \in [a]$. Then $x \sim a$ so there exists some $E' \in \mathcal{P}$ such that $a, x \in E'$. But $a \in E \cap E'$ so $E = E'$. Therefore, $a, x \in E = E'$. In particular, $x \in E$. Thus $[a] \subseteq E$ and so $E = [a]$. We have now shown that the equivalence classes of $\sim$ are the same as the elements of $\mathcal{P}$. $\square$

So every equivalence relation yields a partition and every partition yields an equivalence relation. Now we can use these concepts interchangeably.

Example: Let $f : X \to Y$ be a function. Define $\mathcal{P} = \{f^{-1}(\{f(x)\}) \mid x \in X\}$. In other words, $\mathcal{P}$ is the collection of inverse images of elements of the range of f. We say $\mathcal{P}$ is the collection of *fibers* of f.

For example: Let $f : \{1, 2, 3, 4\} \to \{a, b, c\}$. Let $f(1) = f(2) = a$ and $f(3) = f(4) = b$. Then $f^{-1}\{f(1)\} = f^{-1}\{f(2)\} = f^{-1}(\{a\}) = \{1, 2\}$ and $f^{-1}\{f(3)\} = f^{-1}\{f(4)\} = f^{-1}(\{b\}) = \{3, 4\}$. So for this function f, $\mathcal{P} = \{\{1, 2\}, \{3, 4\}\}$. This is a partition of $\{1, 2, 3, 4\}$.

In general, we can define $x \sim y$ iff $f(x) = f(y)$. This is obviously an equivalence relation. Notice that $[x] = \{y \in X \mid y \sim x\} = \{y \in X \mid f(y) = f(x)\} = f^{-1}(\{f(x)\})$. Thus the fibers of f are precisely the equivalence classes of $\sim$. Therefore, the fibers of f always partition $\mathcal{P}$.

Example: *Congruence modulo n* Let's fix a positive integer $n \in \mathbb{Z}_{>0}$. We say that $a, b \in \mathbb{Z}$ are *congruent mod n* iff n divides $a - b$. This is equivalent to saying that there exists $k \in \mathbb{Z}$ such that $a - b = kn$ (that is $a = b + kn$). Briefly, a and b are congruent mod n iff they are off by a multiple of n. This is denoted: $a \equiv b \pmod{n}$. Notice that this is an equivalence relation.

- $a = a + 0n$ so $a \equiv a \pmod{n}$ (reflexive).
- If $a \equiv b \pmod{n}$, then there exists some $k \in \mathbb{Z}$ such that $a = b + nk$ so $b = a + (-k)n$ (where $-k \in \mathbb{Z}$). Thus $b \equiv a \pmod{n}$ (symmetric).
- Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then there exists $k, \ell \in \mathbb{Z}$ such that $a = b + kn$ and $b = c + \ell n$. Therefore, $a = b + kn = (c + \ell n) + kn = c + (\ell + k)n$ where $\ell + k \in \mathbb{Z}$. Thus $a \equiv c \pmod{n}$ (transitive).

Since this is an equivalence relation, we can speak of its equivalence classes:

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{b \in \mathbb{Z} \mid b = a + kn \text{ for some } k \in \mathbb{Z}\}$$

Let $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ (all of the integral multiples of n). Then let $a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$ (a added to every element of the previous set). Therefore, $[a] = a + n\mathbb{Z}$.

Let's set $n = 4$. Then $\cdots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv \cdots \pmod{4}$. Also, $\cdots \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv \cdots \pmod{4}$. And, for example, $-9 \equiv 43 \pmod{4}$ since $43 - (-9) = 52 = (13)4$ (43 and -9 are off by a multiple of 4). The equivalence classes modulo 4 are...

- $0 + 4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, \ldots\}$
- $1 + 4\mathbb{Z} = \{\ldots, -11, -7, -3, 1, 5, 9, \ldots\}$
- $2 + 4\mathbb{Z} = \{\ldots, -10, -6, -2, 2, 6, 10, \ldots\}$
- $3 + 4\mathbb{Z} = \{\ldots, -9, -5, -1, 3, 7, 11, \ldots\}$

Notice that since $-9 \equiv 43 \equiv 3 \pmod{4}$, they all represent the same equivalence class. This means that as sets $-9 + 4\mathbb{Z} = 43 + 4\mathbb{Z} = 3 + 4\mathbb{Z}$.

Recall the *Division Algorithm* from elementary school: *Suppose $a, b \in \mathbb{Z}$ and $b \neq 0$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.* All the Division Algorithm says it that we can divide with remainder.

Therefore, given any $x \in \mathbb{Z}$, there exists unique $q, r \in \mathbb{Z}$ such that $x = nq + r$ where $0 \leq r < n$. This means that each integer x is equivalent (mod n) to a unique integer $r = 0, 1, \ldots, n-1$.

So the equivalence classes modulo n are precisely: $n\mathbb{Z}$, $1+n\mathbb{Z}$, $2+n\mathbb{Z}$, $\ldots$, $(n-1)+n\mathbb{Z}$. This is exactly what we saw when we were working mod $n = 4$.

When working with equivalence relations a new problem arises. Often we want to define functions and operations in terms of representatives for our equivalence classes. If we are not careful, we can end up with "functions" which aren't it well-defined.

Definition: Something is *well-defined* if its computation does not depend on the chosen representation. In particular, *functions* are well defined since $x = y$ implies that $f(x) = f(y)$ (equivalent inputs yield equivalent outputs).

Theorem: The operations of addition and multiplication modulo n are well-defined. In particular, if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

proof: Suppose that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then there exist $k, \ell \in \mathbb{Z}$ such that $a = a' + kn$ and $b = b' + \ell n$. Therefore, $a + b = (a' + kn) + (b' + \ell n) = a' + b' + (k + \ell)n$ where $k + \ell \in \mathbb{Z}$. Thus $a + b \equiv a' + b' \pmod{n}$. The proof that multiplication is well-defined is similar. $\square$

Since the choice of representation doesn't matter, we can add and multiply whole equivalence classes. For example, let $n = 4$. Then $[2] + [3] = [2 + 3] = [5]$ but $5 \equiv 1 \mod 4$. Therefore, $[2] + [3] = [1]$. Being a bit more lax with notation, we might write "$2 + 3 = 1$" when working mod 4. Notice that $[2] = [18]$ and $[3] = [-5]$ so $[2] + [3] = [18] + [-5] = [13]$ But $13 \equiv 1 \pmod{4}$ so again we get $[2] + [3] = [13] = [1]$.

What is $3^{50} \pmod{4}$? Multiplying 3 by itself 50 times seems quite daunting. So instead let's notice that $3 \equiv -1 \pmod{4}$. Thus (when working mod 4) we have $3^{50} = (-1)^{50} = 1$. That was easy!

The next examples indicate that when dealing with equivalence classes, we should proceed with caution!

Example: Recall that $\mathbb{Q}$ is the set of rational numbers (i.e. fractions of integers). Let's "define" the "function" $f : \mathbb{Q} \to \mathbb{Z}$ by letting $f(p/q) = p$. In other words, f is the "numerator function".

But this *isn't a function*! Notice that $12/9 = 4/3$ but $f(12/9) = 12$ and $f(4/3) = 4$. Equal inputs do *not* give equal outputs. This isn't actually a function. Now of course this could be repaired, we could demand that p/q is a reduced fraction and that $q > 0$. Then the numerator would be uniquely determined. But as it stands, our "function" is no function at all.

Let $\mathbb{Z}_n$ be the set of equivalence classes mod n. We proved above that this set has well-defined addition and multiplication operations. The next example shows that we still need to be careful.

Example: Let "define" the "function" $f : \mathbb{Z}_3 \to \mathbb{Z}_{10}$ by $f([x]) = [2x]$. So we are mapping the equivalence class $[x] = x + 3\mathbb{Z}$ to the class $[2x] = 2x + 10\mathbb{Z}$. Notice that we have changed our modulus from 3 to 10. This causes a problem! Consider that $5 \equiv 8 \pmod{3}$ but $f(5) = 2(5) = 10 \equiv 0 \pmod{10}$ while $f(8) = 2(8) = 16 \equiv 6 \pmod{10}$. So even though $[5] = [8] \pmod{3}$, we have $f([5]) = [10] \neq [16] = f([8]) \pmod{10}$. Since equal inputs do not yield equal outputs, f isn't actually a function!

Example: Let's show $f : \mathbb{Z}_9 \to \mathbb{Z}_3$ where $f([x]) = [2x]$ is well-defined. Suppose that $[x] = [y]$ (in $\mathbb{Z}_9$). Then $x = y + 9k$ for some $k \in \mathbb{Z}$. Now $2x = 2(y + 9k) = 2y + 3(6k)$ and $6k \in \mathbb{Z}$. Thus $f([x]) = [2x] = [2y] = f([y])$ (in $\mathbb{Z}_3$). Thus f is well-defined!