6-18-2013

Equivalence Relations and Partitions

First, I'll recall the definition of an **equivalence relation** on a set X.

Definition. An **equivalence relation** on a set X is a relation $\sim$ on X such that:

1. $x \sim x$ for all $x \in X$. (The relation is **reflexive**.)
2. If $x \sim y$, then $y \sim x$. (The relation is **symmetric.**)
3. If $x \sim y$ and $y \sim z$, then $x \sim z$. (The relation is **transitive**.)

Example. Define a relation on $\mathbb{Z}$ by $x \sim y$ if and only if $x + 2y$ is divisible by 3.

For example:

$2 \sim 11$, since $2 + 2 \cdot 11 = 24$, and 24 is divisible by 3.

$7 \sim -8$, since $7 + 2 \cdot (-8) = -9$, and -9 is divisible by 3.

However, $6 \not\sim 14$, since $6 + 2 \cdot 14 = 34$, and 34 is **not** divisible by 3.

I'll check that this is an equivalence relation. In this proof, two of the parts might be a little tricky for you, so I'll work through the thought process rather than just giving the proof. (You might see if you can work this out yourself before you read on.)

If x is an integer, $x + 2x = 3x$ is divisible by 3. Therefore, $x \sim x$ for all $x \in \mathbb{Z}$, and $\sim$ is reflexive.

Suppose x and y are integers. If $x \sim y$, then $x + 2y$ is divisible by 3. Say $x + 2y = 3n$, where $n \in \mathbb{Z}$. Now

$$\begin{aligned} y + 2x &= (3x + 3y) - (x + 2y) \\ &= (3x + 3y) - 3n \\ &= 3(x + y - n) \end{aligned}$$

Therefore, $y + 2x$ is divisible by 3, so $y \sim x$. Hence, $\sim$ is symmetric.

You might be wondering how I knew to start with "$y+2x = (3x+3y)-(x+2y)$". I reasoned backwards on scratch paper this way.

To prove symmetry, I had to show that if $x \sim y$, then $y \sim x$.

By the definition of $\sim$, that's the same as showing: If $x + 2y$ is divisible by 3, then $y + 2x$ is divisible by 3.

If $x + 2y$ being divisible by 3 is going to force $y + 2x$ to be divisible by 3, there's probably be some connection involving 3, $x + 2y$, and $y + 2x$.

As in many proofs, you often reach a point where you need to play around with the stuff you have. You don't **know** in advance what will work, and there isn't a step-by-step method for finding out. You have to experiment.

So you think: "3?" "$x + 2y$?" "$y + 2x$?" You might try various ways of combining the expressions ... and maybe you realize that $x + 2x = 3x$ and $y + 2y = 3y$ (notice the 3's!), and then:

$$(x + 2y) + (y + 2x) = 3x + 3y.$$

Since the "then" part of what I want to prove involves $y + 2x$, I'll solve the last equation for $y + 2x$:

$$y + 2x = (3x + 3y) - (x + 2y).$$

And there's the equation I started with.

Now suppose x, y, and z are integers. Assume $x \sim y$ and $y \sim z$. This means that $x + 2y$ is divisible by 3, and $y + 2z$ is divisible by 3. I'll express these as equations:

$$x + 2y = 3m \quad \text{for some} \quad m \in \mathbb{Z}.$$

$$y + 2z = 3n \quad \text{for some} \quad n \in \mathbb{Z}.$$

I want to show that $x + 2z$ is divisible by 3. My proof looks like this so far, with the assumptions at the top and the conclusion at the bottom.

$$\begin{array}{ccc} x \sim y & & y \sim z \\ 3 \mid x + 2y & & 3 \mid y + 2z \\ x + 2y = 3m & & y + 2z = 3n \\ & \vdots & \\ & x + 2z = 3(\text{something}) & \\ & 3 \mid x + 2z & \\ & x \sim z & \end{array}$$

How can I get from $x + 2y = 3m$ and $y + 2z = 3n$ to $x + 2z = 3(\text{something})$? *Make what you've got look like what you want.* What I have involves x, y, and z, but what I want seems to involve only x and z. It looks like I want to get rid of the y's. How can I do that? One way is to solve the second equation for y:

$$\begin{aligned} y + 2z &= 3n \\ y &= 3n - 2z \end{aligned}$$

Then plug into the first:

$$\begin{aligned} x + 2y &= 3m \\ x + 2(3n - 2z) &= 3m \\ x + 6n - 4z &= 3m \end{aligned}$$

I look at my target equation $x + 2z = 3(\text{something})$. *Make what you've got look like what you want.* I need $x + 2z$ on the left side, so I'll just do algebra to force it to happen:

$$\begin{aligned} x + 6n - 4z &= 3m \\ x &= 3m - 6n + 4z \\ x + 2z &= 3m - 6n + 6z \end{aligned}$$

The left side is what I want $(x + 2z)$, but I need $3(\text{something})$ on the right ... oh, just factor out 3:

$$x + 2z = 3(m - 2n + 2z).$$

I'll plug this derivation into the proof outline above:

$$\begin{array}{ccc} x \sim y & & y \sim z \\ 3 \mid x + 2y & & 3 \mid y + 2z \\ x + 2y = 3m & & y + 2z = 3n \\ & & y = 3n - 2z \\ & x + 2(3n - 2z) = 3m & \\ & x + 6n - 4z = 3m & \\ & x = 3m - 6n + 4z & \\ & x + 2z = 3m - 6n + 6z & \\ & x + 2z = 3(m - 2n + 2z) & \\ & x + 2z = 3(\text{something}) & \\ & 3 \mid x + 2z & \\ & x \sim z & \end{array}$$

This is a complete proof of transitivity, though some people might prefer more words. Thus, $\sim$ is an equivalence relation.

Notice that if you were presented with this proof without any of the scratchwork or backward reasoning, it might look a little mysterious: You can see each step is correct, but you might wonder how anyone would think of doing those things in that order. This is an unfortunate consequence of the way math is often presented: After the building is finished, the scaffolding is removed, and you may then wonder how the builders managed to get the materials up to the roof!

The lesson here is that you should **not** look at a finished proof and assume that the person who wrote it had a flash of genius and then wrote the thing down from start to finish. While that can happen, more often proofs involve messing around and attempts that don't work and lots of scratch paper! $\square$

Example. If $a, b \in \mathbb{Z}$ and n is a fixed positive integer, define $a \sim b$ if n divides $a - b$ — that is, if $a - b = kn$, for some integer k. This relation is called **congruence mod n**.

Instead of writing $a \sim b$, it's customary to write $a = b \pmod{n}$. For example, $11 = 5 \pmod{3}$, because 3 divides $11 - 5 = 6$. Likewise, $34 = 0 \pmod{17}$, because 17 divides $34 - 0 = 34$.

Here are the three equivalence relation axioms written in this notation:

(a) Let $a \in \mathbb{Z}$. Then $a = a \pmod{n}$.

(b) Let $a, b \in \mathbb{Z}$. If $a = b \pmod{n}$, then $b = a \pmod{n}$.

(c) Let $a, b, c \in \mathbb{Z}$. If $a = b \pmod{n}$ and $b = c \pmod{n}$, then $a = c \pmod{n}$.

As an example, I'll prove (b). Suppose $a = b \pmod{n}$. Then n divides $a - b$, so

$$a - b = kn \quad \text{for some} \quad k \in \mathbb{Z}.$$

Multiplying this equation by -1, I get

$$b - a = (-k)n.$$

Since $-k$ is also an integer, this means that n divides $b - a$, and so $b = a \pmod{n}$.

Try to work out the proofs of (a) and (d) yourself.

You can see that these look like *equations* — and in fact, you can work with them the way you'd work with equations. For example, you can add a number to both sides of an equation, and this works for congruences mod n as well.

To see this, suppose $a = b \pmod{n}$. Let $c \in \mathbb{Z}$. I'll prove that $a + c = b + c \pmod{n}$.

Since $a = b \pmod{n}$, $a - b = kn$ for some integer k. Then

$$(a + c) - (b + c) = kn.$$

This proves that $a + c = b + c \pmod{n}$. $\square$

Equivalence relations give rise to **partitions**. Here's an example before I give the definition. Consider the equivalence relation of congruence mod 3 on $\mathbb{Z}$. The integers break up into three *disjoint* sets:

$$\{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}, \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}, \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

All the elements of a given set are congruent mod 3, and no element in one set is congruent mod 3 to an element of another. The sets divide up the integers like three puzzle pieces. The three sets are called the **equivalence classes** corresponding to the equivalence relation.

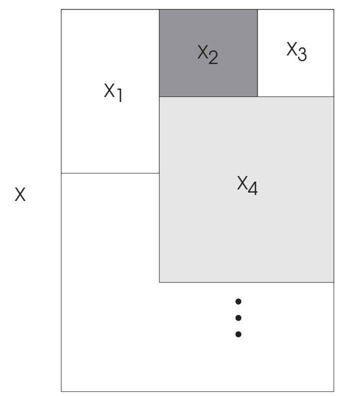
In general, if $\sim$ is an equivalence relation on a set X and $x \in X$, the **equivalence class of** x consists of all the elements of X which are equivalent to x.

Definition. Let X be a set. A **partition** of X is a collection of subsets $\{X_i\}_{i \in I}$ of X such that:

1. $X = \displaystyle\bigcup_{i \in I} X_i$.

2. If $i, j \in I$ and $i \neq j$, then $X_i \cap X_j = \emptyset$.

Thus, the elements of a partition are like the pieces of a jigsaw puzzle:



Example. The four suits (spades, hearts, diamonds, clubs) partition a deck of playing cards (not counting the Joker). Every card is in one of these suits, and no card is in more than one suit. □

Example.

$$\{-2, -1, 0, 1, 2, 3, \ldots\} \quad \text{and} \quad \{\ldots, -3, -2, -1, 0, 1, 2\}$$

do *not* partition the set of integers: Every integer is in one of these sets, but the two sets overlap. □

Example. The set $\mathbb{R}$ of real numbers is partitioned by the set $\mathbb{Q}$ of rational numbers and the set $\mathbb{R} - \mathbb{Q}$ of irrational numbers. Every real number is either rational or irrational, and no real number is both.

In general, if X is a set and S is a subset of X, then $\{S, X - S\}$ is a partition of X. □

Example. If n is a nonzero integer and $a \in \mathbb{Z}$, define

$$[a] = \{b \in \mathbb{Z} \mid b = a \pmod{n}\}.$$

I'll show that these sets are equivalence classes for the congruence mod n relation. This means that I need to show that $x = y \pmod{n}$ if and only if $[x] = [y]$.

Suppose $x = y \pmod{n}$, so $n \mid x - y$. I want to show $[x] = [y]$. If $z \in [x]$, then $z = x \pmod{n}$, so $n \mid z - x$. Hence, $n \mid (z - x) + (x - y) = z - y$, so $z = y \pmod{n}$. This means that $z \in [y]$, and I've shown that $[x] \subset [y]$. The same argument with x and y switched shows that $[y] \subset [x]$, so $[x] = [y]$.

Suppose $[x] = [y]$. I want to show $x = y \pmod{n}$. But $x \in [x] = [y]$, so $x = y \pmod{n}$.

I've shown that the sets $[a]$ are equivalence classes under congruence mod n; $[a]$ is called the **congruence class** of a mod n.

When $n = 2$, the equivalence classes under congruence mod 2 are the even integers and the odd integers.

When $n = 5$, the equivalence classes under congruence mod 5 are integers which leave a remainder of 0, 1, 2, 3, or 4 upon division by 5. In the picture below, the elements in the grey circles in a given line are the elements in a congruence class mod 5.

For example, the first line with the elements -5, 0, 5 shows that elements which leave a remainder of 0 when divided by 5. The whole equivalence class is the infinite set $\{\ldots, -15, -10, -5, 0, 5, 10, 15 \ldots\}$. $\square$

Here is how equivalence relations are related to partitions.

Theorem. Let X be a set. An equivalence relation $\sim$ on X gives rise to a partition of X into **equivalence classes**. Conversely, a partition of X gives rise to an equivalence relation on X whose equivalence classes are exactly the elements of the partition.

Proof. Suppose $\sim$ is an equivalence relation on X. If $x \in X$, let

$$S(x) = \{y \in X \mid y \sim x\}$$

denote the equivalence class of x. $x \sim x$, so $x \in S(x)$. Clearly, $X = \bigcup_{x \in X} S(x)$.

Now some of the $S(x)$'s may be identical; throw out the duplicates. This means that I have $S(x)$'s where $x \in Y$, and Y is a subset of X — and if $x, y \in Y$ and $x \neq y$, then $S(x) \neq S(y)$. Since I've just thrown out duplicates, I still have $X = \bigcup_{x \in Y} S(x)$. I will have a partition if I show that the remaining $S(x)$'s don't intersect.

Suppose $x, y \in Y$, $x \neq y$, but $z \in S(x) \cap S(y)$. I'll show that this gives a contradiction. By definition, $z \sim x$ and $z \sim y$, so by symmetry and transitivity, $x \sim y$.

Now I'll show $S(x) = S(y)$. *The standard way to show two sets are equal is to show each is contained in the other.* Suppose $w \in S(x)$. Then $w \sim x$, but $x \sim y$, so $w \sim y$, and $s \in S(y)$. This shows $S(x) \subset S(y)$. But the argument clearly works the other way around, so $S(y) \subset S(x)$. Hence, $S(x) = S(y)$.

Since I threw out all the duplicates earlier, this is a contradiction. Hence, there is no such z: $S(x) \cap S(y) = \emptyset$. This means that the $S(x)$'s for $x \in Y$ partition X.

Conversely, suppose $\{X_i\}_{i \in I}$ is a partition of X. Define a relation on X by saying $x \sim y$ if and only if $x, y \in X_i$ for some $i \in I$.

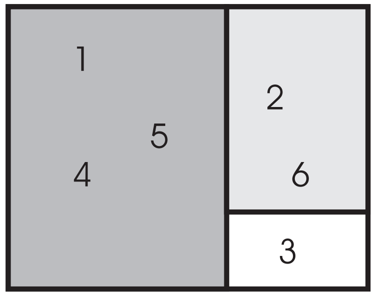
If $x \in X$, $x \in X_i$ for some i because $X = \bigcup_{i \in I} X_i$. Now x is in the same X_i as itself — $x, x \in X_i$ — so $x \sim x$. It's reflexive.

If $x \sim y$, then $x, y \in X_i$ for some i. Obviously, $y, x \in X_i$, so $y \sim x$. It's symmetric.

Finally, if $x \sim y$ and $y \sim z$, then $x, y \in X_i$ and $y, z \in X_j$ for some i and j. Now $y \in x_i \cap X_j$, but this can only happen if $X_i = X_j$. Then $x, z \in X_i$, so $x \sim z$. It's transitive, and hence it's an equivalence relation.

The equivalence classes of $\sim$ are exactly the X_i's, by construction. $\square$

Example. Suppose $X = \{1, 2, 3, 4, 5, 6\}$. Consider the following partition of X:



The equivalence relation defined by this partition is

$$1 \sim 4 \sim 5, \quad 2 \sim 6, \quad 3.$$

In other words, 1, 4, and 5 are equivalence to each other, 2 and 6 are equivalent, and 3 is only equivalent to itself. $\square$

Example. Consider the equivalence relation on $\mathbb{R}$ defined by $x \sim y$ if and only if $x - y \in \mathbb{Z}$ — that is, if $x - y$ is an integer.

Let $x \in \mathbb{R}$. Then $x - x = 0 \in \mathbb{Z}$. Therefore, $x \sim x$, and $\sim$ is reflexive.

Suppose $x \sim y$, so $x - y \in \mathbb{Z}$. Since the negative of an integer is an integer, $y - x \in \mathbb{Z}$. Hence, $y \sim x$, and $\sim$ is symmetric.

Suppose $x \sim y$ and $y \sim z$. Then $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$. But the sum of integers is an integer, so

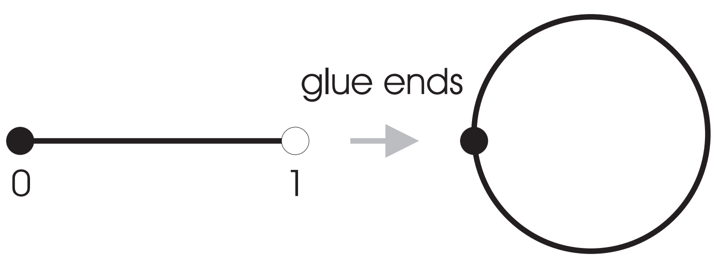
$$x - z = (x - y) + (y - z) \in \mathbb{Z}.$$

Therefore, $x \sim z$, and $\sim$ is transitive. Thus, $\sim$ is an equivalence relation.

Here's a typical equivalence class for $\sim$:

$$\{\ldots, -4.3942, -3.3942, -2.3942, -1.3942, 0.3942, 1.3942, \ldots\}.$$

A little thought shows that all the equivalence classes look like like one: All real numbers with the same "decimal part". Each class will contain one element — 0.3942 in the case of the class above — in the interval $0 \le x < 1$. *Therefore, the set of equivalence classes of* $\sim$ *looks like* $0 \le x < 1$. Moreover, since $0 \sim 1$, it's as if this interval had its ends "glued together":



This is an important use of equivalence relations in mathematics — to "glue together" or *identify* parts of a set to create a new set. $\square$

Example. Let S be the set of integers from 1 to 50. Define $x \sim y$ if the product of the digits in x is the same as the product of the digits in y.

To make the proofs of the axioms simpler, let

$$P(x) = (\text{the product of the digits of } x).$$

Thus, $x \sim y$ means $P(x) = P(y)$.
Since $P(x) = P(x)$, it follows that $x \sim x$, and $\sim$ is reflexive.
Suppose $x \sim y$, so $P(x) = P(y)$. Then $P(y) = P(x)$, so $y \sim x$. Hence, $\sim$ is symmetric.
Suppose $x \sim y$ and $y \sim z$. Then

$$P(x) = P(y) \quad \text{and} \quad P(y) = P(z), \quad \text{so} \quad P(x) = P(z).$$

Therefore, $x \sim z$. Hence, $\sim$ is transitive. Therefore, $\sim$ is an equivalence relation.
Here are the equivalence classes:

Product	Elements
0	0, 10, 20, 30, 40, 50
1	1, 11
2	2, 12, 21
3	3, 13, 31
4	4, 14, 22, 41
5	5, 15
6	6, 16, 23, 32
7	7, 17
8	8, 18, 24, 42
9	9, 19, 33
10	25
12	26, 34, 43
14	27
15	35
16	28, 44
18	29, 36
20	45
21	37
24	38, 46
27	39
28	47
32	48
36	49

Thus, the equivalence class consisting of elements of S whose digits multiply to give 24 consists of 38 $(3 \cdot 8 = 24)$ and 46 $(4 \cdot 6 = 24)$. The largest equivalence class consists of elements whose digits multiply to 0: It has 6 elements. A number of equivalence classes consist of a single element. $\square$

Example. Let $X = \mathbb{R}^2$, the x-y plane. Define $(x_1, y_1) \sim (x_2, y_2)$ to mean that

$$x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

In words, this means that (x_1, y_1) and (x_2, y_2) are the same distance from the origin.
Since $x^2 + y^2 = x^2 + y^2$, it follows that $(x, y) \sim (x, y)$. Hence, the relation is reflexive.
Suppose $(x_1, y_1) \sim (x_2, y_2)$, so

$$x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Then

$$x_2^2 + y_2^2 = x_1^2 + y_1^2.$$

Hence, $(x_2, y_2) \sim (x_1, y_1)$. Hence, the relation is symmetric.
Suppose $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Then

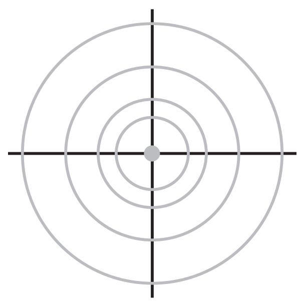
$$x_1^2 + y_1^2 = x_2^2 + y_2^2 \quad \text{and} \quad x_2^2 + y_2^2 = x_3^2 + y_3^2.$$

Hence,

$$x_1^2 + y_1^2 = x_3^2 + y_3^2.$$

Therefore, $(x_1, y_1) \sim (x_3, y_3)$. Hence, the relation is transitive. This show that $\sim$ is an equivalence relation.

The resulting partition of $\mathbb{R}^2$ into equivalence classes consists of circles centered at the origin. The origin is in an equivalence class by itself.



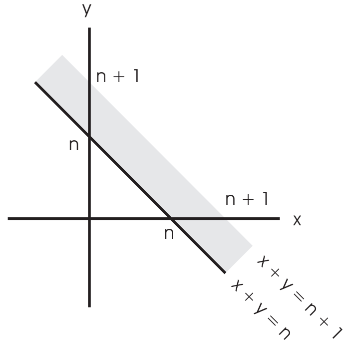
Notice that the axioms for a partition are satisfied: Every point in the plane lies in one of the circles, and no point lies in two of the circles. □

Example. Consider the partition of the x-y plane consisting of the sets

$$S_n = \{(x, y) \mid n \leq x + y < n + 1\}$$

for $n \in \mathbb{Z}$.

Here's a picture of S_n: It consists of the points between $x + y = n$ and $x + y = n + 1$, together with the line $x + y = n$:



You can see that these sets fill up the plane, and no point lies in more than one of the sets.

This partition *induces* an equivalence relation $\sim$ on the plane: Two points are equivalent if they lie in the same S_n.

For example, consider $(2.4, -1.6)$ and $(-2.1, 2.7)$.

$$2.4 + (-1.6) = 0.8 \quad \text{and} \quad -2.1 + 2.7 = 0.6.$$

0.8 and 0.6 both lie between 0 and 1, so $(2.4, -1.6)$ and $(-2.1, 2.7)$ lie in S_0. Therefore, $(2.4, -1.6) \sim (-2.1, 2.7)$.

On other other hand, consider $(5.3, 1.7)$ and $(8, -1.5)$. $5.3+1.7 = 7$, so $(5.3, 1.7) \in S_7$. $8+(-1.5) = 6.5$, so $(8, -1.5) \in S_6$. Therefore, $(5.3, 1.7) \not\sim (8, -1.5)$. $\square$

Example. Define a relation $\sim$ on $\mathbb{R}$ by

$$x \sim y \quad \text{means} \quad |x| + |y| = |x + y|.$$

Which of the axioms for an equivalence relation does $\sim$ satisfy?

For all $x \in \mathbb{R}$,

$$|x| + |x| = 2|x| = |2x| = |x + x|.$$

Therefore, $x \sim x$ for all x, and $\sim$ is reflexive.

Suppose $x \sim y$. This means that $|x| + |y| = |x + y|$. By commutativity of addition, $|y| + |x| = |y + x|$. Hence, $y \sim x$. Therefore, $\sim$ is symmetric.

Transitivity does not hold.

$$|1| + |0| = |1 + 0|, \quad \text{so} \quad 1 \sim 0.$$

$$|0| + |-1| = |0 + -1|, \quad \text{so} \quad 0 \sim -1.$$

However, $1 \not\sim -1$, because

$$|1| + |-1| \neq |1 + (-1)|.$$

Therefore, $1 \sim 0$ and $0 \sim -1$ do not imply $1 \sim -1$. $\square$
