# Some Basic Algebraic Ideas

Math 12, Veritas Prep.

**As a prescript:** I think these notes are very good and very well-written, but they're also quite dense. It will take careful, slow reading—and certainly multiple readings—to understand them.

## Relations and Operations

This is not the place I thought of starting, but it came up as a conversation in one of the classes, so perhaps it is the natural starting place.

What is the difference between saying something like "$A \setminus B$" and and saying "$A \subset B$"? To use a different example: what's the difference between saying something like "$A \cup B$" and saying "$A = B$"? Or if we think about numbers instead of sets: what's the difference between saying "$5 + 2$" and saying "$5 > 2$"? In all of these instances, I'm somehow connecting two things (a set, a number, whatever) with a verb. Other than the fact that the specific ways of combining are different, what's the general difference between the former examples and the latter examples? What do $\setminus$, $\cup$, and $+$ have in common with each other, what do $\subset$, $=$, and $>$ have in common with each other, and what's the difference between these two types of things?

Let's talk about some specific cases before we generalize. What I mean by saying "$A \setminus B$" is that I have two sets, $A$ and $B$, and I've combined these sets in some sort of way such that I've created a third set (which, for lack of a better name, is "$A \setminus B$"). But if I say $A \subset B$, I am not *doing* anything to $A$ and $B$—I am merely describing a *relationship* between them. This can be true or false—either $A$ **is** a subset of $B$ (so "$A \subset B$" is true), or $A$ is **not** a subset of $B$ (so "$A \subset B$" is false).

Perhaps that example, with the arbitrary sets $A$ and $B$, is a bit too abstract. What if I consider the (concrete) sets $\mathbb{R}$ and $\mathbb{Q}$ instead? If I say $\mathbb{R} \setminus \mathbb{Q}$, then I'm combining these two sets, the rationals and the reals, in such a way that I get a new, third set (the irrationals, in this case). But if I say $\mathbb{Q} \subset \mathbb{R}$, I am not creating anything new—I am simply stating a fact, that the rationals are a subset of the reals.

Or consider numbers. If I say, for example, "$5+2$," what I've done is taken two numbers, 5 and 2, and put them together in some sort of way ("addition," whatever that is) that I've created a new number, 7. (Or at least described a new number.) On the other hand, if I say "$5 < 2$", I'm not *creating* anything—I'm not *doing* anything to 5 and 2. I'm just pointing out that 5 is less than 2. I'm describing a state of affairs—I'm stating a fact—and that fact can either be true, or false.

So here's another way to think about it: if I have an **operation**, I'm taking two objects of the same type (sets, numbers, etc.) and creating a third object of that same type (another set, a different number, etc.). If I have a **relationship** (or a **relation**), I'm taking two objects of the same type, and creating (or getting) a truth value.

So here's yet another way to think about it: operations and relationships are both functions. They're functions of two variables, yes, but still functions. If it helps you see why, you could try representing them in function notation: rather than write "$5 + 2$", you could write "$+(5, 2)$ or "$\text{Add}(5, 2)$". Rather than write "$A \cup B$," you could write "$\cup(A, B)$." (This is nothing new or interesting; it's just a different way of writing things.) Likewise with relationships: rather than write $5 = 5$, you could write "$=(5, 5)$" or "$\text{Equals}(5, 5)$" (which would, of course, be true). Or rather than write "$\mathbb{N} \subset \mathbb{Z}$", you could write "$\subset(\mathbb{N}, \mathbb{Z})$," or "$\text{Subset}(\mathbb{N}, \mathbb{Z})$". My point here is: if you're thinking of these guys as functions, an **operation** is a function whose domain (inputs) are objects of one type, and whose range (outputs) are objects of the same type. Numbers added to numbers beget numbers. Sets united with sets are other sets. A **relationship** on the other hand, is a function whose domain (inputs) are objects of some type, and whose range (outputs) are truth-values (i.e., $T$ or $F$). For example: $5 > 2$ is true (T). Or: $\mathbb{C} \subset \mathbb{Z}$ is false (F).

If I have an operation, I can ask: is it **commutative**? Meaning: does the order in which I operate the objects matter? Multiplying numbers, for instance, (any sort of numbers), is commutative: $5 \cdot 2 = 2 \cdot 5$. So is uniting sets: $A \cup B = B \cup A$. Exponentiating numbers, on the other hand, isn't: $5^2 \neq 2^5$, or in calculator

notation, $5 \wedge 2 \neq 2 \wedge 5$. More formally: an operation $*$ on a set $S$ is **commutative** if and only if, for all $a$ and $b$ in $S$, $a * b = b * a$.

I can also ask an operation: are you **associative**? Meaning, if I want to operate a bunch of things, does the sequence matter? Addition of numbers is associative, since if I want to add, say, 5, 2, and 1, it doesn't matter the order in which I do them. I can add 5 and 2, get 7, and then add 1, and I get 8. Or I can add 2 and 1, get 2, add 5, and get 8. That is to say:

$$(5 + 2) + 1 = 5 + (2 + 1)$$

Subtracting numbers, on the other hand, is not commutative:

$$(5 - 2) - 1 = 2 \text{ but } 5 - (2 - 1) = 4$$

So another way of thinking about associativity is that it's whether parentheses matter. Formally, I can define it by saying: an operation $*$ on a set $S$ is **associative** if and only if, for all $a$, $b$, and $c$ in $S$, $a * (b * c) = (a * b) * c$.

Often I have a type of object onto which I usually operate with more than one operation. I have a cancer patient, and sometimes I hack away at their tumor with a scalpel, and sometimes I drug them up with chemo. Probably the better way to put this is: often I have a set, the elements of which I often combine using more than one operation. So I might ask: how do these two operations interact with each other? For example, if I want to both multiply and add numbers, does the order matter? if I want to add two numbers, and then multiply them by a third, is there another way I can get the same result? Yes. For example, I can add 2 and 4, get 6, multiply that by 5, and get 30. Or I can multiply 2 and 5, get 10, multiply 4 and 5, get 20, and then add together 10 and 20 and get 30:

$$5 \cdot (2 + 4) = 5 \cdot 2 \ + \ 5 \cdot 4$$

So this tells me how multiplication **distributes** across addition—how addition and multiplication play together. As we've seen, unions and intersections of sets distribute in the same sort of way:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

But not every two operations distribute in this way. (Not every law that we call a "distribution law" has the same form.) Consider, for example, exponentiation and addition: $a^{b+c} = a^b \cdot a^c$. That's kind of weird—addition inside of exponentiation turns into multiplication outside of exponentiation. Or consider how the operation of union distributes across symmetric difference: $(A \triangle B) \cup C = (A \cup C) \triangle (B \setminus C)$. Very weird.

I could probably even generalize this idea of **distribution**: distribution laws describe not just how one operation interacts with another operation, but how one operation interacts with any function. For example: consider the take-the-derivative function, $\frac{d}{dx}[f(x)]$. This is not an operation, since it only takes one thing as input: it takes as input one function, and as output spits out a second function. (As opposed to, say, addition, which takes two numbers, and spits out a third.)[1] We might ask: how does the operation of addition distribute across differentiation? And the answer is that it does something very nice and clean—something analogous to the way that addition distributes across multiplication, or how uniting distributes across intersecting:

$$\frac{d}{dx}[f(x) + g(x)] = \frac{d}{dx}[f(x)] + \frac{d}{dx}[g(x)]$$

On the other hand, if I want to know how *multiplication* distributes across differentiation, the result is not so clean:

$$\frac{d}{dx}[f(x) \cdot g(x)] = \frac{d}{dx}[f(x)] \cdot g(x) + f(x) \cdot \frac{d}{dx}[g(x)]$$

[1] We could perhaps make a distinction between **binary operations**, which are operations that have two inputs, and **unary operations**, which are operations that only have one input. Both of these are just functions—it's just that the former is a function with one input, and the latter is a function with two inputs.

(Right? This is just the product rule.)

One other thing we should say about operations. We've defined an operation as being something that takes two things "of the same type" and spits out a third thing of that same type. But we could be a bit clearer. What we really mean is something like this: an operation takes two elements from a certain set, and returns elements of a third set. Matrix addition takes two elements from the set of all matrices—i.e., two matrices—and returns a third element from that set (i.e., a third matrix). So we say that operations are usually defined **over** or **with respect to** a certain set.

In this sense, then, we don't—or, according to Wittgenstein, can't—talk about operations in the abstract. There is no such thing as "union"—there is only the union OF SETS. There is no such thing as "addition"—there is only addition of real numbers. Operations are not some Platonic form floating out somewhere—they are a specific relationship between specific elements of specific sets.

On the other hand, the weird thing with the example of addition of real numbers is that we have lots of different types of numbers. There are natural numbers, integers, rational numbers, real numbers, complex numbers, hamiltonians, and so forth, and all of these sets of numbers have some sort of idea of "addition." For example: two is a natural number, three is a natural number, and if we combine these two natural numbers using natural-number-addition, we get five—another natural number. But two is also a real number, three is also a real number, and if we combine them using the operation of real-number-addition, we get five—another real number. These sets of numbers are like Russian nesting dolls, and not only do the numbers pass through from level to level—two is a natural number and an integer and a rational number and a real number and a complex number—the operations pass through, too.

But what if I'm considering the natural numbers 2 and 5, and the operation of subtraction? If I subtract 2 and 5, I get $-3$, which is NOT a natural number. So then subtraction isn't really an operation over the natural numbers, because I can feed it two natural numbers as input, and it'll poop out something that is decidedly not a natural number. The mathy word for this is **closure**, adjective **closed**: the natural numbers are not **closed under** subtraction. The integers, on the other hand, are closed under subtraction. Formally: an operation $*$ is **closed** with respect to a set $S$ if, for all $a \in S$ and $b \in S$, $(a * b) \in S$.

This is important for a variety of reasons. Because, depending on what world you live in, you can get different results. For example, if you want to fully factor

$$x^4 - 25$$

and you only believe in integers, you can only factor[2] it to

$$\left(x^2 - 5\right)\left(x^2 + 5\right)$$

But if you believe in real numbers, you can factor it further to

$$\left(x + \sqrt{5}\right)\left(x - \sqrt{5}\right)\left(x^2 + 5\right)$$

(because $\pm\sqrt{5}$ is an irrational number, which are included in the reals but not in the integers). If you believe in complex numbers, you can factor this yet further as

$$\left(x + \sqrt{5}\right)\left(x - \sqrt{5}\right)\left(x + \sqrt{-5}\right)\left(x - \sqrt{-5}\right)$$

If you live only in the world of natural numbers, you can't subtract.

If you live only in the world of integers, you can't divide.

[2]Think of factoring as being, like differentiation, a unary operation: it takes ONE thing in, and spits out one thing of the same type. It takes in polynomials written one way, and spits out polynomials written in a different way. Or, if you're talking about factoring numbers, it takes in a natural number written one way, and spits it out written a different way. (What's the common theme here? Why do we call factoring of polynomials and factoring of numbers both "factoring"? What makes them similar? What does it mean to "factor" in the abstract? Can we come up with a more fundamental definition of factoring?)

We've defined a lot of concepts in the last three pages, so keeping them straight might be a challenge. Why not try getting a stack of note cards, and on the cards putting the the concept, its definition and an example (your own, not from the text)? Perhaps it might also be helpful to include a not-example as well (ideally one that will usefully limiting the conceptual space: e.g., on your "commutative property" card, it would be true, but not particularly helpful, to write "hippopotamouses are not commutative.")

More broadly, the question is: why do we care about these ideas? why do we care about operations and relations and their properties? We are curious because we are curious about the *formal properties* of mathematical structures—about structural properties that describe not *things*, but rather *the way things interact with each other*. And we're interested in this question in the abstract—we're interested in properties that are independent of what the particular objects are, or what the particular operations are. Because that way we can ask: are some mathematical structures essentially the same? Are they structurally identical? Namely, can we have objects and operations that behave in exactly the same way as an entirely different pair of objects and operations? Can we have a set of objects together with an operation on those objects, such that an entirely different set of objects and an entirely different operation on those objects has exactly the same structural properties? (Or at least shares some structural properties?)

## Problems

Which of these are operations, and which are relationships? (Are any both?) What are they operations/relationships between (i.e., what are the relevant objects they relate/operate on, i.e., what's the set that this operation is defined over)? If they're operations, are they commutative? are they associative? Chose a few operations that operate on the same objects: how do these two operations distribute?

If you don't know what some of these symbols mean, Google "mathematical symbols" or something, and find out. The Wikipedia page is well-done: `http://en.wikipedia.org/wiki/List_of_mathematical_symbols`

| | | | |
|---|---|---|---|
| **1**. $+$ | **8**. $\geq$ | **15**. matrix addition | **21**. $\Rightarrow$ |
| **2**. $-$ | **9**. $\cap$ | **16**. matrix multiplication | **22**. $\iff$ |
| **3**. multiplication | **10**. $\cup$ | **17**. $\wedge$ | **23**. $\subset$ |
| **4**. $\div$ | **11**. $\setminus$ | **18**. $\vee$ | **24**. $\subseteq$ |
| **5**. $<$ | **12**. $\triangle$ | **19**. $\in$ | **25**. perpendicularity |
| **6**. $>$ | **13**. exponentiation | **20**. $\notin$ | **26**. congruence |
| **7**. $\leq$ | **14**. logarithmancy | | **27**. $\neq$ |

## Equivalence Relations

What do we mean when we say "equals," anyway? This is a word and a concept we have been using for a long time—basically our entire academic lives—and so it'd be good to get a more formal grasp of it. We'd like to define the idea of "equals" more formally, so that we can

- better understand what we say when we say "such-and-such is equal to so-and-so", and
- discover other relationships that have the same essence as "="

The usual mathematical generalization of "equals" is something called an **equivalence relation**. An equivalence relation is just a relationship that fulfills certain criteria—namely, those of reflexivity, commutativity, and transitivity (which I explain below). Given some relationship $P$ between objects $x$ and $y$ (or some propositional function $P(x, y)$), $P$ is an equivalence relation if (and only if) the following conditions ("axioms") hold:

- **Reflexivity/Identity**: $xPx$, or, in different notation, $P(x, x)$ is true. Put differently, objects are equal to themselves.
- **Commutativity/Symmetry**: if $xPy$, then $yPx$, or, in different notation, if $P(x, y)$ is true, then $P(y, x)$ must be true. (So there is no sense of "direction", if you will. Compare with, say, addition, and contrast with, say, subtraction.)
- **Transitivity**: If $xPy$ and $yPz$, then $xPz$. Put differently, if $P(x, y)$ and $P(y, z)$ are true, then $P(x, z)$ must be true. (If $x$ is equal to $y$ and $y$ is equal to $z$, then $x$ must be equal to $z$.)

It should be obvious that all three of these conditions hold for our idea of numbers being $=$. But the idea of "congruence" in geometry also fulfills all of these conditions. So do some somewhat unexpected relationships. For instance, consider the relationship $R(n, m)$ (where $n$ and $m$ are integers), defined as being true iff[3] $nm \geq 0$, and $n$ and $m$ are integers:

$$R(n, m) \iff nm \geq 0$$

This is also an equivalence relation. Why? Because it fulfills all three of the axioms for one:

- **Does it fulfill the reflexive property?** Yes. How do we know? An integer can be positive, negative, or zero, so we have three cases to check:
  - if $n$ is positive, then we have a positive times a positive, which must be positive: $n \cdot n = (+)(+) \geq 0$, so then $R(n, n)$ is true.
  - if $n$ is negative, then we have a negative times a negative, which must be positive: $n \cdot n = (-)(-) = (+) \geq 0$, so then $R(n, n)$ is true.
  - if $n$ is zero, then we have zero times zero, which is zero: $n \cdot n = 0 \geq 0$, so then $R(n, n)$ is true.
- **Does it fulfill the commutative property?** Yes. If $nm \geq 0$, then $mn \geq 0$, because multiplication is commutative. So if $R(n, m)$ is true, $R(m, n)$ must be true, too.
- **Does it fulfill the transitive property?** Yes. Here's why:
  - Imagine that $R(x, y)$ and $R(y, z)$ are true. (I've switched letters because I don't want to be ambiguous between the letter "o" (as in $m, n, o$) and the number "0".)
  - then $xy \geq 0$ and $yz \geq 0$
  - both those things are positive, so I can multiply them together, and I must still have a positive: $(xy)(yz) \geq 0$
  - or just $xzy^2 \geq 0$
  - but $y^2$ must be positive, since it's a square
  - so it won't affect the positive-or-negativeness of the formula, and I can divide it off and get just:
  - $xz \geq 0$

[3] I don't remember whether I've introduced the word "iff" before. It's just shorthand for "if and only if," i.e., $\iff$.

– but that's just the same as saying "$R(x, z)$"
– so $R(x, z)$ must be true.
– and so if $R(x, y)$ and $R(y, z)$ are true, then $R(x, z)$ must be true, too.

## Problems

Which of the following are equivalence relationships? Check each of the axioms to either prove that a relationship is an equivalence relationship, or to see where it fails. (I realize that I start these notes by using the letter $P$ to denote an equivalence relation and then suddenly switch to using $R$ without explanation. The difference is meaningless. It's just a letter.)

**1**. $R(x, y)$, where $x, y \in \mathbb{R}$ and $R(x, y) \iff x \geq y$.

**2**. $R(n, m)$, where $n, m \in \mathbb{Z}$, and $R(x, y) \iff n = m$.

**3**. "$x$ hates $y$."

**4**. $R(x, y)$, where $x, y \in \mathbb{R}$ and $R(x, y) \iff |x| = |y|$

**5**. "$n$ and $m$ have the same sign (positive or negative)." (How is this different from the above example with $nm \geq 0$)?

**6**. $R(x, y)$, where $x, y \in \mathbb{R}$ and $R(x, y) \iff |x - y| \leq 3$.

**7**. $R(A, B)$, where $A$ and $B$ are sets and $R(A, B)$ is true iff $A$ and $B$ have the same number of elements (the same cardinality).

**8**. "$a$ is married to $b$"

**9**. "$f'(x) = g(x)$", i.e., $R(f(x), g(x)) \iff g(x)$ is the derivative of $f(x)$.

**10**. $R(x, y)$, where $n, m \in \mathbb{Z}^+$ and $R(x, y) \iff n$ and $m$ have the same number of digits (in base-10).

**11**. $R(x, y)$, where $n, m \in \mathbb{Z}^+$ and $R(x, y) \iff n$ and $m$ have the same final digit (in base-10).

**12**. $R(x, y)$, where $x$ and $y$ are people, and $R(x, y)$ iff "$x$ is friends with $y$".

**13**. $R(x, y)$, where $x$ and $y$ are people, and $R(x, y)$ iff "$x$ is the same age (in years) as $y$".

**14**. $R(x, y)$, where $x$ and $y$ are physical objects, and $R(x, y)$ iff "$x$ is similar to $y$".

**15**. $R(n, m)$, where $x, y \in \mathbb{N}$ and $R(n, m) \iff n$ and $m$ have the same remainder when divided by three.

**16**. "$x$ and $y$ have the same parity" (i.e., $x$ and $y$ (both $\in \mathbb{N}$) are either both even or both odd, "parity" just being a fancy word for even-or-oddness). (How does this differ from the previous problem?)

**12**. Must a relation that is both transitive and symmetric also have the reflexive property? Prove or give a counterexample.

**13**. In trigonometry, we consider angles differing by $2\pi$ to be equivalent. What's the equivalence relation? Can you state it more formally?

**14**. Sometimes we have different fractions that are equivalent, too. $\frac{4}{6} = \frac{2}{3}$, even though $4 \neq 2$ and $6 \neq 3$. What's the equivalence relation here? What's the condition for two fractions being equal? (Suggestion: consider $\frac{a}{b} = \frac{c}{d}$, where $a, b, c$, and $d$ are all integers. What's the relationship between $a, b, c$, and $d$ that makes these two fractions equal?)

## Partitions and Equivalence Classes

One way of thinking about an equivalence relation is logical, which is how I introduced it above. *A propositional function $P(x, y)$ is an equivalence relation if and only if $P(x, y)$ fulfills these three criteria...* But another way of thinking about it is that it's something that chops up a set into a bunch of disjoint subsets (subsets which, taken together, comprise the entire set). It's kind of hard to see this with "=", but consider, say, the equivalence relation "$x$ and $y$ have the same parity": one way of thinking about it is that it splits the world of natural numbers (a world with $\aleph_0$ members) into a world with only two members: the even numbers, and the odd numbers.

$$\text{odds} = \{1, 3, 5, 7 \cdots\}$$
$$\text{evens} = \{2, 4, 6, 8 \cdots\}$$

So in this way of thinking about it, two numbers have the same parity iff they are both sitting together in the same disjoint subset of $\mathbb{N}$. These disjoint subsets are called **partitions**, or sometimes **equivalence classes**.

Or consider modular arithmetic: one way of thinking about arithmetic mod three (for example) is that it splits the world of natural numbers (a world with $\aleph_0$ members) into a world with only three members: 0,1, and 2. All the multiples of three get shoved into the same set, all the multiples of 3 plus one get shoved into the same set, and all the multiples of three plus two get shoved into the same set:

$$0 \mod 3 = \{0, 3, 6, 9, \cdots\}$$
$$1 \mod 3 = \{1, 4, 7, 10, \cdots\}$$
$$2 \mod 3 = \{2, 5, 8, 11, \cdots\}$$

In this way of thinking about it, two numbers are **equal mod three** (or **congruent mod three**) iff they are both sitting together in the same disjoint subset of $\mathbb{N}$.

A friend of mine, a vegan daughter-of-mathematicians, has a food blog, and in introducing a recipe for "tofu scramble," she wrote: "Some people like setting up equivalence classes between non-vegan foods and what they might call 'vegan versions' of non-vegan foods. This recipe, for instance, would be the vegan equivalent of scrambled eggs." So I guess to a vegan, the world of food divides into equivalence classes that look something like this:

$$\{\text{scrambled eggs, tofu scramble}\}$$
$$\{\text{hamburgers, veggie burgers}\}$$
$$\{\text{milk, soy milk, rice milk}\}$$
$$\{\text{beef, chicken, tofu, textured vegetable protein, etc.}\}$$
$$\text{etc.}$$

Formally, I could define a partition in this way: given some set $S$, a set of its subsets $\{K_1, K_2, K_3, \dots\}$ is a **partition** of $S$ (and the $K_i$ **cells** of the partition, or **equivalence classes**) if, and only if, the $K_i$ fulfill two criteria:

- $\bigcap_i (K_i) = \emptyset$ (i.e., none of the $K_i$ have any elements in common), and

- $\bigcup_i (K_i) = S$ (i.e., the $K_i$, taken together, make up the entire set $S$)

Another quick idea/vocab word we should introduce: the idea of an equivalence class of an element. The **equivalence class** of some element $k$ is the set of all elements that are equivalent to $k$. Usually we denote this by putting a horizontal bar over the element; in this case, we'd write the equivalence class of $k$ as $\bar{k}$. Formally, we can define this by saying that given an equivalence relation $\sim$, a set $S$, and some $k \in S$, the **equivalence class** of $k$ is given by:

$$\bar{k} = \{x \in S \,|\, x \sim k\}$$

To return to the example of vegan foods:

$$\overline{\text{beef}} = \{\text{beef, chicken, tofu, textured vegetable protein, etc.}\}$$

Anyway, we'd like to formally prove this idea of a partition and an equivalence relation being really the same thing. But first, we'll have to state it a bit more formally.

> **Theorem: Partitions and equivalence relations are really the same thing—that is, a partition of a set creates an equivalence relation, and (vice-versa) an equivalence relation partitions a set.**

To prove this, we'll need to split it up into two directions (the "vice-versa"): we'll need to show that if we have a partition of a set, then we have a natural equivalence relation (two things are equivalent iff they're in the same cell of the partition), and conversely, if we have an equivalence relation, then that creates a partition (with each cell of the partition containing things that are all equivalent to each other).

**Subtheorem 1 (partitions $\Rightarrow$ equivalence relations):** Given some set $S$, elements $a$ and $b$ of $S$, a partition of $S$ given by $\{K_1, K_2, K_3, \dots\}$, and the relationship $\sim$ defined in the following way:

$$a \sim b \iff \exists i(a \in K_i \wedge b \in K_i)$$

then $\sim$ is an equivalence relation.

As a note: I've written it out all fancy-like, but this is really just a logically-clear way of saying that $a \sim b$ means "$a$ and $b$ are in the same equivalence class."

**Proof:** We've defined some objects and a relationship. We need to show that this relationship fulfills the criteria of an equivalence relationship.

- **Does it fulfill the identity property?** Yes. How do we know? We need to check our definition of this equivalence relation. If we want to know whether $a \sim a$, we can plug $a$ in for $b$, and get:

  $$a \sim a \iff \exists i(a \in K_i \wedge a \in K_i)$$

  But obviously "$a \in K_i \wedge a \in K_i$" is just a ridiculously redundant way of saying "$a \in K_i$". (The two are logically equivalent.) So really, this is the same as saying:

  $$a \sim a \iff \exists i(a \in K_i)$$

  Does there exist an $i$ such that $a \in K_i$? That is to say, is there, in fact, some cell of this partition that $a$ is in? There must be. Otherwise, it wouldn't be a partition of $S$—we'd be leaving an element of $S$ out.

  So this is all just a fancy way of saying, "$a$ is in the same set as itself," and "$a$ is in one of the cells of the partition." Both of those are true, the former by the definition of a set[4] and the latter by the definition of a partition.

[4] Wait a minute...

- **Does it fulfill the commutative property?** Yes. We need to show that $a \sim b \iff b \sim a$—that is, we need to show that $a \sim b$ and $b \sim a$ are logically equivalent. But this is not hard: we have

$$a \sim b \iff \exists i(a \in K_i \wedge b \in K_i)$$

but since we know that "conjunction is commutative" (i.e., $P \wedge Q \iff Q \wedge P$), this is obviously just the same as saying:

$$\iff \exists i(b \in K_i \wedge a \in K_i)$$

but, by our definition of $\sim$, that's just the same as:

$$\iff b \sim a$$

Bam.

- **Does it fulfill the transitive property?** Yes. Here's why:
  We'll need to show that if $a \sim b$ and $b \sim c$, then $a \sim c$. So we have two assumptions (two "givens"):
  - $a \sim b$
  - $b \sim c$

  Or, put differently:
  - $\exists i(a \in K_i \wedge b \in K_i)$
  - $\exists i(b \in K_i \wedge c \in K_i)$

  But part of our assumption is that these two mysterious $K_i$'s (which might not be the same, note) *do* exist. There IS some $K_i$ that fulfills the first criterion, and there's some $K_i$ that fulfills the second criterion. So let's say that the cell that both $a$ and $b$ are in is $K_j$, and the cell that both $b$ and $c$ are in is $K_k$ (sorry for the repeated letters). We don't know yet that $K_i = K_k$—it could be the case that there's some sort of Venn diagrammy thingy going on where $b$ is in the same set as $c$ and $b$ is in the same set as $a$, but $a$ and $b$ aren't in the same set. We need to prove that, in fact, that can't happen—that $a$ and $c$ must be in the same cell of the partition.
  So, convinced of their existence (it's an assumption), and labeling appropriately, we have:
  - $a \in K_j \wedge b \in K_j$
  - $b \in K_k \wedge c \in K_k$

  Moreover, these are both assumptions, so they must both be true—I must really have:
  - $(a \in K_j \wedge b \in K_j) \wedge (b \in K_k \wedge c \in K_k)$

  (I could have added this connective "$\wedge$" much earlier; I thought it would be slightly easier to read if I held off.) But we also know, from logic, that $\wedge$ is associative—meaning, we can rearrange the parenthesis however we like—and it's also commutative, meaning that we can change the order. It also distributes nicely: $(P \wedge Q) \wedge R \iff (P \wedge R) \wedge (Q \wedge R)$. So, basically, if I have a whole bunch of things $\wedge$'d together, I can move them around just as fluidly as I can a whole bunch of things multiplied together (multiplication also obeys all those same laws) So we can rewrite this as:

$$(a \in K_j \wedge c \in K_k) \wedge (b \in K_j \wedge b \in K_k)$$

  However, one of the requirements of the $K_i$ being cells of a partition is that any element is only in one of the cells. Meaning that if $b \in K_j$, and if $b \in K_k$, then we must have $K_i = K_j$ (i.e., those must be just different names for the same cells). But then if $K_j = K_k$, then that transforms this sentence into (replacing all the $k$'s with $j$'s—could have done it the other way around):

$$(a \in K_j \wedge c \in K_j) \wedge \underbrace{(b \in K_j \wedge b \in K_j)}_{\text{but this is tautologically true—viz. } P \wedge P}$$

so we just have:

$$(a \in K_j \wedge c \in K_j)$$

but then there DOES exist some $i$ such that $a \in K_j \wedge c \in K_j$—that $i$ is $j$:

$$\exists i(a \in K_i \wedge c \in K_i)$$

but that's the definition of

$$a \sim c$$

So then if $a \sim b$ and $b \sim c$, then $a \sim c$ must be true. So then $\sim$ must be transitive.

So then $\sim$ fulfills all the criteria for an equivalence relation. So it is one. **A+**

**Subtheorem 2 (equivalence relations ⇒ partitions):** Given some set $S$, elements $a$ and $b$ of $S$, some sets $\{K_1, K_2, K_3, \dots\}$, and the equivalence relationship $\sim$ defined in the following way:

$$a \sim b \iff \exists i(a \in K_i \wedge b \in K_i)$$

then the $\{K_i\}$, taken together, form a partition of $S$.
**Proof:** We will need to show that, given this information, the $\{K_i\}$ really do form a partition of $S$. So we'll need to show that they satisfy the two conditions for a partition.

- **Do the $K_i$, taken together, cover the entire set $S$?** That is to say, is it the case that $\bigcup_i K_i = S$?

  That is to say, is every element $y$ in $S$ in some partition? Or, put more formally, we need to prove that $\forall y \in S\, \exists i(y \in K_i)$.

  How do we start? What do we know that we can use to prove this? We know that $\sim$ is an equivalence relationship on the elements of $S$, and we know that $\sim$ is defined as:

  $$a \sim b \iff \exists i(a \in K_i \wedge b \in K_i)$$

  So.... let's imagine we have some element $y$ in the set $S$. Could be any element. Since $\sim$ is an equivalence relationship, we must have that $y \sim y$. Put differently, for every element $y$ in $S$, $y$ must be $\sim$ to $y$. Or:

  $$\forall y \in S(y \sim y)$$

  But because of how $\sim$ is defined, saying "$y \sim y$" must be equivalent to saying "$\exists i(y \in K_i \wedge y \in K_i)$".

  $$y \sim y \iff \exists i(y \in K_i \wedge y \in K_i)$$

  or just saying:

  $$y \sim y \iff \exists i(y \in K_i)$$

  But then, if we consider our original statement that $\forall y \in S(y \sim y)$, since we now know that saying "$y \sim y$" is the same as saying "$\exists i(y \in K_i)$," we must really just have:

  $$\forall y \in S\, \exists i(y \in K_i)$$

  And that's what we set out to prove.

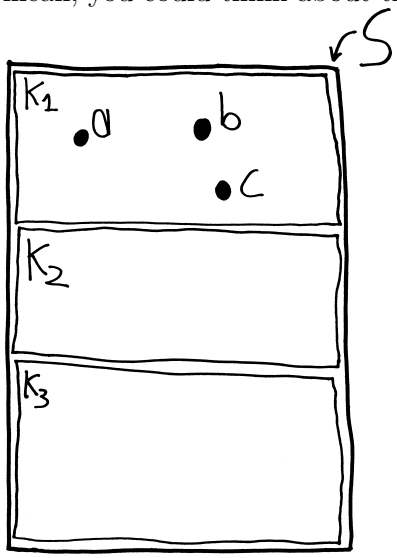
- **Do the $K_i$ not overlap?** That is to say, is it the case that $\bigcap_i (K_i) = \emptyset$? This is the same as proving that there isn't some element of $S$ that is in multiple cells[5], i.e., the same as proving that $\neg\exists y \in S(y \in K_i \wedge y \in K_j)$

  What we'll do, though, is prove this a little differently. We'll prove this by contradiction. We'll assume that in fact what we're trying to prove is false—that we have some element of $S$ that is in two different cells—and in doing so, we'll end up proving that in fact these two different cells must be equal. Thus, we'll prove that any element of $S$ can only be in one cell, and thus, that the $K_i$ don't overlap. Here's the argument:

  - Imagine that we had some element of $S$ that were in multiple cells. Let's call this element $y$, and let's imagine that it's in both $K_i$ and $K_j$.
  - Since $y$ is in $K_i$, it is (by definition) $\sim$ to any other element in $K_i$.
    * Imagine that $m$ is one of those other elements in $K_i$.
    * Then we must have $y \sim m$ (simply by virtue of them sitting together in the same cell).
  - Likewise, because $y \in K_j$, then for any other element $n$ in $K_j$, we must have $y \sim n$.
  - Right? This is just because of our definition of $\sim$; things are $\sim$ to each other when they're in the same partition of $S$.
  - But if $y \sim m$ and $y \sim n$, then by the transitive property—we know $\sim$ is an equivalence relation, so we know the transitive property must hold—-then $m \sim n$.
  - But then $m$ and $n$ are in the same partition.
  - But then we must have that $K_i = K_j$.
  - So then no element of $S$ can be in multiple cells of a partition.

So then the $\{K_i\}$ fulfill all the criteria for being a partition of $S$. So they are one. ∎

My math friends would laugh if they read this and say, "Why are you writing so much?[6] It's obvious!" And, sure. It *is* obvious in a sense. I mean, you could think about this entire proof visually:




So if I just take a set and chop it up into a partition, then obviously things are in the same cell as themselves, obviously the commutative property and the transitive property work, etc... think about it for a couple minutes.

[5]Remember that "cells" is just a fancy name for these subsets of $S$, these $K_i$.

[6]By the way (this is me speaking, not one of my math friends), I could have written out this proof even more pedentically. Be glad I didn't.

But the point here is less the result and more the process. We want to learn how to speak in formal languages. We want to understand what it means to manipulate symbols. Those symbols could be logical ($P \wedge Q$), they could be mathematical ($2 + 3$), they could be the moves on a chessboard, they could be the swapping of stones in a game of Go... we want to understand formal languages, because then we can ask: why is life not a formal language? what's the difference between a proof in math and an argument in Aristotle? why isn't life so clean? is it? do we just not fully understand the formal language that controls the world? or is there some inherent defect (feature?) in formal languages that prevents them from explaining the world? (would that be a good thing?) what would it mean for a formal language to explain the world, anyway? how would we know that it did? what is "the world"? how do we understand it to exist? "Pilate said to him, 'what is truth?' "

Perhaps the real question that my math friends should ask is, "Why are you spending so much time talking about equivalence relations and partitions? Those aren't interesting! Get on to talking about groups! Prove Lagrange's theorem, or something!"

Well, fine. But this is how the discussion in class evolved, and besides, I like the various philosophical applications of this basic set theory stuff—not the questions of mathematical ontology (though those *are* awesome), but the (more superficial) application to higher ideas—you know, understanding this concept of "equivalence," or seeing more clearly that "$\Rightarrow$" is an asymmetric relationship, or learning how to speak with quantifiers.

Also, we proved Cantor's theorem. We're already in the transfinite paradise.