

Day 16

Wednesday June 13, 2012

1 Cardinality

1.1 Bijections and Results

Definition 1. A function $f : D \rightarrow C$ is a **bijection** if and only if it is both injective and surjective.

One may question why a bijection is important. The following should give us an idea why.

Definition 2. If A is a nonempty set, the **identity function on A** , written id_A , is the function from $A \rightarrow A$ with $\text{id}_A(x) = x$ for all $x \in A$.

We say a function $f : D \rightarrow C$ is **invertible** if and only if there is some function $g : C \rightarrow D$ such that

- $f \circ g = \text{id}_C$
- $g \circ f = \text{id}_D$

In which, we call g the **inverse** of f

Lemma 1. *If $f : D \rightarrow C$ is invertible then f is injective*

Proof. Let $f : D \rightarrow C$ be invertible, and take $a, b \in D$, supposing that $f(a) = f(b)$. We want to show $a = b$. Well, as g is a function, it must take $f(a)$ and $f(b)$ to the same place. Therefore, $g(f(a)) = g(f(b))$. But, as g is the inverse of f , $g(f(a)) = a$ and $g(f(b)) = b$, so $a = b$. \square

Lemma 2. *If $f : D \rightarrow C$ is invertible then f is surjective.*

Proof. Let $f : D \rightarrow C$ be invertible, and let $a \in C$. Let g be in the inverse of f . Then for every $x \in C$ we must have $f(g(x)) = x$. In particular, $f(g(a)) = a$. Therefore, a is attained by f . Therefore f is surjective. \square

The more surprising result perhaps:

Lemma 3. *If $f : D \rightarrow C$ is bijective, then f is invertible.*

Proof. Take $f : D \rightarrow C$ bijective. We want to construct an inverse, $g : C \rightarrow D$. Well, define g as:

$$g(x) = y \text{ for } y \in f^{-1}[\{x\}]$$

That is to say, define $g(x)$ by looking at the preimage of $\{x\}$, and then mapping it to an element in this. We need to show this is a well-defined rule. Firstly, does this rule map every element of the domain C ? Well, if $a \in C$ then $f^{-1}[\{a\}] \neq \emptyset$ since f is surjective (ie. a gets hit by at least one value). Therefore, $g(a)$ is defined for every a .

Next we ask does everything land in the codomain. The answer is yes since for any $C' \subseteq C$ we have $f^{-1}[C'] \subseteq D$.

Finally we ask: is it ambiguous? Well, suppose that $g(x) = a$ and $g(x) = b$. We want to show that a and b are equal. As $g(x) = a$ we must have that $a \in f^{-1}[\{x\}]$. Similarly, as $g(x) = b$ we must have $b \in f^{-1}[\{x\}]$. Therefore, we know $f(a) = x$ and $f(b) = x$ by definition. But, by injectivity, $a = b$. \square

Theorem 1. *Let $f : D \rightarrow C$. Then the following are equivalent:*

(a) f is a bijection.

(b) f is invertible.

Proof. The first two lemmas above give us $(b) \rightarrow (a)$. The last gives us $(a) \rightarrow (b)$. □

Lemma 4. *The inverse of a bijection is unique, and a bijection itself.*

Proof. Exercise; For the first, consider there being two inverses, and show they must be equal (similar to the proof that inverses are unique mod p). The second is a straightforward exercise. □

Definition 3. If f is invertible, by the last lemma, f has a unique inverse. Therefore, we give it a name in general: f^{-1} .

We also have these two results:

Lemma 5. *Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$.*

- *If f and g are surjections then $g \circ f$ is a surjection.*
- *If f and g are injections then $g \circ f$ is an injections.*

Proof. I will prove only the first. The second is left as an exercise.

Well $g \circ f : A \rightarrow C$. Take $c \in C$. Want to show that something hits it in A . Well, as $c \in C$ and g is a surjection, there is some $b \in B$ such that $g(b) = c$. As $b \in B$, we have since f is a surjection there is some $a \in A$ such that $f(a) = b$. So,

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

□

Theorem 2. *The compositions of two bijections is a bijection.*

1.2 Cardinality Definition

What does the size of a set mean? This is a hard notion to nail down, really. It's quite easy to talk about when we can write down what the set is. For instance the sets $\{3, 4, 6\}$ and $\{9, 34, 1\}$ both have the same size.

There are 2 reasons to reasons one could argue this (perhaps more, but 2 I can think of).

1. One reason is that we can count the first...1,2,3...and then count the second...1,2,3... and since we counted to the same number in each, they must be the same.
2. Another reason is because we can "pair off" elements from one set with elements from the other. 3 gets paired with 9, 4 gets paired with 34 and 6 gets paired with 1. There are no elements left of either sets after this process, so they must be the same size.

Okay, so we want to make a correspondence between one set of objects and another...Oh! That's what a function is. Okay, so we make a set from one set of object to the other, but we want to make sure everything in the other set actually gets matched up (this is surjective) and we want to make sure we don't overcount things by pairing things up twice (this is injective).

Remark 1. We make the following heuristic: Two set A and B have the same size if there is a bijection between A and B . Since we already have a notion of size for finite sets, we need to make sure our new heuristic conforms to it. This will come in a bit. First let's finite some notation.

Definition 4. We say that two sets A and B are **equinumerous** if there is a bijection between A and B .

Remark 2. Equinumerous is actually a real math word, but I suggest one never says it. It sounds fairly old. We will discover a better phrase later.

Theorem 3. *Equinumerosity is an equivalence relation on sets. That is:*

1. *For every set A , A is equinumerous with itself.*
2. *For every set A and B , if A is equinumerous with B then B is equinumerous with A .*

3. For every A , B , and C , if A is equinumerous with B and B is equinumerous with C , then A is equinumerous with C .

Proof. For the first, clearly $\text{id}_A : A \rightarrow A$ is a bijection (if it's not clear, check this!).

For the second, if $f : A \rightarrow B$ is a bijection, then $f^{-1} : B \rightarrow A$ is a bijection, so B is equinumerous with A .

For the third, we have already shown the compositions of two bijections is a bijection. \square

Remark 3. As there is no set of all sets, the last theorem doesn't even make sense. The last theorem is more of a "morally speaking" theorem.

Definition 5. A set A is **finite** if there is a bijection between the set and $[n]$ for some $n \in \mathbb{Z}^+$. Otherwise, a set is **infinite**.

Definition 6. If A is a set, we write $|A|$ to talk about the equivalence class of A under the equinumerous equivalence relation. Therefore, we say

$$|A| = |B|$$

to say that A and B are equinumerous. Given A , the equivalence class of A is called the **cardinality of A** .

Instead of saying A and B are equinumerous, we will instead say A has the same cardinality as B .

In the case where A is finite and $|A| = |[n]|$, we normally write $|A| = n$; this is slight abuse of notation, but is suggestive.

Theorem 4. Suppose that A and B are finite sets, where there are exactly n members in both A and B . Then there is a bijection between A and B .

Proof. If there is n members of A , then there is a bijection $f : [n] \rightarrow A$. This is just counting the members of A . Similarly, there is a bijection $g : [n] \rightarrow B$. Taking the inverse of f and composing, we get a bijection $g \circ f^{-1} : A \rightarrow B$. \square

This justifies our notion of cardinality. The cardinality of finite sets are equal when they have the same number of elements as we'd expect. But, unfortunately, we don't quite have intuition about infinite sets. Are there different "sizes" of infinite things? Or, maybe "infinite" things are all identified.

Theorem 5 (Cantor 1874). *There are infinite sets which do not have the same size*

This is a theorem which was very revolutionary for the time, and instigated a larger program of Cantor on the infinite sets and sizes (cardinalities). We will, with time, see a proof of this theorem. But first, it will help us greatly to consider infinite sets which do have the same sizes as each other, to perhaps answer why some infinite sets are different than others.

1.3 Hilbert Hotels

We begin with a story, that we are managers of the Hotel Hilbert. Over the years there have been a lot of changes in the hotel. There used to be just a few rooms here and there, but now we have an infinite supply of rooms, each numbered with a positive integer n .

When we finished construction, it was hard to believe that we would need them all, but there's a pretty big wedding in town, and we just filled up! We turned on the No Vacancy sign. Here at the Hotel Hilbert, however, that sign does not mean that we cannot give you a room.

Question 1. A guest comes into our hotel and wants a room. How should we accommodate them?

Answer 1. Well, we can shift everyone down one room. So move the person in room number 1 to room number 2, 2 to 3, etc. Then we can put our new guest in room 1 because it's open!

Question 2. Uh-oh. There's another big wedding in town, and another infinite supply of guests is looking for rooms. Each is wearing a shirt with a different natural number on it. Can we accommodate them?

Answer 2. Of course! We will just have to do some rearranging. We will say that if you are in room i , you have to move to room $2i$. This is quite a long walk for some people, but that's okay. They don't mind. After this, we have all the odd rooms completely open as everyone is now staying in an even room!

Question 3. Okay, one wedding was fine. Two weddings was manageable. But now there are infinitely many weddings in town! Each wedding is assigned a distinct natural number by the city's wedding planning committee. They all want to stay in our hotel. Can we accommodate them?

Answer 3. No problem! We'll just put the existing people to rooms numbered with powers of 2, then the first wedding in rooms with powers of 3, then the next in rooms with powers of 5, etc, the n th in rooms with powers of p where p is the n th prime, and so on. This leaves a lot of rooms empty, but that's okay: infinitely many rooms allows us to be a little less efficient.

2 Countability

So, we like counting things using the numbers that, well, we use to count things: \mathbb{N} .

Definition 7. A set A is called **countable** if and only if it is finite or there is a bijection between the set and \mathbb{N} .

Some people (like people who index their arrays starting at 1 for some reason) count things using \mathbb{Z}^+ . We first show that if you can count a set using one then you can count a set using the other by showing that you can count one using the other.

Theorem 6.

$$|\mathbb{Z}^+| = |\mathbb{N}|$$

Proof. Simply define $f : \mathbb{N} \rightarrow \mathbb{Z}^+$ by

$$f(x) = x + 1$$

This is clearly surjective; if $y \in \mathbb{Z}^+$, then y is a positive natural, so $y-1$ is certainly a natural and $f(y-1) = y$. Similarly, if $x+1 = y+1$ then $x = y$. \square

This really corresponds to our first Hilbert Hotel Problem. We shift all the guests up by one, and then add the new one in the room get gets emptied.

Theorem 7.

$$|\mathbb{Z}| = |\mathbb{N}|$$

Proof. We define $g : \mathbb{Z} \rightarrow \mathbb{N}$ by

$$g(n) = \begin{cases} -2n & \text{if } n \leq 0 \\ 2n-1 & \text{if } n > 0 \end{cases}$$

Clearly g is bijection. For surjective, if you wanted to hit m , if m is even then $m = 2k$ for some k , and $g(-k) = -2k = m$. If m is odd then $m = 2k-1$ for some $k \in \mathbb{N}$, and $g(k) = 2k-1$.

For injective, let $a, b \in \mathbb{Z}$ and suppose $g(a) = g(b)$. Clearly if $a, b \leq 0$ or $a, b > 0$. then $a = b$. So, suffices to only check when they're different. WLOG, $a \leq 0$ and $b > 0$. But then $g(a)$ is even and $g(b)$ is odd, which contradicts $g(a) = g(b)$. \square

This corresponds to the second hotel problem; I have the people who were already there (the non-negatives) and the new people (the negatives) and somehow I have to fit them in their rooms!

Theorem 8.

$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

Proof. This one is tricky. What should we do? \square