Equivalent Sets

Definition Let $A,\ B$ be sets. We say that $\underline{A\text{ is equivalent to }B}$ iff there exists a bijection $f: A \to B$. If A is equivalent to B, we write $A \approx B$ (or $A \simeq B$ or $A \sim B$ or something similar: the notation varies from book to book).

It is intuitively clear that for finite sets $A \approx B$ iff A and B have the same number of elements. Therefore $\{a, b\} \approx \{1, 2\}$ (*assuming that* $a \neq b$) but $\{1, 2, 3\} \not\approx \{1, 2\}$.

Theorem The relation $\approx$ is an equivalence relation among sets.

Proof Let A, B, C be sets.

a) The identity mapping $f(x) = x$ is a bijection $f: A \to A$. Therefore $A \approx A$, so the relation is reflexive.

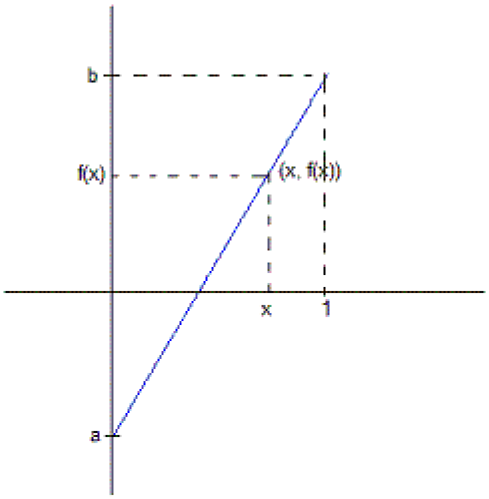
b) If $A \approx B$, then there must exist a bijection $f: A \to B$. Then the function $g = f^{-1}: B \to A$ is also a bijection, so $B \approx A$. Therefore the relation is symmetric. (*Therefore, to show two specific sets* A *and* B *are equivalent, it doesn't matter whether you show that there is a bijection* *from* A *to* B *or that there is a bijection* *from* B *to* A.)

c) Suppose $A \approx B$ and $B \approx C$. Then there are bijections $f: A \to B$ and $g: B \to C$. Then $g \circ f: A \to C$ is a bijection (*check!*) so $A \approx C$. Therefore the relation is transitive.

Examples

1) Suppose $a, b \in \mathbb{R}$ and that $a < b$. Then the intervals $(0, 1)$ and (a, b) are equivalent. We can see this using a "straight line" bijection $f: (0, 1) \to (a, b)$:

$$f(x) = a + (b - a)x \qquad\qquad 0 < x < 1$$



2) Suppose $c, d \in \mathbb{R}$ and that $c < d$. By Example 1), $(0,1) \approx (c,d)$. Since it's also true that $(0,1) \approx (a,b)$, it follows by symmetry and transitivity that $(c,d) \approx (a,b)$: any two "open intervals" in $\mathbb{R}$ are equivalent.

3) Suppose, in Example 1), we change the domain of f to $0 \leq x < 1$. Then the graph of f will also include the point $(0,a)$, and the modified function f is a bijection between $[0,1)$ and $[a,b)$.
Therefore $[0,1) \approx [a,b)$, and it follows that $[c,d) \approx [a,b)$, just as in Example 2).

Similarly, we can "tweak" the domain of f in Example 1) to show that

$$(c,d] \approx [a,b] \quad \text{and that} \quad [c,d] \approx [a,b]$$

4) $(0,1] \approx [0,1)$ because the function $f : (0,1] \rightarrow [0,1)$ given by $f(x) = 1 - x$ is a bijection. Using "domain modifications" like to those in Example 3), show that $(c,d] \approx [a,b)$.

5) $(-\frac{\pi}{2}, \frac{\pi}{2}) \approx \mathbb{R}$ because $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ is a bijection. By Example 2), this means that every interval $(a,b) \approx \mathbb{R}$.

6) $\mathbb{R} \approx (0,\infty)$ because the function $f : \mathbb{R} \rightarrow (0,\infty)$ where $f(x) = e^x$, is a bijection.

Examples

1) $\omega \approx \mathbb{N}$ because the function $f : \{0,1,2,...,\} \rightarrow \{1,2,3,...,\}$ given by $f(x) = x + 1$ is a bijection (*check*!)

2) Let $k \in \mathbb{N}$. Then the function $f : \{1,2,3,...\} \rightarrow \{k, 2k, 3k, ...\}$ given by $f(n) = kn$ is a bijection. So, for example, $\mathbb{N} \approx \{2,4,6,8,...\}$ and $\mathbb{N} \approx \{15,30,45,60,...\}$. By symmetry and transitivity, $\{2,4,6,8,...\} \approx \{15,30,45,60,...\}$.

3) $f : \{..., -3, -2, -1\} \rightarrow \{1,2,3,...\}$ given by $f(x) = -x$ is a bijection, so the set of negative integers is equivalent to the set of positive integers.

4) As a slightly more complicated example, we can also show that $\mathbb{N} \approx \mathbb{Z}$. We can see this using the bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$ given by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

(*For example,* $f(2) = 1,\ f(4) = 2,\ f(6) = 3, ..., f(1) = 0,\ f(3) = -1,\ f(5) = -2, ...$)

f is one-to-one: Suppose $f(m) = f(n)$.

Notice that if m is even and n is odd, then $f(m) > 0$ and $f(n) \leq 0$, so $f(m) \neq f(n)$. Similarly, it cannot be that m is odd and n even. So m, n are either both even or both odd.

If m, n are both even, then $f(m) = f(n) \Rightarrow \frac{m}{2} = \frac{n}{2} \Rightarrow m = n.$

If m, n are both odd, then $f(m) = f(n) \Rightarrow \frac{1-m}{2} = \frac{1-n}{2}$

$\Rightarrow m = n.$

<u>f is onto $\mathbb{Z}$</u>: Let $z \in \mathbb{Z}$:

if $z > 0$, let $n = 2z \in \mathbb{N}$: then $f(n) = \frac{2z}{2} = z.$

if $z \le 0$, let $n = 1 - 2z \in \mathbb{N}$ (*why?*) : then $f(n) = \frac{1-(1-2z)}{2} = z.$

5) We saw earlier (near the end of the notes on functions) that there is a bijection $f : \mathbb{N} \to \mathbb{Q}^+ =$ the set of all positive integers, so $\mathbb{N} \approx \mathbb{Q}^+$.

Using the following theorem, we can combine certain sets that we know are equivalent to conclude that other sets are also equivalent (without needing to explicitly produce a bijection between them).

Theorem Suppose that $\begin{cases} A \approx C & \text{and} \\ B \approx D \end{cases}$

Then i) $A \times B \approx C \times D$

ii) If $A \cap B = \emptyset$ and $C \cap D = \emptyset$, then $A \cup B \approx C \cup D$.

Proof Since $A \approx C$ and $B \approx D$, we know that there are bijections $f : A \to C$ and $g : B \to D$.

i) Define $h : A \times B \to C \times D$ by the formula :

For $(a, b) \in A \times B$, let $h(a, b) = (f(c), g(d)) \in C \times D$

<u>h is onto</u> $C \times D$: Suppose $(c, d) \in C \times D$. Then $c \in C$ so since f is onto, there is an $a \in A$ for which $f(a) = c$. Similarly, there is a $b \in B$ for which $g(b) = d$. Then $(a, b) \in A \times B$ and $h(a, b) = (f(a), g(b)) = (c, d)$.

<u>h is one-to-one</u> : Suppose (a_1, b_1) and $(a_2, b_2) \in A \times B$ and that $h(a_1, b_1) = h(a_2, b_2)$.

By definition of h, this means that$(f(a_1), g(b_1)) = (f(a_2), g(b_2))$, and therefore $f(a_1) = f(a_2)$ and $g(b_1) = g(b_2)$. Since f and g are both one-to-one, this gives us that $a_1 = a_2$ and $b_1 = b_2$. Therefore $(a_1, b_1) = (a_2, b_2)$.

ii) domain$(f) \cap$ domain$(g) = A \cap B = \emptyset$, so $f \cup g = h$ <u>is a function from</u> $A \cup B$ to $C \cup D$. (*There are no points where f and g "disagree" so there is no problem with $f \cup g$ being a function--see Homework 9*). We can write $h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B. \end{cases}$

h is <u>onto</u> $C \cup D$: if $y \in C \cup D$, then $y \in C$ or $y \in D$.

If $y \in C$, then (since f is onto) there is an $a \in A$ for which $y = f(a) = h(a)$ and if $y \in D$, then there is a $b \in B$ for which $y = g(b) = h(b)$.

In both cases, $y \in \text{range}(h)$. Therefore h is onto.

h is one-to-one : Suppose $x, y \in A \cup B$ and $h(x) = h(y)$.

If $x \in A$ and $y \in B$ (*or vice versa*), then $h(x) = f(x) \in C$ and $h(x) = h(y) = g(y) \in D$. This would mean $C \cap D \neq \emptyset$. So either x and y are in A, or x and y are in B.

If $x, y \in A$, then $h(x) = f(x) = f(y) = h(y)$ so, since f is one-to-one, $x = y$. If $x, y \in B$, then $h(x) = g(x) = g(y) = h(y)$, so $x = y$ since g is one-to-one. ●

Examples

1) $\begin{cases} (0,1) \approx \mathbb{R} & \text{and} \\ (0,1) \approx \mathbb{R} \end{cases}$

Part i)(of the Theorem gives us that $(0,1) \times (0,1) \approx \mathbb{R} \times \mathbb{R}$ $-$ that is, the "open box" $(0,1)^2$ in the plane is equivalent to the whole plane $\mathbb{R}^2$.

Using part ii) of the theorem again, we get that the "open box" $(0,1)^3$ in three-space $\mathbb{R}^3$ is equivalent to all of $\mathbb{R}^3$.

2) Since $(0,1] \approx (a,b]$, we conclude that $(0,1]^2 \approx (a,b]^2$

($(0,1]^2$ *is a "box" in the plane that contains its top and right edges, but not its left or bottom edges: draw it.*)

With all these examples, we might be tempted to think that all infinite sets are equivalent but this is not true. The next theorem gives us a way to create (infinitely many) nonequivalent infinite sets.

Theorem For any set A, $A \not\approx \mathcal{P}(A)$.

Proof For a finite set A this is clear because if A contains n elements, then $\mathcal{P}(A) =$ the set of all subsets of A contains 2^n elements.

Suppose, in general, that f is <u>any</u> function $f : A \to \mathcal{P}(A)$. We claim that f <u>cannot be onto</u> and therefore f cannot be a bijection. This will show that $A \not\approx \mathcal{P}(A)$.

If $a \in A$, then $f(a) \in \mathcal{P}(A)$, so $f(a)$ is a subset of A. Therefore it makes sense to ask <u>whether or not</u> $a \in f(a)$.

> *It will help in understanding the proof to keep referring to the following illustration of what's going on*:
>
> *If* $A = \{1, 2, 3\}$, *then* $\mathcal{P}(A) = \{\, \emptyset\,, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\,\}$.
>
> *Suppose (say)* $f : A \to \mathcal{P}(A)$ *is the function given by*
>
> $f(1) = \{1, 2\}$, $f(2) = \{1, 3\}$, $f(3) = \{1\}$
>
> *Then* $1 \in f(1)$, $2 \notin f(2)$ *and* $3 \notin f(3)$

Let $B = \{a \in A : a \notin f(a)\}$. Then $B \subseteq A$, so $B \in \mathcal{P}(A)$. We claim that B is not in the range of f.

> *In the illustration,* $B = \{2, 3\}$, *and, as promised,* B *is not in the range of* f.

<u>Suppose there were</u> an $x \in A$ for which $f(x) = B$. Then either $x \in B$ or $x \notin B$.

> If $x \in B$, then x must satisfy the membership requirement for B: that $x \notin f(x)$. But then $x \notin f(x) = B$, so this is impossible.
>
> If $x \notin B$, then x fails to meet the membership requirement for B: so $x \in f(x)$. But then $x \in f(x) = B$ which is impossible.

Either way, <u>the assumption</u> that there is an x such that $f(x) = B$ <u>leads to a contradiction</u>, so no such x can exist. Therefore f is <u>not</u> onto. ●

Example By the theorem, $\mathbb{N} \not\approx \mathcal{P}(\mathbb{N})$.

Notice that there <u>is</u> a <u>one-to-one</u> (<u>not onto</u>) map $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ (*for example, let* $f(n) = \{n\} \in \mathcal{P}(\mathbb{N})$). If $f : A \to \mathcal{P}(A)$ is such a one-to-one function, then $A \approx f[A] = \text{range}(f) \subseteq \mathcal{P}(A)$. So A is <u>always</u> equivalent to a <u>subset</u> of $\mathcal{P}(A)$ but <u>never</u> equivalent to the whole set $\mathcal{P}(A)$. Intuitively, this means that $\mathcal{P}(A)$ is a “bigger” infinite set than A.

We can continue to apply the power set operation over and over to get

$$\mathbb{N} \not\approx \mathcal{P}(\mathbb{N}),\ \mathcal{P}(\mathbb{N}) \not\approx \mathcal{P}(\mathcal{P}(\mathbb{N})),\ \mathcal{P}(\mathcal{P}(\mathbb{N})) \not\approx \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))), \ldots$$

and thus create a sequence of “larger” and “larger” nonequivalent infinite sets.

We proved that for every set A, $A \not\approx \mathcal{P}(A)$. In particular, $\mathbb{N} \not\approx \mathcal{P}(\mathbb{N})$. However, we can show that $\mathcal{P}(\mathbb{N})$ is equivalent to another familiar set: $\{0,1\}^{\mathbb{N}}$. Recall that $\{0,1\}^{\mathbb{N}}$ denotes the set of all functions $f : \mathbb{N} \to \{0,1\}$. Such an f is a sequence for which every term has value 0, or 1:

if $f \in \{0,1\}^{\mathbb{N}}$, we have values $f(1), f(2), f(3), ..., f(n), ...$ where each $f(n) = 0$ or 1

In other words, $\{0,1\}^{\mathbb{N}}$ is the set of all "binary sequences."

Theorem $\mathcal{P}(\mathbb{N}) \approx \{0,1\}^{\mathbb{N}}$

Proof Define a function $\Phi : \{0,1\}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N})$ as follows:

$$\text{if } f \in \{0,1\}^{\mathbb{N}}, \text{ then } \Phi(f) = \{n \in \mathbb{N} : f(n) = 1\} \in \mathcal{P}(\mathbb{N})$$

If f is a binary sequence, then $\Phi(f)$ is the subset of $\mathbb{N}$ consisting of all those n for which the n^{th} term of the sequence is 1. For example suppose f has values

$$\begin{array}{ccccccc} f(1), & f(2), & f(3), & f(4), & f(5), & f(6), ... & \\ || & || & || & || & || & || & \\ 0\,, & 1\,, & 1\,, & 0\,, & 0\,, & 1 & , ... \end{array}$$

then $\Phi(f) = \{2, 3, 6, ...\}$.

Φ is one-to-one: if $f, g \in \{0,1\}^{\mathbb{N}}$ and $f \neq g$, then there is an $n \in \mathbb{N}$ for which $f(n) \neq g(n)$. Suppose $f(n) = 1$ and $g(n) = 0$. Then $n \in \Phi(f)$ but $n \notin \Phi(g)$, so $\Phi(f) \neq \Phi(g)$. Similarly if $f(n) = 0$ and $g(n) = 1$, then $n \notin \Phi(f)$ but $n \in \Phi(g)$,
so $\Phi(f) \neq \Phi(g)$.

Φ is onto: Suppose $A \in \mathcal{P}(\mathbb{N})$, that is, suppose $A \subseteq \mathbb{N}$. Define a binary sequence f as follows:

$$f(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$$

Then $f \in \{0,1\}^{\mathbb{N}}$ and, by definition, $\Phi(f) = A$. •

Finite Sets

We have informally used the terms "finite set" and "infinite set." We now make a precise definition.

Definition For each $k \in \mathbb{N}$, let $\mathbb{N}_k = \{1, 2, ..., k\}$. A set A is called finite if $A = \emptyset$ or if $(\exists k \in \mathbb{N})\, A \approx \mathbb{N}_k$.

A is called infinite if A is not finite (that is, if $A \neq \emptyset$ and $(\forall k \in \mathbb{N}) A \not\approx \mathbb{N}_k$.

Definition For a finite set A :

i) if $A = \emptyset$, we say that 0 is the cardinal number of A (or that A has cardinality 0), and write $|A| = 0$.

ii) if $A \approx \mathbb{N}_k$, we say that k is the cardinal number of A (or that A has cardinality k), and write $|A| = k$.

We already have a lot of intuitive ideas about how finite sets behave. But now that we have an "official" definition of "finite set," each of these intuitive statements should be proved: this will show that the formal definition of finite set correctly "captures" the intuitive idea of finite set. It turns out that we can prove that our informal ideas about finite sets are actually theorems using the official formal definition for finite sets.
(*As we shall see later: we also have some intuitive ideas about infinite sets. But for infinite sets our intuition is sometimes wrong: for infinite sets, careful proofs become very important.*)

Here is a list of familiar properties of finite sets. They are all proved in Section 5.1 of the textbook; many of the proofs use induction. We are not going to go over those proofs $-$ doing them all is a tedious, it takes a lot of time, and the results, in the end, are just what we thought intuitively would be true. But we will prove one important fact about finite sets, below.

Theorems About Finite Sets

1. If A is finite and $A \simeq B$, then B is finite; a finite set is never equivalent to a proper subset of itself.

2. If A is finite and $x \notin A$, then $A \cup \{x\}$ is finite, and $|A \cup \{x\}| = |A| + 1$.

3. If A is finite and $x \in A$, then $A - \{x\}$ is finite and $|A - \{x\}| = |A| - 1$.

4. Every subset of a finite set is finite.

5. If A and B are finite:

   a) $|A \cup B| = |A| + |B| - |A \cap B|$
   b) If $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$.

6. If A is finite, then $\mathcal{P}(A)$ is finite, and $|\mathcal{P}(A)| = 2^{|A|}$.

7. If $n \in \mathbb{N}$ and $A_1, ..., A_n$ are finite sets, then $A_1 \cup A_2 \cup ... \cup A_n$ is finite.
("*A finite union of finite sets is finite.*")

There is one additional theorem about finite sets that is quite intuitive and which turns out to be unexpectedly useful.

Theorem (The Pigeonhole Principle) Suppose $n, r \in \mathbb{N}$ and that $f : \mathbb{N}_n \rightarrow \mathbb{N}_r$. If $n > r$, then f is not one-to-one.

The idea behind the name is that if there are n "pigeons" to be put into r "pigeonholes" and there are more pigeons (n) than there are pigeonholes (r), then at least two pigeons must go into the same pigeonhole. The Pigeonhole Principle is also called the Dirichlet Box Principle.

Proof The proof is done by induction on $\mathbb{N}$. Suppose r represents a natural number and that $f : \mathbb{N}_n \rightarrow \mathbb{N}_r$. We want to prove $(\forall n \in \mathbb{N})\ P(n)$, where

$P(n)$ is the statement: if $n > r$, then f cannot be one-to-one.

Since r represents a natural number so $r \geq 1$ and so $n \geq 2$. Therefore our induction starts with $n = 2$.

Base case If $n = 2$, then $r = 1$ and $f : \mathbb{N}_2 = \{1, 2\} \rightarrow \{1\} = \mathbb{N}_1$. Therefore f must be constant: $f(1) = 1 = f(2)$. So f is not one-to-one.

Assume that $P(n)$ is true for some particular value $n = k$. That is, our induction hypothesis is

(*) If $f : \mathbb{N}_k \rightarrow \mathbb{N}_r$ (where r is any natural number $< k$), then f is not one-to-one.

We want to prove:

If $f : N_{k+1} \rightarrow \mathbb{N}_r$ (where r is any natural number $< k + 1$), then f is not one-to-one

We prove this by contradiction.

Suppose there is a one-to-one function $f : N_{k+1} \rightarrow \mathbb{N}_r$, where $k + 1 > r$. (**)

$$f : \{1, 2, ..., k, k + 1\} \rightarrow \{1, 2, ..., r\}$$

$f(k + 1)$ is one of the numbers $1, 2, ..., r$. Delete $k + 1$ from the first set (leaving $\mathbb{N}_k$) and $f(k + 1)$ from the second set (leaving $\mathbb{N}_r - \{f(k + 1)\}$).
Then restricting the function f to the smaller domain we have a one-to-one function

$$g = f|\mathbb{N}_k : \mathbb{N}_k \rightarrow \mathbb{N}_r - \{f(k + 1)\}$$

The set on the right ($=$ the codomain of g) has one less element than $\mathbb{N}_r$, so there is a bijection $h : \mathbb{N}_r - \{f(k + 1)\} \rightarrow \mathbb{N}_{r-1}$.

Composing functions, we get a one-to-one function $h \circ g : \mathbb{N}_k \rightarrow \mathbb{N}_{r-1}$,

Since $k + 1 > r$, we have that $k > r - 1$, and the existence of such a one-to-one function $h \circ g$ contradicts the induction hypothesis (*).

So no such function as (**) can exist $-$ which says that $P(k + 1)$ is true.

By PMI, $P(n)$ is true for all $n \in \mathbb{N}$. •

As mentioned earlier, this "obvious" Pigeonhole Principle has lots of applications. Before we look at a few examples, we note one simple corollary.

Corollary If $p, q \in \mathbb{N}$ and $p \neq q$, then $\mathbb{N}_p \not\approx \mathbb{N}_{q}.$

Proof One of p or q is larger than the other $-$ say $p > q$. If $f : \mathbb{N}_p \rightarrow \mathbb{N}_q$ is any function, the, by the Pigeonhole Principle, f cannot be one-to-one, so f cannot be a bijection. ●

The corollary tells us that a set A cannot be equivalent to both $\mathbb{N}_p$ and $\mathbb{N}_q$ if $p \neq q$: otherwise, by transitivity, we would have $\mathbb{N}_p \approx \mathbb{N}_q$. This means that the <u>cardinal</u> number of A is well-defined: if $|A| = p$, then $|A| = q$ is impossible if $q \neq p$.

Example There are two people in Missouri who have the same number of hairs on their heads.

In 2007, the census gives the estimated Missouri population as 5,878,415. Also, various studies indicate that the average number of hairs on a human head is around 150,000, with, of course, lots of variation. (Incidentally, the average number varies with the color of the hair!) But it seems safe to say that every human head has less than 1,000,000 hairs.

Let the population of Missouri be n (where n is some number $> 5,878,415$). Let $r = 1,000,000$. Number the people as $1, 2, 3, ..., n$.

Define a function $f : \{1, 2, 3, ..., k, ...n\} \rightarrow \{1, 2, ..., r\}$ where $f(k) =$ the number of hairs on k's head. Since $n > r$, the Pigeonhole Principle says that f cannot be one-to-one, that is, there are at least two Missourians with the same number of hairs on their heads.

In this example, the "pigeons" are the people in Missouri; you can think of the "pigeonholes" as boxes numbered $1, ..., r$. Each person is placed in the box corresponding to the number of hairs on the head.

In using the Pigeonhole Principle, sometimes some cleverness is required: the key thing (after realizing that the Pigeonhole Principle might solve the problem) is to clearly identify the "pigeons" and the "pigeonholes."

Example Suppose S is a set of N natural numbers. Show that there is a subset of S whose sum is divisible by N.

For instance, if $S = \{5, 12, 19, 31\}$, then $N = 4$ and the subset $\{5, 12, 31\}$ works, and if $S = \{2, 19, 33\}$, then $N = 3$ and the subset $\{33\}$ works; so does the subset $\{2, 19, 33\}$.

Proof Let $S = \{a_1, a_2, ..., a_N\}$ where each $a_i \in \mathbb{N}$. Consider the N subsets $\{a_1\},\ \{a_1, a_2\}, ..., \{a_1, a_2, ..., a_i\}, ..., \{a_1, a_2, ..., a_N\}$.

If any one of the sums $a_1 + a_2 + ... + a_i$ is divisible by N, then the subset $\{a_1, a_2, ..., a_i\}$ works and we are done. So assume that none of these sums is divisible by N. Therefore each of these sums has one of the remainders $1, 2, ..., N - 1$ when divided by N.

Since there are N sums $a_1,\ \ a_1 + a_2,\ \ ...,\ \ a_1 + ... + a_N$ but only $N - 1$ possible remainders, two of these sums must have the same remainder when divided by N (the Pigeonhole Principle). In other words, there are two sums for which

$$a_1 + ... + a_i \quad \equiv_N \quad a_1 + ... + a_i + ... + a_k$$

Subtracting $a_1 + ... + a_i$ from both sides, we get that

$$0 \quad \equiv_N \quad a_{i+1} + ... + a_k$$

so $N|(a_{i+1} + ... + a_k)$. Therefore the subset $\{a_{i+1}, ..., a_k\}$ works.

Here, in Case ii), the "pigeons" are the N sets $\{a_1\},\ ...\ , \{a_1, a_2, ..., a_N\}$ and the "pigeonholes" are the $N - 1$ possible remainders: each set is put into a "pigeonhole" determined by the remainder when its sum is divided by N.

Example Prove that there is a natural number whose digits are all 1's and which is divisible by 7777.

Consider the 7778 numbers $1,\ 11,\ 111, ...,$ $\underline{11...1111}$
$\uparrow$ *this last number contains*
7778 *digits, all* $= 1.$

Assign to each number (*"pigeon"*) in the list, its remainder (*"the pigeonhole"*) when divided by 7777. There are only 7777 possible remainders $(r = 0, 1, ...,$ or $7776),$ so two of the 7778 listed numbers have the same remainder (the Pigeonhole Principle).

Suppose these two are a and b, where $a < b$. Then $b \equiv {}_{7777}\, a,$ so $b - a$ is divisible by 7777.

However, not all the digits of $b - a$ are 1's: if $b = 111\ ...\ 11111$ and
$a = \quad 11111$
then $b - a = 111\, ...\ 00000$ ends in a string of $0's$

In fact, if there are l 1's in $b,$ and there are k 1's in $a,$ then $b - a$ consists of $l - k$ 1's followed by k 0's. We can "cancel out" all the 0's in $b - a$ by dividing by 10^k : so $\frac{b-a}{10^k}$ is a natural number all of whose digits are 1. Is it <u>still</u> divisible by 7777?

Notice that $7777 = 7 \cdot 11 \cdot 101$, so that $b - a = 7777 \cdot m = 7 \cdot 11 \cdot 101 \cdot m$ for some $m \in \mathbb{N}$.

Therefore $\frac{b-a}{10^k} = \frac{7 \cdot 11 \cdot 101 \cdot m}{2^k 5^k} = 7 \cdot 11 \cdot 101 \cdot j = 7777 \cdot j$ for some $j \in \mathbb{N}$ (*we know* $\frac{b-a}{10^k}$ *is a natural number; the* 2*'s and* 5*'s in the denominator must cancel out with* 2*'s and* 5*'s in the prime factorization of* m : $\frac{m}{2^k 5^k} = j \in \mathbb{N}).$

So $\frac{b-a}{10^k}$ is a natural number with only 1's for digits and divisible by 7777.

Example (*taken from the Spring 2008 Missouri MAA Mathematics Competition*) Consider the set of points $\mathbb{Z} \times \mathbb{Z} = \{(z, w) \in \mathbb{R}^2 :$ z and w are both integers$\}$ in $\mathbb{R}^2$. Imagine having a palette containing 4 colors. You choose what color to paint the points in $\mathbb{Z} \times \mathbb{Z}$, in any way you like.

<u>Prove that, when you're done, there must be four points in $\mathbb{Z} \times \mathbb{Z}$ which all have the same color and which form the vertices of a rectangle.</u>

Proof (*We will use the pigeonhole principle, twice.*)

1) For any set of 5 points in $\mathbb{Z} \times \mathbb{Z}$, at least two must have the same color (*pigeonhole principle*). For example, in any "column of 5" $= \{(x,0), (x,1), (x,2), (x,3), (x,4)\}$ two points must have the same color.

2) For any "column of 5", there are 4 ways to color the first point $(x, 1)$; then 4 (independent) ways to color the second point $(x, 2)$; ...; and finally 4 (independent) ways to color the 5th point $(x, 5)$. Altogether, there are $4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 = 4^5 = 1024$ possible color patterns for a "column of 5."

3) Look at the first 1025 "columns of 5" :

$$\begin{array}{ll} \text{Column } 1 & = \{(1,0), (1,1), (1,2), (1,3),\ (1,4)\} \\ \text{Column } 2 & = \{(2,0), (2,1), (2,2), (2,3),\ (2,4)\} \\ \quad\vdots & \\ \text{Column } 1025 & = \{(1025,0),\ (1025,1), (1025,2), (1025,3),\ (1025,4)\} \end{array}$$

Two of these "columns of 5" must have exactly the same color pattern (*by the Pigeonhole principle, used again*). Suppose two such columns are

$$\begin{array}{ll} \text{Column } j & = \{\ (j,0),\ (j,1),\ (j,2),\ (j,3),\ (j,4)\} \\ \text{Column } k & = \{\ (k,0), (k,1),\ (k,2), (k,3),\ (k,4)\} \end{array}$$

Our first observation 1) tells us that two points in Column j have the same color: suppose they are (j, m) and (j, n) (*where* $0 \leq m < n \leq 4$).

Since Column k has the same color pattern, (k, m) and (k, n) are the same color as (j, m) and (j, n).

Then (j, m), (j, n), (k, m), and (k, n) are the same color and are the vertices of a rectangle. ●

Notice that <u>the number of colors</u>, 4, <u>is not important for the argument</u>. If there had been, say, 2008 colors available in the palette, then simply consider "columns of 2009" rather than "columns of 5". For each column, there are 2008^{2009} possible coloring patterns. Look at the first $2008^{2009} + 1$ "columns of 9." All the logic in the argument works in exactly the same way (but the 4 points that you find might turn out to be the vertices of a <u>very</u> large rectangle!)

Infinite Sets

We have defined finite and infinite sets and stated some properties of finite sets. One of these properties of finite sets, the Pigeonhole Principle, turned out to be particularly useful $-$ so we digressed a little to look at how the Pigeonhole Principle could be used. We now turn our attention to infinite sets, where our intuitive ideas can lead us astray: for example, a "whole" set (like $\mathbb{N}$) can be equivalent to one of its proper subsets (like $\mathbb{E} = \{2, 4, 6, ...\}$). So we have to be careful not to jump to conclusions when making statements about infinite sets.

Theorem The set A is infinite if and only if there exists a one-to-one function $f : \mathbb{N} \to A$.

Proof ($\Rightarrow$) Suppose A is infinite. Then

$A \neq \emptyset$ so we can pick an element $a_1 \in A$.
$A \neq \{a_1\}$ since $\{a_1\} \approx \mathbb{N}_1$
and A is not finite.
So $A - \{a_1\} \neq \emptyset$ so we can pick an $a_2 \in A - \{a_1\}$
(and $a_2 \neq a_1$)
$A \neq \{a_1, a_2\}$ since $\{a_1, a_2\} \approx \mathbb{N}_2$
and A is not finite.
So $A - \{a_1, a_2\} \neq \emptyset$ so we can pick an $a_3 \in A - \{a_1, a_2\}$
(and $a_3 \neq a_1,\ a_3 \neq a_2$)

Continue to define the a_n's by induction. Once a_n is defined. then

$A \neq \{a_1, a_2, ..., a_n\}$ since $\{a_1, a_2, ..., a_n\} \approx \mathbb{N}_n$
and A is not finite.
So $A - \{a_1, a_2, ..., a_n\} \neq \emptyset$ so we can pick an $a_{n+1} \in A - \{a_1, a_2, ..., a_n\}$
(and $a_{n+1} \neq a_1, a_2, ..., a_n$)

In this way we have inductively defined a_n for all $n \in \mathbb{N}$ and the terms in the sequence $a_1, a_2, ..., a_n, ...$ are all different (each was chosen in a way that makes it different from all its predecessors). Define $f : \mathbb{N} \to A$ by $f(n) = a_n$. Since the a_n's are all different, f is one-to-one.

For ($\Leftarrow$), we use the contrapositive: suppose A is finite and show that no such one-to-one function f can exist.

If $A = \emptyset$, then there are no functions $f : \mathbb{N} \to A$ (*see earlier discussion of* Y^X)

If $A \approx \mathbb{N}_k = \{1, 2, ..., k\}$, then there is a bijection $h : A \to \mathbb{N}_k$

If there were a one-to-one function $f : \mathbb{N} \to A$, then we could restrict the domain of f to get a "new" one-to-one function $g = f|\mathbb{N}_{k+1} : \mathbb{N}_{k+1} \to A$. Then $h \circ g : \mathbb{N}_{k+1} \to \mathbb{N}_k$ is one-to-one $-$ which contradicts the Pigeonhole Principle.

So, if A is finite, there is no one-to-one function $f : \mathbb{N} \to A$. ●

Note: A function $f : \mathbb{N} \to A$ is a sequence in A. The terms of the sequence are $a_1 = f(1), a_2 = f(2), ..., a_n = f(n), ...,$ and if f is one-to-one, then all these terms are different. So the preceding theorem could be paraphrased as: A is infinite iff there exists a sequence of distinct terms $a_1, a_2, ..., a_n, ...$ in A.

Example The point here is just to illustrate that our official definition of "infinite" gives results that coincide with some of our intuitive ideas about what sets are infinite.

1) The function $f : \mathbb{N} \to \mathbb{R}$ given by $f(n) = n$ is one-to-one. By the preceding theorem, $\mathbb{R}$ is infinite.

2) The function $f : \mathbb{N} \to (0,1)$ given by $f(n) = \frac{1}{n}$ is one-to-one, so the interval $(0,1)$ is infinite.

3) Suppose A is infinite, so that there is a one-to-one function $f : \mathbb{N} \to A$. If $A \subseteq B$, then we can view f also as being a one-to-one function $f : \mathbb{N} \to B$. So B is also infinite.

The following theorem tells us that if a subset $A \subseteq \mathbb{N}$ is "too big to be finite," then A is equivalent to the whole set $\mathbb{N}$. For example, consider the set $\mathbb{E} = \{2, 4, 6, ...\} \subseteq \mathbb{N}$. $\mathbb{E}$ is infinite so (according to the following theorem) $\mathbb{E}$ is equivalent to all of $\mathbb{N}$. In the case of $\mathbb{E}$, this statement is rather obvious: we can easily see that $f : \mathbb{N} \to \mathbb{E}$ given by $f(n) = 2n$ is a bijection. But we want to prove it for an arbitrary infinite subset of $\mathbb{N}$.

Theorem If A is infinite and $A \subseteq \mathbb{N}$, then $A \approx \mathbb{N}$.

Proof $A \neq \emptyset$. By the Well-Ordering Principle (WOP), there is a smallest element in A : call it a_1. Since A is infinite, there is a smallest element, call it a_2, in $A - \{a_1\}$, and $a_2 \neq a_1$.

If we have chosen distinct points $a_1, ..., a_n \in A$, then (since A is infinite) $A - \{a_1, ..., a_n\} \neq \emptyset$, so we let a_{n+1} be the smallest element in $A - \{a_1, ..., a_n\}$ (and a_{n+1} will be different from all the preceding a_i's). In this way, we have defined (inductively) a_n for all $n \in \mathbb{N}$, and all the a_n's are different.

Then define a function $f : \mathbb{N} \to A$ by $f(n) = a_n$; this f is a bijection. •

Definition The set A is called countable if

i) A is finite, or
ii) A is infinite and $A \approx \mathbb{N}$.

If $A \approx \mathbb{N}$, we use the symbol $\aleph_0$ to denote the cardinal number of A : $|\mathbb{N}| = \aleph_0$.
("$\aleph$" is "aleph", the first letter of the Hebrew alphabet. "$\aleph_0$" is read as "aleph-zero" or "aleph null" or "aleph naught" (more British). This notation was first used by George Cantor in his groundbreaking work of the theory of infinite sets (in the later part of the 19th century). We think of $\aleph_0$ as an infinite number: it represents the " number of elements" in the set $\mathbb{N}$ (and in any set equivalent to $\mathbb{N}$).

Examples

Countable Sets

Finite

$\emptyset$ $\quad\quad$ $|\emptyset| = 0$

$\{a, b, c\}$ $\quad\quad$ $|\{a, b, c\}| = 3$

Infinite

$$\begin{cases} \mathbb{N} \\ \mathbb{E} = \{2, 4, 6, 8, ...\} \\ \mathbb{Z} \\ \mathbb{Q}^+ \end{cases}$$

Since $\mathbb{N} \approx \mathbb{E} \approx \mathbb{Z} \approx \mathbb{Q}^+$
we have that $\aleph_0 = |\mathbb{N}| = |\mathbb{E}| = |\mathbb{Z}| = |\mathbb{Q}^+|$

The number of elements in each of these sets
is the same: $\aleph_0$

Uncountable Sets

$\mathcal{P}(\mathbb{N})$ This set is clearly infinite, and $\mathbb{N} \not\approx \mathcal{P}(\mathbb{N})$
(*we proved that for every set* A, $A \not\approx \mathcal{P}(A)$)
so the set is uncountable: $|\mathcal{P}(\mathbb{N})| \neq \aleph_0$

Note: the textbook also uses the term "denumerable" to mean "a countable set that is not finite." Be aware that different books use the terms "denumerable," "countable" (and the term "enumerable") in slightly different ways.

We proved earlier that a set A is infinite iff there exists a one-to-one function $f : \mathbb{N} \to A$. Informally this means that an infinite set is "big enough" to have a one-to-one "copy" of $\mathbb{N}$ put inside it (the "copy" is range(f)). In the same informal spirit, the next theorem says that a countable infinite set is "small enough" that a "copy" of the set can be put inside $\mathbb{N}$.

Theorem The set A is countable iff there exists a one-to-one function $f : A \to \mathbb{N}$.

Proof ($\Leftarrow$) If there does exist a one-to-one function $f : A \to \mathbb{N}$, then A is equivalent to a subset of $\mathbb{N}$, namely, $A \approx$ range(f). If range(f) is finite, then A is finite. But if range(f) is an infinite subset of $\mathbb{N}$, then range$(f) \approx \mathbb{N}$ (by the preceding Theorem). By transitivity, then, $A \approx \mathbb{N}$. So A is countable.

($\Rightarrow$) Suppose A is countable.

If $|A| = 0$, then $A = \emptyset$ and the empty function $\emptyset\ : \emptyset \to \mathbb{N}$ is one-to-one.
If $|A| = k$, then there is a bijection $f : A \to \{1, 2, ..., k\}$, and this same
$f : A \to \mathbb{N}$ is one-to-one
If A in not finite, then, by definition of countable, $A \approx \mathbb{N}$, so there exists a
bijection $f : A \to \mathbb{N}$, and, of course, this f is one-to-one. ●

Corollary A subset of a countable set is countable.

Proof Suppose A is a countable set. Then there is a one-to-one function $f : A \to \mathbb{N}$.
If $B \subseteq A$, then look at the restricted function $g = f|B$. Then $g : B \to \mathbb{N}$ is one-to-one, so, by the theorem, B is countable. ●

Corollary If B is an <u>uncountable</u> set and $B \subseteq C$, then C is uncountable. (*More informally, a set that contains an uncountable set is uncountable.*)

Proof If C were a countable set, then its subset B would have to be countable (by the preceding corollary. ●

Next we will look at another example of a familiar set that is uncountable. Before doing so, we need to call attention to a fact about decimal representations of real numbers.

> *Two <u>different</u> decimal expansions can represent the <u>same</u> real number. For example, $0.1\overline{0} = 0.100000... = 0.09999... = 0.0\overline{9}$ (why?). However, two different decimal expansions can represent the same r<u>eal n</u>umber only if one of the expansions ends in an infinite string of 0's and the other ends in an infinite string of 9's.*

Example The interval $(0,1)$ is not equivalent to $\mathbb{N}$ (and therefore, since the interval $(0,1)$ is infinite, it is uncountable).

Consider any $f:\mathbb{N}\to(0,1)$. We will show f cannot be onto, so that no bijection can exist between $\mathbb{N}$ and $(0,1)$.

Write decimal expansions of all the numbers in range(f) :

$$\begin{aligned}
f(1) &= r_1 = 0.x_{11}\,x_{12}\,x_{13}\ldots\;x_{1n}\ldots\\
f(2) &= r_2 = 0.x_{21}\,x_{22}\,x_{23}\ldots\;x_{2n}\ldots\\
f(3) &= r_3 = 0.x_{31}\,x_{32}\,x_{33}\ldots\;x_{3n}\ldots\\
&\;\;\vdots\\
f(n) &= r_n = 0.x_{n1}\,x_{n2}\,x_{n3}\ldots x_{nn}\ldots\\
&\;\;\vdots
\end{aligned}$$

Now define a real number $y=0.y_1y_2y_3\ldots\;y_n\ldots$ by setting

$$\begin{cases} y_n = 1 & \text{if } x_{nn}\neq 1\\ y_n = 2 & \text{if } x_{nn}=1\end{cases}$$

Then $y\in(0,1)$ Notice that

i) the decimal expansion of y is different from every decimal expansion in the list $-$ specifically, the decimal expansions of y and r_n disagree at the n^{th} decimal place: $y_n\neq x_{nn}$.

ii) the decimal expansion of y is not an alternate decimal representation for any of the r_n's because $0.y_1y_2y_3\ldots\;y_n\ldots$ does not end in either an infinite string of 0's or 9's.

Therefore $(\forall n)\;y\neq r_n$. In other words, $y\;\notin$ ran$\,(f)$ and therefore f is not onto.

The argument in the example is referred to as “Cantor's diagonal argument.”

Example $\mathbb{R}$ is uncountable.

i) One reason: $(0,1)\subseteq\mathbb{R}$ and a set containing an uncountable set must be uncountable (see preceding corollary)

ii) Another reason: we saw earlier that $(0,1)\approx\mathbb{R}$ and a set equivalent to an uncountable set is uncountable (*why*?)

iii) $\mathbb{R}\approx\mathbb{R}\times\{0\}$, so $\mathbb{R}\times\{0\}$ is uncountable; and $\mathbb{R}\times\{0\}\subseteq\mathbb{R}^2$, so $\mathbb{R}^2$ is uncountable. Similarly, $\mathbb{R}^3$, $\mathbb{R}^4$, ... are each uncountable sets.

Definition If a set A is equivalent to $(0,1)$, then we say that the cardinal number of the set A is c. More formally, if $A \approx (0,1)$, then $|A| = c$.

We think of c as an infinite cardinal number: it represents the "number of elements" in the set $(0,1)$, and in any set equivalent to $(0,1)$. For example,

$$c = |(0,1)| = |(a,b)| = |\mathbb{R}| = |(0,\infty)|$$

In his development of set theory, Cantor chose the symbol "c" for the cardinality of these sets because "continuum" was an old name for the real number line.

> At this point, we have not given a precise definition for " $<$ " between infinite cardinal numbers. However, since $\mathbb{N} \subseteq \mathbb{R}$, we intuitively expect that $\aleph_0 \leq c$; and since $\mathbb{N} \not\approx \mathbb{R}$, that $\aleph_0 < c$. When " $\leq$ " and " $<$ " are officially defined, "$\aleph_0 < c$" turns out to be true.
>
> Cantor conjectured, but was unable to prove, that there are no cardinal numbers of "intermediate size" between $\aleph_0$ and c. This conjecture is called the "Continuum Hypothesis." A complete understanding about the Continuum Hypothesis (CH) didn't come until another half-century passed.
>
> Around 1930, a mathematician named Kurt Gödel proved that it is impossible to prove that CH is false (starting with the ZFC axioms for set theory). On the other hand, about 1960, a mathematician named Paul Cohen proved that is it impossible to prove that CH is true (starting with the ZFC axioms for set theory) that CH is true. These results, taken together, mean that CH is "undecidable" (in terms of the ZFC axioms).
>
> One could go back to the ZFC Axioms and add "CH is true" as a new axiom; or add "CH is false" as a new axiom. The result would be two "different set theories" (*these are analogous to Euclidean and non-Euclidean geometries that arise from modifying Euclid's parallel postulate.*)
>
> Fortunately, the issue of whether CH is true or false rarely comes up in doing mathematical research. Therefore there's usually no need to worry about making a choice between these "competing" versions of set theory.

Example $[0,1) \cup (2,3) \approx (0,1)$

A bijection between the two sets is given by $f(x) = \begin{cases} -\frac{1}{2}x + \frac{1}{2} & \text{for } 0 \leq x < 1 \\ \frac{1}{2}x - \frac{1}{2} & \text{for } 2 < x < 3 \end{cases}$

(*Draw a reasonably careful picture!*)

Therefore $|[0,1) \cup (2,3)| = |(0,1)| = c$.

Theorem Suppose we have finitely many countable sets $A_1, ..., A_n$. Then the product set $A_1 \times A_2 \times ... \times A_n$ is countable. In other words, the product of a finite number of countable sets is countable.

Proof Since each set $A_1, ..., A_n$ is countable, we know that there exist one-to-one functions:

$$\begin{array}{l} f_1 : A_1 \to \mathbb{N} \\ f_2 : A_2 \to \mathbb{N} \\ \qquad \vdots \\ f_i : A_i \to \mathbb{N} \\ \qquad \vdots \\ f_n : A_n \to \mathbb{N} \end{array}$$

Let $p_1, ..., p_n$ be the first n prime numbers and use these to define a function $f : A_1 \times A_2 \times ... \times A_n \to \mathbb{N}$ are follows:

$$f(\,(a_1, ..., a_i, ..., a_n)\,) = p_1^{f_1(a_1)} \cdot ... \cdot p_i^{f_i(a_i)} ... \cdot p_n^{f_n(a_n)} = \text{some } n \in \mathbb{N}.$$

This function f is one-to-one:

Suppose $(a_1, ..., a_i, ..., a_n) \neq (b_1, ..., b_i, ..., b_n) \in A_1 \times A_2 \times ... \times A_n$

Then $f(\,(b_1, ..., b_i, ..., b_n)\,) = p_1^{f_1(b_1)} \cdot ... \cdot p_i^{f_i(b_i)} ... \cdot p_n^{fn(b_n)} = \text{some } m \in \mathbb{N}.$

Since $(a_1, ..., a_i, ..., a_n) \neq (b_1, ..., b_i, ..., b_n)$, we know that $a_i \neq b_i$ for some i, and, because f_i is one-to-one, this means that $f_i(a_i) \neq f_i(b_i)$.

Therefore p_i occurs in the prime factorizations of both m and n, but a different number to times in each factorization). By the Fundamental Theorem of Arithmetic, we conclude that $m \neq n$. Therefore f is one-to-one.

Since we have produced a one-to-one function $f : A_1 \times A_2 \times ... \times A_n \to \mathbb{N}$, a previous theorem tells us that $A_1 \times A_2 \times ... \times A_n$ is countable. •

Example Each of the following sets is countable:

$$\mathbb{N} \times \mathbb{Z}$$

$$\mathbb{Q}^+ \times \{0, 1, 2\} \times \mathbb{Z} \times \mathbb{N}$$

$$\mathbb{Z} \times \omega \times \mathbb{N}$$

$$\mathbb{Z} \times \emptyset \times \{1, 2\} \times \mathbb{Q}^+$$

Theorem Suppose $A_1, A_2, ..., A_n,$ ... is a sequence of countable sets (one for each n in the index set $\mathbb{N}$), and suppose that the A_n's are pairwise disjoint. Then $\bigcup_{n=1}^{\infty} A_n$ is countable.

Proof Let $p_n =$ the n^{th} prime number. Then $p_1, p_2, ..., p_n, ...$ is the infinite sequence of prime numbers.

Since each set $A_1, ..., A_n, ...$ is countable, we know that there exist one-to-one functions

$$\begin{gathered} f_1 : A_1 \to \mathbb{N} \\ f_2 : A_2 \to \mathbb{N} \\ \vdots \\ f_i : A_i \to \mathbb{N} \\ \vdots \\ f_n : A_n \to \mathbb{N} \\ \vdots \end{gathered}$$

Define a function $f : \bigcup_{n=1}^{\infty} A_n \to \mathbb{N}$ as follows:

> if $x \in \bigcup_{n=1}^{\infty} A_n,$ then there is a unique i for which $x \in A_i$. Then $f_i(x) \in \mathbb{N}$ and we can let $f(x) = p_i^{f_i(x)}$.

This f is one-to-one: suppose $x \neq y \in \bigcup_{n=1}^{\infty} A_n$.

> i) If x, y are in the same set A_i. Because f_i is one-to-one, $f_i(x) \neq f_i(y)$. Therefore $f(x) = p_i^{fi(x)} \neq p_i^{fi(y)} = f(y),$ by the Fundamental Theorem of Arithmetic (because the exponents for p_i are differ$e$nt).
>
> ii) If $x \in A_i$ and $y \in A_n$ (where $i \neq n),$ then $f(x) = p_i^{fi(x)}$ and $f(y) = p_n^{f_n(y)}$. So $f(x)$ and $f(y)$ factor as powers of two different primes, p_i and p_n. By the Fundamental Theorem of Arithmetic, $f(x) \neq f(y)$.

Therefore $f(x) \neq f(y)$, so f is one-to-one. Since we have produced a one-to-one function $f : \bigcup_{n=1}^{\infty} A_n \to \mathbb{N}$, we conclude that $\bigcup_{n=1}^{\infty} A_n$ is countable. •

The next corollary says that we really do not need the hypothesis "pairwise disjoint" in the theorem. However it was notationally easier to first prove the theorem with the "pairwise disjoint" hypothesis, and (now) to worry about what happens if some of the sets have nonempty intersection.

Corollary Suppose $B_1, B_2, ..., B_n, \ ...$ is a sequence of countable sets (one for each n in the indexing set $\mathbb{N}$). Then $\bigcup_{n=1}^{\infty} B_n$ is countable.

Proof Define
$$\begin{aligned} A_1 &= B_1 \\ A_2 &= B_2 - B_1 \\ A_3 &= B_3 - (B_1 \cup B_2) \\ &\ \vdots \\ A_n &= B_n - (B_1 \cup \dots \cup B_{n-1}) \\ &\ \vdots \end{aligned}$$

Since each $A_n \subseteq B_n$, each A_n is countable. Also, the A_n's are pairwise disjoint:

> Consider A_i and A_n where $i < n$. If $x \in A_i = B_i - (B_1 \cup \dots \cup B_{i-1})$, then $x \in B_i$. Since $i \le n - 1$, $x \in B_1 \cup \dots \cup B_{n-1}$. Therefore $x \notin A_n$, so $A_i \cap A_n = \emptyset$.

Since $A_n \subseteq B_n$, $\bigcup_{n=1}^{\infty} A_n \subseteq \bigcup_{n=1}^{\infty} B_n$. We claim that these sets are actually equal.

> Suppose $x \in \bigcup_{n=1}^{\infty} B_n$. Pick the smallest $n = n_0$ for which $x \in B_{n_0}$. Then $x \notin B_i$ for $i < n_0$ and therefore $x \in A_{n_0} = B_{n_0} - (B_1 \cup \dots \cup B_{n_0 - 1})$, so $x \in \bigcup_{n=1}^{\infty} A_n$. Therefore $\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} B_n$.

The theorem then applies to the A_n's, and we conclude that $\bigcup_{n=1}^{\infty} B_n = \bigcup_{n=1}^{\infty} A_n$ is countable. •

Corollary If $B_1, B_2, ..., B_k$ is a finite collection of countable sets, then $B_1 \cup ... \cup B_k = \bigcup_{n=1}^{k} B_n$ is countable.

(*This seems completely plausible, since we have "less than a full sequence" of countable sets. In order to apply the preceding corollary, we simply "pad out" the sets to form a sequence by adding empty sets to the list.*)

Proof Define $B_n = \emptyset$ for each $n > k$. By the preceding corollary, $\bigcup_{n=1}^{\infty} B_n$ is countable. But $\bigcup_{n=1}^{\infty} B_n = B_1 \cup ... \cup B_k$ since $B_n = \emptyset$ for each $n > k$. •

> In words we can summarize the preceding theorem and its corollaries as follows:
> the union of countably many countable sets is countable
> ↑
> *a finite number, or a sequence* $A_1, ..., A_n, ...$

Examples i) For $n \in \mathbb{N}$, let $A_n = \{\frac{1}{n}.\frac{2}{n}, ..., \frac{n}{n}, \frac{n+1}{n}, \ ... \ \}$ = the set of all positive rationals that can be written with denominator n. Then $\mathbb{Q}^+ =$ the set of all positive rationals $= \bigcup_{n=1}^{\infty} A_n$ is countable.

ii) The function $f(x) = -x$ is a bijection $f : \mathbb{Q}^+ \to \mathbb{Q}^-$ = the set of all negative rationals, so $\mathbb{Q}^-$ is countable. Since the set of all rationals$\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+ =$ the union of finitely many countable sets, $\mathbb{Q}$ is countable.

Transcendental Numbers: An Extended Example

We have proved some not-too-complicated theorems about countable and uncountable sets. But these elementary facts are enough to let us prove an interesting result about real numbers.

A rational number $\frac{p}{q}$ is the root of first-degree polynomial equation with integer coefficients, namely: $qx - p = 0$ (and, conversely, the root of such an equation is a rational number).

We can generalize the idea of a rational number by looking at the real numbers that are roots of higher degree polynomial equations with integer coefficients.

Definition A real number r is called an algebraic number if there is a polynomial

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ \dots \ + a_1 x + a_0$$

with integer coefficients $a_0, a_1, \dots, a_n$ for which $P(r) = 0$.

> *A little less formally: an algebraic real number is one that's a root of some polynomial equation with integer coefficients.*

As remarked above: if $P(x)$ is a degree 1 polynomial with integer coefficients, then a root of $P(x) = 0$ is just a rational number. But, for example all of the following irrationals are also algebraic numbers.

> $\sqrt{2}$ is an algebraic number, because it is a root of a quadratic equation with integer coefficients: $x^2 - 2 = 0$.
>
> $\frac{1}{2} + \frac{1}{6}\sqrt{69}$ is an algebraic number because it is a root of a quadratic equation with integer coefficients: $3x^2 - 3x - 5 = 0$.
>
> $\sqrt[7]{2}$ is algebraic because it is a root of a 7th degree polynomial equation with integer coefficients: $x^7 - 2 = 0$.

A reasonable question would be: are there any real numbers that are not algebraic?

Theorem The set $\mathbb{A} = \{r \in \mathbb{R} : r \text{ is algebraic}\}$ is countable.

Proof For each $n \geq 1$, let $\mathcal{P}_n = \{a_n x^n + \dots + a_1 x + a_0 : a_n, \dots, a_1, a_0 \in \mathbb{Z}\}$
$=$ the set of all polynomials of degree $\leq n$ with integer coefficients (*the degree will be* $< n$ *if the coefficient* a_n *happens to be* 0).
To name a polynomial in $\mathcal{P}_n$, all we need to know is the list of its coefficients. The list of coefficients is $(n+1)$-tuple of integers : $(a_n, a_{n-1}, \ \dots \ , a_0) \in \mathbb{Z} \times \dots \times \mathbb{Z} = \mathbb{Z}^{n+1}$. To put it another way, the function $g : \mathcal{P}_n \to \mathbb{Z}^{n+1}$ given by

$$g(a_n x^n + \dots + a_1 x + a_0) = (a_n, a_{n-1}, \ \dots \ , a_0)$$

is a bijection.

Therefore $\mathcal{P}_n \approx \mathbb{Z} \times ... \times \mathbb{Z} = \mathbb{Z}^{n+1}$ and $\mathbb{Z}^{n+1}$ is a finite product of countable sets. So $\mathcal{P}_n$ is countable and therefore there is a bijection $f : \mathbb{N} \to \mathcal{P}_n$.

Thus the polynomials in the set $\mathcal{P}_n$ can be listed in a sequence:

$$\mathcal{P}_n = \{ \ P_{n,1}(x), P_{n,2}(x), ..., P_{n,k}(x), ... \ \}$$

(*Here,* $P_{n,k} = f(k) =$ *the* k^{th} *term of the sequence* f.)

<u>Each</u> polynomial $P_{n,1}(x), P_{n,2}(x), ..., P_{n,k}(x), ... P_{n,k}$ in this list has degree $\leq n$, and therefore each equation $P_{n,k}(x) = 0$ has <u>at most</u> <u>n</u> <u>roots</u>. So the set

$$R_{n,k} = \{r \in \mathbb{R} : P_{n,k}(r) = 0\} = \{r : r \text{ is a root of } \ P_{n,k}(x) = 0\} \text{ is } \underline{\text{finite}}$$

<u>We now put all this together using our knowledge about countable sets</u>.

$$A_n = \bigcup_{k=1}^{\infty} R_{n,k} = R_{n,1} \cup R_{n,2} \cup ... \cup R_{n,k} \ \cup \ ...$$

$$= \{r : \ r \text{ is a root of a polynomial of degree } \ \leq n \text{ with integer coefficients}\}$$

is a countable union of countable (finite!) sets; so A_n is countable.

Then $\bigcup_{n=1}^{\infty} A_n$ is countable, since it is a countable union of countable sets.

But $r \in \bigcup_{n=1}^{\infty} \mathbb{A}_n \ \Leftrightarrow r$ is in one of the sets $A_n \ \Leftrightarrow \ r$ is a root of a polynomial of degree $\leq n$ with integer coefficients $\Leftrightarrow \ r$ is an algebraic number. So $\mathbb{A} = \bigcup_{n=1}^{\infty} A_n$ is countable. •

Definition A real number which is <u>not</u> algebraic is called <u>transcendental</u>. (*Euler called these numbers "transcendental" because they "transcend the power of algebraic methods." To be more politically correct, we might call them "polynomially challenged."*)

Corollary Transcendental numbers exist.

Proof Let $\mathbb{T}$ be the set of transcendental numbers. By definition, $\mathbb{R} = \mathbb{A} \cup \mathbb{T}$. Since $\mathbb{A}$ is countable and $\mathbb{R}$ is uncountable, $\mathbb{T}$ cannot be empty. •

In fact, this two-line argument actually proves much more: not only is $\mathbb{T}$ <u>nonempty</u>, but $\mathbb{T}$ must be <u>uncountable</u>! In the sense of one-to-one correspondence, there are "many more" transcendental numbers than algebraic numbers on the real line $\mathbb{R}$.

This is an example of a "pure existence" proof – it does tell us that any particular number is transcendental number, and the proof does not give us any computational hints about how to find a specific transcendental number. To do that is harder. Transcendental numbers were first shown to <u>exist</u> by Liouville in 1844. (*Liouville used other (more difficult) methods. The ideas about countable and uncountable sets were not developed until the early 1870's by Georg Cantor. See the biography on the course website.*)

Two famous examples of transcendental numbers are e (proven to be transcendental by Hermite in 1873) and π (Lindemann, 1882).

One method for producing many transcendental numbers is contained in a theorem of the Russian mathematician Gelfand (1934). It implies, for example, that $\sqrt{2}^{\sqrt{2}}$ is transcendental.

> **Gelfand's Theorem** If α is an algebraic number, $\alpha \neq 0$ or 1, and β is algebraic and not rational, then α^{β} is transcendental.

The number e^{π} is also transcendental. This follows from Gelfand's Theorem (which allows complex algebraic numbers) if you know something about the arithmetic of complex numbers:

$e^{\pi} = e^{-i^2\pi}=(e^{i\pi})^{-i}$ and $e^{i\pi} = \cos\pi + i\sin\pi = -1$.
So $e^{\pi} = (-1)^{-i}$, which is transcendental by Gelfand's Theorem.

Arithmetic with Cardinal Numbers

Suppose $|A| = m$ and $|B| = n$ (here, m, n might be finite or infinite cardinal numbers, for example $m = 7$ or $n = \aleph_0$ or $n = c$).

Definition i) $m \cdot n = |A \times B|$
ii) $m + n = |A \cup B|$, provided that A and B are disjoint
iii) $m^n = |A^B|$ (*where, recall,* A^B *denotes the set of all functions from* B *to* A)

So, for example:

i) $2 \cdot 3 = |\{0,1\}| \cdot |\{a,b,c\}| = |\{0,1\} \times \{a,b,c\}|$
$= |\{(0,a),\ (0,b),\ (0,c),\ (1,a),\ (1,b),\ (1,c)\}| = 6$

ii) $\aleph_0 = |\mathbb{N}|$ so, by definition of cardinal numbers, $\aleph_0 \cdot \aleph_0 = |\mathbb{N} \times \mathbb{N}| \underset{\uparrow}{=} |\mathbb{N}| = \aleph_0$
because we already know that $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

Notice that in i), we could just as well have used the sets $\{a,b\}$ and $\{1,2,3\}$ in place of $\{0,1\}$ and $\{a,b,c\}$; and in ii), we could just as well have used $\mathbb{Z}$ or $\mathbb{Q}^+$ instead of $\mathbb{N}$. The answer for $m \cdot n$ would, in both cases, have come out the same. This is because the operations of $\cdot$, $+$, and exponentiation are well-defined: the results do not depend on which particular sets with cardinal numbers m,n, we used during the computation. That this is true is the content of the next theorem.

Theorem If $A \approx C$ and $B \approx D$, then

i) $A \times B = C \times D$
ii) $A \cup B \approx C \cup D$, provided that $A \cap B = \emptyset$ and $C \cap D = \emptyset$
iii) $A^B \approx C^D$

In terms of cardinal arithmetic, i) says that if $|A| = |C| = m$ *and* $|B| = |D| = n$, *then* $|A \times C| = m \cdot n = |C \times D|$: *that is* $m \cdot n$ *is the same whether you compute using the sets* A *and* B, *or the sets* C *and D. A similar interpretation applies to ii) and iii).*

Proof By hypothesis, there exist bijections $f : A \to C$ and $g : B \to D$

i) Define $h : A \times B \to C \times D$ by $h(a,b) = (f(a), g(b)) \in C \times D$.

If $(a,b) \neq (a',b')$, then either $a \neq a'$ (in which case $f(a) \neq f(a')$ since f is one-to-one) or $b \neq b'$ (in which case $g(b) \neq g(b')$). Either way, $h(a,b) \neq h(a',b')$ so h is one-to-one.

If $(c,d) \in C \times D$, then (since f and g are onto) there are elements $a \in A$ and $b \in B$ for which $f(a) = c$ and $f(b) = d$. Then $(a,b) \in A \times B$ and $h(a,b) = (c,d)$. Therefore h is onto.

Therefore h is a bijection, so $A \times B \approx C \times D$.

ii) Let $h = f \cup g$, or as a formula, let $h(x) = \begin{cases} f(x) & \text{for } x \in A \\ g(x) & \text{for } x \in B \end{cases}$ and $h : A \cup B \to C \cup D$. Since A and B are disjoint h is a function, and, since C and D are disjoint, h is also one-to-one (using also f and g are one-to-one). It is easy to check that h is onto $C \cup D$. Therefore $A \cup B \approx C \cup D$.

iii) We want to define a bijection $\Phi : A^B \to C^D$. An element in $h \in A^B$ is a function $h : B \to A$, and we want $\Phi(h)$ to be a function from $D \to C$, that is, we want $\Phi(h) \in C^D$. We can picture the situation as follows : we have the function h, f, g and need to say what the function $\Phi(h)$ is.

$$\begin{tikzcd}
B \arrow[r, "h"'] \arrow[d, "g"] & A \arrow[d, "f"] \\
D \arrow[r, dashed, "\Phi(h)"'] & C
\end{tikzcd}$$

Since f and g are bijections, they each have an inverse function and we can define $\Phi(h) = f \circ h \circ g^{-1} : D \to C$.

Suppose h and h' are two different functions in A^B: $h \neq h'$. This means that there is a point $b \in B$ for which $h(b) \neq h(b')$. Let $d = g(b) \in D$. Then $\Phi(h)(d) = f(h(g^{-1}(d)))$ $= f(h(g^{-1}(g(b)))) = f(h(b))$ and similarly $\Phi(h')(d) = f(h'(b))$. Since $h(b) \neq h(b')$ and f is one-to-one, $\Phi(h)(d) \neq \Phi(h')(d)$. Therefore the functions $\Phi(h)$ and $\Phi(h')$ disagree at the point $d \in D$, so they are different functions: $\Phi(h) \neq \Phi(h')$. Therefore Φ is one-to-one.

Suppose $j \in C^D$, that is suppose $j : D \to C$.

$$\begin{tikzcd}
B \arrow[r, dashed, "h=?"'] \arrow[d, "g"] & A \arrow[d, "f"] \\
D \arrow[r, "j"'] & C
\end{tikzcd}$$

To show that Φ is onto, we need to show that there is a function $h \in A^B$ for which $\Phi(h) = j$. But this is easy: if we let $h = f^{-1} \circ j \circ g$, then $h \in A^B$ and $\Phi(h) = f \circ h \circ g^{-1}$ $= f \circ f^{-1} \circ j \circ g \circ g^{-1} = j \circ g \circ g^{-1} = j$. Therefore Φ is onto.

Thus, Φ is a bijection and therefore $A^B \approx C^D$. •

Examples

1) $2^3 = |\{0,1\}^{\{a,b,c\}}| =$ the number of functions f from $\{a, b, c\}$ to $\{0, 1\}$.
Each such function $f = \{(a, *), (b, **), (c, ***)\}$. Since there are two choices for $*$, and (independent of other choices) two choices for each of $**$ and $***$, there are altogether $2 \cdot 2 \cdot 2 = 8$ ways to create such a function f. So $2^3 = 8$.

In an earlier example, we checked that $2 \cdot 3 = 6$.

Also, $2 + 3 = |\{1, 2\}| + |\{3, 4, 5\}| = |\{1, 2\} \cup \{3, 4, 5\}| = |\{1, 2, 3, 4, 5| = 5.$

Earlier, we defined $+$, $\cdot$, and exponentiation for whole numbers (when we formally constructed the system ω. It's possible to prove that the "old definitions" for $+$, $\cdot$, and exponentiation in ω give the same answers as when the "new definitions" for cardinal arithmetic are applied to finite cardinal numbers. But we won't go into the easy (and tedious) details.

2) Suppose $m = |A|$ (where m is any finite or infinite cardinal number):

$m \cdot 0 = |A| \cdot |\emptyset| = |A \times \emptyset| = |\emptyset| = 0$
$m + 0 = |A| + |\emptyset| = |A \cup \emptyset| = |A| = m$
$m^0 = |A^\emptyset| =$ "the number of functions from $\emptyset$ to A" $= 1$. (*The only such function is the* *<u>empty function</u>* $\emptyset$.)

3) $\aleph_0 + 2 = |\{3, 4, 5, ...\}| + |\{1, 2\}| = |\{3, 4, 5...\} \cup \{1, 2\}| = |\mathbb{N}| = \aleph_0$. (*Notice that since it doesn't matter which (disjoint) sets I use to represent* $\aleph_0$ *and* 2 *in the calculation, I chose the sets in a way that makes the final result particularly easy to see; I could have written* $\aleph_0 + 2 = |\mathbb{Q}^+ \cup \{a, b\}|$, *but then I would have to (momentarily) stop and think: is* $\mathbb{Q}^+ \cup \{a, b\} \approx \mathbb{N}$*?*

4) $c + c = |(-\infty, 0]| + |(0, \infty)| = |(-\infty, 0] \cup (0, \infty)| = |\mathbb{R}| = c.$

5) $2^{\aleph_0} = |\{0, 1\}^{\mathbb{N}}| = |$ the set of all binary sequences $|$. (*In fact,* $2^{\aleph_0}$ *can be simplified: we will see how a bit later*.)
$2^c = |\{0, 1\}^{\mathbb{R}}| = |$ the set of all functions with domain $\mathbb{R}$ and codomain $\{0, 1\}$ $|$

6) For any sets A, B it is true that $A \times B \approx B \times A$ (*why?*) and $A \cup B = B \cup A$. Therefore if $|A| = m$ and $|B| = n$,

i) $m \cdot n = n \cdot m$, and
ii) $m + n = n + m$.

7) A more complicated example: $\aleph_0 + c = c$

$\aleph_0 + c = |\{\,...\,,\,-3,\ -2,\ -1\}| + |(0,\infty)| = |\{...\,,\,-3,\,-2,\,-1\} \cup (0,\infty)|$

We will show that $\{...\,,\,-3,\,-2,\,-1\} \cup (0,\infty) \approx (0,\infty)$. To do this, write $\{...\,,\,-3,\,-2,\,-1\} \cup (0,\infty)$ as the union of three disjoint pieces:

$$\{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\} \ \cup\ ((0,\infty) - \{1,2,3,...\})$$

The set $\{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\}$ is countable, so there exists a bijection

$f : \{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\} \to \mathbb{Z}$. Define

$$h : \{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\} \ \cup\ ((0,\infty) - \{1,2,3,...\}) \ \ \to\ \ (0,\infty)$$

by $\quad h(x) = \begin{cases} f(x) & \text{if } x \in \{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\} \\ x & \text{if } x \in (0,\infty) - \{1,2,3...\} \end{cases}$

(*Informally: h uses f to put elements of* $\{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\}$ *into one-to-one correspondence with the elements* $\{1,2,3,...\}$ *inside* $(0,\infty)$*; h puts the elements remaining in* $(0,\infty) - \{1,2,3,...\}$ *into correspondence with themselves.*)

h is a bijection (*check!*) so

$|\{...\,,\,-3,\,-2,\,-1\} \cup (0,\infty)| =$

$|\{...\,,\,-3,\,-2,\,-1\} \ \cup\ \{1,2,3,...\} \ \cup\ ((0,\infty) - \{1,2,3,...\}| = |(0,\infty)| = c.$

8. In a similar way, it's possible to prove that if m is any infinite cardinal numbers, then $\aleph_0 + m = m$.

Defining an Ordering Among the Cardinal Numbers

Definition Suppose $m = |A|$ and $n = |B|$ are cardinal numbers (possibly infinite). We say that

i) $m \leq n$ if there exists a one-to-one function $f : A \to B$. Since $A \approx \text{range}(f) \subseteq B$, we could say, equivalently, that $m \leq n$ if A is equivalent to a subset of B.

ii) $m < n$ if $m \leq n$ and $m \neq n$. Equivalently, $m < n$ if A is equivalent to a subset of B but A is not equivalent to B.

For example, there is a one-to-one function $f : \mathbb{N} \to \mathbb{R}$ (*namely,* $f(n) = n$), so $\aleph_0 \leq c$. We also know that $\mathbb{N}$ is not equivalent to $\mathbb{R}$, so $\aleph_0 < c$.

We need to check that this relation " $\leq$ " among cardinals is well-defined: that is, we get the same answer for "is $m \leq n$?" if we use different sets C, D for which $|C| = m$ and $|D| = n.$
That is what the following theorem tells us.

Theorem Suppose $A \approx C$ and $B \approx D.$ Then there exists a one-to-one function $f : A \to B$ iff there exists a one-to-one function $g : C \to D.$

Proof We know that there are bijections $h : A \to C$ and $j : B \to D.$

Suppose there is a one-to-one function $f : A \to B.$ Then $g = j \circ f \circ h^{-1} : C \to D$ is a composition of one-to-one functions, so g is one-to-one.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[d, "j"] \\ C \arrow[r, dashed, "g"] & D \end{tikzcd}$$

Conversely, if there exists a one-to-one function $g : C \to D,$ then there must be a one-to-one function $f : A \to B,$ namely, $f = j^{-1} \circ g \circ h : A \to B$ (*draw a similar diagram to illustrate the relation between the functions*). •

Examples

1) $\{0, 1\}$ is equivalent to a <u>subset</u> of $\{1, 2, 3\}$ but $\{0, 1\}$ is not equivalent to $\{1, 2, 3\}$. Therefore $|\{0, 1\}| = 2 < 3 = |\{1, 2, 3\}|$.

2) Let m be a <u>nonzero</u> cardinal number and let A be a set for which $|A| = m.$ Because $\emptyset$ is a subset of A but $\emptyset \not\approx A$, we get that $0 = |\emptyset| < |A| = m.$ Therefore 0 is the smallest cardinal number.

3) There is a one-to-one function $f : A \to \mathcal{P}(A)$, namely, $f(a) = \{a\}$ for each $a \in A.$ Therefore $|A| \leq |\mathcal{P}(A)|$. Since we proved earlier that $A \not\approx \mathcal{P}(A)$, we get that $|A| < |\mathcal{P}(A)|$.

4) There is a one-to-one function $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$, namely, $f(n) = \{n\} \in \mathcal{P}(\mathbb{N})$, and we already know that $\mathbb{N} \not\approx \mathcal{P}(\mathbb{N})$. Therefore

$$\aleph_0 < |\mathcal{P}(\mathbb{N})| = |\{0, 1\}^{\mathbb{N}}|$$

5) $0 < 1 < 2 < \ldots < k < \ldots < \aleph_0 < \ldots < c < \ldots$

$\uparrow$ $\uparrow$

for $k \in \mathbb{N}$????

Are there any cardinal numbers between $\aleph_0$ and c? To say that the answer is "No" is the Continuum Hypothesis (CH) – discussed earlier in these notes. CH is undecidable (starting from the ZFC Axioms for set theory.

There is an important theorem that's very useful for comparing the size of cardinal numbers. We will wrap up these notes by stating the theorem without proof. (*The proof is in the textbook if you care to read it – it's one of the more complicated proofs in the textbook, but you can handle it with some patience and slow reading*.) You are responsible for the statement of the theorem and what it means. We will give a few examples of how it can be used.

Cantor-Schroeder-Bernstein (CSB) Theorem Suppose there exists a one-to-one function $f : A \rightarrow B$ and that there also exists a one-to-one function $g : B \rightarrow A$. Then there must exist a bijection $h : A \rightarrow B$.

Rephrased in terms of cardinal numbers, the CSB Theorem says:

Suppose $m = |A|$ *and* $n = |B|$. *If* $m \leq n$ *and* $n \leq m$, *then* $m = n$

The proof uses the ordered pairs in f *and the ordered pairs in* g *to "assemble" a function* $h : A \rightarrow B$ *that is both one-to-one and onto.*

The CSB Theorem is so useful because it lets us prove that two sets A and B are equivalent by finding two separate one-to-one functions; this is often much easier than trying to find a single function from A to B that is both one-to-one and onto.

Example Suppose $A \subseteq \mathbb{N}$ and that A is infinite. The function $f(a) = a$ is a one-to-one function $f : A \rightarrow \mathbb{N}$. Moreover, we proved earlier that because A is infinite, there must exist a one-to-one function $f : \mathbb{N} \rightarrow A$. By the CSB Theorem, A $\approx \mathbb{N}$. (*We proved this earlier by another method.*)

Here are two more complicated examples.

Example $(0,1) \approx (0,1) \times (0,1) = (0,1)^2$. This might be surprising since one of these sets is "one dimensional" and the other is "two dimensional – yet they have the "same number of elements: $|(0,1)^2| = |(0,1)| = c$.

There are many a "obvious" ways to write a one-to-one function $f : (0,1) \rightarrow (0,1)^2$: for example, $f(x) = (x, \frac{1}{2})$. (f *puts the elements of* $(0,1)$ *into one-to-one correspondence with the "line segment" at height* $\frac{1}{2}$ *inside* $(0,1)^2$. *Of course,* f *is not onto* $(0,1)^2$.)

We now define a one-to-one function $g : (0,1)^2 \rightarrow (0,1)$. This function g has nothing to do with f.

Suppose $(x, y) \in (0,1)^2$. Then $0 < x < 1$ and $0 < y < 1$. Write x and y as decimals (if x or y has two possible decimal expansions, always choose the expansion that ends in a string of zeros: ...$\overline{0}$):

$$x = 0.x_1x_2x_3...x_n... \quad \text{and} \quad y = 0.y_1y_2y_3...y_n...$$

Define a number $z = g(x, y)$ by "interlacing" the digits:

$$z = g(x,y) = 0.x_1y_2x_2y_2x_3y_3...x_ny_n... \quad \in (0,1).$$

For example, $(\frac{1}{2}, \frac{\sqrt{2}}{2}) \in (0{,}1)^2$ *and*
$g(\frac{1}{2}, \frac{\sqrt{2}}{2}) = g(0.5\overline{0}..., \ 0.707106...) = 0.570007010006... \in (0,1).$

g is <u>one-to-one</u>: suppose $(x,y) \neq (x',y') \in (0,1)^2$. Then either $x \neq x'$ or $y \neq y'$. Then either x and x' <u>or</u> y and y' have different decimal expansions. Neither of these decimal expansions ends in an infinite string of 9's, so $g(x,y) = z \neq z' = g(x',y')$ so g is one-to-one.

By the CSB Theorem, there must exist a bijection $h : (0,1) \rightarrow (0,1)^2$, so $(0,1) \approx (0,1)^2$.

Example In the language of cardinal numbers, the last example gives us that

$$c = |(0,1)| = |(0,1) \times (0,1)| = c \cdot c = c^2.$$

Since we proved that multiplication of cardinal numbers is well-defined, we can substitute for $(0,1)$ in this equation any set we know is equivalence to $(0,1)$. For example,

$$c = |(0,1) \times (0,1)| = |\,[0,1) \times (0,1)| = |\mathbb{R} \times \mathbb{R}| = |(0,\infty) \times \mathbb{R}| = |(0,\infty) \times (0,1)| = ...$$

All of the product sets in the equation (since they all have cardinal number c) are equivalent.

Theorem $\{0,1\}^{\mathbb{N}} \approx \mathbb{R}$.

To prove this, we will show that
i) there is a one-to-one function $\phi : \mathbb{R} \rightarrow \{0,1\}^{\mathbb{N}}$ *and that*
ii) there is a one-to-one function $\psi : \{0,1\}^{\mathbb{N}} \rightarrow \mathbb{R}$.
The result then follows using the CSB Theorem.

Before we begin the proof, we need to point out the following elementary fact.

Lemma If $A \approx B$, then $\mathcal{P}(A) \approx \mathcal{P}(B)$.

Proof Suppose $f : A \rightarrow B$ is a bijection. If $C \subseteq A$, then the image set $f[C] \subseteq B$. So we can use f to associate subsets of A to subsets of B.

If C_1 and C_2 are subsets of A and $C_1 \neq C_2$, then one of these sets contains an element not in the other: say $a \in C_1$ but $a \notin C_2$. Then $f(a) \in f[C_1]$ and, <u>because f is one-to-one</u>, $f(a) \notin f[C_2]$. So $f[C_1] \neq f[C_2]$.

If $D \subseteq B$, then $C = f^{-1}[D] \subseteq A$, and <u>because f is onto</u>, $f[C] = f[f^{-1}[D]] = D$. So if $D \subseteq B$, then $D = f[C]$ for some $C \subseteq A$.

Roughly, the preceding just says that we can use f to associate the subsets of A with the subsets of B in a one-to-one correspondence: that is, we can use f define a bijection $\Phi : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$. The next few sentences make this a little more precise.

Define a function Φ: $\mathcal{P}(A) \rightarrow \mathcal{P}(B)$ as follows:

if $C \in \mathcal{P}(A)$, then $\Phi(C) = f[C] \in \mathcal{P}(B)$.

The preceding discussion shows that if $C_1 \neq C_2 \in \mathcal{P}(A)$, then $\Phi(C_1) = f[C_1] \neq f[C_2] = \Phi(C)$, so Φ is one-to-one, and that if $D \in \mathcal{P}(B)$, then $D = \Phi(C)$ where $C = f^{-1}[D] \in \mathcal{P}(A)$. So Φ is a bijection. •

Now we carry out the plan in a proof of the Theorem.

Proof

i) By the Lemma, we know that $\mathcal{P}(\mathbb{Q}) \approx \mathcal{P}(\mathbb{N})$, and we proved earlier that $\mathcal{P}(\mathbb{N})) \approx \{0,1\}^{\mathbb{N}}$. Putting these equivalences together, we know that there is a bijection $h : \mathcal{P}(\mathbb{Q}) \to \{0,1\}^{\mathbb{N}}$. Now define a function k as follows:

$$\text{for } r \in \mathbb{R},\ k(r) = \{q \in \mathbb{Q} : q < r\}$$

For each r, $k(r)$ is a subset of $\mathbb{Q}$, so $k(r) \in \mathcal{P}(\mathbb{Q})$. In other words, $k : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$. This function k is one-to-one:

If $r \neq s \in \mathbb{R}$, then one is smaller than the other: say $r < s$. Choose a rational number q^* between r and s : $r < q^* < s$. Then $q^* \in k(s)$ (*Why? What is* $k(s)$*?*) but $q^* \notin k(r)$, so $k(r) \neq k(s)$.

Composing, we get that the function $\phi = h \circ k : \mathbb{R} \to \{0,1\}^{\mathbb{N}}$ is one-to-one.

ii) Suppose $f \in \{0,1\}^{\mathbb{N}}$. Such an f is a binary sequence :

$$f(1) = a_1, f(2) = a_2, ..., f(n) = a_n, ... \quad \text{where each } a_n = 0 \text{ or } 1.$$

Define a real number using the a_n's to create a decimal:

$$\psi(f) = 0.a_1 a_2 ... a_n ... \quad \in \mathbb{R}$$

so that $\psi : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$.

Note: although all the digits $a_1, a_2, ...$ *in* $\psi(f)$*are either* 0 *or* 1*, we are thinking of* $\psi(f)$ *as an "ordinary" base ten decimal, not as a base two "binary expansion."*

ψ is one-to-one:

if $g \in \{0,1\}^{\mathbb{N}}$, then g is a binary sequence:

$$g(1) = b_1,\ g(2) = b_2,\ ...,\ g(n) = b_n,\ ... ,$$

where each $b_n = 0$ or 1 and at least one b_n.

Suppose $g \neq f$. Then $a_n \neq b_n$ for at least one value of n, so $\psi(g) = 0.b_1 b_2 ... b_n ...$ is a different decimal than $\psi(f) = 0.a_1a_2...a_n...$, and these two decimals cannot both represent the same real number (since neither ends in an infinite string of 9's). In other words, the real number $\psi(g) \neq$ the real number $\psi(f)$. This means that ψ is one-to-one.

By the CSB Theorem, $\{0,1\}^{\mathbb{N}} \approx \mathbb{R}$. •

Example In the language of cardinal numbers, the equivalence $\{0,1\}^{\mathbb{N}} \approx \mathbb{R}$ tells us that $|\{0,1\}^{\mathbb{N}}| \approx |\mathbb{R}| = c$. And because $|\{0,1\}^{\mathbb{N}}|$ is the definition for the cardinal exponentiation $2^{\aleph_0}$, we conclude that $2^{\aleph_0} = c$.

The sequence of cardinal numbers therefore begins:

$$\begin{array}{cccccc} 0 < 1 < 2 < \ldots < & k & < \ldots < \aleph_0 < & \ldots & < & 2^{\aleph_0} < \\ & \uparrow & & \uparrow & & || \\ & \text{for } k \in \mathbb{N} & & ??? & & c \end{array}$$

As we commented earlier, the " ??? " is asking: are there any cardinal numbers between $\aleph_0$ and $2^{\aleph_0}$. The statement that the answer is "no" is called the Continuum Hypothesis (CH) $-$ and CH is "undecidable" from the axioms (ZFC) for set theory.

Of course, there is no "largest" infinite cardinal: larger and larger infinite cardinals in the sequence above turn out to be 2^c, $2^{(2^c)}$, $2^{2^{(2^c)}}$, etc. Given any infinite cardinal m, 2^m is larger still. The reason is that if $|A| = m$, then the definition for 2^m is $|\{0,1\}^A|$, the number of functions with domain A and codomain $\{0,1\}$. And we can prove that $\{0,1\}^A \approx \mathcal{P}(A) \not\approx A$.