The ARITHMETIC of the INFINITE

$$\lim_{x \to 8} \left(\frac{1}{x-8} \right) = \infty$$

$$\lim_{x \to 2} \left(\frac{1}{x-2} \right) = \infty$$

Infinity has perplexed some of the greatest thinkers –

- Aristotle & Zeno
- Galileo
- Newton & Bishop Berkeley
- Gauss

But Georg Cantor discovered a new perspective ...

* "Completed infinities" were legitimate objects.
* Some infinite objects were bigger, in a sense to be made explicit momentarily, than others.

Sets can be compared with one another by investigating mappings among them.

* BIJECTION – ultimate yardstick

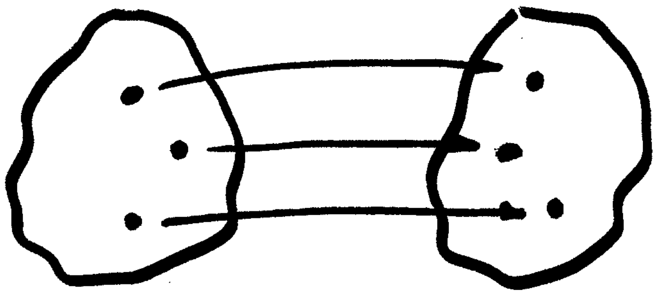
→ Two sets have the same size if there is a bijection between them

- If we had a collection of sets of various standard sizes, we could classify a given set by mapping it to the standard ones... sort of like weighing on a balance

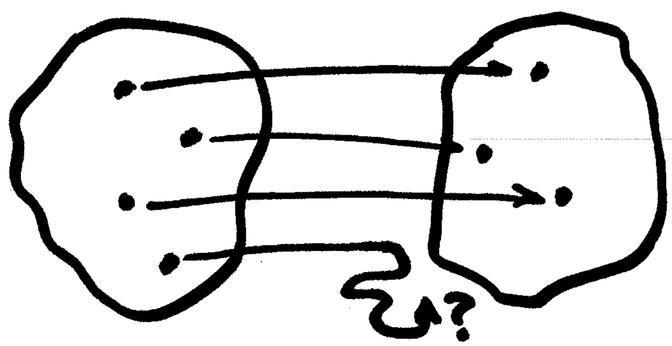
- Given the set S, let's denote its size by $|S|$

- Given sets A & B, if we can find a bijection $\phi : A \to B$, we say $|A| = |B|$, or that A & B are equipollent, or that they have the same cardinality.
- If $\psi : A \to B$ is a surjection, then A has at least enough elements to "cover" all elements in B, and we write $|A| \geq |B|$
- If $\varsigma : A \to B$ is an injection, then B has at least enough seats for all the elements in A, and we write $|A| \leq |B|$

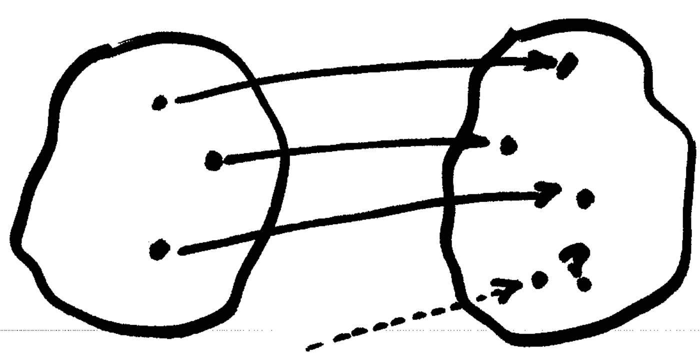
For finite sets this is easy to see:



$|A| = |B|$



$|A| \geq |B|$



$|A| \leq |B|$

* Wait a minute ... what is a

FINITE SET ?

- A finite set is one that may not be mapped bijectively to a proper subset of it (ϕ is finite).

- So an infinite set can be mapped bijectively to a proper subset of it. (This is Richard Dedekind's def^n)

* Does every infinite set have the same cardinality ?

* NO! This was Cantor's epiphany.

- Cantor showed the following: Suppose S is an infinite set and 2^S is its <u>powerset</u>, or family of all subsets. If $|S| = |2^S|$, then there must be a bijection $\phi : S \to 2^S$.
- OK, let's say $s \in S$ is "good" if $s \in \phi(s)$, the subset it gets mapped to. Then s is "evil" if $s \notin \phi(s)$.
- Look at $E = \{s \in S : s \text{ is "evil"}\}$. Since ϕ is assumed to be onto, $\phi^{-1}(E)$ is some element $e \in S$.

- Now either e is good or evil.
If it's good, then $e \in \phi(e) = E$.
But wait.... then it's evil.
OK, if it's evil, then $e \notin E$....
oops, then it must be good.
Evidently there is no way to assign virtue or lack thereof to e.
- The way out is to realize ϕ cannot be surjective. You can see that $s \mapsto \{s\}$ is an injective map from S to 2^S, though, so we conclude

$$|S| < |2^S|.$$

* So where are we?

Given $\phi : A \to B$

- ϕ bijective $\Rightarrow |A| = |B|$
- ϕ injective $\Rightarrow |A| \leq |B|$
- ϕ surjective $\Rightarrow |A| \geq |B|$

and if there is <u>no</u> bijection,

- ϕ injective $\Rightarrow |A| < |B|$
- ϕ surjective $\Rightarrow |A| > |B|$

* For finite sets, the symbols "$\leq, <, \geq, >$" correspond to the usual order symbols for the natural numbers.

- Do we have the right to assume they work the same for infinite sets?
- Not yet.
- For example, if $|A| \leq |B|$ <u>and</u> $|A| \geq |B|$, does that force

$$|A| = |B| \quad ?$$

- Not at all obvious. In fact, it is a major theorem which we will explore in a moment.
- Can we show that "$\leq$" is a partial order on set sizes.... that is to say cardinalities ?

- Well, the identity map $i : A \to A$ is certainly an injection, so $|A| \leq |A|$ and we have reflexivity.
- The composition of injections

  $\phi : A \to B$ and $\psi : B \to C$

  gives $(\psi\phi) : A \to C$, another injection, so if $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$, and we have transitivity.
- At this juncture we can say "$\leq$" defines a <u>preorder</u>. We would like to establish antisymmetry to show that "$\leq$" is a partial order.

  $\longrightarrow$ $|A| \leq |B| \leq |A| \Rightarrow |A| = |B|$

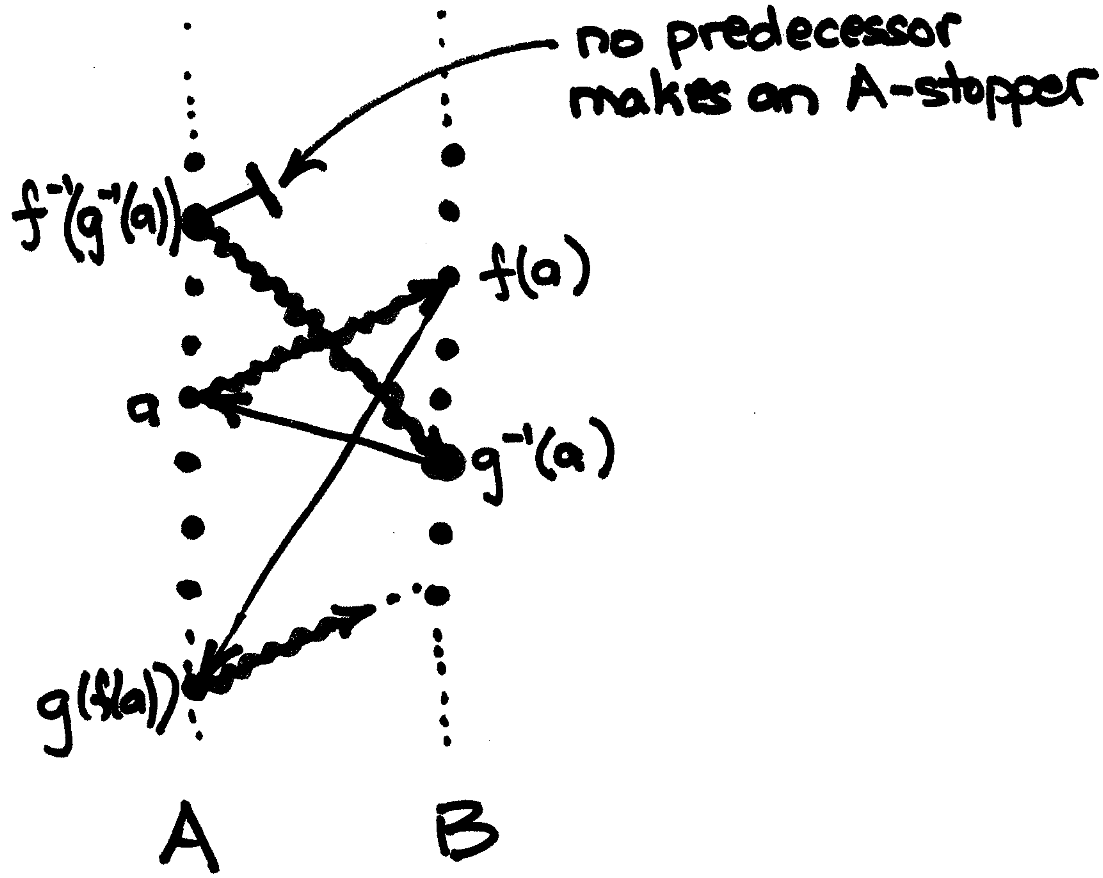
★ Cantor - Schröder - Bernstein Th^{m} (König - 1906)

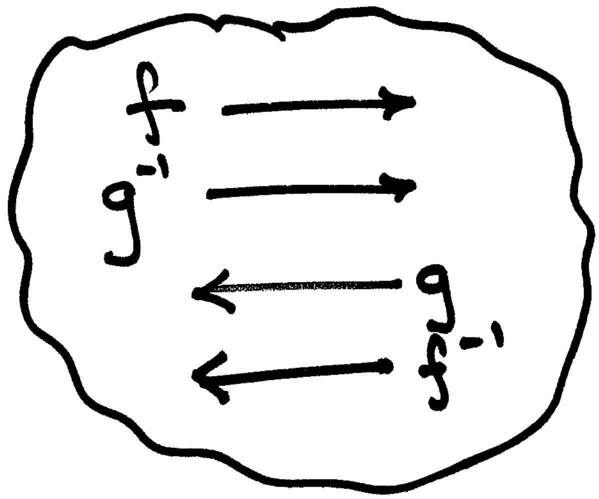
Suppose $|A| \le |B|$ & $|B| \le |A|$, then $|A| = |B|$

You can assume $A \cap B = \emptyset$. If not, form $A' = A \times \{0\}$ and $B' = B \times \{1\}$. There are obvious bijections from A to A' and B to B', and then we can just do the proof in terms of A' and B', if necessary. This is a cute trick to remember for other contexts.

Now we draw an infinite ladder....

König's Ladder





FUN WITH MAPPINGS

stops on element in A, for example

$$\Big|\cdot f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f\cdots g\cdots} \cdots$$

- We form sequences by successive applications of f & g to move right, and g^{-1} & f^{-1} to move left. This assumes starting on some $a \in A$. If we start on some $b \in B$, just interchange f & g.
- To the right, the sequences just keep going, or they loop back in a cycle.
- To the left, the sequences can keep going, loop back, or terminate because no pre-image is available. Recall f & g are injective, not necessarily surjective, so forward is OK but backward is not assured.

- If a sequence terminates in A, call it an A-stopper, and likewise if it terminates in B, call it a B-stopper.
- Note that the collection of sequences partitions $A \cup B$. No two sequences can just partially intersect, since once they have a point in common, the prescribed construction just scrolls thru the entire sequence, so they would be the same.
- Within each sequence, we can define an induced bijection between its A-elements and B-elements.

- For a cyclic sequence, restrict f to A or g to B ... either works.
- For a sequence that runs off indefinitely right and left, do the same.
- For an A-stopper, use the restriction of f.
- For a B-stopper, use the restriction of g.

* Union up these function elements to create the bijection $\phi : A \to B$. Hence $|A| = |B|$, and we are done.

- Now we have "$\leq$" established as a partial order on sets. Can we say "all sets"? That is dangerous.
- Let S be the set of all sets, and define N as the set of all sets <u>not</u> members of themselves. Certainly $N \subset S$, and either $N \in N$ or $N \notin N$. If $N \in N$, then by construction, $N \notin N$ $\rightarrow\leftarrow$. If $N \notin N$, then $N \in N$ $\rightarrow\leftarrow$. We are stuck. Apparently we cannot allow S to be so capacious that something self-contradictory like N can be formed within it.

- This difficulty is caused by self-reference. You can create the same effect purely with words. Call a word "homologous" if it describes itself... like "short". Call it "heterologous" if it does not... like "double-syllabled". What, then, is heterologous? If it is not self-descriptive, then it is, and vice versa.
- The technical device to sidestep this issue in mathematics is to define a class as a collection of sets which share a common property.

- All sets are classes, but some classes, called <u>proper</u>, are not sets. The set of all sets, and the set of all sets not members of themselves, are examples of proper classes. Sets are sometimes called <u>small classes</u>.
- Since most of the structural definitions we have involve sets with some common properties, we have to be careful not to say things like "the set of all rings" and so forth. The class of all rings, Rng, is just fine.

★ It would be nice to have a standard set for each cardinality.

- Consider the following scheme:

  1) $\emptyset$ is an ordinal number

  2) If α is an ordinal number, then so is $\alpha \cup \{\alpha\}$

  3) If S is a set of ordinal numbers, then $\sup S$ is, too

     $$\left(\sup S = \bigcup_{\alpha \in S} \alpha\right)$$

- So the first few are:

$$\emptyset,\ \{\emptyset\},\ \{\emptyset, \{\emptyset\}\},\ \ldots$$

- To preserve our sanity, we set

$$\emptyset = \text{"0"},\ \{\emptyset\} = \text{"1"},\ \text{etc.}$$

- Ordinal numbers represent the order types for all the well-ordered sets. They form the class Ord.
- The preceding construction gives us canonical representatives of each order type.
- Using the 3rd property, we can create infinite ordinals:

$$\omega = \bigcup \alpha \ , \quad \alpha \text{ finite}$$

$$\omega_1 \ (= \Omega) = \bigcup \alpha , \quad \alpha \text{ countable}$$

- Given any ordinal, there is always one just above it, its successor.

- If an ordinal is the immediate successor of another, it is called *regular*.

- Some ordinals are not immediate successors, like ω and ω_1. They are *limit* ordinals.

* Now suppose S is any set.

S may be mapped injectively into at least one ordinal number.

This is assured by the Axiom of Chace.

The ordinals themselves are well-ordered by inclusion.

Define the *cardinal number*

of S to be the least ordinal number into which it can be mapped injectively.

- So a set with 3 elements can be mapped injectively into the ordinals 3, 4, ..., but not 2. So the cardinality of the set is 3, to no one's surprise.

- $\mathbb{N}$ can be mapped injectively into any ordinal equal to or exceeding ω. So $|\mathbb{N}| = \omega$. We usually use a different symbol for cardinal and ordinal numbers once we hit ω. So as a cardinality,

$$\omega = \aleph_0$$

- $\mathbb{R}$ can be mapped into ordinals at least as big as ω_1, so

$$|\mathbb{R}| = \omega_1$$

- If I write $\omega_1 = \aleph_1$, I am accepting the Continuum Hypothesis. This states that there is no distinct cardinal number between $|\mathbb{N}|$ and $|\mathbb{R}|$, or ω and ω_1

So the very next aleph must correspond to $|\mathbb{R}|$.

* So now that we have cardinal numbers, how do they work ARITHMETICALLY?

- If α & β are cardinals, we define $\alpha+\beta$ as the cardinality of $A \cup B$, where $|A| = \alpha$, $|B| = \beta$.

* Cardinal addition is associative and commutative.

- Define $\alpha \cdot \beta$ as the cardinality of $A \times B$.

* Cardinal multiplication is associative, commutative, and distributes over cardinal addition.

★ Given cardinals α, β, γ:

1) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$

2) $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$

• Define $\alpha^{\beta} = |\{f : B \to A\}|$

★ Given cardinals α, β, γ:

1) $(\alpha \cdot \beta)^{\gamma} = \alpha^{\gamma} \cdot \beta^{\gamma}$

2) $\alpha^{\beta} \cdot \alpha^{\gamma} = \alpha^{\beta + \gamma}$

3) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$

★ If $\alpha \leq \beta$

1) $\alpha^{\gamma} \leq \beta^{\gamma}$

2) $\gamma^{\alpha} \leq \gamma^{\beta}$

* For all $n \in \mathbb{N}$:

1) $(\lambda'_0)^n = \lambda'_0$

2) $n \cdot \lambda'_0 = \lambda'_0$

* If $\alpha \geq \beta$ then:

$$\lambda'_\alpha + \lambda'_\beta = \lambda'_\alpha$$

$$\lambda'_\alpha \cdot \lambda'_\beta = \lambda'_\alpha$$

- Note:

$$\lambda'_0 + 1 = \lambda'_0 = \lambda'_0 + \lambda'_0$$

and $\lambda'_0 \cdot 1 = \lambda'_0 = \lambda'_0 \cdot \lambda'_0$

but $\lambda'_0 \neq 1$!!