MAU11602

Lecture 26

2026-03-26

Power sets again

There is a natural injective function from A to $\mathcal{P}A$ for any set A, defined by $i(x) = \{x\}$.

Failure to distinguish properly between x and $\{x\}$ caused much confusion in mathematics in the 19th century and in other subjects, particularly computer science, in the 20th, and maybe still now.

For no set A is this i surjective. $\varnothing \in \mathcal{P}(A)$ but there is no $x \in A$ such that $\varnothing = i(x) = \{x\}$, not even $x = \varnothing$ if $\varnothing$ happens to be a member of A.

Indeed $\varnothing \neq \{\varnothing\}$ is just $0 \neq 1$ if you define natural numbers by the von Neumann representation.

Could there be some other function from A to $\mathcal{P}A$ which is surjective?

Cantor

Could there be some other function from A to $\mathcal{P}A$ which is surjective?
Suppose g is such a function and define
$C = \{x \in A \colon \exists D \in \mathcal{P}A. D = g(x) \wedge (\neg x \in D)\}$.
Then $C \in \mathcal{P}A$. g was assumed to be surjective so there must be a $y \in A$ such that $C = g(y)$.
If $y \in C$ then, by the definition of C, there is a $D \in \mathcal{P}A$ such that $D = g(y)$ and $\neg y \in C$. But then $C = g(y) = D$ so $\neg y \in C$.
On the other hand, if $\neg y \in C$ then there exists a $D \in \mathcal{P}A$ such that $D = g(y)$ and $\neg y \in D$, namely $D = C$. But then y satisfies the condition required to be a member of C, so $y \in C$.
So y is a member of C if and only if it isn't.
Of course we got y by assuming the existence of a surjective function g, so there can be no such g.
There is no surjective function form A to $\mathcal{P}A$, so there's certainly no bijective function, since every bijective function is surjective.

More Cantor

There's also no bijective function from $\mathcal{P}A$ to A, since every bijective function has an inverse, which is also bijective.

Is there an injective function from $\mathcal{P}A$ to A?

No. The Schröder-Bernstein theorem says that if there are injective functions from A to B and from B to A then there's a bijective function from A to B.

There are elementary proof of Schröder-Bernstein but I won't prove it.

Alternatively, we can say A is empty or it isn't. In the former case there is no injective function from $\mathcal{P}A$ to A because there is no function from a non-empty set to an empty set. In the latter case choose an $z \in A$ and define a function g from A to $\mathcal{P}A$ as follows. Letting f be our supposed injective function from $\mathcal{P}A$ to A, define $g(y) = x$ if $f(x) = y$ and $g(x) = z$ if there is no x such that $f(x) = y$.

g is well defined because if there's an x such that $f(x) = y$ then there's only one.

g is surjective because if $x \in \mathcal{P}A$ then $x = g(f(x))$.

But we already know there's no surjective function from A to $\mathcal{P}A$, so f can't exist.

Infinity

We still don't have any infinite sets.

What about the natural numbers?

I defined natural numbers. More precisely I gave necessary and sufficient conditions for something to be a natural number.

I described how to find the successor of a natural number, the sum of two natural numbers, or the product of two natural numbers

I never claimed the natural numbers form a set!

The necessary and sufficient conditions can be used to find a Boolean expression satisfied by the natural numbers and only by the natural numbers, but we can only use Boolean expressions to find subsets, and we don't have a set which we know contains all the natural numbers.

With our current axioms we have no way to prove the existence of any such set.

If there is a set N of natural numbers though then it must be infinite though, because we can use Separation to define a subset of $N \times N$ consisting of those B with $B = A \cup \{A\}$ and check that this is an injective functional relation which is not surjective.

More infinity

To get infinite sets, including a set of natural numbers, we need a further axiom.
One option is an axiom saying there is an infinite set. Another option is an axiom saying that some particular infinite set exists, like the set of natural numbers.
Some older treatments of set theory use the first option but most now choose the second option, where the Axiom of Infinity just says that there is a set whose members are the natural numbers, as defined earlier.
That's what we'll do.

Countability

We say that a set A is *countable* if there is an injective function from A to N.
We say that a set is *uncountable* if it is not countable.
With this definition all finite sets are countable.
To see this, first note that every natural number is not just a member of N but also a subset of N, specifically the subset consisting of all natural numbers smaller than it.
So there is an injective function from any natural number to N, namely the inclusion function.
If F is finite then there's a bijective from F to some natural number, and composing this with the inclusion function gives an injective function from F to N.
Unfortunately many people use the word countable to mean countable and infinite.
Those people still use uncountable to mean uncountable, so for them finite sets are neither countable nor uncountable!
The terms finite and uncountable mean the same thing for everyone, but countable has different meanings for different people and you should probably say "countable or finite" when you mean countable by our definition and "countably infinite" when you mean countable by the other definition.

Uncountable sets

Are there uncountable sets? Yes, by Cantor's theorem the power set of N is uncountable.

More generally, the power set of any countably infinite set is uncountable.

The most important uncountable set is the set of real numbers.

I haven't formally defined the set R of real numbers, and won't, but hopefully you believe that for any $A \in \mathcal{P}N$

$$3 \sum_{j \in A} 10^{-j} + 7 \sum_{j \in N \setminus A} 10^{-j}$$

is a real number and that for any real number there is at most one $A \in \mathcal{P}N$ which works.

Therefore the sum above defines an injective function from $\mathcal{P}N$ to R.

If there were an injective function from R to N then I could compose it with this function to get an injective function from $\mathcal{P}N$ to N.

There is no such function, so R is uncountable.

Any other pair of digits would have worked in place of 3 and 7, except maybe 0 and 9.