MAU11602
Lecture 27
2026-04-01

Induction and smallest natural numbers

Which sets of natural numbers have a smallest member?
Suppose A is a subset of the natural numbers and that A has no smallest member. For which m is

$$\forall n. n \in A \rightarrow m < n?$$

0 is not a member of A because it were it would have to be the smallest member, and $0 < n$ for all non-zero n so 0 satisfies the condition above.
Suppose that there is some m for which m satisfies the condition but $m+1$ does not, i.e. such that all $n \in A$ have $n > m$ but some $n \in A$ has $n \leq m+1$.
The only possibility is $n = m+1$, so $m+1 \in A$ but $n > m$ for all $n \in A$ and hence $n \geq m+1$ for all $n \in A$, so $m+1$ is a smallest member of A, contrary to our assumptions.
So $0 \notin A$ and if $m \notin A$ then $m+1 \notin A$. By induction $n \notin A$ for all natural numbers A.
So if A has no smallest member then it is empty. Equivalently, if A is non-empty then it has a smallest member.

Induction and smallest natural numbers, continued

The principle of mathematical induction implies that every non-empty set of natural numbers has a smallest member.

We can reverse this. If every non-empty set has a smallest member then any property which holds for 0 and holds for $m + 1$ whenever it holds for m must hold for all natural numbers.

We prove this by defining A to be the set of counter-examples.

0 can't be a smallest member of A because it isn't a member of A. $m + 1$ can't be a member of A because then m would not be a member while $m + 1$ is, so m would have the property while $m + 1$ doesn't.

Every natural number is 0 or $m + 1$ for some m so there is no least member and therefore A is empty and there are no counter-examples.

Note the similarity to recursive functions and structural induction.

Which is an axiom and which is a theorem, the principle of mathematical induction or the fact that every non-empty set of natural numbers has a smallest member?

In set theory both are theorems, consequences of set induction, which is also a theorem.

Countable sets

Last time I defined sets to be countable if there is an injective function from the set to the set of natural numbers.

I also mentioned that about half the mathematical community also requires countable sets to be infinite, but I don't.

The set of natural numbers itself is countable, since the identity function is injective.

Suppose f is an injective function from a set A to a set B and B is countable. Then A is countable.

This is true since the composition of injective functions is injective.

As a consequence, subsets of countable sets are countable, since inclusion is injective.

In particular all subsets of the natural numbers are countable.

As another consequence, if there's a bijective function from A to B then A is countable if and only if B is countable.

Also, if A is countable then $A \cap B$ and $A \setminus B$ are countable, no matter what B is, since they're subsets of A.

With the other definition you'd need to change some or all of these to "countable or finite".

Right and left inverses

If f is a function from a set A to a set B then we say that a function g from B to A is a left inverse to f if $g \circ f$ is the identity function on A and is called a right inverse if $f \circ g$ is the identity on B.
If f has a left inverse then it must be injective because $f(x) = f(y)$ implies $g(f(x)) = g(f(y))$ which is just $x = y$.
If f has a right inverse then it must be surjective because for every $y \in B$ there is an $x \in A$ such that $f(y) = x$, namely $y = g(x)$.
If f is an injective function from a non-empty set A to a set B then it has a left inverse. Non-empty means there is some $x \in A$. Injective means that for any $y \in B$ there is at most one $w \in A$ such that $f(w) = y$. We define $g(y) = w$ if there is such a w and $g(y) = x$ if there isn't. Then $g(f(w)) = w$ for all $w \in A$ so g is a left inverse.
Of course if A is empty there can't be a left inverse unless B is also empty.

Right and left inverses, continued

If f is a surjective function from A to B does it necessarily have a right inverse?
Yes, if B is finite. We can prove this by set induction.
Let C be the set of subsets D of B such that there is a function g from D to A such that $f(g(y)) = y$ for all $y \in D$. Then $\varnothing \in C$ and if $D \in C$ and $y \in B$ then we can extend the corresponding our g from D to $D \cup \{y\}$ if y isn't already in D by choosing $g(y) = x$ for some x with $f(x) = y$. By set induction then $B \in C$ and the corresponding g is a right inverse to f.
Also yes, if A the set of natural numbers.
If $y \in B$ then the set of x such that $f(x) = y$ is non-empty, because f is surjective, so it has a least member. Let $g(y) = x$ where x is this least member. Then $f(g(y)) = f(x) = y$ so g is a right inverse.
It's not hard to extend this to the case where A is countable.
Anything beyond these results requires more axioms.

Countability and surjective functions.

If there is a surjective function f from the set N of natural numbers to a set A then A is countable.
This follows immediately from what we just proved and the definition of countability.
Also, if A is non-empty and countable then there is a surjective function from N to A.
That follows from what we proved earlier, since countability means there's an injective funtion from A to N and this function has a left inverse. It is the right inverse of that left inverse and so is surjective.
A common way to prove sets are countable is to combine the results above and find a surjective function to that set from a subset of countable set.
Or, equivalently, if A is countable and R is a relation between A and B which is right unique and right total then B is countable.

More countable sets

The set of (finite) lists of natural numbers is countable.
To see this, we define an injective function as follows.
Take a list and write the individual natural numbers in modified base 2. For example $2, 3, 5, 7, 11$ becomes $2, 11, 21, 111, 211$.
Replace the commas separating the list elements with 3's, so the list above becomes 231132131113211.
That list is the modified base three representation of some natural number. Find it.
In this case it's the representation of 15288286, so our combined function takes the list $2, 3, 5, 7, 11$ to the natural number 15288286.
This function is actually bijective. We can invert it by reversing the steps, i.e. write a natural number in modified base 3, change the 3's to commas and view the result as a list of modified base 2 numbers, and find those numbers.
For example 18 has the modified base 3 representation 123, which corresponds to the list 12, in modified base 2 and $4, 0$ in ordinary decimal representation.
If A is any countable set then lists of members of A form a countable set.

Still more countable sets

The set of lists of natural numbers is countable.
So any subset of the set of lists of natural numbers is countable.
So if there is a surjective function from a subset of the set of lists of natural numbers to a set then that set is countable.
Consider the lists of natural numbers of length 3 where the last element is not zero, e.g. $0, 17, 42$.
To each such list i, j, k we associate the natural number $(i - j)/k$. So the rational number is $-17/42$ is associated to the list $0, 17, 42$.
Every rational number can be represented in this way, so the function taking i, j, k to $(i - j)/k$ is surjective.
Therefore the set of rational numbers is countable.
The representation is not unique, but it doesn't have to be.
We already saw that the set of real numbers is uncountable and every rational number is a real number, so there must be a real number which is irrational.
Of course it's not hard to find individual real numbers which are irrational, like $\sqrt{2}$, but the argument above is very adaptable.

Constructing the rationals

As with the reals, I didn't define the rationals, I just assumed they exist and have the expected properties and then checked whether the set they form is countable or not.
We can turn the preceding slide into a definition of the set of rational numbers though. I will do this wrong first.
Let's say that rational numbers *are* lists of three natural numbers with the last one being non-zero.
We define arithmetic operations on them in a way consistent with interpreting (i, j, k) as $(i - j)/k$, e.g.

$$\frac{i_1 - j_1}{k_1} + \frac{i_2 - j_2}{k_2} = \frac{i_1 \cdot k_2 - j_1 \cdot k_2}{k_1 \cdot k_2} + \frac{k_1 \cdot i_2 - k_2 \cdot j_2}{k_1 \cdot k_2} = \frac{(i_1 \cdot k_2 + k_1 \cdot i_2) - (j_1 \cdot k_2 + k_1 \cdot j_2)}{k_1 \cdot k_2}$$

so we define the sum of (i_1, j_1, k_1) and (i_2, j_2, k_2) to be
$(i_1 \cdot k_2 + k_1 \cdot i_2, j_1 \cdot k_2 + k_1 \cdot j_2, k_1 \cdot k_2)$.
This is clearly commutative, and you can check that it's associative.