On the foundations of mathematics

Uli Krähmer

University of Glasgow

Glasgow 5.11.2011

The natural numbers

- The starting point of all mathematics is counting, one of our fundamental intellectual abilities that leads to the definition of the **natural numbers**

$$1, 2, 3, 4, 5, \ldots$$

- We denote the set of all these numbers by the symbol $\mathbb{N}$,

$$\mathbb{N} := \{1, 2, 3, 4, 5, \ldots\}$$

Here $:=$ is the symbol we will use when defining something, and the curly brackets $\{\}$ are used to denote sets.

Infinity

- The set $\mathbb{N}$ of natural numbers is **infinite**.
- Here is a 3000 year old attempt to define what that means:

Definition (Yajurveda)

If you remove a part from infinity or add a part to infinity, still what remains is infinity.

- We will instead now first define what we mean by a **finite set** and then all sets that are not finite will simply be called infinite.

Functions

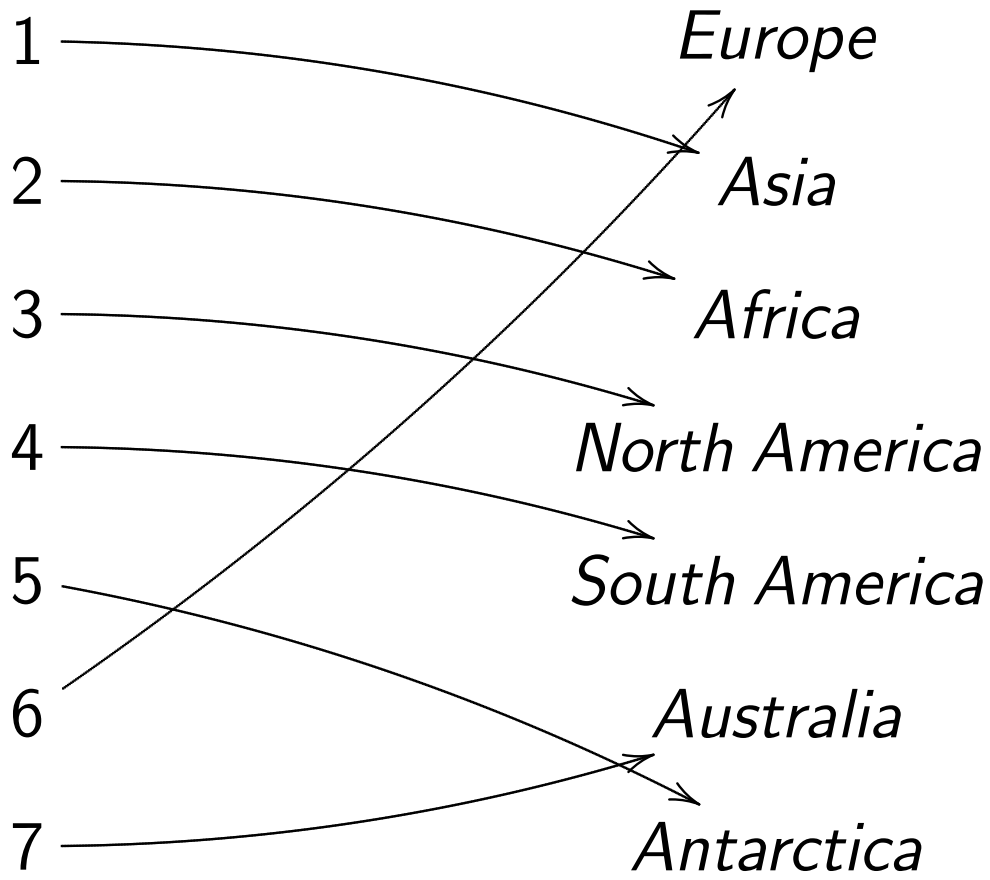
- What does it mean to count the elements in a set?
- We could say it means to build a machine in which you input a number between 1 and n (where n stands for the number of elements in the set), and the machine outputs the corresponding element of the set.
- More generally and abstractly, we call such a machine that takes inputs from some set and produces by some fixed rule an output that is an element of a possibly different set a **function**.
- The sentence "f is a function that maps elements of a set X to elements of a set Y" is abbreviated

$$f : X \to Y,$$

and we write $f(x)$ for the output assigned to an input x.

A picture of a function $f : X \to Y$

- Here $X = \{1, 2, 3, 4, 5, 6, 7\}$ and Y is the set of all continents.



- Thus we have for example $f(6) = \textit{Europe}$.

Bijectivity

- When counting the elements of a set, each element therein is of course counted exactly once.
- More abstractly, we define:

Definition

A function $f : X \to Y$ is **bijective** *if for each element y of Y there exists a unique element x of X with $f(x) = y$.*

- Equivalently, $f : X \to Y$ is bijective it there is an **inverse function** $g : Y \to X$ which maps an element y in Y to the unique x in X such that $f(x) = y$, that is, one for which we have

$$f(g(y)) = y, \quad g(f(x)) = x$$

for all elements x of X and all elements y of Y.

Finite and infinite sets

- Now we use our new language to formally define:

Definition

A set X is said to **have** *n* **elements** *if there exists a bijective function*

$$f : \{1, 2, 3, \ldots, n\} \to X.$$

A nonempty set X for which there is no natural number n such that X has n elements is called **infinite**.

- The next one is more subtle than you might think:

Definition

One says a set X has **as many elements as** *a set Y (or that they have the same* **cardinality***) if there is a bijective function $f : X \to Y$.*

This makes sense for infinite sets as well!

Rational numbers

- Consider the set $\mathbb{Q}_+$ of numbers that can be written as fractions of two natural numbers,

$$\mathbb{Q}_+ := \left\{ \frac{m}{n} \mid m, n \text{ are natural numbers} \right\}.$$

  This notation means take all those things left of the bar $\mid$ which are formed using the rules right of the bar.
- We will now prove something that might come as a surprise:

Theorem

The set $\mathbb{Q}_+$ is **countable**, *that is, has as many elements as $\mathbb{N}$.*

Prime factorisation

- Every natural number m has a factorisation into powers of pairwise different prime numbers $p_1, \ldots, p_r$:

$$m = p_1^{i_1} \times p_2^{i_2} \times \cdots \times p_r^{i_r}.$$

  This is unique up to reordering the primes.

- Some examples:

$$24 = 8 \times 3 = 2^3 \times 3,$$

$$180 = 5 \times 36 = 5 \times 4 \times 9 = 2^2 \times 3^2 \times 5,$$

$$289835 = 5 \times 7^3 \times 13^2.$$

Prime factorisation and fractions

- Given a fraction
$$\frac{m}{n},$$
we can write both m, n in their prime factorisations,
$$\frac{m}{n} = \frac{p_1^{i_1} \times \cdots \times p_r^{i_r}}{q_1^{j_1} \times \cdots \times q_s^{j_s}}.$$

- Note we may assume that none of the primes occurring in the enumerator occurs in the denominator. For if some prime occurs in both, we can cancel the fraction until the common prime has disappeared from either enumerator or denominator.
- Example:
$$\frac{8}{42} = \frac{4}{21} = \frac{2^2}{3 \times 7}.$$

The bijective function

- Now consider the function

$$f : \mathbb{Q}_+ \to \mathbb{N}$$

that maps $\frac{m}{n}$ expressed as on the previous slide to

$$f\left(\frac{m}{n}\right) := p_1^{2\times i_1} \times \cdots \times p_r^{2\times i_r} \times q_1^{2\times j_1 - 1} \times \cdots \times q_s^{2\times j_s - 1}.$$

We will prove this function is bijective by writing down the inverse function.

- But first two examples:

$$f\left(\frac{2}{3}\right) = 2^2 \times 3^1 = 4 \times 3 = 12,$$

$$f\left(\frac{22}{49}\right) = 2^2 \times 11^2 \times 7^3 = 4 \times 121 \times 343 = 166012.$$

The inverse function

- Write any natural number n as

$$n = p_1^{2\times i_1} \times \cdots \times p_r^{2\times i_r} \times q_1^{2\times j_1 - 1} \times \cdots \times q_s^{2\times j_s - 1}$$

with the p_i's and q_j's mutually different primes. This is just the prime factorisation of n, ordered in such a way that we first list those primes that occur with an even exponent.

- Now the inverse function $g : \mathbb{N} \to \mathbb{Q}_+$ of f is given by

$$g(n) := \frac{p_1^{i_1} \times \cdots \times p_r^{i_r}}{q_1^{j_1} \times \cdots \times q_s^{j_s}}$$

- Example:

$$n = 180 = 5 \times 36 = 5 \times 4 \times 9 = 2^2 \times 3^2 \times 5,$$

$$g(180) = \frac{2^1 \times 3^1}{5} = \frac{2 \times 3}{5} = \frac{6}{5}.$$

Exercises

- Which of the following functions are bijective?
  1. The function $q : \mathbb{N} \to \mathbb{N}$ that maps a number n to $n^2 = n \times n$.
  2. The function $p : P \to T$, where P is the set of all current Scottish Premier League players and T is the set of all current teams, and p assigns to a player his team.
  3. The function $s : \mathbb{Q}_+ \to \mathbb{Q}_+$ that divides every fraction by 17.
- For f, g from the lecture, compute $g(n)$ for as many $n = 1, 2, 3, \ldots$ as you wish (maybe up to 10 or 20), and then $g(100)$ and $f\left(\frac{44}{15}\right)$.
- Prove that the set of all **integers** $\mathbb{Z}$ (natural numbers decorated with a sign $\pm$) is countable. Is the set of natural numbers greater or equal to 5 countable?

The reals

- The **real numbers** $\mathbb{R}$ are those that can be written using decimal expansion as e.g. in

$$\pi = 3.14159265358979323846264338327950288419 7...$$

- I claim the following:

Theorem

$\mathbb{R}$ *is* **uncountable**, *i.e. its cardinality is not equal to that of* $\mathbb{N}$.

So $\mathbb{R}$ is more infinite than $\mathbb{N}$!

The proof - I

- Assume there is a bijective function $f : \mathbb{N} \to \mathbb{R}$ that counts all the real numbers,

$$f(1), f(2), f(3), ...$$

- Now we define a real number x as follows: x is of the form

$$0.x_1x_2x_3...$$

where we choose the n-th digit x_n different from the n-th digit after the decimal dot in $f(n)$, but not equal to 9. For example, if

$$\begin{aligned} f(1) &= 3.14159... \\ f(2) &= 2.71828... \\ f(3) &= 11.23456, \end{aligned}$$

then x could begin with

$$0.285...$$

The proof - II

- By construction, x differs from $f(n)$ in the n-th digit after the decimal dot. Hence $x \neq f(n)$ for all natural numbers n, and therefore f is not bijective in contradiction to our assumption. This proves the theorem.
- We have proved here a statement using a strategy known as **reductio ad absurdum** - instead of proving directly that a statement is true one assumes it is not, and then shows this leads to a contradiction.

The power set

- Let X be any set.

Definition

The power set $\mathcal{P}(X)$ is the set of all subsets of X.

- Example: If $X = \{1, 2, 3\}$, then $\mathcal{P}(X)$ has 8 elements:

$$\{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}$$

  and the empty set $\emptyset = \{\}$.
- If X has n elements, then $\mathcal{P}(X)$ has 2^n elements - encode a subset $E \subset X$ in a number written in binary code using as many bits as X has elements. The number corresponding to E has the i-th bit equal to 0 if the i-th element of X is not in E and equal to 1 otherwise (obviously we have to number the elements of X).

Cantor's theorem

- Let X be any set.

Theorem

There is no **surjective** *function $f : X \to \mathcal{P}(X)$, that is, no function such that every element of $\mathcal{P}(X)$ is of the form $f(x)$ for some x.*

- For finite sets this is obvious as $2^n > n$ for all natural numbers n. The thrilling bit is that the theorem holds for all sets whatsoever.

The proof - I

- Assume $f : X \to \mathcal{P}(X)$ is a function as in the theorem and define a set that mathematicians would cryptically write as follows:

$$C := \{x \in X \mid x \notin f(x)\}$$

The symbol $\in$ means "is an element of ", and $\notin$ means the opposite. So C contains exactly those elements x of X that are *not* elements of the corresponding $f(x)$. Recall, f assigns to x an element $f(x)$ of the power set, that is, $f(x)$ is a subset of X, hence it makes sense to ask whether x is an element of $f(x)$.

The proof - II

- We have assumed f is surjective. So there exists a $c \in X$ such that $C = f(c)$. Hence we can ask: Is c an element of C?
- If it were, then c is an element of $f(c) = C$. But C was defined to be the set of those elements x of X with $x \notin f(x)$, so this leads to a contradiction.
- But the other way round we also get a contradiction! If it were not, $c \notin C = f(c)$, then c satisfies the defining condition that determines the elements of C, so this is also a contradiction.
- Hence the whole assumption at the beginning must have been wrong. The theorem is proven.

Cantor's paradox

- We have talked a lot about sets. But what is this, a set?
- Our intuition says: take any well-defined notion at all, and there will be the set of all the individual incarnations of that notion.
- So how about the set S of all sets? It sounds like a very philosophical thing, but still like something one can define.
- However, every subset of S is a set, hence an element of S. Therefore we can define a surjective function $f : S \to \mathcal{P}(S)$ that maps these to themselves and all other sets to the empty set.
- You might think I have just confused you with all these words, but the following is deadly serious and the naked truth:

Cantor's paradox

The set of all sets does not exist.

Axiomatic set theory

- More precisely: If we assume we can do with sets the things we naively assume we can do with them, then there can not be a set that contains all sets as elements, the sheer concept leads to unavoidable logical contradictions.
- In modern mathematics, one thus begins by admitting that debating what a set is is beyond mathematics. We simply assume these beings exist, that they can be elements of each other or not, and that certain rules called **axioms** restrict the use of these words. For example, the **axiom of extensionality** says that two sets that have the same elements are the same sets. Then the whole of mathematics as you know it is constructed using these axioms.
- The fundamental upshot is: Mathematics is *not* about an absolute truth, it is a game with players and rules that we have chosen following our naive intuition.

Exercises

- A function $f : X \to Y$ is **injective** if whenever we have $f(x) = f(y)$ for two elements x, y of X, then $x = y$. Show that for any set X there is an injective function $f : X \to \mathcal{P}(X)$.
- Show that a function $f : X \to Y$ is bijective if and only if it is injective and surjective.
- Which of the functions in the exercises of the first half were injective? Which ones were surjective?
- **Russell's paradox** is a variation of Cantor's paradox that demonstrates the issues with naive set theory in a slightly different way: Contemplate the set R of all sets that do not contain themselves as elements,

$$R := \{X \mid X \notin X\}$$

Now ask yourself whether $R \in R$ or $R \notin R$.