Inductive definitions

Examples:

- $\mathrm{add} : \mathbb{N}^2 \to \mathbb{N}$

$$\begin{cases} \mathrm{add}(m, 0) & = & m \\ \mathrm{add}(m, n+1) & = & \mathrm{add}(m, n) + 1 \end{cases}$$

- $S : \mathbb{N} \to \mathbb{N}$

$$\begin{cases} S(0) & = & 0 \\ S(n+1) & = & \mathrm{add}(n, S(n)) \end{cases}$$

The function

$$\rho_{a,f} : \mathbb{N} \longrightarrow A$$

inductively defined from

$$\begin{cases} a \in A \\ f : \mathbb{N} \times A \longrightarrow A \end{cases}$$

is the unique such that

$$\begin{cases} \rho_{a,f}(0) &= a \\ \rho_{a,f}(n+1) &= f\big(n, \rho_{a,f}(n)\big) \end{cases}$$

Examples:

- $\mathrm{add} : \mathbb{N}^2 \longrightarrow \mathbb{N}$

  $\mathrm{add}(m, n) = \boldsymbol{\rho}_{m,f}(n)$ for $f(x, y) = y + 1$

- $S : \mathbb{N} \longrightarrow \mathbb{N}$

  $S = \boldsymbol{\rho}_{0,\mathrm{add}}$

BIJECTIONS

$$\begin{tikzcd} A \arrow[r, bend left, "f"] & B \arrow[l, bend left, dashed, "\exists g"] \end{tikzcd}$$

bijection

$$\left\{ \begin{aligned} g \circ f &= id_A \\ f \circ g &= id_B \end{aligned} \right. \implies$$

g is unique

Typically denoted f^{-1}

Proposition 153 *For all finite sets* A *and* B,

$$\#\mathrm{Bij}(A,B) = \begin{cases} 0 & , \textit{if } \#A \neq \#B \\ n! & , \textit{if } \#A = \#B = n \end{cases}$$

PROOF IDEA:

$A = \{a_1, \ldots, a_n\}$

$B = \{b_1, \ldots, b_m\}$

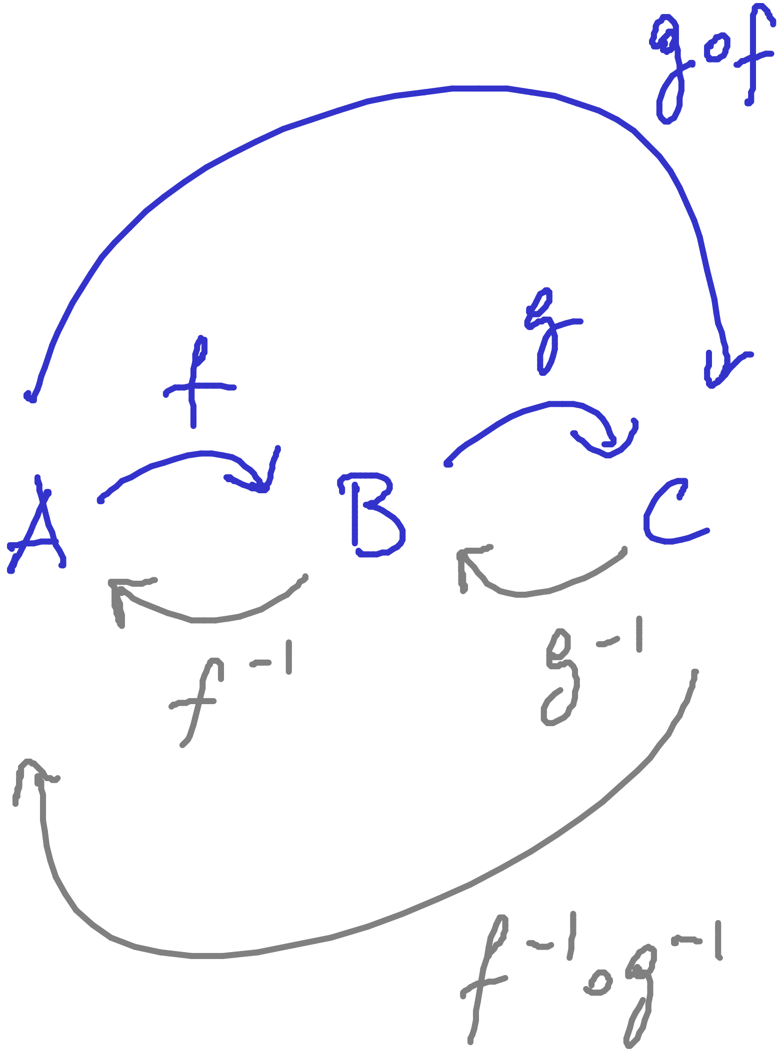
If $n \neq m$, A and B are not in bijective correspondence.

Suppose $n = m$.

$$\begin{array}{ccccccc} n \text{ choices} & & (n-1) \text{ choices} & & (n-2) \text{ choices} & & 1 \text{ choice} \\ b_{i_1} & & b_{i_2} \neq b_{i_1} & & b_{i_3} \neq b_{i_2}, \ \neq b_{i_1} & & b_{i_n} \\ \uparrow & & \uparrow & & \uparrow & \cdots & \uparrow \\ a_1 & & a_2 & & a_3 & & a_n \end{array}$$

$\boxtimes$

Theorem 154 *The identity function is a bijection, and the composition of bijections yields a bijection.*



Definition 155 *Two sets* A *and* B *are said to be* isomorphic *(and to have the* same cardinatity*) whenever there is a bijection between them; in which case we write*

$$A \cong B \quad \textit{or} \quad \#A = \#B \quad .$$

Examples: exercise:

1. $\{0, 1\} \cong \{\mathbf{false}, \mathbf{true}\}$.
2. $\mathbb{N} \cong \mathbb{N}^+$, $\mathbb{N} \cong \mathbb{Z}$, $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$, $\mathbb{N} \cong \mathbb{Q}$.

$\mathbb{N}^+ = \{n \in \mathbb{N} \mid n \geq 1\}$

$$
\begin{tikzcd}
\mathbb{N} \arrow[r, bend left, "succ"] & \mathbb{N}^+ \arrow[l, bend left, "pred"]
\end{tikzcd}
$$

$$0 \le n \longmapsto n+1 \longmapsto (n+1)-1 = n$$

$$1 \le n \longmapsto (n-1) \longmapsto (n-1)+1 = n$$

	0	1	2	...	m	...
0	0	1	3	6 .		
1	2	4	7	. .		
2	5	8	.			
⋮	9	. .				
n	. . .					
⋮						

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(m, n) \longmapsto 2^m \cdot (2n+1) - 1$$

__claim__ bijection.

Calculus of bijections

- $A \cong A \;,\; A \cong B \implies B \cong A \;,\; (A \cong B \wedge B \cong C) \implies A \cong C$
- If $A \cong X$ and $B \cong Y$ then

$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad,\quad A \times B \cong X \times Y \quad,\quad A \uplus B \cong X \uplus Y \quad,$$

$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad,\quad (A \rightharpoonup B) \cong (X \rightharpoonup Y) \quad,$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad,\quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$

$(b.c)^a = b^a . c^a$

- $A \cong [1] \times A$, $(A \times B) \times C \cong A \times (B \times C)$, $A \times B \cong B \times A$
- $[0] \uplus A \cong A$, $(A \uplus B) \uplus C \cong A \uplus (B \uplus C)$, $A \uplus B \cong B \uplus A$
- $[0] \times A \cong [0]$, $(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$
- $(A \Rightarrow [1]) \cong [1]$, $(A \Rightarrow (B \times C)) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $([0] \Rightarrow A) \cong [1]$, $((A \uplus B) \Rightarrow C) \cong (A \Rightarrow C) \times (B \Rightarrow C)$
- $([1] \Rightarrow A) \cong A$, $((A \times B) \Rightarrow C) \cong (A \Rightarrow (B \Rightarrow C))$
- $(A \rightharpoonup B) \cong (A \Rightarrow (B \uplus [1]))$
- $\mathcal{P}(A) \cong (A \Rightarrow [2])$

(Un)Currying

$c^{a.b} = (c^b)^a$

Characteristic (or indicator) functions

$$\mathcal{P}(A) \cong (A \Rightarrow [2])$$

$$S \subseteq A \longmapsto \left(\chi_S : A \to \{0,1\} : a \longmapsto \begin{cases} 0, & a \notin S \\ 1, & a \in S \end{cases} \right)$$

$$S \mapsto \chi_S \mapsto \sigma(\chi_S) = S$$

$$f \mapsto \sigma f \mapsto \chi_{\sigma f} = f$$

$$\chi_S(a) = \begin{cases} 0 & , a \notin S \\ 1 & , a \in S \end{cases}$$

$$\begin{array}{c} \sigma f \\ \shortparallel \\ \{a \in A \mid f(a) = 1\} \subseteq A \end{array} \longleftarrow\!\shortmid \; f : A \to \{0,1\}$$

NB: $\forall f : A \to [2].\ \exists!\, S \subseteq A.\ \chi_S = f.$

Finite cardinality

Definition 160 *A set A is said to be* finite *whenever $A \cong [n]$ for some $n \in \mathbb{N}$, in which case we write $\#A = n$.*

Theorem 161 *For all* $m, n \in \mathbb{N}$,

1. $\mathcal{P}\big([n]\big) \cong [2^n]$

2. $[m] \times [n] \cong [m \cdot n]$

3. $[m] \uplus [n] \cong [m + n]$

4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$

5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$

6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

Infinity axiom

$\boxed{\text{There is an infinite set, containing } \emptyset \text{ and closed under successor.}}$

BIJECTIONS

__Fact__: Let $f : A \to B$.

f is bijective.

iff

$$\forall b \in B.\ \exists!\, a \in A.\ f(a) = b.$$

iff

$$\forall b \in B.\ \exists a \in A.\ f(a) = b$$

surjection

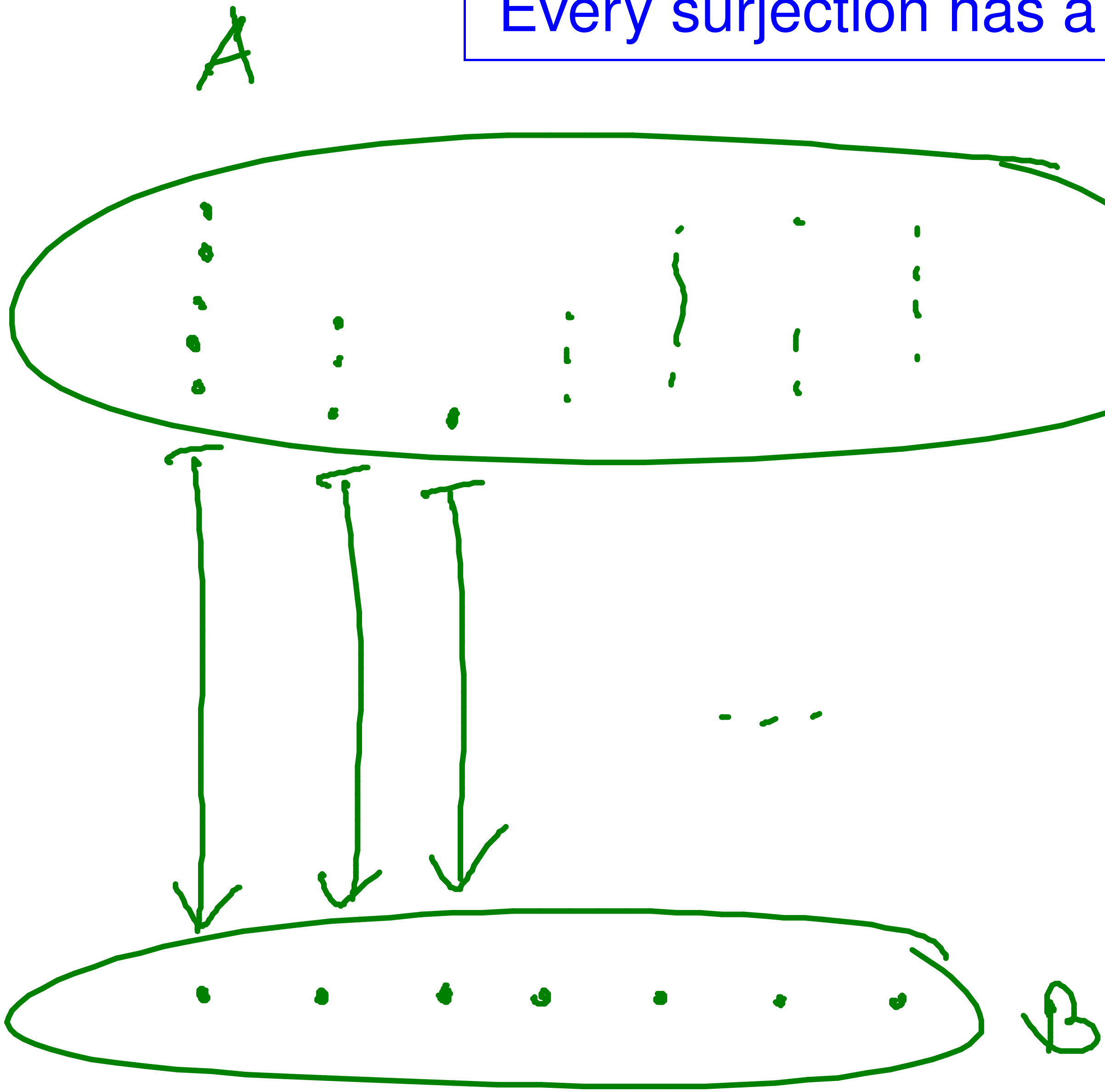
and

$$\forall a_1, a_2 \in A.\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

injection

Axiom of choice

Every surjection has a section.



$e \circ c = id_B$

$$\begin{tikzcd} \exists a \arrow[d, mapsto] & \in & A \arrow[d, "e"] \\ e(a) = \forall b & \in & B \arrow[u, bend left, dashed, "\exists c"] \end{tikzcd}$$

NB
$\mathbb{N} \not\twoheadrightarrow \mathcal{P}(\mathbb{N})$

Unbounded cardinality

Theorem 180 (Cantor's diagonalisation argument) *For every set* A*, no surjection from* A *to* $\mathcal{P}(A)$ *exists.*

PROOF: Suppose we have a surjection

$$e : A \twoheadrightarrow \mathcal{P}(A)$$

$$\forall S \subseteq A.\ \exists a \in A.\ e(a) = S$$

Def Let $S = \{ a \in A \mid a \notin e(a) \}$

$$\exists a \in A.\ e(a) = S$$

Then $a \in S \iff a \notin e(a)$

$\Updownarrow$

$a \in e(a)$

$\not\downarrow$ $\boxtimes$

$a_1 \mapsto e(a_1)$

$a_2 \mapsto e(a_2)$

$\vdots \qquad \vdots$

$a_i \mapsto e(a_i)$

$\vdots \qquad \vdots$

$a_1 \in S \iff a_1 \notin e(a_1)$

$a_2 \in S \iff a_2 \notin e(a_2)$

$\vdots$

$a_i \in S \iff a_i \notin e(a_i)$

Corollary 183 *The sets*

$$\mathcal{P}(\mathbb{N}) \;\cong\; \big(\mathbb{N} \Rightarrow [2]\big) \;\cong\; [0,1] \;\cong\; \mathbb{R}$$

are not enumerable.

Corollary 184 *There are* non-computable *infinite sequences of bits.*

Replacement axiom

$\boxed{\text{The direct image of every definable functional property on a set is a set.}}$

Set-indexed constructions

For every mapping associating a set A_i to each element of a set I, we have the set

$$\bigcup_{i \in I} A_i \;=\; \bigcup \{A_i \mid i \in I\} \;=\; \{a \mid \exists i \in I.\, a \in A_i\} \quad .$$

Examples:

1. Indexed disjoint unions:

$$\biguplus_{i \in I} A_i \;=\; \bigcup_{i \in I} \{i\} \times A_i$$

2. Finite sequences on a set A:

$$A^* \;=\; \biguplus_{n \in \mathbb{N}} A^n$$

Foundation axiom

$\boxed{\text{The membership relation is well-founded.}}$

Thereby, providing a

Principle of $\in$*-Induction* .