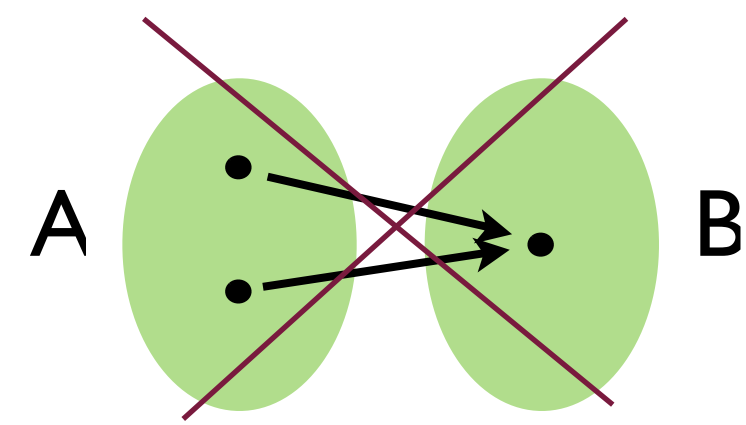
Special functions

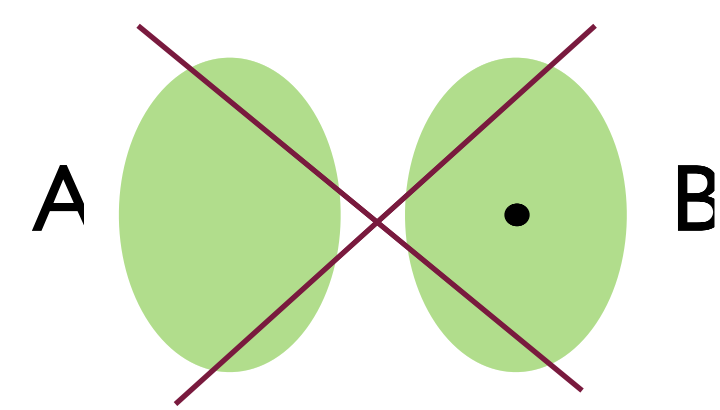
Def. A function $f: A \longrightarrow B$ is injective iff

for all $a, b \in A$, if $f(a) = f(b)$ then $a = b$.



Def. A function $f: A \longrightarrow B$ is surjective iff

for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.



Def. A function $f: A \longrightarrow B$ is bijective iff

for all $b \in B$, there exists unique $a \in A$ with $f(a) = b$.

Simple characterisations

Lemma I1: A function $f: A \longrightarrow B$ is injective iff

for all $b \in B$, $|f^{-1}(\{b\})| \leq 1$.

at most one incoming arrow

injection

Lemma S1: A function $f: A \longrightarrow B$ is surjective iff

$|f^{-1}(\{b\})| \geq 1$ for all $b \in B$ iff

$f(A) = B$.

at least one incoming arrow

surjection

Lemma B1: A function $f: A \longrightarrow B$ is bijective iff

$|f^{-1}(\{b\})| = 1$ for all $b \in B$ iff

f is both injective and surjective.

exactly one incoming arrow

bijection

Some properties

Lemma I2: Let $f: A \longrightarrow B$ be injective and let $A' \subseteq A$. Then

$f(x) \in f(A')$ iff $x \in A'$.

if holds always!

Prop. I3: Let $f: A \longrightarrow B$ be injective and let $A' \subseteq A$. Then

$f^{-1}(f(A')) = A'$.

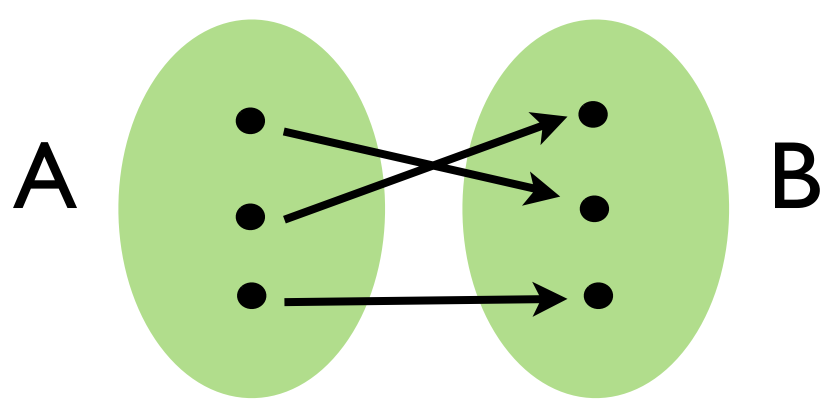
Prop. S2: Let $f: A \longrightarrow B$ be surjective and let $B' \subseteq B$. Then

$f(f^{-1}(B')) = B'$.

Inverse function

Let f:A $\longrightarrow$ B be a bijection

well defined only if f is bijective!



Def. The inverse function f^{-1}: B $\longrightarrow$ A is defined as

$$f^{-1}(b) = a \text{ iff } f(a) = b, \quad b \in B.$$

Lemma B2: The inverse function f^{-1} for a bijection f is bijective.

Function composition

Let $f: A \longrightarrow B$ and $g: B \longrightarrow C$

Function composition

Let $f: A \longrightarrow B$ and $g: B \longrightarrow C$

"after"

$g \circ f : A \longrightarrow B \longrightarrow C$

Def. The composition $g \circ f$ is a function $g \circ f : A \longrightarrow C$ given by

$$g \circ f\,(a) = g(f(a)), \text{ for } a \in A.$$

Lemma I4: Let $f: A \longrightarrow B$ and $g: B \longrightarrow C$ be injective. Then $g \circ f$ is injective.

Lemma S3: Let $f: A \longrightarrow B$ and $g: B \longrightarrow C$ be surjective. Then $g \circ f$ is surjective.

Corollary B2: Let $f: A \longrightarrow B$ and $g: B \longrightarrow C$ be bijective. Then so is $g \circ f$.

A characterization of bijections

Theorem B3: A function $f: A \longrightarrow B$ is bijective iff there exists a function $g: B \longrightarrow A$ with $g \circ f = id_A$ and $f \circ g = id_B$.

$id_A: A \longrightarrow A$,
$id_A(a) = a$, for all $a \in A$

Equality of functions

Let $f: A \longrightarrow B$ and $g: C \longrightarrow D$

Def. The functions $f: A \longrightarrow B$ and $g: C \longrightarrow D$ are equal iff

(1) $A = C$

(2) $B = D$

(3) for all $a \in A$, $f(a) = g(a)$.

dom f = dom g

cod f = cod g

The structure of natural numbers

is helpful for proving properties

$\forall n[n \in \mathbb{N} : P(n)]$

The structure of natural numbers

On natural numbers we can define a notion of a successor, a mapping

s: $\mathbb{N} \to \mathbb{N}$

by s(n) = n+1

The successor mapping imposes a structure on the set that enables us to count:

1) there is a starting natural number 0
2) for every natural number n, there is a next natural number s(n) = n+1.

(Some) Peano Axioms

Important properties

(1) Different natural numbers have different successors:

$\forall n,m\ [n,m \in \mathbb{N} : s(m) = s(n) \Rightarrow m = n]$

stated positively

s is injective!

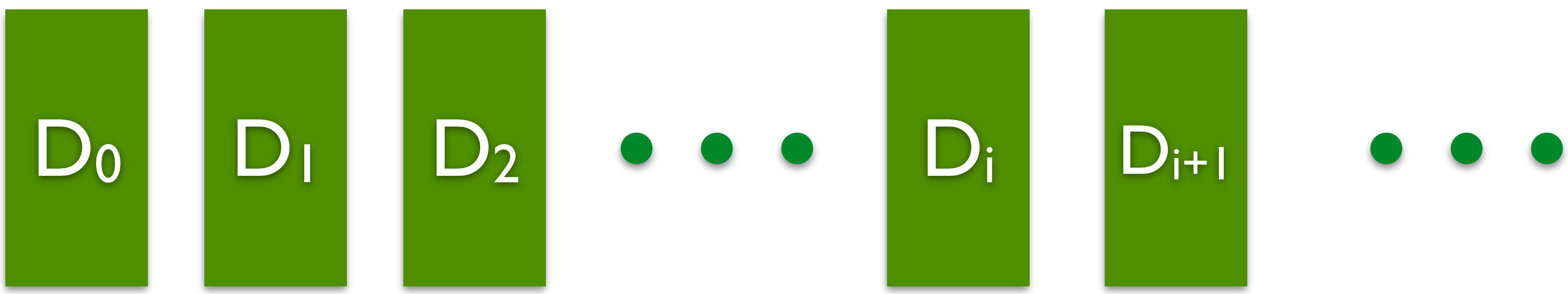
(2) 0 is not a successor: $\forall n\ [n \in \mathbb{N} : \neg\ (s(n) = 0)\ ]$

(3) All natural numbers except 0 are successors:

$\forall n[n \in \mathbb{N} \wedge \neg(n = 0) : \exists m[m \in \mathbb{N} :\ n = s(m)]$

There is more to it - induction

Imagine an infinite sequence of dominos



If we know that

1. D_0 falls
2. The dominos are close enough together so that if D_i falls, then D_{i+1} falls (for all $i \in \mathbb{N}$)

Then we can conclude that every domino D_n ($n \in \mathbb{N}$) falls!

induction

Induction

P - unary predicate over $\mathbb{N}$

$$P(0) \wedge \forall i \, [i \in \mathbb{N} : P(i) \Rightarrow P(i+1)] \Rightarrow \forall n \, [n \in \mathbb{N} : P(n)]$$

$\forall$ elim with 0

$\Rightarrow$ elim

$P(0)$

$P(0) \Rightarrow P(1)$

$P(1)$

$P(1) \Rightarrow P(2)$

$P(2)$

$P(2) \Rightarrow P(3)$

...

Variant of the Peano Axiom:

Let $K \subseteq \mathbb{N}$ have the property that

(a) $0 \in K$ and

(b) for all $n \in \mathbb{N}$, $n \in K \Rightarrow (n+1) \in K$.

Then $K = \mathbb{N}$.

Induction

$P(0) \wedge \forall i\,[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)] \Rightarrow \forall n\,[n \in \mathbb{N} : P(n)]$

P - unary predicate over $\mathbb{N}$

. . .

(m) $P(0)$

{Assume}

(k) **var** $i; i \in \mathbb{N}$

(k+1) $P(i)$

. . .

(l-1) $P(i+1)$

{⇒-intro on (k+1) and (l-1)}

(l) $P(i) \Rightarrow P(i+1)$

{∀-intro on (k) and (l)}

(l+1) $\forall i[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)]$

{induction on (m) and (l+1)}

(l+2) $\forall n[n \in \mathbb{N} : P(n)]$

Basis

induction hypothesis

Induction step

Inductive definitions

Inductive proof: truth is passed on

Inductive definition: construction is passed on

well defined by induction

Example

The sequence of real numbers $(a_i \mid i \in \mathbb{N})$ is defined inductively by

$$a_0 = 2$$
$$a_{i+1} = 2a_i - 1$$

a	a	a	a	a	…
2	3	5	9	17	…

proof by induction

Conjecture

For all $n \in \mathbb{N}$ it holds that

$$a_n = 2^n + 1$$