Ideas of mathematical proof

Slides Week 22

Mappings. Cardinalities.

Injective mappings

Definition

A mapping $f : A \to B$ is **injective** (or **one-to-one**)

if different elements are sent to different:

$x_1 \neq x_2 \;\Rightarrow\; f(x_1) \neq f(x_2)$

(the same: $f(x_1) = f(x_2) \;\Rightarrow\; x_1 = x_2$).

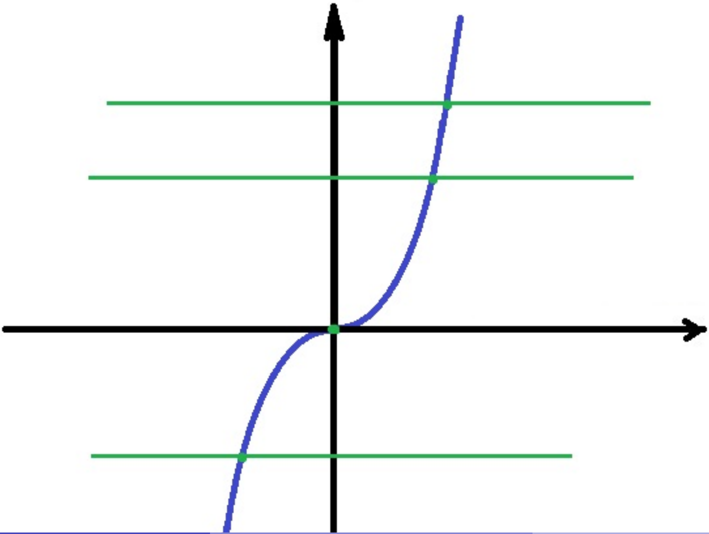
Example

$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$

is not injective, since, e.g., $f(-2) = f(2)$.

Example

$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^3$ is injective:

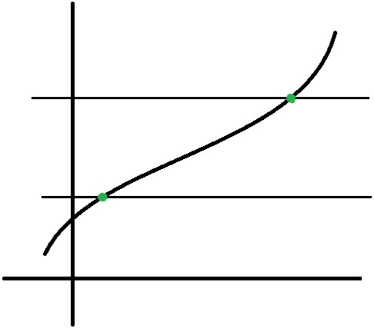


Horizontal Line Test for functions

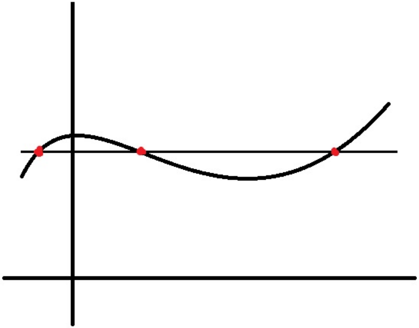
For $A, B \subseteq \mathbb{R}$, a mapping $f : A \to B$ is injective

if it satisfies the "Horizontal Line Test":

every horizontal line has at most one intersection point with the graph.



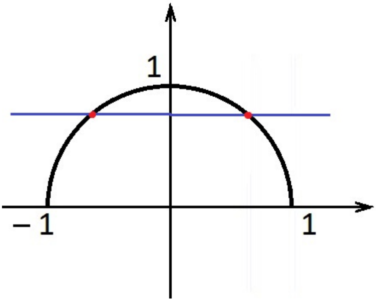
injective



not injective

Example

Is $f : [-1, 1] \to \mathbb{R}, \quad f(x) = \sqrt{1 - x^2},$ injective?



fails Horizontal Line Test: not injective.

Without picture: e.g. $f(1) = f(-1)$.

Example

Let T be the set of triangles and let $f : T \to \mathbb{R}$, where $f(t) =$ area of t.

Then f is not injective, as $\exists$ different triangles with equal areas.

Example

Let $S = \{$all circles on the plane centred at $(0,0)\}$ and let $f : S \to \mathbb{R}$, where $f(c) =$ area of c.

This f is injective: for every area there is only one radius giving this area, and only one circle with centre $(0,0)$ with this radius.

Example

Let $A = \mathscr{P}(\{a, b, c\})$ (all subsets of $\{a, b, c\}$),

and let $f : A \to A$, where $f(X) = X \cap \{a\}$.

This f is not injective: e.g., $f(\{a\}) = \{a\} = f(\{a, b\})$.

Surjective mappings

Definition

A mapping $f : A \to B$ is **surjective** (or **onto**)

if $f(A) = B$.

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

Example

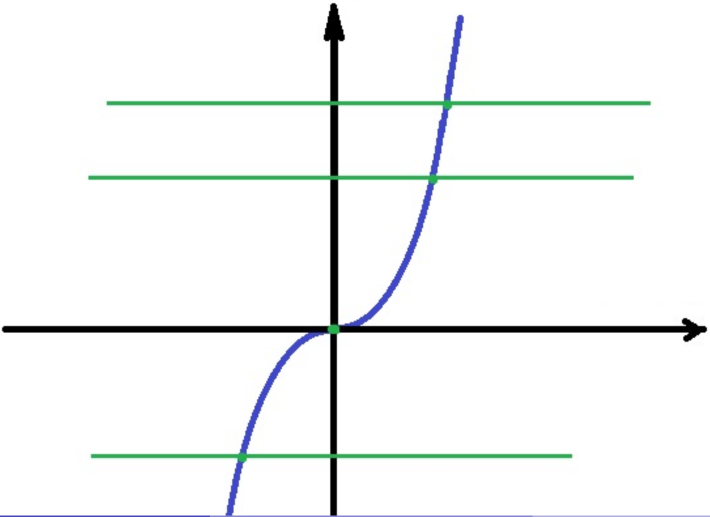
$f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x^2$

is not surjective, since $f(x) \geq 0$ for all x,

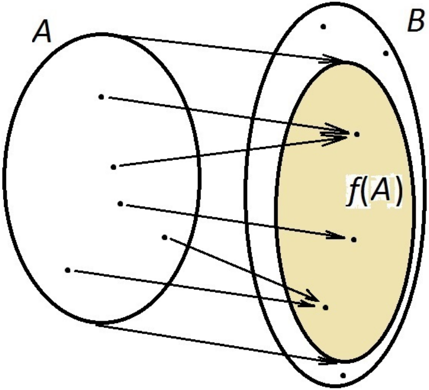
so e.g. $-1 \notin f(A)$.

Example

$f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x^3$, is surjective.



Remark: Any mapping $f : A \to B$, can be 'made surjective' by changing the codomain B to $f(A)$, so the same rule, but for $f : A \to f(A)$.



E.g.: $f : \mathbb{R} \to \{x \in \mathbb{R} \mid x \geq 0\}$, $f(x) = x^2$ is now surjective.

Bijective mappings

Definition

A mapping $f : A \to B$ is **bijective**

(or is a **one-to-one correspondence**)

if it is both injective and surjective.

Example

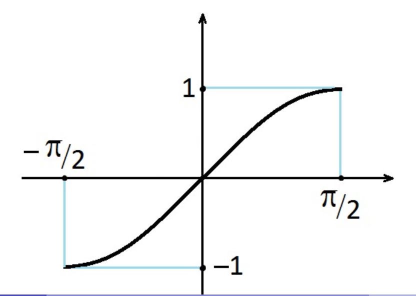
$f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^3$ is bijective.

Example

$f : \mathbb{R} \to \mathbb{R}$ with $f(x) = \sin x$
is neither surjective, nor injective.

Change codomain: $f : \mathbb{R} \to [-1, 1]$, $f(x) = \sin x$
is now surjective, but not injective ($\sin(a + 2\pi) = \sin a$).

Change domain: $f : [-\pi/2, \pi/2] \to [-1, 1]$,
then $f(x) = \sin x$ is now also injective, so a bijection:



Inverse images

Definition

Given a mapping $f : A \to B$,

the **full inverse image** of an element $b \in B$

is the set $f^{-1}(b) = \{a \in A \mid f(a) = b\}$.

Note: f^{-1} is not a mapping in general.

Example

Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$.

Then $f^{-1}(4) = \{-2, 2\}$.

Full inverse image as full solution

Example

Let $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sin x.$

Find $f^{-1}(0.5).$

Solutions of equation $f(x) = 0.5, \; \sin x = 0.5$

$f^{-1}(0.5) = \{k\pi + (-1)^k \pi/6 \mid k \in \mathbb{Z}\}.$

Example

Let $A = \mathscr{P}(\{a, b, c\})$ (all subsets of $\{a, b, c\}$),

and let $f : A \to A, \quad f(X) = X \cap \{a\}$.

Find the full inverses images of all elements of $f(A)$.

The image is $f(A) = \{\varnothing, \{a\}\}$.

Full inverse images:

$f^{-1}(\varnothing) = \{\varnothing, \{b\}, \{c\}, \{b, c\}\}$

(all subsets X with $X \cap \{a\} = \varnothing$, that is, $X \not\ni a$).

$f^{-1}(\{a\}) = \{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$

(all subsets Y with $Y \cap \{a\} = \{a\}$, that is, $Y \ni a$).

Definition

For $f : A \to B$

an **inverse image** (or a **pre-image**) of $b \in B$

is any $a \in f^{-1}(b)$ that is, any a such that $f(a) = b$.

Only makes sense for $b \in f(A)$,

(sometimes they put $f^{-1}(b) = \varnothing$ for $b \notin f(A)$).

Example

For $f(x) = \sin x$,

a pre-image of 0.5 is $\pi/6$, and $5\pi/6$, etc.

Remark: injective means precisely that

$|f^{-1}(b)| = 1$ for all $b \in f(A)$, a unique pre-image.

Example

Let $A = \mathscr{P}(\{u, v, w\})$ (all subsets of $\{u, v, w\}$),

and let $f : A \to \{0, 1, 2, 3, 4, 5\}$, $f(X) = |X|$.

What is $f^{-1}(2)$? Answer: $= \{\{u, v\}, \{u, w\}, \{v, w\}\}$.

In particular, f is not injective.

$f^{-1}(0) = \{\varnothing\}$.

$f^{-1}(5)$ undefined (or $f^{-1}(5) = \varnothing$).

Inverse mapping

Definition

Suppose that $f : A \to B$ is a bijection.

Then $f^{-1} : B \to A$ can be regarded as a mapping:

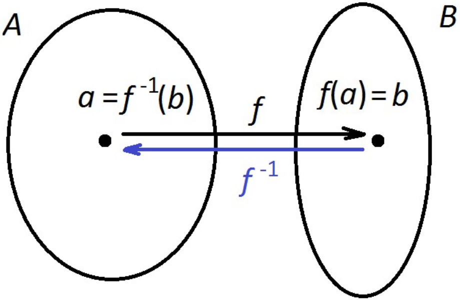
$f^{-1}(b) = a$ such that $f(a) = b$

is well defined $\forall b$ since such a is unique for a bijection.

Then f^{-1} is called the **inverse mapping** of f.

Diagram for inverse mapping

On the diagram this means reversing those arrows:



Remark: So-called 'abuse of notation':

generally $f^{-1}(b)$ is the set of all pre-images.

Even for a bijection, when $f(a) = b$,

strictly speaking, $f^{-1}(b) = \{a\}$.

But the same notation is used to denote

the inverse mapping (when it exists!): $f^{-1}(b) = a$.

Example

Verify that $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \dfrac{5x+3}{8}$

is a bijection and find the inverse mapping.

Injective: if $\dfrac{5x_1+3}{8} = \dfrac{5x_2+3}{8}$, then

$5x_1 + 3 = 5x_2 + 3, \;\; 5x_1 = 5x_2, \;\; x_1 = x_2,$ as req.

Surjective: for any $y \in \mathbb{R}$ find x such that $f(x) = y$,

$\dfrac{5x+3}{8} = y$, easily solved: $x = \dfrac{8y-3}{5}$.

So, $f^{-1}(y) = \dfrac{8y-3}{5}$.

Example

We know that

$$f : [-\pi/2, \pi/2] \to [-1, 1], \;\; f(x) = \sin x,$$

is a bijection.

Hence it has inverse $f^{-1} : [-1, 1] \to [-\pi/2, \pi/2]$,

denoted by $\sin^{-1}$ or arcsin.

Example

Show that the mapping

$$f : [2, \infty) \to [-3, 0), \qquad f(x) = \frac{3}{1-x}$$

is a bijection, and find the inverse mapping.

Injective: if $\dfrac{3}{1-x_1} = \dfrac{3}{1-x_2}$,

then $3(1-x_2) = 3(1-x_1)$, $\qquad 1-x_2 = 1-x_1$,

$x_2 = x_1$, as req.

Surjective: for any $y \in [-3, 0)$

need $x \in [2, \infty)$ such that

$$f(x) = \frac{3}{1-x} = y; \quad 3 = y(1-x); \quad x = 1 - \frac{3}{y}$$

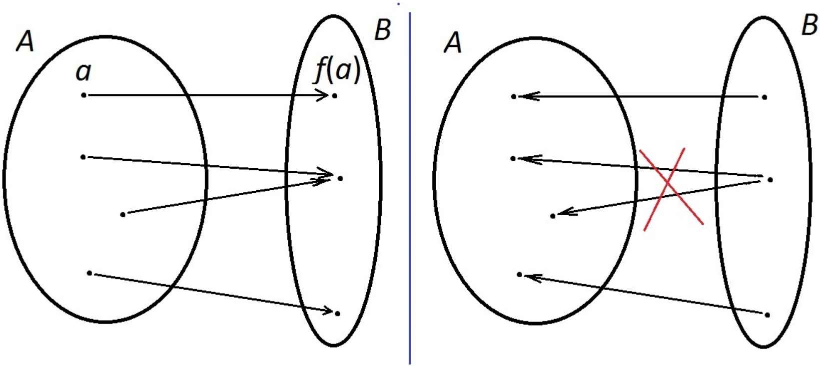
also need ≥ 2, check: $1 - \frac{3}{y} \geq 2, \quad -\frac{3}{y} \geq 1,$

(since $y < 0$) $\Leftrightarrow$ $-3 \leq y$, so true for $y \in [-3, 0)$.

Inverse mapping: $f^{-1}(y) = 1 - \frac{3}{y},$

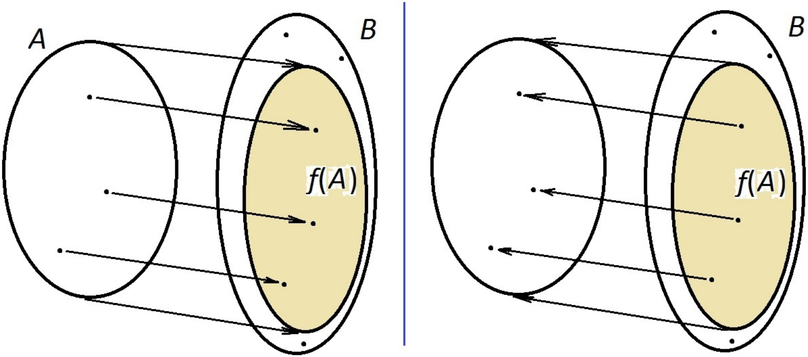
$f^{-1} : [-3, 0) \to [2, \infty).$

Remark: Non-injective mapping has no inverse:



'Reversing arrows' is not a mapping, since pre-image is not unique.

Injective but not surjective mapping $f : A \to B$ has no inverse $B \to A$ since elements outside $f(A) \neq B$ have no pre-images:



But 'reversing arrows' makes a mapping
$f^{-1} : f(A) \to A$,
which is the inverse of $f : A \to f(A)$.

Example

Let $C = \{\text{all circles on the plane centred at } (0,0)\}$.
Let $f : C \to \mathbb{R}$, $f(c) =$ area of c.

Is injective, but not surjective (say, $-1 \notin$ image).

Becomes bijective for $f : C \to (0, \infty)$,

since for $b > 0$ there is a circle centred at $(0,0)$

with area b: of radius $\sqrt{b/\pi}$.

Hence then there is inverse mapping:

$f^{-1} : (0, \infty) \to C$

$f^{-1}(b) =$ circle of radius $\sqrt{b/\pi}$ centred at $(0,0)$.

Proposition

The inverse of a bijection $f : A \to B$

is a *bijection* $f^{-1} : B \to A$*.*

Proof: f^{-1} is injective: $f^{-1}(b_1) = a = f^{-1}(b_2)$

means $b_1 = f(a) = b_2$. But f is a mapping,

so must be well defined: $b_1 = b_2$, as required.

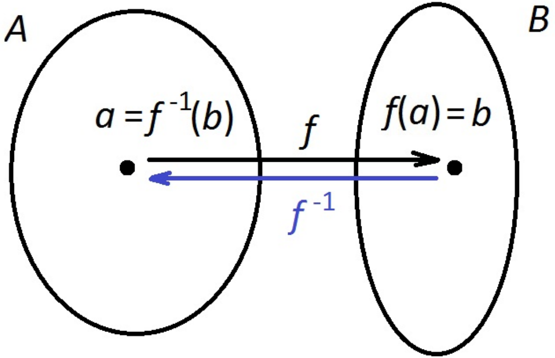
f^{-1} is surjective: for any $a \in A$

we have $a = f^{-1}(f(a))$, so $a \in f^{-1}(B)$. □

Proposition

If $f : A \to B$ is a bijection, then $(f^{-1})^{-1} = f$.

Note: $(f^{-1})^{-1}$ exists because f^{-1} is also a bijection.



Composite mappings

Definition

Let $f : A \to B$ and $g : B \to C$ be mappings

such that the codomain of f is (in) the domain of g,

then the **composite** mapping $g \circ f : A \to C$

is defined by the rule

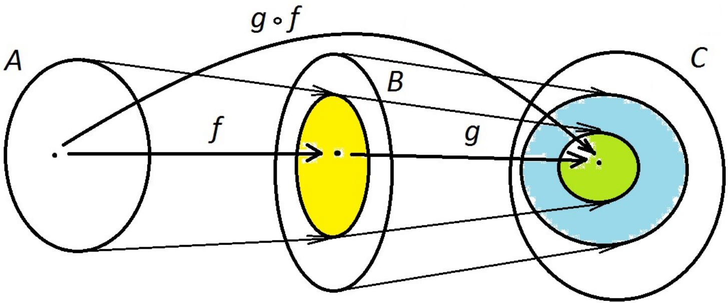
$(g \circ f)(a) = g(f(a))$ for all $a \in A$.

'Function of a function', or 'chain function':

Example

$y = (\sin x)^2$ is the composite of $\sin x$ and x^2.

Image of composite mapping



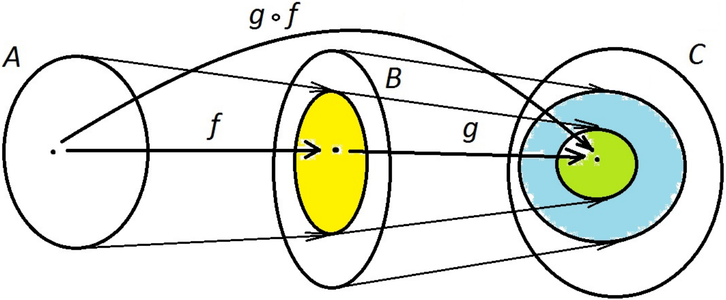
Yellow is $f(A)$, blue and green $g(B)$,

green is the image of $g \circ f$, that is,

$(g \circ f)(A) = g(f(A))$.

Useful notation

$$g \circ f : A \xrightarrow{f} B \xrightarrow{g} C, \qquad (g \circ f)(x) = g(f(x))$$



Example

Let $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sin x,$

and $g : \mathbb{R} \to \mathbb{R}, \quad g(y) = y^2.$

What are $f \circ g$ and $g \circ f$ (if exist)?
What are their images?

$g \circ f : \mathbb{R} \xrightarrow{\sin x} \mathbb{R} \xrightarrow{y^2} \mathbb{R}.$ Then $(g \circ f)(x) = (\sin x)^2.$

The image of f is $[-1, 1]$.

The image of $g \circ f = (\sin x)^2$ is $[0, 1]$
as this is the image of $[-1, 1]$ under $g : x \to x^2$.

Different: $f \circ g : \mathbb{R} \xrightarrow{x^2} \mathbb{R} \xrightarrow{\sin y} \mathbb{R}$

$(f \circ g)(x) = \sin(x^2)$. Image is $[-1, 1]$

Example

Let $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = 2x + 1$

and $g : [0, \infty) \to \mathbb{R}, \quad g(x) = \sqrt{x}$.

Then $f \circ g : [0, \infty) \to \mathbb{R}$ is defined: $2\sqrt{x} + 1$.

But $g \circ f$ is not defined: $f(\mathbb{R}) = \mathbb{R} \not\subseteq$ domain of g.

Changing domain may help: $f_1 : [-0.5, \infty) \to \mathbb{R}$,

$f_1(x) = 2x + 1$; image of f_1 is $[0, \infty)$;

then $g \circ f_1$ is defined: $g \circ f_1 : [-0.5, \infty) \to \mathbb{R}$,

$(g \circ f_1)(x) = \sqrt{2x + 1}$.

Remark: Usually, $f \circ g \neq g \circ f$. Moreover, often only one of these mappings is defined (exists).

Example

Let $A = \mathscr{P}(\{u, v, w\})$ (all subsets of $\{u, v, w\}$),

and let $f : A \to \mathbb{R}$, $f(X) = |X|$.

Let $g : \mathbb{R} \to \mathbb{R}$, $g(x) = 3^x$.

Which of $f \circ g$ and $g \circ f$ exist?

Then $g \circ f : A \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R}$ exists.

E.g., $(g \circ f)(\{u, v\}) = 3^2 = 9$,

$(g \circ f)(\varnothing) = 3^0 = 1$, or $(g \circ f)(\{u, v, w\}) = 3^3 = 27$.

But, of course, $f \circ g$ is not defined: $g(\mathbb{R}) \not\subseteq A$.

Theorem

Let $f : A \to B$ *and* $g : B \to C$ *be two mappings (such that the codomain of* f *is the domain of* g*).*

(a) *If both* f *and* g *are injective, then the composite* $g \circ f$ *is also injective.*

(b) *If both* f *and* g *are surjective, then the composite* $g \circ f$ *is also surjective.*

(c) *If both* f *and* g *are bijective, then the composite* $g \circ f$ *is also bijective.*

Proof: (a) f and g are injective, need $g \circ f$ injective:

$x_1 \neq x_2 \ \Rightarrow \ f(x_1) \neq f(x_2)$, since f is injective.

Then $g(f(x_1)) \neq g(f(x_2))$, since g is injective.

As required: $(g \circ f)(x_1) \neq (g \circ f)(x_2)$.

(b) f and g are surjective, need $g \circ f$ surjective:

For any $c \in C$ there is $b \in B$ such that $g(b) = c$, since g is surjective.

There is also $a \in A$ such that $f(a) = b$, since f is surjective.

Then $g(f(a)) = g(b) = c$, so $(g \circ f)(a) = c$, as req.

(c) f and g are bijective, need $g \circ f$ bijective:

follows from (a) and (b). □

Identity mapping

Definition

For a set A, the **identity mapping** $\mathrm{Id}_A : A \to A$ is defined as $\mathrm{Id}_A(x) = x$.

Proposition

Suppose that $f : A \to B$ *is a bijection. Then*

(a) $f^{-1} \circ f = \mathrm{Id}_A$;

(b) $f \circ f^{-1} = \mathrm{Id}_B$.

Proof: (a) For any $a \in A$

$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a$ by definition of f^{-1}.

(b) For any $b \in B$ there is $a \in A$

such that $f(a) = b$, since f is bijection.

Then $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(f^{-1}(f(a)))$

(by definition of f^{-1}) $= f(a) = b$. □

Cardinalities

For a finite set A, its cardinality $|A|$

$=$ is the number of elements.

If $|A| = n < \infty$, then $A = \{a_1, a_2, \ldots, a_n\}$,

where all a_i are different.

This means a bijection $f : \{1, 2, \ldots, n\} \to A$

(so that we write $a_i = f(i)$).

Clearly, two finite sets A, B have the same cardinality

$|A| = |B|$ if there is a bijection $f : A \to B$.

Cardinalities of infinite sets

Definition

Two sets A, B have **the same cardinality** denoted $|A| = |B|$ if there is a bijection $f : A \to B$.

Example

Let $A = \{2^i \mid i \in \mathbb{N}\}$ and $B = \{3k \mid k \in \mathbb{N}\}$.

Clearly, $2^i \to 3i$ is a bijection, so $|A| = |B|$.

Both have the same cardinality as $\mathbb{N}$.

For example, $i \to 2^i$ gives a bijection $\mathbb{N} \to A$.

Equal cardinalities as an equivalence

Remark. We know: if $f : A \to B$ is a bijection,

then $f^{-1} : B \to A$ is a bijection; symmetric

if $f : A \to B$ and $g : B \to C$ are bijections,

then $(g \circ f) : A \to C$ is a bijection; transitive

$\mathrm{Id}_A : A \to A$ (when $a \to a$) is a bijection. reflexive

Hence $|A| = |B|$ is an equivalence relation.

Equivalence classes are called **cardinal numbers**.
For finite sets cardinal numbers are the same as positive integers. (Or numbers are thus defined...)

We can say bijection between A and B,

since if there is a bijection $f : A \to B$,

then we also have a bijection $f^{-1} : B \to A$.

Part 'equal' to the whole

Example

Let $A = \{2^i \mid i \in \mathbb{N}\} \subseteq \mathbb{N}$ and $A \neq \mathbb{N}$.

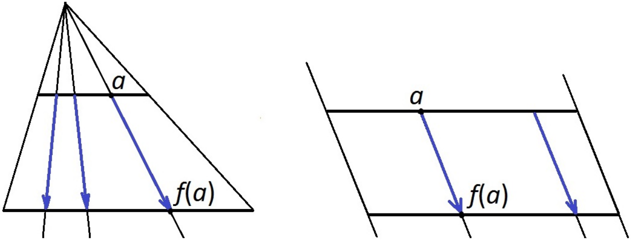
But $|A| = |\mathbb{N}|$, as we saw:

for example, $i \to 2^i$ gives a bijection $\mathbb{N} \to A$.

Example

Prove that any two closed segments on the real line (of non-zero length) have the same cardinality.

Bijection by geometry: arrange one above another, draw straight lines as on the picture.
(For equal lengths, consider parallel lines.)

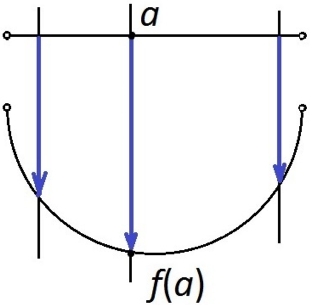


Bijection: injective: different $\rightarrow$ different;
surjective: every point on the lower segment covered.

Example

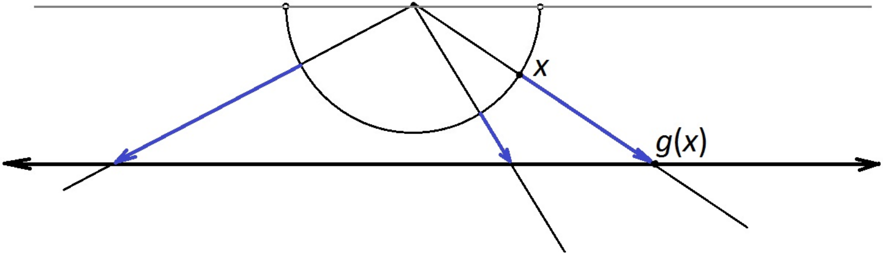
Prove that $|(0,1)| = |\mathbb{R}|$.

First a bijection f from the open interval $(0,1)$ to a semicircle S of diameter 1 without endpoints as on the picture:



Stereographic projection

Then a bijection from the semicircle onto the whole real line (so-called stereographic projection):



As we proved above, the composite $g \circ f$ of bijections is a bijection: $(0,1) \xrightarrow{f} S \xrightarrow{g} \mathbb{R}$

from $(0,1)$ onto $\mathbb{R}$. Hence, $|(0,1)| = |\mathbb{R}|$.

Countable sets

Definition

A set A is **countable infinite** if $|A| = |\mathbb{N}|$;

that is, if there is a bijection $f : \mathbb{N} \to A$.

Then we often write $a_i = f(i)$,

so that $A = \{a_1, a_2, \ldots\}$ is a sequence,

where all a_i are different (= injective)

and all elements of A occur (=surjective).

$|A| = |\mathbb{N}|$ exactly when A can be written as a sequence

Definition

A set is **countable**,

if it is either finite, or countable infinite.

Notation. The cardinality of $\mathbb{N}$

is denoted $|\mathbb{N}| = \aleph_0$ (read "aleph-naught").

So any countable infinite set has cardinality $\aleph_0$.

E.g.: $|\{2^i \mid i \in \mathbb{N}\}| = \aleph_0$

$= |\{3k \mid k \in \mathbb{N}\}| = |\mathbb{N}| = \aleph_0$.

Example

Prove that $|\mathbb{Z}| = \aleph_0$.

Proof: Need a bijection $\mathbb{N} \to \mathbb{Z}$,

that is: represent $\mathbb{Z}$ as a sequence $a_1, a_2, \ldots,$
where all a_i are different and all integers occur.

No need to produce a formula:
it is sufficient to describe such a sequence,
so that it is clear that every element occurs exactly once.

Here, for example: $0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$.

This really means that we define a bijection

$$\begin{array}{c|cccccccccc} \mathbb{N} = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ \mathbb{Z} = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & \cdots \end{array}$$

Remark: For this sequence

$0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$

a formula can be easily produced:

$$f(k) = \begin{cases} 0 & \text{if } k = 1, \\ k/2 & \text{if } k \text{ is even,} \\ (1-k)/2 & \text{if } k \text{ is odd and } > 1. \end{cases}$$

But that sequence, or that table, is actually clearer

than proving that this formula gives a bijection!

Usually bijection is not unique: e.g.
$0, 1, 2, -1, -2, 3, 4, -3, -4, 5, 6, -5, -6, \ldots$
is just as good.

Extra element

Example

Prove that $|\{w\} \cup \mathbb{N}| = |\mathbb{N}|$.

Proof: We need a bijection: $\mathbb{N} \to \{w\} \cup \mathbb{N}$:

E.g.: $1 \to w,\ 2 \to 1,\ 3 \to 2,\ \ldots$

Or simply a sequence

$w, 1, 2, 3, \ldots,$

which clearly contains all elements of $\{w\} \cup \mathbb{N}$ exactly once.

Extra point in geometry

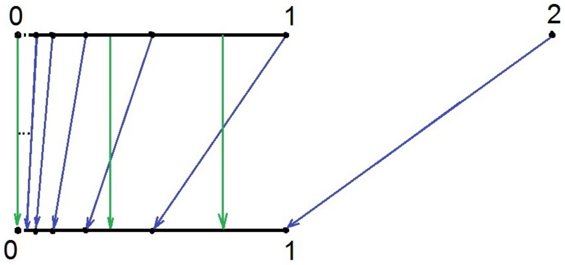
Example

Prove that $|\{2\} \cup [0,1]| = |[0,1]|$.

Proof: Idea: isolate a sequence,

which can be 'shifted' to accommodate extra point,

and all the rest send 'to itself'.



Sequence: $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$ (without 0)

Map by blue lines: $2 \to 1, \quad 1 \to \frac{1}{2}, \quad \frac{1}{2} \to \frac{1}{3}, \ldots$
and each of the other points to itself (by green arrows):

$u \to u$ for all $u \neq \frac{1}{k}$.

Bijection: injective: different to different,
surjective: all covered.

We can say: $1 + \infty = \infty$ (more precise later).

$\mathbb{Z}$ consists of 'two infinities': negative, positive

but still $\aleph_0 + \aleph_0 = \aleph_0$, as we showed above.

Infinite hotel

'Infinite hotel': rooms $1, 2, 3, \dots$

Even if all rooms are occupied, by guests $a_1, a_2, \dots$,

when one more guest arrives,

can still be accommodated:

every guest moves to the next room, so 1st room becomes available.

Now infinitely many more guests arrive $b_1, b_2, \dots$.

Can still be accommodated: a_i moves to room $2i$, so all odd numbers become free, and each b_j is given room $2j - 1$.

$|\mathbb{N} \times \mathbb{N}| = \aleph_0$

Now suppose that we have ‘infinitely many guests from each of infinitely many galaxies’, Can the infinite hotel still accommodate them all?

‘Infinitely many infinities’:

Important Example

Prove that $|\mathbb{N} \times \mathbb{N}| = \aleph_0$,

by constructing a bijection from $\mathbb{N}$

to the set of pairs $\mathbb{N} \times \mathbb{N} = \{(i, j) \mid i, j \in \mathbb{N}\}$.

(Here, (i, j) is the jth guest from the ith galaxy.)

$|\mathbb{N} \times \mathbb{N}| = \aleph_0$

Need a bijection from $\mathbb{N} \to \mathbb{N} \times \mathbb{N} = \{(i,j) \mid i,j \in \mathbb{N}\}$

Arrange the pairs in the infinite table (matrix)

$$
\begin{matrix}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) & \cdots \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{matrix}
$$

$|\mathbb{N} \times \mathbb{N}| = \aleph_0$ continued

.... and indicate a path going over this table such that all pairs are numbered in turn, without repetitions:

$$
\begin{array}{cccccccccc}
1 & \rightarrow & 2 & & 6 & \rightarrow & 7 & & 15 & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \cdots \\
3 & & 5 & & 8 & & 14 & & \cdots & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \ddots & & \\
4 & & 9 & & 13 & & \ddots & & & \\
 & \swarrow & & \nearrow & & \ddots & & & & \\
10 & & 12 & & \ddots & & & & & \\
\downarrow & \nearrow & & & & & & & &
\end{array}
$$

$|\mathbb{N} \times \mathbb{N}| = \aleph_0$ continued

$$
\begin{array}{cccccccccc}
1 & \rightarrow & 2 & & 6 & \rightarrow & 7 & & 15 & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \cdots \\
3 & & 5 & & 8 & & 14 & & \cdots & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \ddots & & \\
4 & & 9 & & 13 & & \ddots & & & \\
 & \cdots & & \cdots & & \ddots & & & &
\end{array}
$$

Meaning a mapping: $1 \to (1,1)$, $2 \to (1,2)$, $3 \to (2,1)$, $4 \to (3,1)$, $5 \to (2,2)$, $\ldots$

The whole infinite table of pairs is covered by this zig-zag path, so every pair is assigned unique number that is mapped to it. So this is a bijection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, so, $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph_0$.

Properties of countable sets

Theorem

Let A *be a countable infinite set,* $|A| = \aleph_0$.

(a) *If* $A_1 \subseteq A$, *then* A_1 *is countable (either finite, or* $|A_1| = \aleph_0$*).*

(b) *If* $B \to A$ *is an injection, then* B *is countable (either finite, or* $|B| = \aleph_0$*).*

Proof of (a):

Given $|A| = \aleph_0$ and $A_1 \subseteq A$;

need A_1 finite or $|A_1| = \aleph_0$.

We have $A = \{a_1, a_2, \dots\}$ is a sequence,

where all the a_i are different.

Going consecutively over this sequence in order,

we pick the first element that is in A_1, say, a_{i_1},

then the next in A_1, say, a_{i_2}, and so on.

If at some step there are no more elements in A_1,

then A_1 is finite.

… If this process does not stop, we obtain a representation of A_1 as a sequence $A_1 = \{a_{i_1}, a_{i_2}, a_{i_3}, \dots\}$, where all the a_{i_k} are different, because all the a_i were different.

And every element of A_1 is eventually picked, since the sequence $A = \{a_1, a_2, \dots\}$ contains all elements of $A \supseteq A_1$.

This means we have a bijection $f : \mathbb{N} \to A_1$ by the rule $f(k) = a_{i_k}$, so $|A_1| = |\mathbb{N}| = \aleph_0$. $\square$

Proof of (b): Given $|A| = \aleph_0$

and an injection $g : B \to A$; need: B is countable.

We know $g : B \to g(B)$ is a bijection onto the image,

so that $|B| = |g(B)|$,

that is, B has the same cardinality as $g(B)$.

The image $g(B) \subseteq A$ is countable by part (a).

Hence the result. □

Theorem: $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$

The set of rational numbers $\mathbb{Q}$ *is countable infinite (that is,* $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$*).*

Proof. First consider positive rational numbers $\mathbb{Q}^+$.

Every number $r \in \mathbb{Q}^+$ has a unique representation as a reduced fraction $r = m/n$ with $m, n \in \mathbb{N}$ coprime.

Then the mapping $f : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$ by the rule

$$f(m/n) = (m, n)$$

is well defined since these m, n are unique for r:

$m_1/n_1 = m_2/n_2$ with $(m_1, n_1) \neq (m_2, n_2)$ only with reduction — impossible as we only use reduced.

The mapping f is clearly injective.

Thus, we have an injective mapping $f : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$.

By Example above, $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Recall part (b) of the preceding theorem:

If $B \to A$ is injective, and $|A| = \aleph_0$,

then B is countable.

By this theorem we now have $|\mathbb{Q}^+| = \aleph_0$.

The whole of $\mathbb{Q}$:

We proved $|\mathbb{Q}^+| = \aleph_0$,

so $\mathbb{Q}^+ = \{r_1, r_2, r_3, \dots\}$ is a sequence.

Now we can write the whole $\mathbb{Q}$ as the sequence: e.g.,

$\{0, r_1, -r_1,\ r_2, -r_2,\ r_3, -r_3, \dots\}$.

All positive and all negative rationals are here.

Hence $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$. $\square$

Remark. It may seem strange that $|\mathbb{Q}| = |\mathbb{N}|$,

because $\mathbb{Q}$ is 'dense' on the real line,

while $\mathbb{N}$ consists of 'separate' points.

Indeed, if other properties are considered:

closeness, or order, or convergence of subsequences,

then $\mathbb{Q}$ and $\mathbb{N}$ are different.

But when $\mathbb{Q}$ and $\mathbb{N}$ are viewed as 'pure' ('bare') sets,

without those additional properties,

then we proved they indeed have

'the same number of elements'.

Counterintuitive fact (optional)

We know $|\mathbb{Q}| = \aleph_0$,

or $\mathbb{Q}$ can be listed as a sequence: $\mathbb{Q} = \{a_1, a_2, \dots\}$.

Cover a_1 with interval of length 1 centred at a_1,

then cover a_2 with interval of length $1/2$ centred at a_2,

then a_3 with interval of length $1/4$ centred at a_3, ...

cover a_i with interval of length $1/2^{i-1}$ centred at a_i.

As a result all rational points will be covered with nonzero length intervals.

One might think, then the whole $\mathbb{R}$ is covered by these intervals! But no: the sum of lengths is $1 + 1/2 + 1/4 + \cdots = 2$.