2.2 Proof techniques

We explore various types of proofs by observing them in action. Note that a particular statement will often have more than one proof, and these can be of very different types.

Example 2.5 (Direct proof)**.** The square of any odd integer is an odd integer.

It is essential, in the beginning, to correctly identify the shape of the mathematical statement. This can be done by rephrasing the given statement in order to put it in a more standard form (e.g. "if A then B"), without changing the meaning. For our example, this could be

If n is an odd integer, then n^2 is an odd integer.

It is also essential to know the mathematical meaning of each word in a statement. In our case, we need to remember the definition of *odd integer*: $n \in \mathbb{Z}$ is odd if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$.

Proof. let $n = 2k+1$, $k \in \mathbb{Z}$

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$, $k \in \mathbb{Z}$

$= 2(2k^2+2k) + 1 \Rightarrow n^2$ is odd.

Example 2.6. If $n \in \mathbb{Z}$ and n^2 is even, then n is even.

Proof. Suppose n is odd

then $n = 2k+1$

$n^2 = (2k+1)^2 \cdots n^2$ is odd

which contradict to "n^2 is not even"

So. if $a \in \mathbb{Z}$ and n^2 is even, then n is even

proof by contradiction

n^2 is even $\Rightarrow n$ is even

n is odd $\Rightarrow n^2$ is odd

contrapositive

Example 2.7 (Proof by contradiction)**.** $\sqrt{2} \notin \mathbb{Q}$.

This is pithy but its brevity obscures the logical content. An alternative is

$$\text{The equation } x^2 = 2 \text{ has no solution in } \mathbb{Q}.$$

or even

$$\text{There exists no } x \in \mathbb{Q} \text{ such that } x^2 = 2.$$

Proof. suppose : $x = \frac{a}{b} \in \mathbb{Q}$ such that $x^2 = 2$ ↙ in lowest term so gcd(p, q) = 1

$$x^2 = \frac{a^2}{b^2} = 2$$

$$a^2 = 2b^2$$

a^2 is even

so a is even, write $a = 2p$

$$(2p)^2 = 2b^2$$

$$4p^2 = 2b^2$$

$$2p^2 = b^2$$

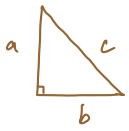
b^2 is even, b is even

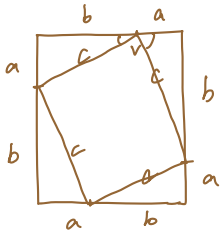
so a, b has a common divisor 2, contradict to "$\frac{a}{b}$" is in lowere

Example 2.8 (Geometric proof)**.** If a, b, c are the side lengths of a right triangle, with c the length of the side opposite the right angle, then

$$a^2 + b^2 = c^2.$$

Proof.





$$c^2 + 4 \cdot \frac{ab}{2} = (a+b)^2$$

$$c^2 + 2ab = (a+b)^2 = a^2 + b^2 + 2ab$$

exactly 2 divisor

Example 2.9 (Proof by contradiction)**.** The number of prime numbers is infinite.

Recall that $n \in \mathbb{N}$ is *prime* if it has exactly two positive divisors (namely 1 and n).

We will need a fact that we do not prove here: Every integer $n > 1$ has at least one prime divisor.

Proof. by contradiction

suppose the set of prime number is finite

$P = \{p_1, \cdots p_m\}$

let $x = p_1 p_2 \cdots p_m + 1$ Then $x > 1$ is integer

Then x has a prime divisor q $\quad qa + 1 = b$

$q \neq p_i$ for $i = 1, \cdots, m$.

$q \in P$ contradiction

2.3 Functions

utive

A *function* $f\colon A \to B$ consists of

- a set A called the *domain* of f
- a set B called the *codomain* of f
- a rule f that specifies how to map each element $a \in A$ to an element $f(a) \in B$.

Example 2.10.

$$\begin{aligned} f\colon [1,2] &\to \mathbb{R} \quad \text{given by} \quad f(x) = \frac{1}{x} \\ g\colon \text{Students} &\to \mathbb{N} \quad \text{given by} \quad g(x) = \text{ID number of } x. \end{aligned}$$

ain der of division of n by 2

r is surjective

We say that two functions $f\colon A \to B$ and $g\colon C \to D$ are *equal* if all of the following conditions are satisfied:

- Their domains are equal as sets: $A = C$.
- Their codomains are subsets of the same set: $B \subset S$, $D \subset S$.
- Their rules agree at every point of the domain: $f(x) = g(x)$ for all $x \in A$.

Example 2.11 (Three distinct functions)**.**

$$f\colon [1,2] \to \mathbb{R} \quad \text{given by} \quad f(x) = \frac{1}{x}$$
$$g\colon \mathbb{R} - \{0\} \to \mathbb{R} \quad \text{given by} \quad g(x) = \frac{1}{x}$$
$$h\colon \mathbb{R} - \{0\} \to \mathbb{R} \quad \text{given by} \quad h(x) = \log(|x|).$$

Example 2.12 (Two equal functions)**.**

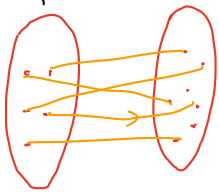
$$f\colon \mathbb{R} \to [0,\infty) \quad \text{given by} \quad f(x) = \cos^2(x)$$
$$g\colon \mathbb{R} \to [-1,1] \quad \text{given by} \quad g(x) = 1 - \sin^2(x)$$

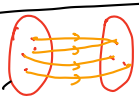
Let $f\colon A \to B$ be a function.

We say that f is *injective* if for all $x, y \in A$, if $f(x) = f(y)$ then $x = y$.

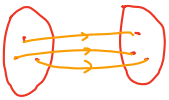
We say that f is *surjective* if for all $b \in B$, there exists $a \in A$ such that $b = f(a)$.

We say that f is *bijective* if it is both injective and surjective.





Example 2.13.



Given functions $f\colon A \to B$ and $g\colon B \to C$, we can form their *composition* $g \circ f\colon A \to C$ by

$$(g \circ f)(x) = g(f(x)) \qquad \text{for all } x \in A.$$

For any set S, there is a special function called the *identity (function) on S*. It is denoted $\mathrm{id}_S\colon S \to S$ and given by

$$\mathrm{id}_S(x) = x \qquad \text{for all } x \in S.$$

A function $f\colon A \to B$ is *invertible* if there exists a function $g\colon B \to A$ such that

$$g \circ f = \mathrm{id}_A \qquad \text{and} \qquad f \circ g = \mathrm{id}_B.$$

Challenge: Prove that if a function g as above exists, then it is unique. (The statement should remind you of something, and you need to take that argument and translate it into the world of functions.)

We are therefore justified in calling g ***the*** *inverse of f* and denoting it f^{-1}.

Proposition 2.14. A function $f\colon A \to B$ is invertible if and only if it is bijective.

Proof.

2.4 Counting

Mathematically, to count a set S means to produce a bijection between S and some "standard" set.

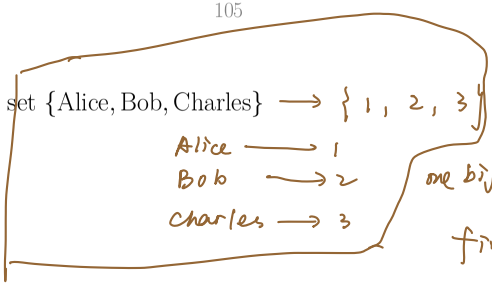
The set S is *finite* if it is empty or there exists a bijection between S and $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. If n exists, it is unique, and it is called the *cardinality (or size)* of S and denoted $\#S$.

The set S is *infinite* if it is not finite.

The set S is *countably infinite* if there exists a bijection between S and $\mathbb{N}$.

The set S is *countable* if it is finite or countably infinite.

Example 2.15. The set $\{\text{Alice}, \text{Bob}, \text{Charles}\}$



Example 2.16. The set $2\mathbb{N} = \{2k \mid k \in \mathbb{N}\} = \{2, 4, 6, \ldots\}$

Example 2.17. The set of integers $\mathbb{Z}$

$\mathbb{Z} \longrightarrow \mathbb{N}$

$n \longrightarrow 2n$ if $n > 0$

$n \longrightarrow 1-2n$ if $n \leq 0$

Claim bijection

① f injective

suppose $f(x) = f(y)$

$f(n) = \begin{cases} 2n & \text{if } n > 0 \\ -2n & \text{if } n \leq 0 \end{cases}$

if $f(x) = f(y)$ is even

$2x = 2y \Rightarrow x = y$.

let $m \in \mathbb{N}$

(a) if m is even.

$m = 2k$ for some $k \in \mathbb{N}$

$\hookrightarrow f(k) = 2k = m$

(b) if m is odd

$m = 1-2k$ for some

so $f(k) = 1-2(-k) = 1$

Theorem 2.18 (Schröder–Bernstein)**.** If A and B are sets and there exist injective functions $f\colon A \to B$ and $g\colon B \to A$, then there exists a bijection from A to B.

Corollary 2.19. The set of rational numbers $\mathbb{Q}$ is countable.

Proof. Consider the function $f\colon \mathbb{Q} \to \mathbb{Z}$ defined as follows:

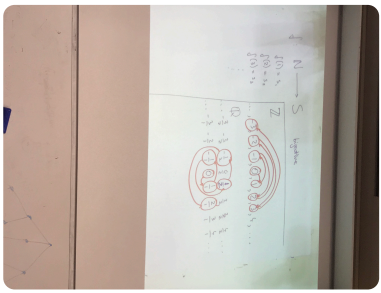
$$f(0) = 0, \qquad f(1) = 1, \qquad f(-1) = -1,$$

and, for other positive rationals in lowest terms $\frac{m}{n}$,

$$f(m/n) = 2^m(2n+1),$$

while for other negative rationals in lowest terms $-\frac{m}{n}$,

$$f(-m/n) = -2^m(2n+1).$$



Example 2.20. The set of real numbers $\mathbb{R}$ is uncountable

consider $S = \{x \in \mathbb{R} \mid x = 0, a_1, a_2, a_3 \cdots, \text{with } a_i = 0 \text{ or } 1\}$

Claim: S is uncountable

proof By contradiction, Suppose S is countable, so can ennumerate S 列举

$S_1 = 0, a_1^{(1)} \cdot a_2^{(1)} \cdot a_3^{(1)} a_4^{(1)} \cdots$

$S_2 = 0. a_1^{(2)} \cdot a_2^{(2)} a_3^{(2)} \cdot a_4^{(2)} \cdots$

$S_3 = 0. a_1^{(3)}, a_2^{(3)} a_3^{(3)} \cdot a_4^{(3)} \cdots$

$S_4 = 0. a_1^{(4)} \cdot a_2^{(4)} \cdot a_3^{(4)} \cdot a_4^{(4)}$

Cantor's dia argume

Manufacture

$x = 0. \overline{a_1^{(1)}}\ \overline{a_2^{(2)}}\ \overline{a_3^{(3)}} \cdot \overline{a_4^{(4)}} \cdots$

so $x \neq S_n$ for all $n \in \mathbb{N}$

But $x \in S$. Contradict.

S is subset to $\mathbb{R}$

$\mathbb{R}$ is uncountable

Commutative diagrams

$M_{n\times n}(\mathbb{Z}) \xrightarrow{R} M_{n\times n}(F_2)$

$\mathbb{Z} \xrightarrow{r} F_2$

Question:

is A true that

$r(\det(A)) = \det(R(A))$ for all $A \in M_{n\times n}(F_2)$

$(a,b) \in \mathbb{Z} \times \mathbb{Z} \xrightarrow{r\times r} F_2 \times F_2 \to (r(a), r(b))$

$a+b \in \mathbb{Z} \xrightarrow{r} F_2$

2.5 The principle of mathematical induction

Certain mathematical statements are actually infinite collections of statements indexed by the natural numbers, for instance:

For any $n \in \mathbb{N}$, the sum of the first n positive integers is $n(n+1)/2$.

This is made of:

$P(n)$

$1 = \frac{1(1+1)}{2}$

$1+2 = \frac{2\times 3}{2}$

$1+2+3 = \frac{(1+3)\times 3}{2} = 6$

The principle of mathematical induction I. Let $\{P(n) \mid n \in \mathbb{N}\}$ be a collection of mathematical statements. If

(a) $P(1)$ is true, and

(b) for all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

by induction on n

Base case $P(1)$ $\quad 1 = \frac{(1+1)1}{2}$ ✓

Induction step fix $k \in \mathbb{N}$

assume $P(k)$ is true

prove $P(k+1)$ is true

least element

Example 2.21. For all $n \in \mathbb{N}$ we have

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Proof.

image

The principle of mathematical induction is equivalent to the *least element property* of the natural numbers:

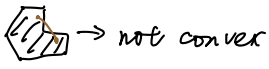
Every non-empty subset of $\mathbb{N}$ has a least element.

Proposition 2.22. If the principle of mathematical induction holds, then the least element property holds.

Proof. We first restate the least element property in a more induction-friendly way:

For all $n \in \mathbb{N}$, every subset of ~~$\mathbb{N}$ has a least element~~ $\mathbb{N}$ that contains an element $\leq n$ has a le

Example 2.23. The sum of the interior angles of an n-sided convex polygon is $(n-2)\pi$, for any $n \geq 3$.



for any two points (the line between the points) is within the

Proof.

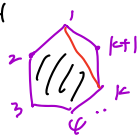
$n=3$ interior angle is $(3-2)\pi$

$\alpha+\beta+\gamma = \pi$.

induction step for $k \in \mathbb{N}$ $k \geq 3$

suppose k is true $(k-2)\pi$

for $k+1$



$(k-2)\pi + \pi$

$= (k-1)\pi$

$= (k+1-2)\pi$

so $k+1$ is true

Principle of mathematical induction II. Let $\{P(n) \mid n \in \mathbb{N}\}$ be a collection of mathematical statements. If

(a) $P(1)$ is true, and

(b) for all $k \in \mathbb{N}$, $\Big(P(1)$ and $P(2)$ and... and $P(k)\Big) \Rightarrow P(k+1)$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

This appears to be a **weaker** principle than Mathematical induction I (think about it!), but they are actually equivalent.

Example 2.24. Every integer $n \geq 2$ factors into a product of primes.

Proof. let $S = \{n \in \mathbb{Z} \mid n \geq 2$ and n is not a product of primes$\}$

To show $S = \emptyset$

suppose $S \subset \mathbb{N}$ is not $\emptyset$

By the least element property, S is a smallest element N

$N \in S$, $\rightarrow$ N is not prime

so it has a small divisor $k \in \mathbb{Z}$ $1 < k < N$ $N = k$

By minimality of N both k and $l \notin S$

Then $N = kl = p_1 \cdots p_r q_1 \cdots q_l$ contradictory to "S smalles

Example 2.25. If n is an odd integer then $n(n^2-1)$ is divisible by 24. 3×8

Proof.

n odd $\Rightarrow n = 2k+1 \quad k \in \mathbb{Z}$

$n(n^2-1) = n(n+1)(n-1)$ divisible by 8

3 consecutive integer

$\Rightarrow$ one of them is a multiple of 3

$n(n^2-1) = (2k+1)(2k+2)(2k)$

$= 4k(k+1)(2k+1)$ divisible by 3

($k+1$: multiple of 2)

since 3 and 8 don't have a common divisor

Example 2.26. For each $n \in \mathbb{N}$, the number of ways of cutting a stick of length n into pieces of integer length is 2^{n-1}.

Experiment:

$1 = 1$ $\quad 2^{1-1}$

$2 = 2$ $\quad = 1+1$ $\quad 2^{2-1}$

$3 = 3$ $\quad = 2+1$ $\quad = 1+2$ $\quad = 1+1+1$ $\quad 2^{3-1}$

$4 = 4$ $\quad = 1+3$ $\quad = 3+1$ $\quad = 2+2$ $\quad = 1+1+1+1$ $\quad = 1+1+2$ $\quad = 2+1+1$ $\quad = 1+2+1$ $\quad 2^{4-1}$

Proof.

By induction

$n = 1$

Induction step

$S(k+1) = 1 + S(1) + S(2) + \cdots + S(k)$.

suppose $S(1) \cdots S(k)$ holds that $S(k) = 2^{k-1}$

$S(k+1) = 1 + 2^{1-1} + 2^{2-1} + \cdots + 2^{k-1}$

$= 1 + \frac{2(1-2^k)}{1-2}$

$= 2^k - 1 + 1 = 2^k$

2.6 Inequalities

In addition to its arithmetic operations and their properties, the set of real numbers $\mathbb{R}$ has the structure given by the order relation denoted $a > b$. This satisfies:

(P1) If $a > 0$ and $b > 0$ then $a + b > 0$ and $ab > 0$.

(P2) For every $a \in \mathbb{R}$, exactly one of the following statements is true: $a = 0$, $a < 0$, or $a > 0$.

Example 2.27. The square of any nonzero real number is positive.

Proof.

Example 2.28. Find $n_0 \in \mathbb{N}$ such that $n^3 > (n+1)^2$ for all $n \geq n_0$.

[*Hint*: Add $3k^2 + 3k + 1$ to both sides of $k^3 > (k+1)^2$.]

Example 2.29. Find $n_0 \in \mathbb{N}$ such that $n! > n^3$ for all $n \geq n_0$.

[*Hint*: Reduce to the polynomial case by multiplying both sides of $k! > k^3$ by $(k+1)$.]

3 Vector spaces and linear transformations

3.1 Axiomatic definition of vector spaces

If you try to describe properties that are common to the spaces $\mathbb{R}^n$ that we have been working with, you may eventually end up with the following:

A *vector space V over a field $\mathbb{F}$* is a set with two operations

- addition $V \times V \to V$, $(\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} + \mathbf{v}$
- scalar multiplication $\mathbb{F} \times V \to V$, $(\lambda, \mathbf{u}) \mapsto \lambda\mathbf{u}$

satisfying the axioms

(a) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$

(b) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

(c) There exists an element $\mathbf{0} \in V$ such that $\mathbf{u} + \mathbf{0} = \mathbf{u}$.

(d) For all $\mathbf{u} \in V$ there exists an element denoted $-\mathbf{u}$ with the property that $\mathbf{u}+(-\mathbf{u}) = \mathbf{0}$.

(e) $(\lambda\mu)\mathbf{v} = \lambda(\mu\mathbf{v})$

(f) $(\lambda + \mu)\mathbf{v} = \lambda\mathbf{v} + \mu\mathbf{v}$

(g) $\lambda(\mathbf{u} + \mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v}$

(h) $1\mathbf{u} = \mathbf{u}$

Example 3.1 (Real n-dimensional space)**.** For any $n \in \mathbb{N}$, the space $\mathbb{R}^n$ is a vector space over $\mathbb{R}$.

So is $\mathbb{R}^0 = \{\mathbf{0}\}$.

Example 3.2 (Space of $m \times n$ matrices)**.**

Example 3.3 (Space of functions)**.** Fix a set S and consider

$$\mathcal{F}(S, \mathbb{R}) = \{f : S \to \mathbb{R}\}.$$

Example 3.4 (Space of polynomials)**.**

Example 3.5 (Space of polynomials of bounded degree)**.**