Introduction: naive set theory

$$\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \dots, \} \\
\mathbb{Z} &= \{0, \pm 1, \pm 2, \dots, \} \\
\mathbb{Z}_+ &= \{0, 1, 2, \dots, \} \\
\mathbb{Q} &= \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\} \\
\mathbb{C} &= \{a + bi \mid a, b \in \mathbb{R}\} \\
\mathbb{C}_q &= \{a + bi \mid a, b \in \mathbb{Q}\}
\end{aligned}$$

Recall: given sets X and Y, a relation from X to Y is a subset of $X \times Y$, where $\times$ denotes the cartesian product of X and Y.

A relation $f \subseteq X \times Y$ is a function from X to Y such that $\forall x \in X$, $\exists! y \in Y$ such that $(x, y) \in f$. We write $f(x) = y$, and denote f as $f : X \to Y$.

X is the **domain** of f and Y is the **codomain**. The range $\text{ran}(f) = \{f(x) \mid x \in X\} \subseteq Y$.

The graph of a function $\text{Graph}(f) = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$.

Examples

$$\text{id}_x : X \to X, \text{id}_X(x) = x$$

This is the identity function.

The Characteristic Function: If $A \subseteq X$

$$\mathbf{1}_A : X \to \mathbb{R},\ \mathbf{1}_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Algebra of Functions

Let X be any set, and $(X; \mathbb{R}) = \{f : X \to \mathbb{R}\}$ represent the function space of X with codomain $\mathbb{R}$.

Let $f, g \in \mathcal{F}(X; \mathbb{R})$. Then, $(f + g)(x) = f(x) + g(x)$, and $(f \cdot g)(x) = f(x) \cdot g(x)$.

If $t \in \mathbb{R}$, then $(tf)(x) = tf(x)$ (scalar multiplication). If $g(x) \neq 0 \forall x \in X$, then $\left(\frac{f}{g}\right)(x) := \frac{f(x)}{g(x)}$.

Finally, we have composition. If $f : X \to Y$ and $g : Y \to Z$ are functions, then $g \circ f(x) = g(f(x))$.

Injective, Subjective, and Bijective

A function $f : X \to Y$ is a **injective** map, then, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.For example, the shift map $S : \mathbb{N} \to \mathbb{N},\ S(n) = n + 1$ is injective.

Any strictly increasing function $f : I \to \mathbb{R}$, where I is any interval, is injective.

A function f is **surjective** if $\forall y \in Y, \exists x \in X$ such that $f(x) = y$.

Consider the function $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^3 - 2x + 1$. We can show that this function is surjective because $\lim_{x \to \infty} f(x) = \infty$, $\lim_{x \to -\infty} f(x) = -\infty$. Due to the intermediate value theorem, we get that $\text{ran}(f) = \mathbb{R}$.

f is **bijective** if it is injective and surjective.

Invertibility

Let $f : X \to Y$ be a function. f is **left-invertible** if $\exists g : Y \to X$ such that $g \circ f = \text{id}_X$. f is **right-invertible** if $\exists h : Y \to X$ such that $f \circ h = \text{id}_Y$.

f is **invertible** if $\exists k : Y \to X$ such that $f \circ k = \text{id}_Y$ and $k \circ f = \text{id}_X$.

Proposition

f is invertible if and only if f is left and right invertible.

Forward direction: This is via the definition of invertibility.

Reverse direction: Suppose g is a left-inverse of f, and h is a right-inverse of f. Therefore, $g \circ f = \text{id}_X$, and $f \circ h = \text{id}_Y$. Observe that $g = g \circ \text{id}_Y$. Therefore, $g = g \circ (f \circ h)$. Via associativity, $g = (g \circ f) \circ h = \text{id}_X \circ h = h$.

Theorem

If $f : X \to Y$ is a function:

1. f is injective $\Leftrightarrow$ f is left-invertible.
2. f is surjective $\Leftrightarrow$ f is right-invertible.
3. f is bijective $\Leftrightarrow$ f is invertible.

We will prove the first proposition in the forward direction. Suppose f is injective. Given $y \in \text{ran}(f)$, we know that $\exists! x_y \in X$ such that $f(x_y) = Y$, by the definition of injective.

Let $g : Y \to X$. We will define g as follows:

$$g(y) = \begin{cases} x_y & y \in \text{ran}(f) \\ x_0 & y \notin \text{ran}(f) \end{cases}$$

Where x_0 is an arbitrary point in X. We can see that $g \circ f = \text{id}_X$.

For example, the function $\text{Sin}(x)$ defined as $\sin(x)$ restricted to $[-\pi/2, \pi/2]$ has an inverse, $\arcsin(x) : [-1, 1] \to [-\pi/2, \pi/2]$.

Cardinality and Finitude

Which set is "larger," $\{1, 2, 3\}$ or $\{1, 2, 3, 4\}$? $\mathbb{N}$ or $\mathbb{N}_0$? $\mathbb{Z}$ or $\mathbb{Q}$?

In order to prove that one set is "the same size" as the other, we can create pairs. For two sets A and B, we can show that A is the same size as B by creating a function. For example, to show that $\mathbb{N}$ and $\mathbb{N}_0$ have the same size, we create $s : \mathbb{N} \to \mathbb{N}_0$, $s(n) = n + 1$.

Definition

Sets A and B have the same **cardinality** if $\exists$ bijection $f : A \to B$. We write $\text{card}(A) = \text{card}(B)$.

Example

Given $a < b$ and $c < d$, we know that $\text{card}([a, b]) = \text{card}([c, d])$.

We can create a linear function from $[a, b]$ to $[c, d]$, and since linear functions are bijections, we know that $\text{card}([a, b]) = \text{card}([c, d])$.

Example 2

$$\text{card}\left((0,1)\right) = \text{card}(\mathbb{R})$$

- $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$ is a bijection:
  - tan is strictly increasing (and thus injective)
  - $\lim_{x\to\infty} \tan(x) = \infty$ and $\lim_{x\to-\infty} \tan(x) = -\infty$, and by intermediate value theorem, tan is surjective
- $\ell : (0,1) \to (-\pi/2, \pi/2)$ is a bijection as it is a linear function between two intervals.
- Therefore, our bijection is $\tan \circ \ell : (0,1) \to \mathbb{R}$.

Definition

A set F is **finite** if F is empty or $\exists n \in \mathbb{N}$ such that $\text{card}(F) = \text{card}\left(\{1, 2, \dots, n\}\right)$. A non-finite set is called infinite.

We can *enumerate* F by creating a function $\sigma : \{1, 2, \dots, n\} \to F$, such that $x_j = \sigma(j)$ for $F = \{x_1, x_2, \dots, x_n\}$.

Proposition

If $m \neq n$, then $\text{card}\{1, 2, \dots, m\} = \text{card}\{1, 2, \dots, n\}$.

WLOG, suppose $m > n$.

Suppose toward contradiction that $f : \{1, 2, \dots, m\} \to \{1, 2, \dots, n\}$ is our bijection. This means there are m "pigeons" and n "holes."

One hole, j, must contain at least two pigeons (i.e., $f(i) = f(k) = j$ for some $i \neq k \in \{1, 2, \dots, m\}$). Since f is assumed to be injective, this is a contradiction.

Proposition

$\mathbb{N}$ is infinite.

Suppose toward contradiction that $\mathbb{N}$ is finite. Thus, $\exists m \in \mathbb{N}$ such that $f : \mathbb{N} \to \{1, 2, \dots, m\}$ is a bijection.

Consider the inclusion $i : \{1, 2, \dots, m+1\} \to \mathbb{N}$. i is injective.

Then, $f \circ i : \{1, 2, \dots, m+1\} \to \{1, 2, \dots, m\}$ is an injection, but by the pigeonhole principle, this cannot be. Therefore, we have reached a contradiction.

Proposition

If A is infinite, $\exists i : \mathbb{N} \hookrightarrow A$.

$\exists a_1 \in A$, as $A \neq \emptyset$.

$A \setminus \{a_1\} \neq \emptyset$, so $\exists a_2 \in A \setminus \{a_1\}$.

$A \setminus \{a_1, a_2\} \neq \emptyset$, so $\exists a_3 \in A \setminus \{a_1, a_2\}$.

$\vdots$

We thus get a sequence $\{a_1, a_2, \dots\}$ of distinct elements of A.

Consider $f : \mathbb{N} \to A$, $f(n) = a_n$. f is injective as a_n are distinct.

Example

$$\text{card}(\mathbb{Z}) = \text{card}(\mathbb{N})$$

$$f : \mathbb{Z} \to \mathbb{N}$$

$$f(m) = \begin{cases} 2m+1 & m \geq 0 \\ -2m & m < 0 \end{cases}$$

f is a bijection as $g : \mathbb{N} \to \mathbb{Z},\ g(n) = (-1)^{n+1}\left\lfloor \frac{n}{2} \right\rfloor$ is the inverse of f.

Definition

Given any set X, $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ is the **power set** of X.

$2^X := \{f \mid f : X \to \{0,1\}\}$.

Proposition

$$\text{card}(\mathcal{P}(X)) = \text{card}(2^X)$$

Let $\varphi : \mathcal{P}(X) \to 2^X$.

For $A \subseteq X$, put $\varphi(A) := \mathbf{1}_A$.

Consider $\psi : 2^X \to \mathcal{P}(X)$. $\psi(f) = f^{-1}(\{1\}) = \{x \in X \mid f(x) = 1\}$.

Then, $\psi \circ \varphi(A) = \psi(\mathbf{1}_A) = \mathbf{1}^{-1}(\{1\}) = A$,

and, we claim $\varphi(\psi(f)) = \varphi(f^{-1}(\{1\})) = \mathbf{1}_{f^{-1}(\{1\})} = f$.

Cantor's theorem

$$\nexists \text{ surjection } \mathbb{N} \to (0,1)$$

Fact from calculus: $\forall \sigma \in (0,1)$, σ can be written uniquely as a decimal expansion.

$$\sigma = \sum_{k=1}^{\infty} \frac{\sigma_k}{10^k}$$

Where $\sigma_k \in \{0,1,\dots,9\}$ and not terminating in 9s.

Suppose toward contradiction that $\exists r : \mathbb{N} \to (0,1)$ that is a surjection. Write $r(n) = 0.\sigma_1(n)\sigma_2(n)\sigma_3(n)\dots$, and $\sigma_j(n) \in \{0,1,\dots,9\}$, and not terminating in 9s.

Consider $\tau : \mathbb{N} \to \{0,1,\dots,9\}$:

$$\tau(n) = \begin{cases} 3 & \sigma_n(n) = 2 \\ 2 & \sigma_n(n) \neq 2 \end{cases}$$

Let $\tau = 0.\tau(1)\tau(2)\tau(3)\dots$. Since r is surjective, $\exists m \in \mathbb{N}$ such that $r(m) = 0.\sigma_1(m)\sigma_2(m)\dots\sigma_m(m)\dots = \tau = 0.\tau(1)\tau(2)\dots\tau(m)\dots$.

This implies that $\sigma_m(m) = \tau(m)$, which is definitionally not true, which is our contradiction.

Comparing Cardinalities

- $\text{card}(A) \leq \text{card}(B) \Rightarrow \exists f : A \hookrightarrow B$
- $\text{card}(A) < \text{card}(B) \Rightarrow \text{card}(A) \leq \text{card}(B), \text{card}(A) \neq \text{card}(B)$

For example, $X \subseteq Y \Rightarrow \text{card}(X) \leq \text{card}(Y)$ because $i : X \hookrightarrow Y, i(x) = x$ is an injection.

Transitive Property

If $\text{card}(A) \leq \text{card}(B) \leq \text{card}(C)$, then $\text{card}(A) \leq \text{card}(C)$.

The composition of two injective functions is injective.

Canonical Set Comparisons

Via the inclusion map, we know the following:

$$\text{card}(\mathbb{N}) \leq \text{card}(\mathbb{Z}) \leq \text{card}(\mathbb{Q}) \leq \text{card}(\mathbb{R})$$

Cantor-Schröder-Bernstein

For any set A, $\text{card}(A) < \text{card}(\mathcal{P}(A))$.

Let us construct a function: $f : A \to \mathcal{P}(A)$, where $a \mapsto \{a\}$.

f is injective, as if $\{a\} = \{a'\}$, $a = a'$. So, $\text{card}(A) \leq \text{card}(\mathcal{P}(A))$.

Claim $\nexists g : A \to \mathcal{P}(A)$, g is surjective.

Suppose toward contradiction that such a g exists. Consider $S : \{a \in A \mid a \notin g(a)\}$.

Since g is onto, $\exists a_0 \in A$ with $g(a_0) = S$. $a_0 \in g(a_0) \Leftrightarrow a_0 \in S \Leftrightarrow a_0 \notin g(a_0)$. $\perp$

Equivalent Propositions

(i) $\text{card}(A) \leq \text{card}(B)$

(ii) $\exists f : A \hookrightarrow B$

(iii) $\exists g : B \to A$, g surjection.

By definition, (i) $\Leftrightarrow$ (ii).

(ii) $\Rightarrow$ (iii) If $f : A \hookrightarrow B$, f is left-invertible, and thus $\exists g : B \to A$ with $g \circ f = id_A$. So, g is right-invertible, so g is surjective.

(iii) $\Rightarrow$ (ii) If $g : B \to A$ is surjective, then g is right-invertible, so $\exists f : A \to B$ such that $g \circ f = id_B$. So, f is left-invertible, so f is injective.

Corollary

If $f : A \to B$ is any map, $\text{card}(f(A)) \leq \text{card}(A)$.

Consider $g : A \to f(A)$, where $g(a) = f(a)$. So, g is onto, so $\exists$ an injection $f(A) \hookrightarrow A$.

More Cardinality of Canonical Sets

Consider the map $q : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}, q(m,n) = \frac{m}{n}$. This map is *not* injective, as $2/4 = 1/2$. However, it is surjective, meaning $\text{card}(\mathbb{Q}) \leq \text{card}(\mathbb{Z} \times \mathbb{N})$.

Earlier, we showed that $\exists h : \mathbb{Z} \leftrightarrow \mathbb{N}$. Consider $H : \mathbb{Z} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, defined as $H(m,n) = (h(m), n)$.

Claim H is a bijection.

Proof of Injection If $H(m_1, n_1) = H(m_2, n_2)$, then $h(m_1) = h(m_2)$, and $n_1 = n_2$, and since h is bijective, $m_1 = m_2$, and $n_1 = n_2$, so $(m_1, n_1) = (m_2, n_2)$.

Proof of Surjection Let $(k, \ell) \in \mathbb{N} \times \mathbb{N}$. We want to find $(m,n) \in \mathbb{Z} \times \mathbb{N}$ such that $H(m,n) = (k, \ell)$. Set $n = \ell$, and since h is surjective, set $m \in \mathbb{Z}$ such that $h(m) = k$.

Therefore $\text{card}(\mathbb{Z} \times \mathbb{N}) = \text{card}(\mathbb{N} \times \mathbb{N})$.

We claim that $\text{card}(\mathbb{N} \times \mathbb{N}) = \text{card}(\mathbb{N})$. First, we need to find $\varphi : \mathbb{N} \times \mathbb{N} \hookrightarrow \mathbb{N}$. Consider $\varphi(m,n) = 2^m \cdot 3^n$. By the Fundamental Theorem of Arithmetic, φ is injective.

Bringing together our inequalities, we have:

$$\begin{aligned}
\text{card}(\mathbb{N}) &\leq \text{card}(\mathbb{Q}) \\
&\leq \text{card}(\mathbb{Z} \times \mathbb{N}) \\
&= \text{card}(\mathbb{N} \times \mathbb{N}) \\
&\leq \text{card}(\mathbb{N})
\end{aligned}$$

Cardinality Rules

(i) $\text{card}(A) \leq \text{card}(A)$ (Reflexivity)

(ii) $\text{card}(A) \leq \text{card}(B) \leq \text{card}(C) \Rightarrow \text{card}(A) \leq \text{card}(C)$ (Transitivity)

(iii) $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(B) \leq \text{card}(A) \Rightarrow \text{card}(A) = \text{card}(B)$ (Cantor-Schröder-Bernstein)

(iv) Either $\text{card}(A) \leq \text{card}(B)$ or $\text{card}(B) \leq \text{card}(A)$.

Proof of (iii) We have injections $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$.

Let $A_0 \setminus \text{ran}(g)$. Let $A_1 = g \circ f(A_0)$. Note that $A_0 \cap A_1 = \emptyset$. Let $A_2 = g \circ f(A_1)$. Note that $A_0 \cap A_2 = \emptyset$.

Claim We claim $A_1 \cap A_2 = \emptyset$. If $\exists z \in A_1 \cap A_2$, then $z = g(f(x_0))$ for some $x_0 \in A_0$, and $z = g(f(x_1))$ where $x_1 \in A_1$. However, g and f are injective, so $g \circ f$ is injective, so $x_0 = x_1$, but $A_0 \cap A_1$. $\perp$

We let $A_n = g \circ f(A_{n-1})$ for arbitrary n, and $A_\infty = \bigcup_{n\geq 0} A_n$. If $a \notin A_\infty$, then $a \notin A_0$, so $a \in \text{ran}(g)$. Define $h : A \to B$.

$$h(x) = \begin{cases} f(x) & x \in A_\infty \\ y_x & x \notin A_\infty \end{cases}$$

Where y_x is the unique element in B with $g(y_x) = x$.

Claim We claim h is the desired bijection.

Proof of Injection Suppose $h(x_1) = h(x_2)$.

If $x_1, x_2 \in A_\infty$, then by the definition of H, $f(x_1) = f(x_2)$, f is injective, so $x_1 = x_2$.

Suppose $x_1, x_2 \notin A_\infty$. Then, by definition, $h(x_1) = y_{x_1}$ and $h(x_2) = y_{x_2}$, then $g(y_{x_1}) = g(y_{x_2})$, so $x_1 = x_2$.

WLOG, suppose $x_1 \in A_\infty$, and $x_2 \notin A_\infty$. $h(x_1) = f(x_1) = h(x_2) = y_{x_2}$. Then, $g(f(x_1)) \in A_\infty = g(y(x_2)) = x_2 \notin A_\infty$. This case is not possible.

Thus, h is injective.

Proof of Surjection Let $y \in B$. Set $x := g(y)$.

Suppose $x \notin A_\infty$. Then, $h(x) = y_x$, where y_x is the unique element in B with $g(y_x) = x = g(y)$, so $y = y_x$, so $h(x) = y$.

If $x \in A_\infty$. We know that $x \notin A_0$, as $x \in \text{ran}(g)$. So, $x = g(f(z))$ for some $z \in A_{m-1}$. Since g is injective, $y = f(z)$, $z \in A_\infty$. Thus, $h(z) = f(z) = y$.

Therefore, we have $\text{card}(\mathbb{Q}) = \text{card}(\mathbb{N})$.

Countability

A set X is *countable* if $\exists f : x \hookrightarrow \mathbb{N}$ ($\text{card}(X) \leq \text{card}(\mathbb{N})$). $\text{card}(\mathbb{N}) = \aleph_0$. If X is countable and infinite, X is *denumerable*.

Corollary to Cantor-Schröder-Bernstein

If X is denumerable, then $\text{card}(X) = \aleph_0$.

Since X is infinite, $\exists f : \mathbb{N} \hookrightarrow X$. Since X is countable, $\exists g : X \hookrightarrow \mathbb{N}$. By Cantor-Schröder-Bernstein, $\text{card}(X) = \text{card}(\mathbb{N})$, so $\text{card}(X) = \aleph_0$.

Thus, we have:

$$\text{card}(\mathbb{N}) = \text{card}(\mathbb{Z}) = \text{card}(\mathbb{Q})$$

(as shown earlier)

Countability under Union

The countable union of countable sets is countable. If I is a countable indexing set and for each $i \in I$, A_i is countable, then $\bigcup\limits_{i\in I} A_i$ is countable.

Since each A_i is countable, $\exists \pi_i : \mathbb{N} \twoheadrightarrow A_i$. Consider the function

$$\pi : I \times \mathbb{N} \to \bigcup_{i\in I} A_i$$

defined as $\pi(i,j) = \pi_i(j)$.

Claim 1 π is a surjection.

Proof 1 Let $x \in \bigcup_{i\in I} A_i$. $\exists i_0$ such that $x \in A_{i_0}$. Since π_{i_0} is surjective, $\exists k \in \mathbb{N}$ with $\pi_{i_0}(k) = x$. $\pi_{i_0}(k) = \pi(i_0, k)$. Therefore, π is surjective.

Claim 2 $I \times \mathbb{N}$ is countable.

Proof 2 We know $\exists f : I \hookrightarrow \mathbb{N}$ since I is countable. Thus, $g : I\times\mathbb{N} \hookrightarrow \mathbb{N}\times\mathbb{N}$, $(i,n) \mapsto (f(i), n)$. Recall, $\mathbb{N}\times\mathbb{N} \hookrightarrow \mathbb{N}$, $(m,n) \mapsto 2^m \cdot 3^n$ is an injection. By composing these maps, $I\times\mathbb{N} \hookrightarrow \mathbb{N}$. Since π is onto, and $I \times \mathbb{N}$ is countable, $\bigcup_{i\in I} A_i$ is countable.

Continuum Hypothesis

We saw that $\text{card}(\mathbb{N}) < \text{card}(\mathcal{P}(\mathbb{N})) = \text{card}(2^{\mathbb{N}})$, where $2^{\mathbb{N}}\{f \mid f : \mathbb{N} \to \{0,1\}\}$.

Theorem $\text{card}(\mathbb{R}) = \text{card}(I) = \text{card}(2^{\mathbb{N}})$, where I is any non-degenerate interval.

Lemma 1 $\text{card}([0,1]) \leq \text{card}(2^{\mathbb{N}})$.

Proof 1 Every $t \in [0,1]$ has a binary expansion.

$$t = \sum_{k=1}^{\infty} \frac{\sigma_k}{2^k}$$

where $\sigma_k \in \{0,1\}$.

Consider $2^{\mathbb{N}} \xrightarrow{\varphi} [0,1]$, defined as $\phi(f) = \displaystyle\sum_{k=1}^{\infty} \frac{f(k)}{2^k}$. Set $f : \mathbb{N} \to \{0,1\}$, $f(k) = \sigma_k$.

Therefore, φ is surjective, so $\exists\{0,1\} \hookrightarrow 2^{\mathbb{N}}$, so $\text{card}([0,1]) \leq 2^{\mathbb{N}}$

Lemma 2 $\text{card}([0,1]) = \text{card}(\mathbb{R})$.

Proof 2 We have $[0,1] \overset{i}{\hookrightarrow} \mathbb{R}$ via inclusion, so $\text{card}([0,1]) \leq \text{card}(\mathbb{R})$.

Also, $\text{card}(\mathbb{R}) = \text{card}((0,1)) \leq \text{card}([0,1])$, so by Cantor-Schröder-Bernstein, $\text{card}(\mathbb{R}) = \text{card}([0,1])$.

Lemma 3 Any two non-degenerate intervals I and J have the same cardinality.

Proof 3 We can create injections $I \hookrightarrow J$ and vice-versa.

Lemma 4 $\text{card}(2^{\mathbb{N}}) \leq \text{card}([0,1])$.

Proof 4 $\psi : 2^{\mathbb{N}} \to [0,1]$. Where $\psi(f) = \sum_{k=1}^{\infty} \frac{f(k)}{3^k}$.

ψ is well-defined:

$$0 \leq \sum_{k=1}^{\infty} \frac{f(k)}{3^k} \leq \sum_{k=1}^{\infty} \frac{1}{3^k} \leq \frac{1}{2} \leq 1$$

We claim ψ is injective. Suppose $f \neq g$ in $2^{\mathbb{N}}$. Let $k_0 = \min\{k \mid f(k) \neq g(k)\}$. WLOG, $f(k_0) = 0, g(k_0) = 1$. Let $t_f = \sum_{k>k_0}^{\infty} \frac{f(k)}{3^k}$, $t_g = \sum_{k>k_0}^{\infty} \frac{g(k)}{3^k}$.

Therefore, $\psi(f) = \sum_{k=1}^{k_0-1} \frac{f(k)}{3^k} + 0 + t_f$, and $\psi(g) = \sum_{k=1}^{k_0-1} + \frac{1}{3^{k_0}} + t_g$.

Suppose toward contradiction $\psi(f) = \psi(g)$. Then, $t_f = \frac{1}{3^{k_0}} + t_g$, or $t_f - t_g = \frac{1}{3^{k_0}}$.

$$\begin{aligned}|t_f - t_g| &= |\sum_{k>k_0} \frac{f(k)}{3^k} - \sum_{k>k_0} \frac{g(k)}{3^k}| \\ &\leq \sum_{k>k_0} \frac{|f(k) - g(k)|}{3^k} \\ &\leq \sum_{k>k_0} \frac{1}{3^k} \\ &= \frac{(1/3)^{k_0+1}}{1-(1/3)} \\ &= \frac{1}{2} \cdot \frac{1}{3^{k_0}}\end{aligned}$$

$\perp$

We have thus shown:

$$\text{card}(\mathbb{R}) = \text{card}([0,1]) = \text{card}(2^{\mathbb{N}})$$

We know that

$$\aleph_0 = \text{card}(\mathbb{N}) = \text{card}(\mathbb{Q}) = \text{card}(\mathbb{Z}) < 2^{\aleph_0} = \text{card}(2^{\mathbb{N}}) = \text{card}(\mathbb{R}) = \text{card}(I)$$

However, the existence of an infinity with cardinality strictly greater than $\aleph_0$ and strictly less than $2^{\aleph_0}$ is an axiom (i.e., it can be an assumption or not).

Ordering

Let X be a non-empty set. A relation on X is a subset of $X \times X$.

- R is *reflexive* if $\forall x \in X,\ (x, x) \in R$.
- R is *transitive* if $(x, y), (y, z) \in R \to (x, z) \in R$.
- If R is *antisymmetric* $(x, y), (y, x) \in R \to x = y$.

If R is reflexive, transitive, and antisymmetric, then R is an *ordering* of X.

If R is an ordering of X, then we write:

$$(x, y) \in R \Leftrightarrow xRy \Leftrightarrow x \leq_R y$$

- $x \leq_R x\ \forall x \in X$
- $x \leq_R y,\ y \leq_R z \to x \leq_R z$
- $x \leq_R y,\ y \leq_R x \to x = y$

Additionally, $x <_R y$ means $x \leq_R y$ and $x \neq y$.

Algebraic ordering of $\mathbb{N}_0$

$n \leq_a m \Leftrightarrow \exists k \in \mathbb{N}_0$ such that $n + k = m$

$\mathbb{N}$ ordered via division

$$n \leq_D m \Leftrightarrow n|m$$

Under this definition, it is false that $2 \leq_D 5$, but it is true that $4 \leq_D 20$.

Inclusion Let S be any set, and let $X = \mathcal{P}(S)$. For $A, B \in \mathcal{P}(S)$, we define $A \leq_i B \Leftrightarrow A \subseteq B$.

Containment With X defined as above, $A \leq_c B \Leftrightarrow A \supseteq B$.

For $\mathcal{F}(X, \mathbb{R}) = \{f \mid f : X \to \mathbb{R}\}$, we can define $f \leq g \Leftrightarrow f(x) \leq g(x)\ \forall x \in X$.

Types of Orderings

- An ordering $\leq$ of X is *total* or *linear* if $\forall x, y \in X, x \leq y$ or $y \leq x$.
- An ordering is *directed* if $\forall x, y \in X\ \exists z \in X$ such that $x \leq z$ and $y \leq z$.

If X is a totally ordered set, X is directed.

For example, all the following orderings are directed but not total:

$$(\mathbb{N}_0, \leq_D),\ (\mathcal{P}(S), \leq_i),\ (\mathcal{P}(S), \leq_c)$$

Upper/Lower Bounds

(i) Let $(X, \leq)$ be an ordered set, $A \subseteq X$. A is bounded above if $\exists v \in X$ with $a \leq v\ \forall a \in A$. Such a v is an upper bound.

(ii) A is bounded below if $\exists \ell \in X$ such that $a \geq \ell\ \forall a \in A$. Such a w is a lower bound.

(iii) If v is an upper bound of A and $v \in A$, then v is the greatest element of A, or $\max(A) = v$.

(iv) If ℓ is a lower bound for A and $\ell \in A$, then ℓ is the least element of A, or $\min(A) = \ell$.

(v) If u is an upper bound for A, and $u \leq v$ for all other upper bounds v of A, then u is the *least upper bound* of A, or $\sup(A) = u$ (for *supremum*).

(vi) If ℓ is a lower bound for A, and $\ell \leq g$ for all other lower bounds g of A, then ℓ is the *greatest lower bound* of A, or $\inf(A) = \ell$ (for *infimum*).

(vii) If A is bounded above and below, then A is bounded.

Well-Ordering Principle

With $(\mathbb{N}, \leq_a)$, every nonempty $A \subseteq \mathbb{N}$ has a least element.

Examples

Example 1

For $A \subseteq (\mathbb{N}, \leq_a)$, $A = \{2, 3, \dots, 12\}$, we have the following:

Bounded Above? Yes.

Upper Bounds $12, 13, 14, \dots$

Greatest Element 12

Example 2

For $A \subseteq (\mathbb{N}, \leq_D)$, $A = \{2, 3, \dots, 10\}$

Bounded Above? Yes.

Upper Bounds $10!$

Greatest Element? No.

Supremum $2^3 \cdot 3^2 \cdot 5 \cdot 7$

Bounded Below? Yes.

Lower Bound 1

Least Element? No.

Infimum 1

Example 3

For $\mathcal{A} \subseteq (\mathcal{P}(S), \leq_i)$, $A = \{A_i\}_{i \in I} \subseteq \mathcal{P}(S)$.

Supremum $\bigcup_{i \in I} A_i$

Infimum $\bigcap_{i \in I} A_i$

Complete Sets

An ordered set $(X, \leq)$ is *complete* if for all $A \subseteq X$ bounded, $\inf(A)$ and $\sup(A)$ exist.

For example, $\mathbb{Q}$ is *not* complete, as there is not a largest rational number less than $\sqrt{2}$, for example.

Ordering of $\mathbb{Z}$

$$n \leq_a m \Leftrightarrow \exists k \in \mathbb{N}_0,\ n + k = m$$

This defines a total and complete ordering.

Define $\mathbb{Z}^+ = \{m \in \mathbb{Z} \mid 0 \leq_a m\}$

Properties of $\mathbb{Z}^+$

(i) $m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}^+,\ m \cdot n \in \mathbb{Z}^+$

(ii) $m \in \mathbb{Z}$, then $m \in \mathbb{Z}^+$ or $-m \in \mathbb{Z}^+$

(iii) $m, -m \in \mathbb{Z}^+$, then $m = 0$

(iv) $m \leq_a n \Leftrightarrow n - m \in \mathbb{Z}^+$

Ordering of $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

Recall the ordering of $\mathbb{Z}$:

$$n \leq_a m \overset{\text{def}}{\Longleftrightarrow} \exists k \in \mathbb{N}_0 \text{ with } n + k = m$$

Claim $\leq_a$ is an ordering of $\mathbb{Z}$

We claim that $\mathbb{Z}^+ = \{m \in \mathbb{Z} \mid 0 \leq_a m\}$. Thus, $\mathbb{Z}^+ = \mathbb{N}_0$.

Properties of $\mathbb{Z}^+$

(i) $m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}^+,\ m \cdot n \in \mathbb{Z}^+$

(ii) $m \in \mathbb{Z}$, then $m \in \mathbb{Z}^+$ or $-m \in \mathbb{Z}^+$

(iii) $m, -m \in \mathbb{Z}^+$, then $m = 0$

(iv) $m \leq_a n \Leftrightarrow n - m \in \mathbb{Z}^+$

Other Properties of $\mathbb{Z}$

(1) $n \leq_a m \Leftrightarrow m - n \in \mathbb{Z}^+$

(2) $m \leq_a n$ and $p \leq_a q \Rightarrow m + p \leq_a n + q$

(3) $m \leq_a n$ and $p \in \mathbb{Z}^+ \Rightarrow pm \leq_a pn$

(4) $m \leq_a n \Rightarrow -m\ {}_a{\geq} n$

(5) $\leq_a$ is total.

(6) If $a\ {}_a{>}{-}$, and $ab\ {}_a{\geq}0$, then $b\ {}_a{>}0$

(7) If $a > 0$ and $ab\ {}_a{\geq}ac$, then $b \geq c$.

Proof of (3):
$m \leq_a n \Rightarrow \exists k \in \mathbb{N}_0$ with $m + k = n$.
$\Rightarrow pm + pk = pn$
$pk \in \mathbb{N}_0$ by the properties of $\mathbb{Z}^+$. So, $pm \leq_a pn$

Proof of (5):
Let $m, n \in \mathbb{Z}$. Consider $m - n$.
By (ii), $m - n \in \mathbb{Z}^+$ or $-(m - n) \in \mathbb{Z}^+$. Thus, $m - n = k$ for some $k \in \mathbb{Z}^+$, or $-(m - n) = \ell$ for some $\ell \in \mathbb{Z}^+$.
Thus, $n \leq_a m$ in the first case, or $m \leq_a n$ in the second case.

We now want an ordering on Q.

Creating the Rationals

Recall that $Q = \mathbb{Z} \times \mathbb{Z}^* = \{(a,b) \mid a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0\}$. Consider the equivalence relation:

$$(a,b) \sim (c,d) \overset{\text{def}}{\Longleftrightarrow} ad = bc$$

We will let $\mathbb{Q} = \{[(a,b)] \mid (a,b) \in Q\}$ be the set of all equivalence classes in Q. We write:

$$[(a,b)] = \frac{a}{b}$$

We define addition as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

We must check that addition is well-defined: $\frac{a'}{b'} = \frac{a}{b}$ and $\frac{c'}{d'} = \frac{c}{d}$, then $\frac{a'd'+c'b'}{b'd'} = \frac{ad+bc}{bd}$.

We define multiplication as follows:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

These operations make $\mathbb{Q}$ a **field**:

Fields

A ring is a nonempty set set R equipped with two binary operations:

- $+ : R \times R \to R$, $(a,b) \mapsto a+b$ (“addition”)
- $\cdot : R \times R \to R$, $(a,b) \mapsto a \cdot b$ (“multiplication”)

such that the following hold:

(1) $(a+b)+c = a+(b+c)$

(2) $\exists z \in R$ such that $a+z = a = z+a\ \forall a \in R$; there is at most one such z. Set $z = 0_R$.

(3) $\forall a \in R, \exists b \in R$ such that $a+b = 0_R = b+a$; there is at most one such b. Set $b = -a$.

(4) $\forall a,b \in R,\ a+b = b+a$.

(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(6) $a \cdot (b+c) = a \cdot b + a \cdot c$, $(a+b) \cdot c = a \cdot c + b \cdot c$

The above six rules define a ring. If $(R,+,\cdot)$ satisfies $ab = ba$, R is a commutative ring.

If there exists $u \in R$ such that $ua = au = a\ \forall a \in R$, R is a unital ring; there is at most one unit. Set $u = 1_R$

An integral domain is a unital, commutative ring such that $ab = 0 \Rightarrow a = 0 \vee b = 0$. For example, $\mathbb{Z}$ is an integral domain. However, $c(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continuous}\}$ is a unital, commutative ring, but there exist two functions such that $f, g \neq \mathbf{0}$, but $f \cdot g = \mathbf{0}$.

A field is a unital, commutative ring such that every element has a multiplicative inverse.

$$\forall a \in R, a \neq 0_R, \exists b \in R, \text{ with } ab = 1_R$$

There is only one such b. Set $b = a^{-1}$.

Proof that $\mathbb{Q}$ is a Field:

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

Provided that $\frac{a}{b} \neq 0_{\mathbb{Q}}$.

Additionally, $\mathbb{Z} \overset{j}{\hookrightarrow} \mathbb{Q}$, $j(n) = \frac{n}{1}$ is injective.

Ordering of $\mathbb{Q}$

$$\frac{a}{b} \leq_a \frac{c}{d} \Leftrightarrow ad \leq_a bc \in \mathbb{Z}$$

Prove that this ordering is well-defined.

Order Embedding

$\leq$ is a well-defined total ordering of $\mathbb{Q}$, and $j : \mathbb{Z} \hookrightarrow \mathbb{Q}$, $j(n) = \frac{n}{1}$ is an order embedding.

$$j(n) \leq j(m) \Leftrightarrow n \leq_a m \in \mathbb{Z}$$

Properties of $\mathbb{Q}^+$

$$\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q \geq 0_{\mathbb{Q}}\}$$

(i) $q_1, q_2 \in \mathbb{Q}^+ \Rightarrow q_1 + q_2 \in \mathbb{Q}^+$, $q_1 q_2 \in \mathbb{Q}^+$

(ii) $q \in \mathbb{Q} \Rightarrow q \in \mathbb{Q}^+ \vee -q \in \mathbb{Q}^+$

(iii) $\pm q \in \mathbb{Q}^+, q = 0$

(iv) $x \leq y, !u \leq v \Rightarrow x + u \leq y + v$

(v) $x \leq y,\ 0 \leq z \Rightarrow zx \leq zy$

Ordering of $\mathbb{R}$, cont'd

An **ordered field** is a field F equipped with a total ordering $\leq_F$ such that:

(i) if $s \leq_F t$, and $x \leq_F y$, then $s + x \leq_F t + y$

(ii) if $s \leq_F t$ and $0 \leq_F z$, then $zs \leq_F zt$

For example, $\mathbb{Q}$ with its ordering is an ordered field.

Proposition 1: If $(F, \leq_F)$ is an ordered field, we define $F^+ = \{x \in F, x\ {}_F{\geq} 0\}$ with the following properties:

(1) $x, y \in F^+ \Rightarrow x + y \in F^+, xy \in F^+$

(2) $x \in F \Rightarrow x \in F^+, -x \in F^+$

(3) $\pm x \in F^+ \Rightarrow x = 0_F$

Proofs

(1) Let $x, y \in F^+$. Then, $x \geq 0$ and $y \geq 0$, so by property (i) of an ordered field, $x + y \geq 0 + 0 = 0$, so $x + y \in F^+$. Additionally, we have $x \cdot y \geq x \cdot 0 = 0$, so $xy \in F^+$.

(2) Let $x \in F$. Since the ordering on F is total, $x \geq 0$ or $0 \geq x$. In the first case, $x \in F^+$. In the second case, we add $-x$ to both sides, so by (i), $-x \geq 0$, so $-x \in F^+$.

(3) We have $x \geq 0$ and $-x \geq 0$. So $x \geq 0$ and $x + (-x) \geq x + 0$, so $x \geq 0$ and $0 \geq x$. So, $x = 0$ by antisymmetry.

Note: $x \leq_F y \Leftrightarrow y - x \in F^+$.

Proposition 2: Let F be an ordered field. Then, the following is true:

(1) $\forall a \in F$, $a^2 \in F^+$

(2) $0, 1 \in F^+$

(3) If $n \in \mathbb{N}$, $n \cdot 1_F = \underbrace{1_F + 1_F + \cdots + 1_F}_{n \text{ times}}$

(4) If $x \in F^+$, and $x \neq 0$, then $x^{-1} \in F^+$

(5) If $xy > 0$, then $x, y \in F^+$, or $-x, -y \in F^+$

(6) If $0 < x \leq y$, then $0 < y^{-1} \leq x^{-1}$

(7) If $x \leq y$, then $-y \leq -x$

(8) $x \geq 1 \Rightarrow x^2 \geq x \geq 1$, and $0 \leq x \leq 1 \Rightarrow 0 \leq x^2 \leq x \leq 1$.

Proofs

(1) Let $a \in F$. Then, $a \in F^+$ or $-a \in F^+$.

Case 1 If $a \in F^+$, then by the previous proposition, $a^2 \in F^+$.

Case 2 If $-a \in F^+$, then by the previous proposition, $(-a)(-a) = a^2 \in F^+$.

(2) $0 \geq 0$, so $0 \in F+$. $1 = 1 \cdot 1 = 1^2 \in F^+$ by the previous result.

(3) $n \cdot 1_F = \underbrace{1_F + 1_F + \cdots 1_F}_{n \text{ times}} \in F^+$ by the previous proposition.

(4) Let $x \neq 0, x \in F^+$. Suppose toward contradiction that $x^{-1} \notin F^+$, then $-x^{-1} \in F^+$. Thus, $x \cdot (-x^{-1}) \in F^+$, so $-1 \in F^+$, but $1 \in F^+$, so $1 = 0$. $\perp$

(5) Let $xy > 0$, meaning $xy \in F^+$. Suppose toward contradiction that $x > 0$ and $y < 0$. So, $x > 0$ and $-y > 0$, so $(x)(-y) > 0$, so $-(xy) \in F^+0$, so $xy = 0$. $\perp$

(6) Let $0 < x \leq y$. We know $x^{-1} \in F^+$, so $x^{-1}x \leq x^{-1}y$. So $1 \leq x^{-1}y$. We also know $y \in F^+$, so $y^{-1} \in F^+$. So, $1 \cdot y^{-1} \leq x^{-1} \cdot y \cdot y^{-1}$.

(7) Let $x \leq y$. Then, $0 \leq y - x$, so $-y \leq -x$.

(8) Let $x \geq 1$. Then, $x \cdot x \geq 1 \cdot x \geq 1$.

Order Axiom

$\mathbb{R}$ is an ordered field. The injection $\mathbb{Q} \hookrightarrow \mathbb{R}$, $i(q) = q$ is an order embedding.

Rational Orderings

Proposition 1: If $a \leq b$, then $a \leq \frac{1}{2}(a+b) \leq b$

Proof

$2a = a + a \leq a + b \leq b + b$, all by property (i) of an ordered field.

Therefore, $2a \leq a + b \leq 2b$. Since $2 = 1 + 1 \in \mathbb{R}^+$, $2^{-1} \in \mathbb{R}^+$, so $(2a)/2 \leq \frac{1}{2}(a+b) \leq (2b)/2$, so $a \leq \frac{1}{2}(a+b) \leq b$.

Proposition 2: If $a \geq 0$ and $(\forall \varepsilon > 0), a \leq \varepsilon$.

Proof

If $a \geq 0$ and $a \neq 0$, then $a > 0$. So, we have that $\frac{1}{2}a < a$. Let $\varepsilon = \frac{1}{2}a$. We also have that $a \leq \varepsilon = \frac{1}{2}a < a$, so $a < a$. $\perp$

Arithmetic and Geometric Means

Given $a_1, a_2, \dots, a_n \in \mathbb{R}^+$:

Arithmetic Mean

$$= \frac{\sum_{i=1}^{n} a_i}{m}$$

Geometric Mean

$$= \sqrt[m]{a_1 a_2 \cdots a_m}$$

Arithmetic Mean-Geometric Mean Inequality

Let $a, b \geq 0$.

$$(ab)^{1/2} \leq \frac{1}{2}(a+b)$$

If $x, y \geq 0$, $x \leq y \Leftrightarrow x^2 \leq y^2$.

$$0 \leq x \cdot x \leq x \cdot y \leq y \cdot y \qquad \text{by property (ii) of ordered fields}$$

Therefore,

$$\begin{aligned}
(ab)^{1/2} &\leq \frac{1}{2}(a+b) \\
ab &\leq \frac{1}{4}(a^2 + 2ab + b^2) \\
4ab &\leq a^2 + 2ab + b^2 \\
0 &\leq a^2 - 2ab + b^2 \\
0 &\leq (a-b)^2 && \text{by definition}
\end{aligned}$$

Challenge: Prove for m.

Remark: The harmonic mean is defined as:

$$\frac{n}{\displaystyle\sum_{i=1}^{n} \frac{1}{a_i}}$$

Bernoulli's Inequality

If $x \geq -1$, then $(1+x)^n \geq 1 + nx$, for any $n \in \mathbb{N}_0$

By induction, we know that for $n = 0$ and $n = 1$, this holds.

Assume the inequality holds for some $m \geq 1$.

$$\begin{aligned}
(1+x)^{m+1} &= (1+x)^m(1+x) \\
&\geq (1+mx)(1+x) && \text{by the inductive hypothesis} \\
&= 1 + x + mx + mx^2 \\
&= 1 + (m+1)x + mx^2 \\
&\geq 1 + (m+1)x
\end{aligned}$$

Cauchy's Inequality

Let $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}$. Then

$$\left|\sum_{j=1}^{n} a_j b_j\right| \leq \left(\sum_{j=1}^{n} a_j^2\right)^{1/2} \left(\sum_{j=1}^{n} b_j^2\right)^{1/2}$$

In linear algebra language, this is equivalent to $\vec{v} \cdot \vec{w} \leq \|\vec{v}\| \cdot \|\vec{w}\|$.

Consider $f : \mathbb{R} \Rightarrow \mathbb{R}$

$$f(x) = \sum_{i=1}^{n} (a_j - b_j x)^2$$

We know that $f(x) \geq 0$ for all $x \in \mathbb{R}$

$$\begin{aligned}
&= \sum_{i=1}^{n} (a_j^2 - 2a_j b_j x + b_j^2 x^2) \\
&= \left(\sum_{j=1}^{n} b_j^2\right) x^2 + \left(\sum_{j=1}^{n} -2a_j b_j\right) x + \sum_{j=1}^{n} a_j^2 \\
&= Ax^2 + Bx + C
\end{aligned}$$

Therefore, $\Delta = B^2 - 4AC \leq 0 \Rightarrow B^2 \leq 4AC$

$$\left(-2\sum_{j=1}^{n} a_j b_j\right)^2 \leq 4\left(\sum_{j=1}^{n} a_j\right)\left(\sum_{j=1}^{n} b_j\right)$$
$$\left|\sum_{j=1}^{n} a_j b_j\right| = \left(\sum_{j=1}^{n} a_j\right)^{1/2}\left(\sum_{j=1}^{n} b_j\right)^{1/2}$$

As we know from linear algebra, the way we get equality is when $\vec{v} = c\vec{w}$, or that $a_j = cb_j \ \forall j$ for some $c \in \mathbb{R}$.

Triangle Inequality

Given $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}$

$$\left(\sum_{j=1}^{n}(a_j + b_j)^2\right)^{1/2} \leq \left(\sum_{j=1}^{n} a_j^2\right)^{1/2} + \left(\sum_{j=1}^{n} b_j^2\right)^{1/2}$$

In linear algebra, this is equivalent to $\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$.

$$\begin{aligned}
\sum (a_j + b_j)^2 &= \sum a_j^2 + \sum 2a_j b_j + \sum b_j^2 \\
&\leq \sum a_j^2 + 2\left(\sum a_j^2\right)^{1/2}\left(\sum b_j^2\right)^{1/2} + \sum b_j^2 && \text{by Cauchy} \\
&= \left(\left(\sum a_j^2\right)^{1/2} + \left(\sum b_j^2\right)^{1/2}\right)^2
\end{aligned}$$

we take square roots to get our end result

Metrics and Norms on $\mathbb{R}^n$

Consider $|\cdot| : \mathbb{R} \to \mathbb{R}$, defined as follows:

$$|x| := \begin{cases} x, & x \in \mathbb{R}^+ \\ -x, & x \notin \mathbb{R}^+ \end{cases}$$

Theorems about Absolute Value:

(i) $|ab| = |a||b|$
(ii) $|a^2| = |a|^2$
(iii) $|-a| = |a|$
(iv) $|a| \in \mathbb{R}^+$
(v) $-|a| \leq a \leq |a|$
(vi) $|a| \leq \delta \Rightarrow -\delta \leq a \leq \delta$ for $\delta > 0$
(vii) $|a + b| \leq |a| + |b|$, $|a - b| \leq |a| + |b|$, $||a| - |b|| \leq |a - b|$

Proofs

Proof of (i)

Case 1: If $a, b \in \mathbb{R}^+$, then $|a| = a$, and $|b| = b$, and $ab \in \mathbb{R}^+$, so $|ab| = ab$

Case 2: If $a, b \notin \mathbb{R}^+$, then $|a| = -a$, and $|b| = -b$. Additionally, $(-a)(-b) = ab \in \mathbb{R}^+$, so $|ab| = ab$. The LHS $= ab$, and the RHS $= ab$.

Case 3: $a \in \mathbb{R}^+$, $-b \in \mathbb{R}^+$. Then, $|a||b| = (a)(-b) = -ab$. Then, since $a(-b) \in \mathbb{R}^+$, $-ab \in \mathbb{R}^+$, so $|ab| = -ab$. Therefore, the LHS and RHS are equal.

Proof of (vii) Having established that $|a+b| \leq |a| + |b|$, we will show that $||a| - |b|| \leq |a - b|$.

$$\begin{aligned} |a| &= |a - b + b| \\ &\leq |a - b| + |b| \\ |a| - |b| &\leq |a - b| \end{aligned}$$

Similarly, by exchanging a for b

$$\begin{aligned} |b| - |a| &\leq |b - a| \\ |b| - |a| &\leq |a - b| \end{aligned}$$

Let $t = |a| - |b|$. We have shown that

$$\begin{aligned} \pm t &\leq |a - b| \\ -|a - b| \leq t &\leq |a - b| \\ |t| &\leq |a - b| \end{aligned}$$

Absolute Values, cont'd

Recall:

$$|x| = \begin{cases} x, & x \in \mathbb{R}^+ \\ -x, & x \notin \mathbb{R}^+ \end{cases}$$

If we want to find all $x \in \mathbb{R}$ such that $|x - 1| \leq |x|$, we would split up into cases:

$x \leq 0$ $x - 1 \leq -1$, so $|x| = -x$ and $|x - 1| = 1 - x$, so $1 - x \leq -x$, so $0 \geq 1$. $\perp$

$0 < x \leq 1$ $|x| = x$ and $|x - 1| = 1 - x$, so $1 - x \leq x$, so $x \geq \frac{1}{2}$, so $\frac{1}{2} \leq x \leq 1$.

$1 < x$ $|x| = x$ and $|x - 1| = x - 1$, so $x - 1 \leq x$, so $-1 \leq 0$, which is true $\forall \mathbb{R}$ in the interval, so $x > 1$.

Therefore, we have $x \in \left(\frac{1}{2}, \infty\right)$ as that which satisfies this inequality.

Bounded Sets

A subset $A \subseteq \mathbb{R}$ is **bounded** $\Leftrightarrow$ $\exists c \geq 0$ such that $\forall x \in A,\ |x| \leq c$.

($\Rightarrow$) Suppose $A \subseteq \mathbb{R}$ is bounded. Then, $\exists \ell, u \in \mathbb{R}$ such that $\ell \leq x \leq u$ $\forall x \in A$. Let $c := \max\{|\ell|, |u|\}$.

Since $|u| \leq c$, we have that $x \leq c$.

Since $|\ell| \leq c$, and $-|\ell| \leq x$, we get that $-x \leq |\ell| \leq c$.

Since $x \leq c$ and $-x \leq c$, $|x| \leq c$.

($\Leftarrow$) If such a c exists, then $|x| \leq c$ if and only if $-c \leq x \leq c$. Thus, $-c$ is the lower bound and c is the upper bound.

Bounded Functions

Let D be any set. A function $f : D \to \mathbb{R}$ is bounded if $\text{ran}(D) \subseteq \mathbb{R}$ is bounded.

Example

Let $f : [3,7] \to \mathbb{R}$, $f(x) = \frac{x^2+2x+1}{x-1}$. Show that f is bounded.

$3 \leq x \leq 7 \Rightarrow 2 \leq x-1 \leq 6 \Rightarrow \frac{1}{6} \leq \frac{1}{x-1}\frac{1}{2} \Rightarrow \frac{1}{|x-1|} \leq \frac{1}{2}$.

Also, $4 \leq x+1 \leq 8 \Rightarrow 16 \leq x^2+2x+1 \leq 64 \Rightarrow |x^2+2x+1| \leq 64$.

So, $|f(x)| \leq 32$.

Distance Metrics

For $s, t \in \mathbb{R}$, we will define $d(s,t) = |s-t|$ to be the **distance** between s and t.

Properties:

(i)
$$\begin{aligned} d :& \mathbb{R} \times \mathbb{R} \to [0, \infty) \\ &(s,t) \mapsto d(s,t) \geq 0 \end{aligned}$$

(ii) $d(s,t) = d(t,s)$

(iii) $d(s,r) \leq d(s,t) + d(t,r)$

(iv) $d(s,s) = 0$

(v) If $d(s,t) = 0$, then $s = t$.

Let $v = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $w = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$.

- 1-norm:
$$\|v\|_1 = \sum_{j=1}^{n} |x_j|$$

- ∞-norm:
$$\|v\|_\infty = \max_{j=1}^{n} |x_j|$$

- 2-norm:
$$\|v\|_2 = \left(\sum_{j=1}^{n} x_j^2 \right)^{1/2}$$

Properties of the Norms

Properties: With v, w above, let $p = 1, 2, \infty$. The following are true:

(1) $\|v\|_p \geq 0$

(2) $\|v + w\|_p \leq \|v\|_p + \|w\| + p$

(3) $\|\vec{0}\|_p = 0$

(4) $\|v\|_p = 0 \Rightarrow v = \vec{0}$

(5) $\forall t \in \mathbb{R},\ \|tv\|_p = |t|\|v\|_p$

Proofs

Let $p = \infty$. We will prove (2).

Say $\|v\|_{infty} = |x_i|$ and $\|w\|_\infty = |y_k|$. We want to show that $\|v + w\|_\infty = \max_{j=1}^n |x_j + y_j| \leq |x_i| + |y_k|$.

Note that $\forall j$

$$\begin{aligned} |x_j + y_j| &\leq |x_j| + |y_j| && \text{Triangle Inequality} \\ &\leq |x_i| + |y_k| \\ &= \|v\|_\infty + \|w\|_\infty \end{aligned}$$

Therefore, $\|v + w\|_\infty \leq \|v\|_\infty + \|w\|_\infty$.

Distances and Norms

A **norm** on $\mathbb{R}^n$ is a function $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}^+$, $v \mapsto \|v\|$, satisfying the following properties for $v \in \mathbb{R}^n$:

(1) $\|v\| \geq 0$

(2) $\|v + w\| \leq \|v\| + \|w\|$

(3) $\|\vec{0}\| = 0$

(4) $\|v\| = 0 \Rightarrow v = \vec{0}$

(5) $\forall t \in \mathbb{R},\ \|tv\| = |t|\|v\|$

If $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}^+$ is a norm, we define $d_{\|\cdot\|} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$, defined as follows:

$$d_{\|\cdot\|}(v, w) = \|v - w\|$$

for $v, w \in \mathbb{R}^n$.

The properties of distance in $\mathbb{R}$ still hold for distance in $\mathbb{R}^n$:

(1) $d(v, w) = d(w, v)$

(2) $d(u, w) \leq d(u, v) + d(v, w)$

(3) $d(v, v) = 0$

(4) $d(v, w) = 0 \Rightarrow v = w$

Metric Spaces

A **metric space** is a nonempty set X equipped with a function $d : X \times X \to \mathbb{R}^+$, $(x, y) \mapsto d(x, y) \geq 0$. The metric has the following properties:

(1) $d(x, y) = d(y, x)\ \forall x, y \in X$

(2) $d(x, z) \leq d(x, y) + d(y, z)\ \forall x, y, z \in X$

(3) $d(x, x) = 0$

(4) $d(x, y) = 0 \Leftrightarrow x = y$

The map d is called a *metric* on X.

Metric Spaces, Open Sets, and Closed Sets

Examples of Metric Spaces:

- $\mathbb{R}$ with $d(x,y) = |x-y|$.
- $\mathbb{R}^n$ with the *Euclidean metric*:

$$\begin{aligned} d_2(v,w) &= \|v-w\|_2 \\ &= \left(\sum_{j=1}^{n}(x_j-y_j)^2\right)^{1/2} \end{aligned}$$

- $\mathbb{R}^n$ with the 1-norm:

$$\begin{aligned} d_1(v,w) &= \|v-w\|_1 \\ &= \sum_{j=1}^{n}|x_j-y_j| \end{aligned}$$

- $\mathbb{R}^n$ with the ∞-norm:

$$\begin{aligned} d_\infty(v,w) &= \|v-w\|_\infty \\ &= \max_{j=1}^{n}|x_j-y_j| \end{aligned}$$

Let (X,d) be a metric space.

(1) The **open ball** centered at $x_0 \in X$ with radius δ is:

$$U(x_0,\delta) := \{x \in X \mid d(x,x_0) < \delta\}$$

(2) The **closed ball** centered at $x_0 \in X$ with radius δ is:

$$B(x_0,\delta) := \{x \in X \mid d(x,x_0) \leq \delta\}$$

(3) A set $U \subseteq X$ is **open** if $\forall x \in U$, $\exists \delta > 0$ such that $U(x,\delta) \subseteq U$.

(4) A set $C \subseteq X$ is **closed** if $\overline{C} = X - C \subseteq X$ is open.

Examples

In $\mathbb{R}$ with $d(s,t) = |s-t|$:

$$\begin{aligned} U(x_0,\delta) &= \{y \in \mathbb{R} \mid d(y,x_0) < \delta\} \\ &= \{y \in \mathbb{R} \mid |y-x_0| < \delta\} \\ &= (x_0-\delta, x_0+\delta) \\ B(x_0,\delta) &= [x_0,\delta,x_0+\delta] \end{aligned}$$

The interval $A = [1,\infty)$ is not open, as $\forall \delta > 0$, $U(1,\delta) \not\subseteq [1,\infty)$.

However, A is closed, as $\overline{A} = (-\infty,1)$ is open: given $t \in \overline{A}$, choose $\delta = 1-t$. Let $s \in V_\delta(t)$. Then, $s \in (t-\delta,t+\delta)$, so $s \in (t-(1-t), t+(1-t))$, or $s \in (2t-1,1)$, so $s < 1$.

Exercises

Show that the following are open:

- (a,b)
- (a,∞)
- $(-\infty,b)$

and that the following are closed:

- $[a,b]$
- $[a,\infty)$
- $(-\infty,b]$

In $(\mathbb{R}^2,d_2)$, $B(0_{\mathbb{R}^2},1)$ is the **unit disc** centered at $(0,0)$.

However, in $(\mathbb{R}^2, d_\infty)$:

$$\begin{aligned} B(0_{\mathbb{R}^2}, 1) &= \{v \in \mathbb{R}^2 \mid \|v\|_\infty \leq 1\} \\ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid \max\{|x|, |y|\} \leq 1 \right\} \end{aligned}$$

is the **unit square**.

Finding a Supremum

Let $0 \neq A \subseteq \mathbb{R}$. Let $u \in \mathbb{R}$ be an upper bound for A. The following are equivalent:

(i) $u = \sup(A)$

(ii) If $t < u$, then $\exists a_t \in A$ such that $a_t > t$

(iii) $(\forall \varepsilon > 0)(\exists a_\varepsilon \in A)$ with $u - \varepsilon < a_\varepsilon$

Proofs

(i) $\Rightarrow$ (ii): Given $t < u$, if no such $a \in A$ with $t < a$ exists, then $a \leq t \ \forall a \in A$. Thus t would be an upper bound. However, $t < u$ and u is the supremum of A. $\perp$

(ii) $\Rightarrow$ (iii): Given $\varepsilon > 0$, set $t = u - \varepsilon < u$. So, by (ii), $\exists a_t$ with $t < a_t$. Thus, $u - \varepsilon \leq a_t$. Set $a_\varepsilon = a_t$.

(iii) $\Rightarrow$ (i): Let v be an upper bound for A. Suppose $v < u$. Then, set $\varepsilon = u - v > 0$. By (iii), $\exists a_\varepsilon \in A$ with $u - \varepsilon < a_\varepsilon$. So $u - (u - v) < a_\varepsilon$, so $v < a_\varepsilon$, meaning v cannot be an upper bound. $\perp$

Supremum Example

$\sup[0, 1) = 1$: Certainly, 1 is an upper bound for $[0, 1)$. Let $\varepsilon > 0$.

If $\varepsilon \geq 1$, pick $t = \frac{1}{2}$. Then, $1 - \varepsilon < 0 < \frac{1}{2}$

If $0 < \varepsilon < 1$, let $t = (1 - \varepsilon) + \frac{\varepsilon}{2} = 1 - \varepsilon/2$. Then, $t \in [0, 1)$, and $1 - \varepsilon < 1 - \varepsilon/2 = t$

Finding an Infimum

Let $\emptyset \neq A \subseteq \mathbb{R}$. Let $\ell \in \mathbb{R}$ be a lower bound for A. The following are equivalent:

(i) $\ell = \inf(A)$

(ii) If $t > \ell$, $\exists a_t$ such that $t > a_t$

(iii) $(\forall \varepsilon > 0)(\exists a_\varepsilon \in A)$ with $\ell + \varepsilon > a_\varepsilon$

Infimum Example

$\inf \left\{ \frac{1}{n} \mid n \geq 1 \right\}$: Clearly, $0 < \frac{1}{n} \ \forall n \geq 1$. Let $\varepsilon > 0$.

We need to find $a \in \left\{ \frac{1}{n} \mid n \geq 1 \right\}$ with $\varepsilon > a$. By the Archimedean Property, $\exists m \in \mathbb{N}$ such that $\frac{1}{m} < \varepsilon$. Let $a_\varepsilon = \frac{1}{m}$.

More on Supremum/Infimum

- If $A \subseteq \mathbb{R}$ and $\max(A) = u$, then $u = \sup(A)$: u is an upper bound of A by the definition of max, and if $v \neq u$ is any upper bound of A, then $u < v$ since $u \in A$.
- If $\min(A) = \ell$, then $\ell = \inf(A)$ (by the same logic).
- If A is not bounded above, $\sup(A) = +\infty$, and if A is not bounded below, then $\inf(A) = -\infty$.
- If $A \subseteq B$, then $\sup(A) \leq \sup(B)$.
- If $A \subseteq B$, then $\inf(A) \geq \inf(B)$: Let $\ell_A = \inf(A)$ and $\ell_B = \inf(B)$. By definition, $\ell_B \leq b \ \forall b \in B$. Since $A \subseteq B$, $\ell_B \leq a \ \forall a \in A$. Thus, ℓ_B is a lower bound for A. By definition of ℓ_A, $\ell_B \leq \ell_A$.

Let $A, B \subseteq \mathbb{R}$ and $t \in \mathbb{R}$. Then, the following are also sets:

(1) $A + B = \{a + b \mid a \in A, b \in B\}$

(2) $A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$

(3) $t \cdot A = \{ta \mid a \in A\}$

(4) $A + t = \{a + t \mid a \in A\}$

For example, we have the following results:

- $\sup(A + B) = \sup(A) + \sup(B)$
- $\sup(A + t) = \sup(A) + t$
- $\inf(-A) = -\sup(A)$

Completeness Axiom

If $\emptyset \neq A \subseteq \mathbb{R}$ is bounded above, then $\sup(A)$ exists.

Well-Ordering Property: if $\emptyset \neq S \subseteq \mathbb{N}$, then $\min(S)$ exists.

Therefore, we can prove that if $F \subseteq \mathbb{Z}$ is bounded, then F has a least and greatest element.

Archimedean Property: Proof

If $x \in \mathbb{R}$, then $\exists n_x \in \mathbb{N}$ such that $x \leq n_x$.

Suppose there exists no natural number greater than x, then $\mathbb{N}$ is bounded above by X. Let $u = \sup(\mathbb{N})$. By the Completeness Axiom, $u \in \mathbb{R}$ exists. Let $\varepsilon = 1$. Then, $\exists n \in \mathbb{N}$ with $u - 1 < n$. So, $u < n + 1$, but $n + 1 \in \mathbb{N}$, so u cannot be an upper bound.

Corollary to the Archimedean Property

$$\forall t > 0 \; \exists n \in \mathbb{N} \ni \frac{1}{n} < t$$

Corollary: Powers of 2

$$\forall t > 0 \; \exists m \in \mathbb{N} \ni \frac{1}{2^m} < t$$

By the corollary to the Archimedean Property, we know that $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < t$. By Bernoulli's inequality with $x = 1$, we have $2^n \geq n$, so $2^{-n} < n^{-1} < t$.

Corollary: In Between Integers

$$\forall x \in \mathbb{R} \; \exists n_x \in \mathbb{Z} \ni n_x - 1 \leq x < n_x$$

Assume $x \geq 0$. Let $S_x = \{n \mid n \in \mathbb{N} \; x < n\}$.

$S_x \neq \emptyset$ by the Archimedean Property. By the well-ordering property, let $n_x = \min(S_x)$.

Therefore, $x < n_x$. Also, $n_x - 1 \notin S_x$. Therefore $n_x - 1 \leq x$.

Density Theorems

Let (X, d) be any metric space. A subset $D \subseteq X$ is **dense** if $\forall x \in X, \; \varepsilon > 0, U(x, \varepsilon) \cap D \neq \emptyset$.

In the case of $X = \mathbb{R}$ and $d(s,t) = |s - t|$, $D \subseteq \mathbb{R}$ is dense if given any open interval I, $I \cap D \neq \emptyset$.

A metric space is **separable** if it admits a *countable* dense subset.

Density of the Rationals

$\mathbb{Q} \subseteq \mathbb{R}$ is dense.

Let $I = (a, b)$ be an open interval. We may assume that $a, b \in \mathbb{R}$ are finite.

Then, $b - a > 0$. By the Archimedean property corollary, $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < b - a$, meaning $1 < nb - na$.

There exists also an integer m $m - 1 \leq na < m$, implying that $a\frac{m}{n}$. Also, $m \geq na + 1 < nb$. Therefore, $\frac{m}{n} < b$.

So, $\frac{m}{n} \in \mathbb{Q} \cap (a, b)$.

Density of the Irrationals

$\mathbb{R} \setminus \mathbb{Q}$ is dense.

Assume $\sqrt{2}$ exists. Let $I = (a, b)$ be any open interval. Then, $\frac{a}{\sqrt{2}} < \frac{b}{\sqrt{2}}$.

Find $q \in \mathbb{Q}$ such that $\frac{a}{\sqrt{2}} < q < \frac{b}{\sqrt{2}}$.

Then, $a < q\sqrt{2} < b$, where $q\sqrt{2} \in \mathbb{R}$ and $q\sqrt{2} \notin \mathbb{Q}$.

Uniqueness of $\sqrt{2}$

$$\exists! x > 0 \ x^2 = 2$$

Existence: Let $S = \{t \in \mathbb{R} \mid 0 < t,\ t^2 < 2\}$. S is nonempty because $1 \in \S$, and S is bounded above because $y > 2 \Rightarrow y^2 > 4$.

So, by the completeness axiom, $x := \sup(S)$ exists, and $x \geq 1$.

Claim: $x^2 = 2$

Contradiction 1: Assume $x^2 < 2$. We want to show that $\exists n \in \mathbb{N}$ such that $x + \frac{1}{n} \in S$. By this assumption, we find that

$$\begin{aligned} 0 < x + \frac{1}{n} \in S &\Leftrightarrow \left(x + \frac{1}{n}\right)^2 < 2 \\ &\Leftrightarrow x^2 + \frac{2x}{n} + \frac{1}{n^2} \end{aligned}$$

Observe:

$$\begin{aligned} x^2 + \frac{2x}{n} + \frac{1}{n^2} &\leq x^2 + \frac{2x}{n} + \frac{1}{n} \\ &= x^2 + \frac{1}{n}(2x + 1) \end{aligned}$$

We want to find $n \in \mathbb{N}$ with:

$$x^2 + \frac{1}{n}(2x + 1) < 2 \Leftrightarrow \frac{1}{n} < \frac{2 - x^2}{2x + 1}$$

Therefore, by the Archimedean Property corollary, we know that n must exist.

Contradiction 2: We know that $x^2 \geq 2$. Since $x = \sup(S)$, $\forall m \in \mathbb{N}$, $\exists t_m \in S$ with $x - \frac{1}{m} < t_m$, so $\left(x - \frac{1}{m}\right)^2 < t_m^2 < 2$.

Therefore, $x^2 - \frac{2x}{m} + \frac{1}{m^2}$, so $x^2 - \frac{2x}{m} < 2$, so $0 \leq x^2 - 2 < \frac{2x}{m}$.

So, $0 \leq \frac{x^2 - 2}{2x} < \frac{1}{m}$, so $x^2 - 2 = 0$, so $x^2 = 2$.