Introduction to Analysis

UT Knoxville, Spring 2023, MATH 341

Mike Frazier, Peter Humphries, Alex Zhang

February 17, 2023

Contents

Preface

These are my notes for the **Introduction to Analysis** course at the University of Tennessee (MATH 341). It is compiled from several sources including lecture notes by Dr. Michael Frazier and Dr. Peter Humphries, as well as online resources such as the Mathematics Stack Exchange.

The first few weeks of the course are spent reviewing the material taught in **Introduction to Abstract Mathematics** (MATH 300): logic, set theory, number systems, and cardinality. They serve as a “primer” for the following material on real analysis.

1 Introduction

Real analysis is the branch of mathematics concerned with the study of functions, limits, and continuity of real numbers. It encompasses a wide range of concepts and techniques, including differentiation and integration. Real analysis serves as a foundation for many areas of mathematics and science, and its principles are used extensively in various computational techniques and algorithms.

In this course, we will focus on the central idea of convergence, which is fundamental to many of these concepts and techniques. To motivate our exploration of convergence, we will examine classic iterative methods that rely on the concept of convergence to approximate solutions.

Example 1.0.1 ▸ Newton's Method

Given $c > 0$, suppose we want to calculate $\sqrt{c}$. Start with some initial guess $x_1 > 0$.

$$\begin{aligned}
\text{Let} \quad x_2 &\coloneqq \frac{1}{2}\left(x_1 + \frac{c}{x_1}\right) \\
\text{Let} \quad x_3 &\coloneqq \frac{1}{2}\left(x_2 + \frac{c}{x_2}\right) \\
&\vdots \\
\text{Let} \quad x_{n+1} &\coloneqq \frac{1}{2}\left(x_n + \frac{c}{x_n}\right)
\end{aligned}$$

We find that $\lim_{n\to\infty} x_n = \sqrt{c}$.

Does this method work for all $c > 0$ and $x_1 > 0$? Assuming $\lim_{n\to\infty} x_n = x$ converges, then:

$$\begin{aligned}
& & x_{n+1} &= \frac{1}{2}\left(x_n + \frac{c}{x_n}\right) \\
&\implies & x &= \frac{1}{2}\left(x + \frac{c}{x}\right) \\
&\implies & 2x &= x + \frac{c}{x} \\
&\implies & x &= \frac{c}{x} \\
&\implies & x^2 &= c \\
&\implies & x &= \sqrt{c}
\end{aligned}$$

The above calculation only makes sense if we know the sequence converges. Consider the sequence $x_{n+1} = 6 - x_n$ where $x_1 = 4$. Then:

$$x_1 = 4, \quad x_2 = 2, \quad x_3 = 4, \quad x_4 = 2, \quad \ldots$$

Since this sequence does not converge, there is no limit when n approaches infinity.

Let's look at a more complicated iterative method.

Example 1.0.2 ▸ Picard's Method

Suppose we had to solve $y' = f(x, y)$ where $y(x_0) = y_0$ (i.e. find a function y that satisfies our two conditions). As it turns out, we can use an iterated method to solve this as well.

- Start with an initial guess $y_1(x)$
- Define $y_{n+1}(x) \coloneqq y_0 + \displaystyle\int_{x_0}^{x} f(t, y_n)\, dt$.

Provided that f and y_0 are "well-behaving", then the sequence of functions $y_n(x)$ converges to the solution $y(x)$.

This idea that an infinite sequence of functions can converge suggests some notion of "distance" between functions. We can use a number of metrics for distance, some possibilities including:

- $\displaystyle\int_a^b |f(x) - g(x)|\, dx$ (total area between the two functions)
- $\sup\{x : x = |f(x) - g(x)|\}$ (max possible "vertical" distance between the two curves)

2

Logic and Proofs

Formal logic is the foundation of mathematics. It enables us to construct logically consistent models by starting with a set of axioms and systematically deducing new statements from them. This process not only helps us to prove known results but also to uncover new mathematical concepts and theorems.

2.1 Basic Logic

Definition 2.1.1 ▶ Statement

A ***statement*** is a claim that is either true or false.

$$p \,:\, \text{some claim}$$

We usually denote statements with a letter like p. For example, we can write "$p : x > 2$", which means p represents the statement "x is greater than 2". Throughout this chapter, we will use p and q to represent arbitrary statements.

Definition 2.1.2 ▶ Conjunction

Logical ***conjunction*** is an operation that takes two statements and produces a new statement that is true only when both input statements are true.

$$p \wedge q \,:\, p \text{ is true } \textbf{and } q \text{ is true}$$

Definition 2.1.3 ▶ Disjunction

Logical ***disjunction*** is an operation that takes two statements and produces a new statement that is true when at least one of the input statements is true.

$$p \vee q \,:\, p \text{ is true } \textbf{or } q \text{ is true}$$

Conjunction and Disjunction follow our intuition of "and" and inclusive "or", respectively. We can visualize the two logical connectives using ***truth tables***.

Example 2.1.1 ▶ Truth Table of Conjunction

p	q	$p \implies q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 2.1.2 ▶ Truth Table of Disjunction

p	q	$p \implies q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition 2.1.4 ▶ Negation

The ***negation*** of a statement is a statement with opposite truth values.

$$\neg p$$

Definition 2.1.5 ▶ Implication

An ***implication*** "p implies q" states "if p is true, then q is true".

$$p \implies q$$

In the implication $p \implies q$, we call p the ***hypothesis*** and q the ***conclusion***. If the hypothesis is false to begin with, then the implication is not really meaningful. Instead of assigning those kinds of implications no truth value, we simply consider them true by convention. These kinds of truths are called ***vacuous truths***.

Example 2.1.3 ▸ Truth Table of Implication

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 2.1.4 ▸ Simple Statements

Let $p : x > 2$ and $q : x^2 > 1$. Consider the following statements:

- "For all real numbers x, $p \implies q$"

  True. If $x > 2$, then $x^2 > 1$.[a]

- "For all real numbers x, $q \implies p$"

  False. Consider $x = 1.1$. Then $x^2 = 1.21 > 1$, but $x = 1.1 < 2$.

[a] This is normally where we would rigorously prove such a statement, but we will omit this for now.

Definition 2.1.6 ▸ Logical Equivalence

p and q are ***logically equivalent*** if $p \implies q$ and $q \implies p$.

$$p \iff q$$

In other words, $p \iff q$ means that p and q share the same truth value. Either p and q are **always both true**, or p and q are **always both false**. Logical equivalence says nothing about the truth of p and q themselves.

We can also say "p if and only if q" or "p iff q" to denote logical equivalence.

Example 2.1.5 ▶ Truth Table of Logical Equivalence

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

Definition 2.1.7 ▶ Converse

Given the implication $p \implies q$, its ***converse*** statement is $q \implies p$.

It's important to note that an implication and its converse have no intrinsic equivalence.

Example 2.1.6 ▶ Truth Table of Converse

p	q	$p \implies q$	$q \implies p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Definition 2.1.8 ▶ Contrapositive

Given the implication $p \implies q$, its ***contrapositive*** statement is $\neg q \implies \neg p$.

Unlike the converse, an implication and its contrapositive are logically equivalent. To help our intuition, we can construct a truth table.

Example 2.1.7 ▸ Truth Table of Contrapositive

p	q	$\neg p$	$\neg q$	$p \implies q$	$\neg q \implies \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

As we can see, no matter what the truth values of the hypothesis and conclusion are, an implication and its contrapositive always have the same truth values.

> When constructing a truth table, we must include **all** intermediate statements, not just the final statement.

2.2 Proofs and Proof Techniques

While truth tables are a useful tool for evaluating simple statements, they quickly become impractical when dealing with more complex propositions. Moreover, they do not offer insights into the reasoning behind such statements. In contrast, proofs can provide us with a deeper understanding of logical relationships and help us reason about complex statements.

In particular, we often need to prove implications of the form $p \implies q$, where the truth of p guarantees the truth of q. To do so, we can use a variety of proof techniques:

1. ***Direct Proof:*** Assume p is true, then reason that q must be true as well.
2. ***Proof by Contradiction:*** Assume both p and $\neg q$ are true, then logically derive some contradiction.
3. ***Proof by Contrapositive:*** Assume $\neg q$ is true, then reason that $\neg p$ must be true as well.

In mathematical proofs, there are two main types of reasoning: direct and indirect. A direct proof shows a clear path from the premises to the conclusion, providing valuable insights into the underlying mathematics. In contrast, indirect proofs rely on a contradictory hypothesis to establish the truth of the conclusion. While indirect proofs can be useful when a direct proof is not readily available, they may be less insightful since they do not provide much context surrounding the premises.

However, it is worth noting that an indirect proof may be easier to find than a direct proof in certain cases. While a direct proof requires identifying the correct path that leads to the conclusion, an indirect proof only needs to deduce any contradictory statement. Despite this advantage, indirect proofs should be used sparingly and only when a direct proof is not feasible.

Technique 2.2.1 ▶ Proof by Contradiction

To prove $p \implies q$ by contradiction, we carry out the following steps:

1. Assume p is true, and suppose for the sake of contradiction $\neg q$ is true.
2. Logically derive a statement that contradicts something we know to be true.
3. Ultimately conclude that q must be true.

In terms of logic notation, proof by contradiction follows:

$$[(p \wedge (\neg q)) \implies \text{Contradiction}] \implies [p \implies q]$$

Example 2.2.1 ▶ Truth Table of Proof by Contradiction

p	q	$p \implies q$	$\neg q$	$p \wedge (\neg q)$	$\neg\, [p \wedge (\neg q)]$
T	T	T	F	F	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	F	T

By the above truth table, we can safely assume the following logical equivalence:

$$(p \implies q) \iff \neg\, [p \wedge (\neg q)]$$

Technique 2.2.2 ▶ Proof by Contrapositive

To prove $p \implies q$ by contrapositive, we carry out the following steps:

1. Assume $\neg q$ is true.
2. Directly prove that $\neg p$ is true.

In terms of logic notation, proof by contrapositive follows:

$$(\neg q \implies \neg p) \iff (p \implies q)$$

We can actually prove this using proof by contradiction!

Example 2.2.2 ▸ Logical Equivalence of Contrapositive

Given statements p and q, $p \implies q$ and $\neg q \implies \neg p$ are equivalent.

Proof. Assume $p \implies q$. To prove $\neg q \implies \neg p$, we can suppose for contradiction that $\neg q$ and p are both true. But $p \implies q$, so q is true which contradicts $\neg q$. Hence, the assumption that p is true was incorrect. Thus, $\neg q \implies \neg p$.

Assume $\neg q \implies \neg p$. From above, we have $\neg(\neg p) \implies \neg(\neg q)$, so $p \implies q$. □

Example 2.2.3 ▸ Proving Simple Logic Statements

Let p, q, and r be arbitrary statements. Prove that $[p \implies (q \lor r)] \iff [(p \land \neg q) \implies r]$.

Proof. Assume $p \implies (q \lor r)$. Suppose $p \land \neg q$. Then p is true, so $q \lor r$ is true by assumption. Also, $\neg q$ is true, so r must be true from $q \lor r$.

Assume $(p \land \neg q) \implies r$. Suppose p is true. There are two possibilities:

1. If q is true, then $q \lor r$ is true.
2. If $\neg q$ is true, then $p \land \neg q$ is true. Thus, r is true by assumption. Hence, $q \lor r$ is true.

□

3 Naive Set Theory

Instead of forming a rigorous, axiomatic basis for sets, we will simply take an informal approach to sets guided by our intuition. Ultimately, our introduction to real analysis does not fiddle with the fine details of set theory, so it's safe to take a naive approach to set theory.

3.1 Sets

Definition 3.1.1 ▸ Set

A ***set*** is a collection of distinct objects.

For example, $\mathbb{N} \coloneqq \{1, 2, 3 \dots\}$ is the set of all natural numbers, and $\mathbb{Z} \coloneqq \{\dots, 1, 2, 3, \dots\}$ is the set of all integers. It's conventional to use capital letters to denote sets and use lowercase letters to denote elements of sets. Throughout this chapter, we will use A and B to represent arbitrary sets.

Definition 3.1.2 ▸ Membership, $\in$

We write $a \in A$ to mean "a is in A".

Definition 3.1.3 ▸ Subset, $\subseteq$

A is a ***subset*** of B if everything in A is also in B.

$$A \subseteq B \iff \forall (x \in A)(x \in B)$$

Definition 3.1.4 ▸ Set Equality, $=$

A ***equals*** B if A is a subset of B and B is a subset of A.

$$A = B \iff (A \subseteq B \wedge B \subseteq A)$$

Definition 3.1.5 ▶ Proper Subset, $\subsetneq$

A is a ***proper subset*** of B if A is a subset of B but B is not a subset of A.

$$A \subsetneq B \iff (A \subseteq B \land B \nsubseteq A)$$

In other words, A is a proper subset of B if everything in A is also in B, but B has something that A does not.

> Among mathematical texts, the generic subset symbol $\subset$ has no standardized definition. Some use it to represent subset or equal; others use it to represent proper subset. We will simply not use $\subset$ to avoid any ambiguity.

Definition 3.1.6 ▶ Empty Set ($\varnothing$)

The ***empty set*** is the set that contains no elements.

$$\varnothing \coloneqq \{\}$$

As convention, we assume that $\varnothing$ is a subset of every set, including itself.

Technique 3.1.1 ▶ Proving a Subset Relation

To prove that $A \subseteq B$:

1. Let x be an arbitrary element of A.
2. Show that $x \in B$.

To prove that $A \nsubseteq B$, choose a specific $x \in A$ and show $x \notin B$.

Example 3.1.1 ▶ Proving Simple Subset Relation

Suppose that $A \subseteq B$ and $B \subseteq C$. Prove that $A \subseteq C$.

Proof. Let $x \in A$ be arbitrary. Since $A \subseteq B$, then $x \in B$. Similarly, since $B \subseteq C$, then $x \in C$. Therefore, $A \subseteq C$. □

Definition 3.1.7 ▶ Union

The ***union*** of two sets is the set of all things that are in one or the other set.

$$A \cup B \coloneqq \{x : x \in A \lor x \in B\}$$

Definition 3.1.8 ▸ Intersection

The ***intersection*** of two sets is the set of all things that are in both sets.

$$A \cap B := \{x : x \in A \wedge x \in B\}$$

More generally, we can apply union and intersection to an arbitrary number of sets, finite or infinite. We use a notation similar to summation using $\sum$. Let Λ be an indexing set, and for each $\lambda \in \Lambda$, let A_λ be a set.

$$\bigcup_{\lambda \in \Lambda} A_\lambda = \{x : x \in A_\lambda \text{ for some } \lambda \in \Lambda\}$$
$$\bigcap_{\lambda \in \Lambda} A_\lambda = \{x : x \in A_\lambda \text{ for all } \lambda \in \Lambda\}$$

Example 3.1.2 ▸ Indexed Sets

For $n \in \mathbb{N}$, let $A_n = \left[\frac{1}{n}, 1\right] = \left\{x \in \mathbb{R} : \frac{1}{n} \leq x \leq 1\right\}$. Prove that:

(a) $\bigcup_{n=1}^{\infty} = (0, 1]$

(b) $\bigcap_{n=1}^{\infty} = \{1\}$

Proof of (a). Suppose $x \in \bigcup_{n=1}^{\infty} A_n$. Then there exists $n \in \mathbb{N}$ such that $x \in A_n = \left[\frac{1}{n}, 1\right]$. That is, $0 < \frac{1}{n} \leq x \leq 1$. Therefore, $x \in (0, 1]$.

Suppose $x \in (0, 1]$. Then $x > 0$, so there exists $n_0 \in \mathbb{N}$ such that $\frac{1}{n_0} < x$. Then $\frac{1}{n_0} \leq x \leq 1$, so $x \in A_{n_0}$. Therefore, $x \in \bigcup_{n=1}^{\infty} A_n$. □

Proof of (b). Suppose $x \in \bigcap_{n=1}^{\infty} A_n$. Then $x \in A_1 = \{1\}$.

Suppose $x \in \{1\}$. Then $x = 1 \in \left[\frac{1}{n}, 1\right]$ for all $n \in \mathbb{N}$. Therefore, $x \in \bigcap_{n=1}^{\infty} A_n$. □

Definition 3.1.9 ▸ Set Minus

The ***set difference*** of two sets is the set of all things that are in first set but not the second set.

$$A \setminus B = \{x \in A : x \notin B\}$$

Definition 3.1.10 ▸ Complement

Let X be a set called the ***universal set***. The ***complement*** of A in X is defined as $X \setminus A$.

$$A^c = X \setminus A = \{x \in X : x \notin A\}$$

Theorem 3.1.1 ▸ De Morgan's Laws for Sets

Suppose X is a set, and for any subset S of X, let $S^c = X \setminus S$. Suppose that $A_\lambda \subseteq X$ for every λ belonging to some index set Λ. Prove that:

(a) $\left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)^c = \bigcap_{\lambda\in\Lambda} A_\lambda^c$;

(b) $\left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)^c = \bigcup_{\lambda\in\Lambda} A_\lambda^c$.

Proof of (a). First, let $a \in \left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)^c$. Then, $a \in X \setminus \left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)$, so $a \in X$ but $a \notin \left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)$. Thus, $a \notin A_\lambda$ for any $\lambda \in \Lambda$, so $a \in X \setminus A_\lambda$ for all $\lambda \in \Lambda$. In other words, $a \in \bigcap_{\lambda\in\Lambda} A_\lambda^c$.

Next, let $a \in \bigcap_{\lambda\in\Lambda} A_\lambda^c$. Then $a \in A_\lambda^c$ for all $\lambda \in \Lambda$, so $a \in X$ but $a \notin A_\lambda$ for all $\lambda \in \Lambda$. That is, $a \notin \left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)$. In other words, $a \in \left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)^c$. □

Proof of (b). First, let $a \in \left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)^c$. Then, $a \in X \setminus \bigcap_{\lambda\in\Lambda} A_\lambda$, so $a \in X$ but $a \notin \bigcap_{\lambda\in\Lambda} A_\lambda$. That is, $a \notin A_\lambda$ for some $\lambda \in \Lambda$. Thus, $a \in X \setminus A_\lambda$ for some $\lambda \in \Lambda$. Therefore, $a \in \bigcup_{\lambda\in\Lambda} A_\lambda^c$.

Next, let $a \in \bigcup_{\lambda\in\Lambda} A_\lambda^c$. Then $a \in A_\lambda^c$ for some $\lambda \in \Lambda$, so $a \in X$ but $a \notin A_\lambda$ for some $\lambda \in \Lambda$. That is, $a \notin \left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)$. Therefore, $a \in \left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)^c$. □

3.2 Functions

We generally think of functions as a "map" or "rule" that assigns numbers to other numbers. For example, $f(x) = 2x$ maps $1 \mapsto 2$, $2 \mapsto 4$, etc. More formally, we define functions in terms of sets.

Definition 3.2.1 ▸ Cartesian Product

Let X and Y be sets. The ***Cartesian product*** of X and Y is the set of all ordered pairs (x, y) where $x \in X$ and $y \in Y$.

$$X \times Y := \{(x, y) : x \in X \wedge y \in Y\}$$

Definition 3.2.2 ▶ Relation

Let X and Y be sets. A ***relation*** between X and Y is a subset of the Cartesian product $X \times Y$.

Definition 3.2.3 ▶ Function

Let X and Y be sets. A ***function*** from X to Y is a relation from X to Y such that for every $x \in X$, there exists a unique $y \in Y$ where $(x, y) \in f$.

More formally, a ***function*** $f : X \to Y$ is a subset of $X \times Y$ satisfying:

1. $\forall(x \in X)\,[\exists(y \in Y)((x, y) \in f)]$
2. $(x, y_1), (x, y_2) \in f \implies y_1 = y_2$

Given $f : X \to Y$, we call X the ***domain*** of f and Y the ***codomain*** of f. Given $x \in X$, we write $f(x)$ to denote the unique element of Y such that $(x, y) \in f$.

$$f(x) = y \iff (x, y) \in f$$

Definition 3.2.4 ▶ Function Image

Let $f : X \to Y$ be a function and $A \subseteq X$. The ***image*** of A under f is the set containing all possible function outputs from all inputs in A.

$$f[A] := \{f(a) : a \in A\}$$

Given $f : X \to Y$, we call $f[X]$ the ***range*** of f.

Example 3.2.1 ▶ Function Images

Suppose $f : X \to Y$ is a function, and $A_\lambda \subseteq X$ for each $\lambda \in \Lambda$. Then:

(a) $f\left[\bigcup_{\lambda \in \Lambda} A_\lambda\right] = \bigcup_{\lambda \in \Lambda} f\left[A_\lambda\right]$

(b) $f\left[\bigcap_{\lambda \in \Lambda} A_\lambda\right] \subseteq \bigcap_{\lambda \in \Lambda} f\left[A_\lambda\right]$

In this example, we will only prove the “forward” direction. That is, we want to show that $f\left[\bigcup_{\lambda\in\Lambda} A_\lambda\right] \subseteq \bigcup_{\lambda\in\Lambda} f\left[A_\lambda\right]$.

Proof of (a). Let $y \in f\left[\bigcup_{\lambda\in\Lambda} A_\lambda\right]$. By definition of Function Image, there exists $x \in \bigcup_{\lambda\in\Lambda} A_\lambda$ such that $y = f(x)$. Thus, there exists $\lambda_0 \in \Lambda$ such that $x \in \lambda_0$. That is, $y \in f\left[A_{\lambda_0}\right]$. Therefore, $y \in \bigcup_{\lambda\in\Lambda} f\left[A_\lambda\right]$. ▢

Definition 3.2.5 ▸ Function Inverse Image

Let $f : X \to Y$ be a function and $B \subseteq Y$. The ***inverse image*** of B under f is the set containing all possible function inputs whose output is in B.

$$f^{-1}[B] \coloneqq \{x \in X : f(x) \in B\}$$

Note the following logical equivalence:

$$x \in f^{-1}[B] \iff f(x) \in B$$

Example 3.2.2 ▸ Function Inverse Images

Suppose $f : X \to Y$ is a function, and $B_\lambda \subseteq Y$ for each $\lambda \in \Lambda$. Then:

$$f^{-1}\left[\bigcup_{\lambda\in\Lambda} B_\lambda\right] = \bigcup_{\lambda\in\Lambda} f^{-1}\left[B_\lambda\right]$$

Again, we will only prove the “forward direction”.

Proof. Let $x \in f^{-1}\left[\bigcup_{\lambda\in\Lambda} B_\lambda\right]$. Then, $f(x) \in \bigcup_{\lambda\in\Lambda} B_\lambda$. That is, $f(x) \in B_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Thus, $x \in f^{-1}\left[B_{\lambda_0}\right]$, so $x \in \bigcup_{\lambda\in\Lambda} f^{-1}\left[B_\lambda\right]$. ▢

3.3 Injective and Surjective

Definition 3.3.1 ▸ Injective, One-to-one

A function $f : X \to Y$ is ***injective*** or ***one-to-one*** if no two inputs in X have the same output in Y.

$$\forall(x_1, x_2 \in X)\,[x_1 \neq x_2 \implies f(x_1) \neq f(x_2)]$$

Technique 3.3.1 ▸ Proving a Function is Injective

To prove a function $f : X \to Y$ is injective:

1. Let $x_1, x_2 \in X$ where $f(x_1) = f(x_2)$.
2. Reason that $x_1 = x_2$.

Example 3.3.1 ▸ Proving Injectivity

$f(x) = -3x - 7$ is injective.

Proof. Suppose $f(x_1) = f(x_2)$. Then $-3x_1 + 7 = -3x_2 + 7$, so $-3x_1 = -3x_2$. Thus, $x_1 = x_2$, so f is injective. □

Example 3.3.2 ▸ Disproving Injectivity

Prove that $f(x) = x^2$ is not injective.

Proof. $f(-1) = 1$ and $f(1) = 1$, but $-1 \neq 1$. Thus, f is not injective. □

Definition 3.3.2 ▸ Surjective, Onto

A function $f : X \to Y$ is ***surjective*** or ***onto*** if everything in Y has a corresponding input in X.

$$\forall(y \in Y)\,[\exists(x \in X)(f(x) = y)]$$

Note that $f : X \to f[X]$ is **always** surjective.

Technique 3.3.2 ▸ Proving a Function is Surjective

To prove a function $f : X \to Y$ is surjective:

1. Let $y \in Y$ be arbitrary.
2. "Undo" the function f to obtain $x \in X$ where $f(x) = y$.

Example 3.3.3 ▸ Proving Surjectivity

Prove that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = -3x + 7$ is surjective.

Proof. Let $y \in Y$ be arbitrary. Let $x \coloneqq \frac{y-7}{-3}$. Then $x \in \mathbb{R}$, and:

$$\begin{aligned} f(x) &= -3\left(\frac{y-7}{-3}\right) + 7 \\ &= (y-7) + 7 \\ &= y \end{aligned}$$

Therefore, f is surjective. □

Definition 3.3.3 ▸ Bijective

A function $f : X \to Y$ is ***bijective*** if it is both injective and surjective.

Definition 3.3.4 ▸ Function Composition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. The ***composition*** of f and g is a function $g \circ f : X \to Z$ defined by:

$$(g \circ f)(x) \coloneqq g(f(x))$$

Theorem 3.3.1 ▸ Composition Preserves Injectivity and Surjectivity

Suppose $f : X \to Y$ and $g : Y \to Z$ are functions.

(a) If f and g are injective, then $g \circ f$ is injective.

(b) If f and g are surjective, then $g \circ f$ is surjective.

(c) If f and g are bijective, then $g \circ f$ is bijective.

Proof of (a). Let $x_1, x_2 \in X$. Suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then, $g(f(x_1)) = g(f(x_2))$. Because g is injective, we have $f(x_1) = f(x_2)$. Because f is injective, we have $x_1 = x_2$. Therefore, $g \circ f$ is injective. ▢

Proof of (b). Let $z \in Z$. Because g is surjective, there exists an element $y \in Y$ such that $g(y) = z$. Because f is surjective, there exists an element $x \in X$ such that $f(x) = y$. Thus, $(g \circ f)(x) = g(f(x)) = g(y) = z$. Therefore, $g \circ f$ is surjective. ▢

Proof of (c). We know that from (a) and (b) composition preserves injectivity and surjectivity. Thus, composition must also preserve bijectivity. ▢

Definition 3.3.5 ▸ Inverse Function

Let $f : X \to Y$ be a bijection. The ***inverse function*** of f is a function $f^{-1} : Y \to X$ defined by:

$$f^{-1} \coloneqq \{(y, x) \in Y \times X : (x, y) \in f\}$$

The notation for inverse functions conflicts with the notation for inverse images. A key distinction to make it that only bijections can have an inverse function, but we can apply the inverse image to any function. Thus, given a bijection $f : X \to Y$, we know $f^{-1}(f(x)) = x$ for all $x \in X$, and $f(f^{-1}(y)) = y$ for all $y \in Y$.

Example 3.3.4

Let $f : X \to Y$ and $g : Y \to X$ be functions such that $(g \circ f) = x$ for all $x \in X$, and $(f \circ g)(y) = y$ for all $y \in Y$. $f^{-1} = g$.

Proof. todo: finish proof ▢

4

Number Systems

Our goal is to create an axiomatic basis for the real numbers $\mathbb{R}$. We need to establish axioms for $\mathbb{R}$ and then derive all further properties from the axioms. We would like these axioms to be as minimal and agreeable as possible; however, finding axioms that characterize $\mathbb{R}$ is not easy. Instead, we'll start from the natural numbers $\mathbb{N}$ and expand from there.

4.1 Natural Numbers $\mathbb{N}$ and Induction

How do we define the natural numbers? Listing every natural number is definitely not an option. We could try to define the natural numbers as $\mathbb{N} := \{1, 2, \ldots\}$. However, the "…" is ambiguous. Instead, we can define $\mathbb{N}$ in terms of its properties.

Definition 4.1.1 ▸ Peano Axioms for $\mathbb{N}$

The ***Peano axioms*** are five axioms that can be used to define the natural numbers $\mathbb{N}$.

1. $1 \in \mathbb{N}$
2. Every $n \in \mathbb{N}$ has a successor called $n + 1$.
3. 1 is **not** the successor of any $n \in \mathbb{N}$.
4. If $n, m \in \mathbb{N}$ have the same successor, then $n = m$.
5. If $1 \in S$ and every $n \in S$ has a successor, then $\mathbb{N} \subseteq S$.

Note that there is not one "prescribed" way to do define the natural numbers. This is just the most popular approach.

From the fifth Peano axiom, we can derive a new proof technique for proving statements about consecutive natural numbers.

Theorem 4.1.1 ▸ Principle of Induction

Let $P(n)$ be a statement for each $n \in \mathbb{N}$. Suppose that:

1. $P(1)$ is true, and
2. if $P(n)$ is true, then $P(n + 1)$ is true.

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

Proof. Let $S := \{n \in \mathbb{N} : P(n)\}$. Then $1 \in S$ because $P(1)$ is true. Note that if $n \in S$, then $P(n)$ is true. Hence, $P(n+1)$ is true by assumption, so $n+1 \in S$. By the fifth Peano axiom, we have $\mathbb{N} \subseteq S$. Since S was defined as a subset of $\mathbb{N}$, we have $\mathbb{N} = S$. Therefore, $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

A proof by induction has a "domino effect". Imagine a domino for each natural number 1, 2, 3, and so on, arranged in an infinite row. Knocking the 1st domino will knock them all down.

$$\underbrace{P(1)}_{\text{by 1.}} \implies \underbrace{P(2)}_{\text{by 2.}} \implies \underbrace{P(3)}_{\text{by 2.}} \implies \cdots$$

Technique 4.1.1 ▸ Proof by Induction

To prove a statement $P(n)$ for all $n \in \mathbb{N}$, we need to prove two statements:

1. ***Base Case:*** Prove $P(1)$.
2. ***Induction Step:*** Assume $P(n)$ is true from some $n \in \mathbb{N}$, then prove $P(n) \implies P(n+1)$.

It is crucial that we actually use our assumption that $P(n)$ is true in the induction step. Otherwise, our proof is most likely wrong.

Example 4.1.1 ▸ Simple Proof by Induction

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Proof. Let $P(n)$ be the statement $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Base Case: When $n = 1$, LHS $= 1$ and RHS $= \frac{1(1+1)}{2} = 1$, so $P(1)$ is true.

Induction Step: Assume that $P(n)$ is true for some $n \in \mathbb{N}$. Then:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2} + 1\right) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

That is, $P(n+1)$ is true. By the Principle of Induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

4.2 Integers $\mathbb{Z}$

From the natural numbers, we can easily construct the integers. First, we assume the existence an operation, addition $(+)$ and multiplication $(\cdot)$. On $\mathbb{N}$, we assume addition and multiplication satisfy the following properties for all $a, b, c \in \mathbb{N}$:

- ***Commutativity*** $a + b = b + a$ $a \cdot b = b \cdot a$
- ***Associativity*** $(a + b) + c = a + (b + c)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- ***Distributivity*** $a \cdot (b + c) = a \cdot b + a \cdot c$
- ***Identity*** $1 \cdot n = n$

Sort out this wonky formatting

We can expand this number system by including:

1. an ***additive identity*** ($n + 0 = n$ for all $n \in \mathbb{N}$)
2. ***additive inverses*** (for all $n \in \mathbb{N}$, add $-n$ so $-n + n = 0$)

From this, we can construct the set of integers.

Definition 4.2.1 ▸ Integers $\mathbb{Z}$

The set of ***integers*** is defined as:

$$\mathbb{Z} \coloneqq \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$$

Definition 4.2.2 ▸ Even, Odd, Parity

Let $a \in \mathbb{Z}$.

- a is ***even*** if there exists $k \in \mathbb{Z}$ where $a = 2k$.
- a is ***odd*** if there exists $k \in \mathbb{Z}$ where $a = 2k + 1$.
- ***Parity*** describes whether an integer is even or odd.

Theorem 4.2.1 ▸ Parity Exclusivity

Every integer is either even or odd, never both.

TODO: prove this

Example 4.2.1 ▶ Parity of Square

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

Proof. We proceed by contraposition. Suppose n is not even. Then n is odd, and thus can be expressed as $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then:

$$\begin{aligned} n^2 &= (2k+1)(2k+1) \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Since the integers are closed under addition and multiplication, then $4k^2+4k \in \mathbb{Z}$. Thus, n^2 is odd. □

4.3 Rational Numbers $\mathbb{Q}$

We can further expand this number system by the following:

1. Include ***multiplicative inverses*** (for all $n \in \mathbb{Z} \setminus \{0\}$, define $1/n$ such that $n \cdot 1/n = 1$)
2. Define $m \cdot 1/n := m/n$ when $n \neq 0$.

From this, we can construct the set of rational numbers.

Definition 4.3.1 ▶ Rational Numbers $\mathbb{Q}$

The set of ***rational numbers*** is defined as:

$$\mathbb{Q} := \left\{ \frac{m}{n} : m, n \in Z \wedge n \neq 0 \right\}$$

To ensure multiplication works as intended, we also define $\frac{m}{n} \cdot \frac{k}{l} := \frac{m \cdot k}{n \cdot l}$.

We say $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ if and only if $m_1 n_1 = m_2 n_2$ where $n_1, n_2 \neq 0$. In other words, $\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \iff m_1 n_2 = m_2 n_1$. Thus, $\mathbb{Q}$ is the set of equivalence classes for this relation.

If $n = kp$ and $m = kq$, where $k, p, q \in \mathbb{Z}$, $k \neq 0$, $q \neq 0$, then:

$$\frac{n}{m} = \frac{kp}{kq} = \frac{k}{p}, \quad \text{because } kpq = kqp$$

If n and m have no common factor (except ±1), then we say that $n/m \in \mathbb{Q}$ is in the "lowest terms" or "reduced terms". The set $(Q, +, \cdot)$ forms a field. However, we cannot write $x = n/m$

where $x^2 = 2$.

Fix this whole section up. Very confusing.

Theorem 4.3.1 ▸ $\sqrt{2}$ is not a Rational Number

$\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose for contradiction $\sqrt{2}$ is a rational number. Then, there exist $n, m \in \mathbb{Z}$ such that $(n/m)^2 = 2$. If $n = kp$ and $m = kq$, then we can "cancel" the common factor k to write $n/m = p/q$. That is, we can assume that n and m have no (non-trivial) common factors. Now, $n^2/m^2 = 2$, so by multiplying both sides by m^2, we get $n^2 = 2m^2$. Thus, n^2 is an even number, so n is also even (Example 4.2.1). Then, we can write $n = 2k$ where $k \in \mathbb{Z}$. Then:

$$\begin{aligned} \implies \quad (2k)^2 &= 2m^2 \\ \implies \quad 4k^2 &= 2m^2 \\ \implies \quad 2k^2 &= m^2 \end{aligned}$$

Then m^2 is even, so m is even. Thus, m and n are both even, so they are multiples of 2. This contradicts the fact that we defined n/m in the lowest terms. □

Does there exist $r \in \mathbb{Q}$ such that $r^2 = 3$?

Definition 4.3.2 ▸ Divides

For $a, b, \in \mathbb{Z}$, we say a ***divides*** b if b is a multiple of a.

$$a \mid b \iff \exists(c \in \mathbb{Z})(b = ac)$$

Theorem 4.3.2 ▸ Division Algorithm

Suppose $a, b \in \mathbb{Z}$. Then $a = kb + r$ where $k \in \mathbb{Z}$ and $r \in \mathbb{Z}$ where $0 \leq r < a$.

Need proof here

Example 4.3.1

If $p \in \mathbb{N}$ and $3 \mid p^2$, then $3 \mid p$.

Proof. By the division algorithm, $p = 3k + j$ where $k \in \mathbb{Z}$ and $j \in \mathbb{Z}$ where $0 \leq j < 3$. Then, $p^2 = (3k+j)^2 = 9k^2+6kj+j^2$. Suppose that $3 \mid p^2$. Then, $p^2 = 3l = 9k^2+6kj+j^2$. Thus:

$$j^2 = 3l - 9k^2 - 6kj = 3(l - 3k^2 - 2kj)$$

We have $3 \mid j^2$. Hence, $j \neq 1, j \neq 2$, leaving only $j = 0$. Therefore, $p = 3k + 0$, so $3 \mid p$. □

Example 4.3.2 ▶ $\sqrt{3}$ is not a Rational Number

Proof. Suppose for contradiction $\sqrt{3}$ is a rational number. Then, there exist $n, m \in \mathbb{Z}$ such that $({}^{n}\!/\!_{m})^2$. If n and m share a common factor, then we can “cancel” the common factor to where ${}^{n}\!/\!_{m} = {}^{kp}\!/\!_{kq} = {}^{p}\!/\!_{q}$. Thus, we may assume that n and m have no nontrivial common factor.

$$\begin{aligned} \left(\frac{n}{m}\right)^2 &= 3 \\ \implies \quad \frac{n^2}{m^2} &= 3 \\ \implies \quad n^2 &= 3m^2 \end{aligned}$$

Thus, $3 \mid n^2$, so $3 \mid n$ by the previous lemma. Writing $n = 3k$ for some $k \in \mathbb{Z}$, we have:

$$\begin{aligned} (3k)^2 &= 3m^2 \\ \implies \quad 9k^2 &= 3m^2 \\ \implies \quad 3k^2 &= m^2 \end{aligned}$$

That is, $3 \mid m^2$ so $3 \mid m$. Thus, 3 divides both n and m. This contradicts the fact that we defined ${}^{n}\!/\!_{m}$ in the lowest terms. □

4.4 Fields

Definition 4.4.1 ▶ Field

A ***field*** is a set F with two defined operations, addition and multiplication, satisfying the following for all $a, b, c \in F$:

Axiom	Addition	Multiplication
Associativity	$(a+b)+c=a+(b+c)$	$(ab)c=a(bc)$
Commutativity	$a+b=b+a$	$ab=ba$
Distributivity	$a(b+c)=ab+ac$	$(a+b)c=ac+bc$
Identities	$\exists(0\in\mathbb{F})(a+0=a)$	$\exists(1\in\mathbb{F})(1\neq 0\wedge 1a=a)$
Inverses	$\exists(-a\in\mathbb{F})(a+(-a)=0)$	$(a\neq 0)\iff\exists(a^{-1}\in\mathbb{F})(aa^{-1}=1)$

All the “standard facts” of arithmetic and algebra in $\mathbb{R}$ follows from these axioms.

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are infinite fields, but $\mathbb{Z}_p$ (arithmetic modulo p) is a finite field if p is prime.

More generally, F_q where $q=p^k$ is a finite field.

Theorem 4.4.1 ▸ Facts about Fields

Let F be a field. For all $a,b,c\in F$:

(a) if $a+c=b+c$, then $a=b$

(b) $a\cdot 0=0$

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

(d) $(-a)\cdot(-b)=a\cdot b$

(e) if $a\cdot c=b\cdot c$ and $c\neq 0$, then $a=b$

(f) if $a\cdot b=0$, then $a=0$ or $b=0$

(g) $-(-a)=a$

(h) $-0=0$

Proof of (g).

$$\begin{aligned}
-(-a) &= -(-a)+0\\
&= -(-a)+(a+(-a))\\
&= -(-a)+(-a+a)\\
&= (-(-a)+(-a))+a\\
&= ((-a)+-(-a))+a\\
&= 0+a\\
&= a+0\\
&= a
\end{aligned}$$

□

4.5 Ordered Fields

Definition 4.5.1 ▶ Ordered Field

An ***ordered field*** is a field with a relation $<$ such that for all $a, b, c \in F$:

Axiom	Description
Trichotomy	Only one is true: $a < b$, $a = b$, or $b < a$
Transitivity	if $a < b$ and $b < c$ then $a < c$
Additive Property	if $b < c$, then $a + b < a + c$
Multiplicative Property	if $b < c$ and $0 < a$, then $a \cdot b < a \cdot c$

We then define $>$ as the inverse relation of $<$.

Theorem 4.5.1 ▶ Facts about Ordered Fields

- if $a < b$ then $-b < -a$
- if $a < b$ and $c < 0$, then $cb < ca$
- if $a \neq 0$, then $a^2 = a \cdot a > 0$
- $0 < 1$
- if $0 < a < b$ then $0 < {}^1\!/_b < {}^1\!/_a$

Although $\mathbb{C}$ is a field, it is not an ordered field. We can certainly define some kind of "order" on $\mathbb{C}$, but there is no way to make it satisfy the four axioms of an ordered field. For example, $i^2 = -1 < 0$, contradicting the fact that any nonzero number's square is greater than 0 in an ordered field.

$\mathbb{R}$ and $\mathbb{Q}$ are ordered fields.

Definition 4.5.2 ▶ Absolute Value

Let F be an ordered field. For $a \in F$, we define the ***absolute value*** of a as:

$$|a| := \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases}$$

We can think of $|a-b|$ as the distance between a and b. More generally, $|a-b| = d(a,b)$ is the metric we will be using throughout real analysis.

Theorem 4.5.2 ▶ Properties of Absolute Value

- $|a| \geq 0$, $a \leq |a|$, and $-a \leq |a|$
- $|ab| = |a||b|$

Theorem 4.5.3 ▶ Triangle Inequality

Let F be an ordered field. For any $a, b \in F$, $|a+b| \leq |a| + |b|$.

Proof. There are two cases to consider. If $a + b \geq 0$, then:

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

If $a + b < 0$, then:

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

□

4.6 Completeness

Definition 4.6.1 ▶ Bounded Above, Bounded Below, Bounded

Let F be an ordered field, and let $A \subseteq F$.

- A is ***bounded above*** if there exists $b \in F$ such that $a \leq b$ for all $a \in A$. In this context, b is an ***upper bound*** for A.
- A is ***bounded below*** if there exists $c \in F$ such that $c \leq a$ for all $a \in A$. In this context, c is a ***lower bound*** for A.
- A is ***bounded*** if A is bounded above and bounded below.

Example 4.6.1 ▶ Upper and Lower Bounds

Consider the set $(0,1) := \{x \in \mathbb{R} : 0 < x < 1\}$.

- $(0,1)$ is bounded above by 1 and any number greater than 1.
- $(0,1)$ is bounded below by 0 and any negative number.

Consider the set $[3,\infty) := \{x \in \mathbb{R} : 3 \leq x\}$.

- $[3,\infty)$ is not bounded above.
- $[3,\infty)$ is bounded below by 3 and any number less than 3.

Definition 4.6.2 ▶ Maximum, Minimum

Let F be an ordered field, and let $A \subseteq F$.

- If there exists $M \in A$ such that M is an upper bound for A, then M is the ***maximum*** of A, denoted $M = \max A$
- If there exists $m \in A$ such that m is a lower bound for A, then m is the ***minimum*** of A, denoted $m = \min A$.

Note that from the above example, $(0,1)$ has neither a maximum nor a minimum. However, 3 is the minimum of $[3,\infty)$.

Definition 4.6.3 ▶ Supremum

Let F be an ordered field, and let $A \subseteq F$. $s \in F$ is a ***supremum*** of A if:

1. s is an upper bound for A, and
2. if t is an upper bound for A, then $s \leq t$.

In other words, the supremum is the least upper bound for A. If A has a supremum, then that supremum is unique.

Prove this

Theorem 4.6.1 ▶ Maximum is the Supremum

Let F be an ordered field, and let $A \subseteq F$. If A has a maximum M, then $M = \sup A$.

Proof. Since $M = \max A$, we know M is an upper bound for A. Let t be an upper bound for A. Since $M \in A$, then $t \geq M$. Thus, M is less than or equal to any upper bound t, so $M = \sup A$. □

Example 4.6.2 ▸ Supremum of $(0, 1)$

Prove that $\sup(0,1) = 1$.

Proof. First, note that 1 is an upper bound for $(0,1)$. Next, suppose that $t \in \mathbb{Q}$ is an upper bound for $(0,1)$. Since $0 < {}^{1}/_{2} < 1$, then $0 < {}^{1}/_{2} \leq t$. By transitivity, $t > 0$. Suppose for contradiction $t < 1$. Because $0 < t < 1$, we have $1 < 1 + t < 2$. Dividing across by 2, we have ${}^{1}/_{2} < {}^{1+t}/_{2} < 1$. That is, ${}^{1+t}/_{2} \in (0,1)$. But $t < 1$, so $2t < 1 + t$. Thus, $t < {}^{1+t}/_{2}$. This contradicts our assumption that t is an upper bound for $(0,1)$. Therefore, $t \geq 1$, so $\sup(0,1) = 1$. □

Definition 4.6.4 ▸ Completeness

An ordered field F is ***complete*** if every nonempty subset of F that is bounded above has a supremum in F.

Theorem 4.6.2 ▸ $\mathbb{Q}$ is not complete

Proof sketch. Let $A \coloneqq \{x \in \mathbb{Q} : x^2 < 2\}$. In other words, $A = \left(-\sqrt{2}, \sqrt{2}\right) \subseteq \mathbb{Q}$. Then A is nonempty and bounded above. Suppose for contradiction that $\mathbb{Q}$ is complete. Then A has a supremum, say $s = \sup(A)$. Consider the following cases:

1. If $s^2 < 2$, let $n \in \mathbb{N}$ such that $\left(s + {}^{1}/_{n}\right)^2 < 2$. Then $s + {}^{1}/_{n} \in A$, contradicting s being an upper bound for A.
2. If $s^2 > 2$, let $n \in \mathbb{N}$ such that $\left(s - {}^{1}/_{n}\right)^2 > 2$. Then $s - {}^{1}/_{n}$ is an upper bound smaller than s, contradicting s being the least upper bound (supremum).
3. If $s^2 = 2$, then $s \notin \mathbb{Q}$ (Theorem 4.3.1).

Thus, $A \subseteq \mathbb{Q}$ does not have a supremum. Therefore, $\mathbb{Q}$ is not complete. □

Definition 4.6.5 ▸ Real Numbers $\mathbb{R}$

The ***real numbers*** are a set $\mathbb{R}$ with two operations, $+$ and $\cdot$, and order relation $<$ such that:

1. $(R, +, \cdot)$ is a field,
2. $(\mathbb{R}, +, \cdot, <)$ is an ordered field, and
3. $(\mathbb{R}, +, \cdot, <)$ is complete.

Alternatively, $\mathbb{R}$ can be constructed explicitly using “Dedekind cuts”. Either way, $\mathbb{R}$ is the **only** unique complete ordered field up to isomorphism. That is, if there is some other imposter complete ordered field $\mathbb{R}'$, we can map every element of $\mathbb{R}$ to $\mathbb{R}'$ such that we preserve all the operations and relations between things in $\mathbb{R}$. More formally, there exists an isomorphism $T : \mathbb{R} \to \mathbb{R}'$ where T is bijective, and:

- $T(x + y) = T(x) + T(y)$
- $T(xy) = T(x)T(y)$
- $x < y \iff T(x) < T(y)$

Additionally, $\mathbb{N} \subseteq \mathbb{R}$ where $\mathbb{N}$ satisfies the Peano axioms.

Theorem 4.6.3 ▸ $\sqrt{2}$ is a Real Number

Proof sketch. Let $A \coloneqq \left\{x \in \mathbb{R} : x^2 < 2\right\}$.

- Show $A \neq \varnothing$ and A is bounded above
- Completeness says $s \coloneqq \sup A$ exists
- Show $s^2 = 2 \implies s = \sqrt{2} \in \mathbb{R}$.

More generally, if $n, m \in \mathbb{N}$, then $\sqrt[n]{m} \in \mathbb{R}$. □

5 Suprema and Infima

Definition 5.0.1 ▶ Infimum

Let F be an ordered field, and let $A \subseteq F$. s is the ***infimum*** of A if:

1. s is a lower bound for A, and
2. s is greater than every other lower bound for A.

We can prove that the existence of infima is already implied by completeness.

Theorem 5.0.1 ▶ Existence of Infima in $\mathbb{R}$

Let $A \subseteq \mathbb{R}$ be nonempty and bounded below. Then A has an infimum in $\mathbb{R}$.

Proof. Let $A \subseteq \mathbb{R}$ be nonempty and bounded below. Let B be the set of all lower bounds for A. In other words, $B \coloneqq \{b \in \mathbb{R} : \forall(a \in A)(b < a)\}$. Since A is bounded below, then B is nonempty. Note also that B is bounded above by element of A. By completeness, $s \coloneqq \sup B$ exists. Now, we need to show that $\sup B = \inf A$.

1. Every $a \in A$ is an upper bound for B, and $\sup B$ is the least upper bound for B. Then, $\sup B \leq a$. That is, $\sup B$ is a lower bound for A.

2. Let t be a lower bound for A. Then, by definition of B, it follows that $t \in B$. Then $t \leq \sup B$ as required.

Therefore, $\sup B = \inf A$ in $\mathbb{R}$. □

Theorem 5.0.2 ▶ Well-Ordering Principle

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

Proof. We will use induction. For convenience, let $P(n)$ represent the following statement: "If $A \subseteq \mathbb{N}$ and $A \cap \{1, 2, \dots, n\} \neq \emptyset$, then A has a minimum."

Base Case: First, we will prove $P(1)$. If $A \subseteq \mathbb{N}$ and $A \cap \{1\} \neq \emptyset$, then $1 \in A$, so A has a minimum.

Induction Step: Assume that $P(n)$ holds for some $n \in N$. Suppose $A \subseteq \mathbb{N}$ and $A \cap$

$\{1, 2, \ldots, n+1\} \neq \varnothing$.

1. If $A \cap \{1, 2, \ldots, n\} \neq \varnothing$, then A has a minimum by $P(n)$.
2. If $A \cap \{1, 2, \ldots, n\} = \varnothing$, then $n+1 \in A$, so $\min A = n+1$.

By induction, $P(n)$ holds for all $n \in \mathbb{N}$. If $A \subseteq \mathbb{N}$ and $A \neq \varnothing$, then there exists $m \in A$ such that $m \in \mathbb{N}$. By $P(m)$ (which is true by induction), the set A has a minimum. □

Theorem 5.0.3 ▶ Pushing Supremum

Let A be a nonempty subset of $\mathbb{R}$, and let b, c be real numbers.

(a) If $a \leq b$ for all $a \in A$, then $\sup A \leq b$.

(b) If $c \leq a$ for all $a \in A$, then $c \leq \inf A$.

Intuition: Consider the interval $A := (0, 1)$. Because $a \leq 1$ for all $a \in (0, 1)$, we have $\sup A \leq 1$. Because $0 \leq a$ for all $a \in (0, 1)$,we have $0 \leq \inf A$.

Proof of (a). Since $a \leq b$ for all $a \in A$, then b is an upper bound for A. By completeness, A has a supremum, and $s := \sup A$ is the least upper bound for A. Thus, $s \leq b$. □

Proof of (b). □

Example 5.0.1

Suppose $A, B \subseteq \mathbb{R}$, $A \neq \varnothing$, $A \subseteq B$, and B is bounded above. Prove that A is bounded above and $\sup A \leq \sup B$.

Proof. Since $A \subseteq B$ and $A \neq \varnothing$, then $B \neq \varnothing$. Also, B is bounded above, so B has a supremum (by completeness). Let $a \in A$ be arbitrary. Then $a \in B$, so $a \leq \sup B$. Thus, A is bounded above, so A has a supremum (by completeness). By Pushing Supremum, $\sup A \leq \sup B$. □

Theorem 5.0.4 ▶ Approximation Property of Suprema and Infima

Suppose A is a nonempty subset of $\mathbb{R}$, and $s, r \in \mathbb{R}$. Then:

(a) $s = \sup A$ if and only if (i) s is an upper bound for A, and (ii) for all $\epsilon > 0$, there exists $a \in A$ such that $s - \epsilon < a$.

(b) $r = \inf A$ if and only if (i) r is a lower bound for A, and (ii) for all $\epsilon > 0$, there exists $a \in A$ such that $a < r + \epsilon$.

Intuition: If we nudge the supremum ever so slightly to the left, then we must have moved past something in A.

Proof of (a). Let $s := \sup A$. Then (i) holds by definition of suprema. To prove (ii), let $\epsilon > 0$. Since $s - \epsilon < s$, then $s - \epsilon$ is not an upper bound for A. Therefore, there exists $a \in A$ such that $s - \epsilon < a$.

Conversely, suppose that (i) and (ii) hold. We need to show $s = \sup A$. From (i), we know that s is an upper bound for A. Now, we need to show that s is the least upper bound. Let t be an upper bound for A. Suppose for contradiction that $t < s$. Let $\epsilon := s - t > 0$. Then $t = s - \epsilon$. By (ii), there exists $a \in A$ such that $a > s - \epsilon = t$. This contradicts t being an upper bound for A. Thus, there is no upper bound less than s. Therefore, $s = \sup A$. □

5.1 Consequences of Completeness

Theorem 5.1.1 ▶ $\mathbb{N}$ is not Bounded Above

Proof. Suppose for contradiction $\mathbb{N}$ is bounded above. Since $\mathbb{N}$ is not empty, then $\mathbb{N}$ has a supremum in $\mathbb{R}$. Let $s := \sup \mathbb{N} \in \mathbb{R}$. Then $n \leq s$ for all $n \in \mathbb{N}$. By the Peano axioms, n has a successor $n + 1 \in \mathbb{N}$, so $n + 1 \leq s$ for all $n \in \mathbb{N}$. Therefore, $n \leq s - 1$ for all $n \in \mathbb{N}$. This contradicts s being the least upper bound for $\mathbb{N}$. □

Theorem 5.1.2 ▶ Archimedean Principle

Suppose $x, y \in \mathbb{R}$ where $x > 0$. Then, there exists $n \in \mathbb{N}$ such that $nx > y$.

Intuition: This is basically an extension of the fact that $\mathbb{N}$ is not bounded above.

Proof. Since y/x is not an upper bound for $\mathbb{N}$, then there exists $n \in \mathbb{N}$ such that $n > y/x$. Since $x > 0$, then $nx > y$. □

Theorem 5.1.3 ▶ Density of $\mathbb{Q}$ in $\mathbb{R}$

Suppose $x, y \in \mathbb{R}$ where $x < y$. Then there exists $r \in Q$ such that $x < r < y$.

Intuition: Given any two different real numbers, there's some rational number between them.

Proof. We will consider three cases:

1. If $x \geq 0$, then $0 \leq x < y$. Since $y - x > 0$, then by the Archimedean Principle, there exists $n \in \mathbb{N}$ such that $n(y - x) > 1$. We want to show there is a natural number between nx and ny. Let $A := \{k \in \mathbb{N} : k > nx\}$. Since $\mathbb{N}$ isn't bounded above, then A is not empty. By the Well-Ordering Principle, A has a minimum. Let $m := \min A$. Then $m > nx$, and $m - 1 \leq nx$. Thus, $m \leq nx + 1$, so:

   $$nx < m \leq nx + 1 < ny$$

   Dividing across by n yields $x < {}^{m}/_{n} < y$. Note that $m, n \in \mathbb{N} \subseteq \mathbb{Z}$, so ${}^{m}/_{n} \in \mathbb{Q}$.

2. If $x < 0$ and $y > 0$, then $x < 0 < y$ where $0 \in \mathbb{Q}$.

3. If $x < 0$ and $y \leq 0$, then $x < y \leq 0$. Multiplying across by -1, we have $-x > -y \geq 0$. By the first case, there must exist $t \in \mathbb{Q}$ where $-y < t < -x$. Multiply across by -1 again to attain $y > -t > x$ where $-t \in \mathbb{Q}$.

This completes the proof. □

Theorem 5.1.4 ▶ $\sqrt{2}$ is a Real Number

There exists $s \in \mathbb{R}$ such that $s^2 = 2$.

Proof. Let $A := \left\{x \in \mathbb{R} : x^2 < 2\right\}$. Since $0^2 < 2$, then $0 \in A$, so A is not empty. Also, A is bounded above, for example by 2. By completeness, A must have a supremum in $\mathbb{R}$. Let $s := \sup A$. We will use trichotomy to show that $s^2 = 2$.

1. If $s^2 > 2$, then...

> **Scratchwork:** We need to show that this is not possible, i.e. show there is some $s - {}^{1}/_{n}$ that is less than s but is still an upper bound for A. We want $(s - {}^{1}/_{n})^2 > 2$. Then, $s^2 - {}^{2s}/_{n} + {}^{1}/_{n^2} > 2$. We can chop off the ${}^{1}/_{n^2}$, reducing the inequality to $s^2 - {}^{2s}/_{n} > 2$. Thus, we need to choose $n > \frac{2s}{s^2-2}$.

… let $n \in \mathbb{N}$ such that $n > \frac{2s}{s^2-2}$. Then:

$$\begin{aligned} & n > \frac{2s}{s^2-2} \\ \implies \quad & s^2 - \frac{2s}{n} > 2 \\ \implies \quad & s^2 - \frac{2s}{n} + \frac{1}{n^2} > 2 \\ \implies \quad & \left(s - \frac{1}{n}\right)^2 > 2 \end{aligned}$$

Thus, $s - {}^1\!/_n$ is an upper bound for A that is less than s. This contradicts s being the supremum for A.

2. If $s^2 < 2$, then…

> **Scratchwork:** Again, we need to show that this is not possible. We know that in this case, $s \in A$, so we need to find another thing in A that is bigger than s. In other words, we want some $(s + {}^1\!/_n)^2 < 2$. Then, $s^2 + {}^{2s}\!/_n + {}^1\!/_{n^2} < 2$. Choose $n > {}^1\!/_{2s}$ and $n > \frac{4s}{2-s^2}$.
>
> $$\left(s + \frac{1}{n}\right)^2 = s^2 + \frac{2s}{n} + \frac{1}{n^2}$$

… let $n \in \mathbb{N}$ such that $n > \max\left\{\frac{1}{2s}, \frac{4s}{2-s^2}\right\}$. Then $\frac{1}{n} < 2s$ and $s^2 + \frac{4s}{n} < 2$. So:

$$\begin{aligned} \left(s + \frac{1}{n}\right)^2 &= s^2 + \frac{2s}{n} + \frac{1}{n^2} \\ &< s^2 + \frac{2s}{n} + \frac{2s}{n} \\ &= s^2 + \frac{4s}{n} < 2 \end{aligned}$$

That is, $s + \frac{1}{n} \in A$. This contradicts s being an upper bound for A.

By trichotomy, $s^2 = 2$. ▢

Theorem 5.1.5 ▸ Nested Interval Property

Suppose that for each $n \in \mathbb{N}$, $a_n, b_n \in \mathbb{R}$ with $a_n \leq b_n$, and $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ for all $n \in \mathbb{N}$. Then $\bigcap_{n=1}^{\infty} [a_n, b_n] \neq \varnothing$.

Intuition: We can move the two borders of an open interval closer and closer to each other, and it won't be empty.

Proof. Note that $a_n \leq a_{n+1} \leq a_{n+2} \leq \ldots$ and $\ldots \leq b_{n+2} \leq b_{n+1} \leq b_n$. If $k \leq n$, then $a_k \leq a_n \leq b_n$.

- If $k \leq n$, then $a_k \leq a_n \leq b_n$.
- If $k \geq n$, then $a_k \leq b_k \leq b_n$.

That is, $a_k \leq b_n$ for all $k_n \in \mathbb{N}$. Let $A \coloneqq \{a_k : k \in \mathbb{N}\}$. Then A is bounded above, for example by b_1. Also, A is not empty. By completeness, A has a supremum. Let $s \coloneqq \sup A$. Note that since s is an upper bound for A, then $a_n \leq \sup A$ for all $n \in \mathbb{N}$. Also note that $\sup A$ is the least upper bound for A, so $\sup A \leq b_n$ for all $n \in \mathbb{N}$. Thus, $a_n \leq \sup A \leq b_n$ for all $n \in \mathbb{N}$, so $\sup A \in [a_n, b_n]$ for all $n \in \mathbb{N}$. Thus, $\sup A \in \bigcap_{n=1}^{\infty}[a_n, b_n]$, so it is not empty. ▢

The nested interval property is actually false for open intervals!

$$\forall(x \in (0,1))\exists(n \in \mathbb{N})(1/n < x \implies x \notin (0, 1/n))$$

6

Cardinality

Definition 6.0.1 ▶ Cardinality

Cardinality is a measure of the amount of elements in a set, denoted $|A|$. We say two sets have the same cardinality if there exists a bijection between them.

For finite sets, we can think of cardinality as the number of elements in that set. For infinite sets, cardinality can sometimes go against our intuition. For any sets A, B, C:

1. $|A| = |A|$
2. if $|A| = |B|$, then $|B| = |A|$
3. if $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

Hence, equality of cardinalities is an equivalence relation.

Example 6.0.1 ▶ Cardinality of $\mathbb{N}$ and $2\mathbb{N}$

Let $2\mathbb{N} \coloneqq \{2n : n \in \mathbb{N}\}$ (i.e. the set of even natural numbers). Then $|\mathbb{N}| = |2\mathbb{N}|$.

Proof. To show that these two sets have the same cardinality, we need to find some bijection between the sets. Let $f : \mathbb{N} \to 2\mathbb{N}$ be a function defined by $f(n) = 2n$. Note that f is well-defined (i.e. is actually a function) because $f(n) \in 2\mathbb{N}$ for all $n \in \mathbb{N}$. To prove that f is a bijection, we need to prove it is both injective and surjective.

1. Let $n_1, n_2 \in \mathbb{N}$ such that $f(n_1) = f(n_2)$. Then $2n_1 = 2n_2$, so $n_1 = n_2$. Thus, f is injective.

2. Let $m \in 2\mathbb{N}$. Then $m = 2k$ for some $k \in \mathbb{N}$, so $m = 2k = f(k)$ for some $k \in \mathbb{N}$. Thus, f is surjective.

Therefore, f is a bijection, so $|\mathbb{N}| = |2\mathbb{N}|$. ▢

Example 6.0.2 ▶ Cardinality of Intervals

Let $a, b \in \mathbb{R}$ where $a < b$. Then $|(0, 1)| = |(a, b)|$.

Proof. We need to find a bijection from $(0,1)$ to (a,b). We need to "scale" the interval $(0,1)$ to the width of (a,b), then translate it to match (a,b). Define $f : (0,1) \to (a,b)$ by $f(x) = a+(b-a)x$. (We need to check f is well-defined). Let $x \in (0,1)$. Then $0 < x < 1$, so multiplying by $(b-a)$ which is positive gives $0 < (b-a)x < b-a$. Adding a, we get $a < a+(b-a)x < b$. Now we need to show f is a bijection:

1. Let $x_1, x_2 \in (0,1)$ such that $f(x_1) = f(x_2)$. Then $a+(b-a)x_1 = a+(b-a)x_2$. Subtracting a from both sides, we get $(b-a)x_1 = (b-a)x_2$. Since $(b-a) \neq 0$, we can divide both side by $(b-a)$ to get $x_1 = x_2$.

2. Let $y \in (a,b)$.

> **Scratchwork:** We want to find some $x \in (0,1)$ where $y = f(x) = a+(b-a)x$. Using some algebra to solve for x, we have $x = \frac{y-a}{b-a}$

Let $x = \frac{y-a}{b-a}$. First, we show $x \in (0,1)$:

$$\begin{aligned} & a < y < b \\ \implies \quad & 0 < y-a < b-a \\ \implies \quad & 0 < \frac{y-a}{b-a} < 1 \end{aligned}$$

Thus, $x \in (0,1)$. Also:

$$f(x) = a+(b-a)\left(\frac{y-a}{b-a}\right) = a+(y-a) = y$$

Thus, f is surjective.

Therefore, f is a bijective, so $|(0,1)| = |(a,b)|$. □

Definition 6.0.2 ▸ Power Set

Let A be a set. The ***power set*** of A is the set of all subsets of A.

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

For example, the power set of $\{1,2,3\}$ is $\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. For any finite set with n elements in it, its power set has 2^n elements in it.

Example 6.0.3 ▸ Cardinality of $\mathbb{N}$ and $\mathcal{P}(N)$

$|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$

Proof. We will show that any function $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ cannot be surjective, and thus not bijective. Let $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ be any function defined by $f(n) = A_n$. Note $A_n \subseteq \mathbb{N}$, so $A_n \in \mathcal{P}(A)$. Now we will define a set that isn't in $f[\mathbb{N}]$. For each $n \in \mathbb{N}$, if $n \in A_n$, then $n \notin A$, and if $n \notin A_n$, then $n \in A$. More formally, $A \coloneqq \{n \in \mathbb{N} : n \notin A_n\}$. For all $k \in \mathbb{N}$, note that:

- if $k \in A_k$, then $k \notin A$, so $A \neq A_k$, and
- if $k \notin A_k$, then $k \in A_k$, so $A \neq A_k$.

Hence, $A \subseteq \mathbb{N}$, but $f(k) \neq A$ for any $k \in \mathbb{N}$. Thus, f is not surjective. □

Definition 6.0.3 ▸ Finite, Countably Infinite, Countable, Uncountable

Let A be a set. We say A is:

- ***finite*** if $A \neq \varnothing$ or $|A| = |\{1, 2, \dots, n\}|$ for some $n \in \mathbb{N}$.
- ***countably infinite*** if $|A| = |N|$.
- ***countable*** if A is finite or countably infinite
- ***uncountable*** if A is not countable

Theorem 6.0.1 ▸ $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof. We know from Example 6.0.3 that $\mathcal{P}(\mathbb{N})$ is not countably infinite. We need to show that $\mathcal{P}(\mathbb{N})$ is not finite. Since $\{1\} \in \mathcal{P}(\mathbb{N})$, then it cannot be empty. Suppose for contradiction $|\{1, 2, \dots, n\}| = |\mathcal{P}(\mathbb{N})|$ for some $n \in \mathbb{N}$, then there exists a bijection $f : \{1, 2, \dots, n\} \to \mathcal{P}(\mathbb{N})$. Define $g : \mathbb{N} \to \{1, 2, \dots, n\}$ by:

$$g(k) = \begin{cases} k, & 1 \leq k \leq n \\ 1, & k > n \end{cases}$$

Then g is surjective, so $f \circ g : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ is surjective. This contradicts the fact that no such function exists (by Example 6.0.3). □

Generally, there is never a bijection from a set to its power set.

Intuition: A set is countable if its elements can be "listed" or "counted". That is, for finite sets:

$$X = \{x_1, x_2, \dots, x_n\} = \{x_k\}_{k=1}^{n}$$

For infinitely countable sets:

$$X = \{x_1, x_2, \dots\} = \{x_k\}_{k=1}^{\infty}$$

If X is finite, then there exists a bijection $f : \{1, 2, \dots, n\} \to X$. Thus, $X = \{f(1), f(2), \dots, f(n)\}$. If X is countably infinite, then there exists a bijection $f : \mathbb{N} \to X$. Thus, $X = \{f(1), f(2), \dots\}$.

Theorem 6.0.2 ▶ Subsets of Countable Sets are Countable

The subset of a countable set is still countable. (i.e. a countable set cannot contain an uncountable subset).

Proof. Let X be a countable set, and let $A \subseteq X$. We will consider two cases. First, if A is finite, then A is countable, and we are done. Otherwise, A is infinite, and hence X is infinite. Then X is countably infinite, so $X = \{x_1, x_2, \dots\} = \{x_k\}_{k=1}^{\infty}$.

Idea: Our set A might look something like $\{x_3, x_4, x_6, \dots\}$. We need to align these indices to 1, 2, 3, and so on. We'll let $k_1 = \min\{3, 4, 6, \dots\}$, let $k_2 = \min\{4, 6, \dots\}$, and so on.

Let $k_1 \coloneqq \min\{k \in \mathbb{N} : x_k \in A\}$. Let $a_1 \coloneqq x_{k_1}$. For all $j \in \mathbb{N}$ such that $j > 1$, we define $k_j \coloneqq \min\{k \in \mathbb{N} : (x_k \in A) \wedge (k > k_{j-1})\}$. Let $a_j \coloneqq x_{k_j}$. Then $1 \leq k_1 < k_2 < k_3 < \dots$, so k_j approaches infinity. Let $g : \mathbb{N} \to A$ be a function defined by $g(j) = a_j$. We need to show that g is both injective and surjective, and thus a bijection.

- Suppose that $g(j_1) = g(j_2)$ for some $j_1, j_2 \in \mathbb{N}$. Then $a_{j_1} = a_{j_2}$, so $x_{k_{j_1}} = x_{k_{j_2}}$. Then $k_{j_1} = k_{j_2}$, so $j_1 = j_2$. Thus, g is injective.
- Let $a \in A$ Since $A \subseteq X$, then $a \in X$. Thus, $a = x_l$ for some $l \in \mathbb{N}$. Let $m \coloneqq \min\{j \in \mathbb{N} : k_j \geq l\}$. Since $m \in \{j \in \mathbb{N} : j_k \geq l\}$, then $k_m \geq l$. Also, $m - 1 \notin \{j \in \mathbb{N} : k_j \geq l\}$, so $k_{m-1} < l$. Now, $k_m = \min\{k \in \mathbb{N} : (x_k \in A) \wedge (k > k_{m-1})\}$. But $x_l \in A$, and $l > k_{m-1}$, so $l \in \{k \in \mathbb{N} : (x_k \in A) \wedge (k > k_{m-1})\}$. Thus, $k_m \leq l$, because k_m is the

minimum of the set containing l. By trichotomy, $k_m = l$. Therefore:

$$g(m) = a_m = x_{k_m} = x_l = a$$

So g is surjective.

Since g is a bijection, then $|\mathbb{N}| = |A|$, so $|A|$ is countable. □

Theorem 6.0.3 ▶ Injectivity and Cardinality

Suppose $A = \varnothing$. Then A is countable if and only if there exists an injective function $f : A \to \mathbb{N}$.

Proof. First, suppose A is a countable set. We consider two cases:

- If A is countably infinite, then there exists a bijection $f : A \to \mathbb{N}$.
- If A is finite, then there exists a bijection $f : A \to \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$. Let $g : \{1, 2, \dots, n\} \to \mathbb{N}$ be a function defined by $g(x) = x$ (i.e. an inclusion mapping). Then f and g are both injective, so $g \circ f : A \to \mathbb{N}$ is injective.

Conversely, suppose $f : A \to \mathbb{N}$ is an injection. Then $f[A] \subseteq \mathbb{N}$, so $f[A]$ is countable by Theorem 6.0.2. Define $g : A \to f[A]$ by $g(a) = f(a)$. Then g is injective because f is injective, and g is surjective because $g[A] = f[A]$. Thus, g is a bijection, so $|A| = |f[A]|$. Therefore, A is countable. □

Theorem 6.0.4 ▶ $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

$\mathbb{N} \times \mathbb{N}$ is countable.

Proof. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function defined by $f(n, m) = 2^n 3^m$. We now show that f is bijective. To prove surjectivity, suppose $f(n_1, m_1) = f(n_2, n_2)$. Then $2^{n_1} 3^{m_1} = 2^{n_2} 3^{m_2}$.

- If $n_1 > n_2$, then $2^{n_1 - n_2} = 3^{m_2 - m_1}$. Since $n_1 > n_2$, we have $n_1 - n_2 > 0$, so $2^{n_1 - n_2} \in \mathbb{N}$. Then also $3^{m_2 - m_1} \in \mathbb{N}$. But $2^{n_1 - n_2}$ is even, and $3^{m_2 - m_1}$ is odd. This contradicts the fact that $2^{n_1 - n_2} = 3^{m_2 - m_1}$.
- If $n_2 > n_1$, then $3^{m_1 - m_2} = 2^{n_2 - n_1}$. By a similar argument, $2^{n_2 - n_1}$ is even and $3^{m_1 - m_2}$ is odd, producing the same contradiction.
- If $n_1 = n_2$, then $2^{n_1} = 2^{n_2}$, so cancelling gives $3^{m_1} = 3^{m_2}$. Thus, $m_1 = m_2$.

Hence, $(n_1, m_1) = (n_2, m_2)$, so f is injective. □

Index

Definitions

Examples

Techniques

Theorems