Introduction to Analysis

UT Knoxville, Spring 2023, MATH 341

Mike Frazier, Peter Humphries, Alex Zhang

February 7, 2023

Contents

Preface

These notes attempt to give a concise overview of the **Introduction to Analysis** course at the University of Tennessee (MATH 341). The contents of these notes come from Dr. Michael Frazier's lecture notes, Dr. Peter Humphries' lecture notes, and various online resources like the Mathematics Stack Exchange.

The first few weeks of the class are spent reviewing content from **Introduction to Abstract Mathematics** (MATH 300). As such, there will be much repeated content. Afterwards, we focus on analysis of real functions.

1 Introduction

Our goal is to understand the theory of real functions in one variable. Specifically, we will deal with functions, limits, sequences, convergence, continuity, differentiation, and integration. The same ideas, concepts, and techniques are used to study more complicated mathematics.

We will primarily focus on the idea of **convergence**. Many computational techniques and algorithms rely on iteration—successive approximations getting closer to an actual solution. In order for those algorithms to work, they need to converge towards an actual solution.

To motivate our quest to learn about convergence, let's look at some classic iterative methods.

Example 1.0.1 ▸ Newton's Method

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

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

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:

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

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 $n \to \infty$! In chapter 14, we will cover the Monotone Convergence Theorem, which states that any bounded monotone sequence converges.

Example 1.0.2 ▸ Monotone Convergence Theorem

Suppose that $c > 0$ and $x_1 > 0$. Then, for $n \geq 2$, the sequence $x_{n+1} = \frac{1}{2}\left(x - N + \frac{c}{x_n}\right)$ is:

- **bounded below** because $x_n > \sqrt{c}$ when $n \geq 2$, and
- **decreasing** because $x_n + 1 < x_n$ for $n \geq 2$.

Therefore, x_n converges by the Monotone Convergence Theorem, and $\lim_{n\to\infty} x_n = \sqrt{c}$.

Let's look at a more complicated iterative method.

Example 1.0.3 ▸ 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 $y(x)$.

The 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

Logic is the backbone of all formal mathematics. When building a logically sound model of mathematics, we start with a small collection of axioms. We then work with those axioms to deduce other logically sound statements, reaffirming what we already knew and discovering new ideas along the way.

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

The ***conjunction*** of two statements is itself a statement, which is true if and only if the two statements are both true.

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

Definition 2.1.3 ▶ Disjunction

The ***disjunction*** of two statements is itself a statement, which is true if and only if at least one of the 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 quick way to gauge whether simple statements hold, they become impractical once we involve more complicated statements. Furthermore, truth tables don't really show intuition behind complicated statements whereas proofs should ultimately fuel our intuition.

Very often, we will have to prove some implication like $p \implies q$. Recall how an implication is only false if p is true but q is false. Therefore, we would only have to consider that case where p is true but q is false. We can prove an implication is true by simply showing that such a case could never happen. There are three simple proof techniques for doing so:

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 a direct proof, the reasoning to get from p to q provides a lot of insight about the context of p and the surrounding mathematics. Similarly, the direct reasoning in proof by contrapositive provides context surrounding $\neg q$. However, the reasoning done in a proof by contradiction is based on a contradictory hypothesis. Thus, it is often less insightful and is typically avoided when a direct proof is readily available.[1]

That being said, it is sometimes easier to find a proof by contradiction than a direct proof. Whereas direct proof needs to deduce the correct path that leads to the conclusion, a proof by contradiction only needs to deduce any contradictory statement.

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:

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

Example 2.2.1 ▸ Truth Table of Proof by Contradiction

p	q	$p \implies q$	$\neg q$	$p \land (\neg q)$	$\neg [p \land (\neg q)]$
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:

$$(p \implies q) \iff \neg [p \land (\neg q)]$$

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.

[1] https://math.stackexchange.com/a/1688

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 $[p \implies (q \vee r)] \iff [(p \wedge \neg q) \implies r]$.

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

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

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

▢

3 Naive Set Theory

Set theory is a whole other can of worms that really isn't that meaningful right now. Instead of constructing an axiomatic basis for sets, we will just take a naive approach and define sets informally. That way, we can avoid the chicanery and get to what really matters.

3.1 Sets

Definition 3.1.1 ▸ Set

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

For example, $\mathbb{N} \coloneqq \{1, 2, 3 \ldots\}$ is the set of all natural numbers, and $\mathbb{Z} \coloneqq \{\ldots, 1, 2, 3, \ldots\}$ 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.

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

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 mathematics textbook, 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 avoid using $\subset$ to avoid any ambiguity.

Definition 3.1.6 ▶ Empty Set ($\varnothing$)

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

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

As a convention, we will assume that $\varnothing$ is a subset of any 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.

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

Definition 3.1.8 ▶ Intersection

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

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

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. In formal mathematics, it's conventional to actually 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 $y \in Y$.

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

Definition 3.2.2 ▸ Relation

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

Definition 3.2.3 ▸ Function

Let X and Y be sets. A ***function*** from X to Y is a subset of $X \times Y$ 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.

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

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

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

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

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

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

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

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

A function $f : X \to Y$ is ***surjective*** 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 $\square$

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 $\mathbb{N} \coloneqq \{1, 2, \ldots\}$. 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 axiom, we can derive a new proof technique for proving an arbitrary statement for all 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 $n \in \mathbb{N}$. ▢

A proof by induction kind of has a "domino effect". We set up the dominoes by proving $P(n) \implies P(n+1)$ and knock over the first domino by proving $P(1)$. The result is that all the dominoes will topple each other, leaving no domino standing.

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

Technique 4.1.1 ▸ Proof by Induction

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

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*** $1 \cdot n = n$

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:

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

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 $x^2 = 2$.

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

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

Proof. Suppose for contradiction $\sqrt{2}$ is a rationa 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 $0 \le r < a$.

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 $0 \le j < 3$. 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.

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

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

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

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 egnerally, $|a-b| = d(a,b)$ is the metric we are using.

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:

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

$\square$

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, Infimum

Let F be an ordered field, and let $A \subseteq F$. If there exists $s \in F$ such that:

1. s is an upper bound for A, and
2. $s < t$ for any upper bound t for A,

then s is the ***supremum*** of A, denoted $s = \sup A$.

If A has a supremum, then that supremum is unique. ()

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 $M = \sup A$. $\square$

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

Index

Definitions

Examples

Techniques

Theorems