Math 13: Intro to Abstract Math

Eli Griffiths

March 13, 2023

Table of Contents

A Paradigm Shift: Proofs

Compared to computational math classes, the pivotal component of higher level mathematics are **proofs**. A proof is generally

1. An argument that establishes the truth of a statement
2. Evidence that helps establish the truth of a statement

Conventionally in lower division math courses, algebraic manipulation and identities were utilized to assert the truth of some statement. More often, questions will be more abstract and therefore require tools or logic extending beyond the familiar world of computation.

1.1 Showing vs. Proving

Consider a rudimentary problem such as follows.

> **Conjecture 1.** If n is any odd integer, then $n^2 - 1$ is a multiple of 8.

It is tempting to immedietaly attempt to prove the conjecture using isolated computations as follows

$$\begin{aligned} n^2 - 1 &= (2k+1)^2 - 1 \\ &= 4k^2 + 4k \\ &= 4\underbrace{k(k+1)}_{even} \\ &= 8m \end{aligned}$$

While computational sequences can be useful to understand the skeleton of an argument, one should strive to produce a proof that exists independent of the conjecture or proposition. Therefore a more flushed out proof of conjecture 1 can be written out.

> ***Proof.*** Let n be an odd integer. By definition there exists an integer k such that $n = 2k + 1$. Note that
>
> $$\begin{aligned} n^2 - 1 &= (2k+1)^2 - 1 \\ &= 4k^2 + 4k \\ &= 4k(k+1). \end{aligned}$$
>
> If k is even, $k(k+1)$ is even and if k is odd, $k(k+1)$ is also even. Therefore by definition of eveness, there is an integer m such that $k(k+1) = 2m$. Therefore $n^2 - 1 = 4(2m) = 8m$. ■

Propositions

Definition 1 (Propositions)**.** A proposition is any statement that is either true or false

Examples of propositions are *"I had pizza on thursday"* or symbolic proposition such as $1+1=3$. Each of these statements can be assigned either true or false. It is helpful however to abstract propositions as variables. Using variables, we can define multiple useful operatives that act upon them. Truth tables provide a way to concretely define these operations. Assume there are propositions P and Q.

2.1 Proposition Operatives

Propositional operatives are defined through truth tables. Truth tables lay out all possible outcomes given a certain set of inputs. Some of the most common operatives are displayed in Table 2.1.

P	Q	$\wedge$	$\vee$	$\Rightarrow$	$\Leftrightarrow$	$\neg P$	$\neg Q$
T	T	T	T	T	T	F	F
T	F	F	T	F	F	F	T
F	T	F	T	T	F	T	F
F	F	F	F	T	T	T	T

Table 1: Truth table for common operatives

2.2 Translation of Operatives

Define the propositions P, Q, and R as

- P: Irvine is a city in California
- Q: Irvine is a city in Scotland
- R: Irvine has seven letters

Simple sentences using these propositions have symbolic representations. Some examples are

1. Irvine is a city in California and Irvine does not have seven letters
   - $P \wedge \neg R$
2. Irvine is a city in California and Irvine does not have seven letters
   - $P \wedge \neg R$
3. Irvine is a city in California and Irvine does not have seven letters
   - $P \wedge \neg R$

2.3 Operations on Conditionals

There are three introductory manipulations on conditionals that will be used

- Negation
- Converse
- Contrapositive

If given 2 propositions P and Q then the above bullets turn into

- $P \wedge \neg Q$
- $Q \implies P$
- $\neg Q \implies \neg P$

Theorem 1 (Contrapositive)**.** The contrapositive of an implication is logically equivalent to the original implication

Proof. Given two propositions P and Q, logical equivalence between $P \implies Q$ and $\neg Q \implies \neg P$ can be established directly.

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

■

The contrapositive is often useful as it changes an implication into something possibly easier to show.

Theorem 2. If there are 2 integers x and y and their sum $x + y$ is odd, then one of x or y are odd.

Proof. The symbolic representation of the theorem is

$$P \implies Q.$$

Where P is the statement that $x + y$ is odd, and Q is the statement that either x or y are odd. A direct proof here will not work out well, meaning a contrapositive approach may be better. The contrapositive of this implication is $\neg Q \implies \neg P$, or in written word: "If x and y have the same parity (both are even, both are odd), then their sum $x + y$ is even". This splits into two **cases**.

Case 1: Both are Even

Suppose that x and y are both even integers. There are integers k_1 and k_2 such that $x = 2k_1$ and $y = 2k_2$. Their sum is equal to $x + y = 2k_1 + 2k_2 = 2(k_1 + k_2)$. The resulting sum $2(k_1 + k_2)$ is even.

Case 2: Both are Odd

Suppose that x and y are both odd integers. There are integers k_1 and k_2 such that $x = 2k_1$ and $y = 2k_2$. Their sum is equal to $x + y = 2k_1 + 1 + 2k_2 + 1 = 2(k_1 + k_2 + 1)$. The resulting sum $2(k_1 + k_2 + 1)$ is even.

Therefore $x + y$ is even if both x and y have the same parity. ■

2.4 De Morgans Laws

Theorem 3 (De Morgans Laws)**.** Let P and Q be propositions. Then

1. $\neg(P \wedge Q) = \neg P \vee \neg Q$
2. $\neg(P \vee Q) = \neg P \wedge \neg Q$

Proof. Let P and Q be propositions.

De Morgans Law #1

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

Both produce the same outcomes, therefore they are logically equivalent

De Morgans Law #2

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

Both produce the same outcomes, therefore they are logically equivalent. ■

Take for example the statement

Cacao had one dinner and Lubu had one dinner

This proposition can be expresses as $P \wedge Q$, and therefore its negation, by De Morgans Law is $\neg P \vee \neg Q$. In words: "Caco had no dinner or Lubu had no dinner"

Definition 2 (Contradictions and Tautologies)**.**

Contradiction	A statement that is always false
Tautology	A statement that is always true

Method's of Proof

There are 4 standard proof methods, namely

- Direct Proof
- Contrapositive
- Contradiction
- Induction[1]

Each assume and show different things, but in the end are all logically equivalencies to $P \implies Q$. Therefore their usage varys depending on given information. Table shows what is assumed and what is shown in each method.

Method	**Direct**	**Contradiction**	**Contrapositive**
Assume	P	$P \wedge \neg Q$	$\neg Q$
Show	Q	Contradiction	$\neg P$

Compared to a direct proof or a contrapositive argument, a contradictive proof is slightly more subtle in its reasoning as doesn't directly assume one side of an implication to show the other.

Theorem 4 (Proof by Contradiction)**.** Given two propositions P and Q, if the assumption that P and $\neg Q$ are true results in a contradiction, then $P \implies Q$ is true.

Proof. Given two propositions P and Q, if the assumption that both P and $\neg Q$ are true arises in a contradiction, then $P \wedge \neg Q$ is false. $P \wedge \neg Q$ is logically equivalent to $\neg(P \implies Q)$. Therefore if $P \wedge \neg Q$ is false, then $P \implies Q$ is true. ■

Example. Prove the following statement: *suppose* $x \in \mathbb{Z}$ *and* $3x + 5$ *is even, then* $3x$ *is odd.*

This will be proved in each manner of proof (except induction). Firstly a direct proof.

Proof.

■

[1] Will be discussed later

3.1 Definition Pushing

Often, a definition is not limited to the specific case it concerns. Many times it can be proven to hold in other alternative cases. The act of expanding a definitions scope is called *definition pushing*. Here's an example of expanding the definition of integer divisibility.

Definition 3 (Divisbility)**.** Let $n, p \in \mathbb{Z}$. Then we say "n is divisible by p" if $\exists k \in \mathbb{Z}$ such that $n = pk$.

Theorem 5 (Square Divisibility)**.** Let $n \in \mathbb{Z}$. If n is divisible by p, then n^2 is divisible by p^2.

Proof. Let $n, p \in \mathbb{Z}$ such that n is divisible by p. By definition of divisiblity there exists $k \in \mathbb{Z}$ such that $n = pk$. Squaring both sides results in $n^2 = p^2k^2$. Since $k^2 \in \mathbb{Z}$, it follows that n^2 is divisible by p^2. ■

3.2 Proof by Counter Example

Consider Theorem 5 again. This time a proof by contradiction can be used.

Proof. Let $n, p \in \mathbb{Z}$. Assume towards contradiction that $p|n$ and $p^2 \nmid n^2$. Consider the case where $n = 8$ and $p = 2$. It is true that $p|n$. It follows that $n^2 = 64$ and $p^2 = 4$. It is also true that $p^2|n^2$. ■

In this instance, rather than find a general falsehood, a simple case can be used to disprove or prove the entire theorem. Cases like these are called *counter-examples* as they run counter to the proposition.

Divisibility and Modularity

4.1 Remainders and Mod

Calling back to elementary, when dividing an integer by another integer, it often resulted in there being a remainder. A more concrete definition can be offered when dividing by 3.

Definition 4. Let $a \in \mathbb{Z}$. There exists $k \in \mathbb{Z}$ and $n \in \{0, 1, 2\}$ such that $a = 3k + n$. In this case, n represent the remainder of a when divided by 3.

Consider now the following conjecture.

Conjecture 2. If $n \in \mathbb{Z}$, then n^2 has a remainder of 0 or 1 when divided by 3.

There is very little given information to prove this conjecture. However, the limited nature of remainders constricts what needs to be examined into something useable. By definition, all integers can be represented as a multiple of 3 plus a remainder. It also implies that the remainder of integers divided by 3 is cyclic, cycling between $\{0, 1, 2\}$.

Set Theory I

5.1 Sets

Definition 5 (Sets)**.** A set can be defined as a 'well-defined' collection of objects. Objects themselves can also be other sets. The set containing no elements is the empty set, denoted as $\varnothing$.

Sets are denoted using curly brackets in some form or another. There are many ways to notate a set.

Type	Representation	Meaning
Explicit	$\{1, 2, 3, 4, 5\}$	Sometimes called roster notation, a set can be defined via an exhaustive list of its elements
Implicit	$\{1, 2, 3 \ldots\}$	Similar to roster notation. Outlines a pattern and implies its continuation
Set-Builder	{ Elements : Condition }	Set-builder notation outlines what the elements of the set look like, under the given conditions outlined on the right
Open Interval	(a, b)	$(a, b) = \{x \in \mathbb{R} : a < x < b\}$
Closed Interval	$[a, b]$	$[a, b] = \{x \in \mathbb{R} : a \geq x \leq b\}$

Definition 6 (Cardinality)**.** A set A is *finite* if the set has finitely many elements. The number of elements within A, denoted as $|A|$, is the cardinality of A. If A has infinitely many elements, then its cardinality is infinite and is said to be an *infinite set*.

Consider the set $A = \{1, 10 - 5, 4\}$. We say that the cardinality of A is finite and therefore $|A| = 4$. Alternatively, the set $B = (1, 2)$ has an infinite cardinality and is therefore an infinite set.

5.2 Subsets

Definition 7 (Subset)**.** If A and B are sets, A is a *subset* of B if all the elements of A are in B. This is denoted as

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

Additionally, if $A \neq B$ and $A \neq \varnothing$, then A is a *proper subset* of B. This is denoted as

$$A \subset B \iff \forall x \in A, x \in B \text{ and } \exists y \in B \text{ s.t. } y \notin A.$$

Now with all of these definitions, useful tools can be constructed.

Theorem 6 (Set Equality)**.** Two sets are equal if and only if they are subsets of each other

Proof. Let A and B be sets and suppose that $A = B$. A and B have the same elements so $x \in A$ if and only if $x \in B$. Now, $A \subseteq B$ since $x \in A \implies x \in B$ and $B \subseteq A$ since $x \in B \implies x \in A$. Therefore, $A = B$ if and only if A and B are subsets of each other. ■

Functions

6.1 Introduction to Functions

Definition 8 (Function)**.** A function f is a *'rule'* that assigns elements from a domain set A to a codomain set B with a **one-to-one** correspondence.

If a function f maps elements from a set A to a set B, then it is notated as

$$f : A \to B.$$

When considering an element $a \in A$ and its corresponding functional mapping $b \in B$, we say that $b = f(a)$ and also that

$$f : a \mapsto b.$$

which reads as f maps a to b.

6.2 Classification

There are three important classifications of functions.

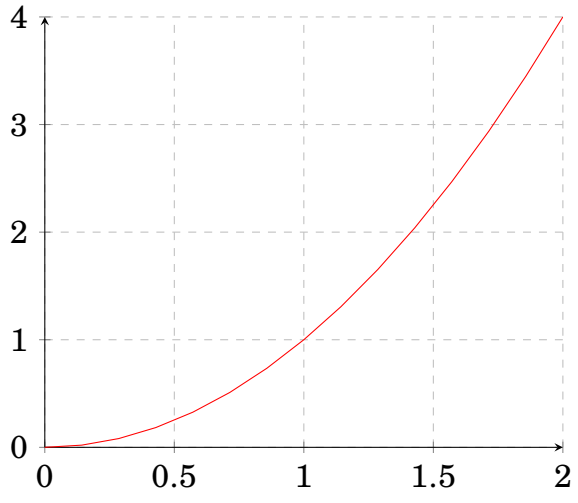
Definition 9 (Injectivity)**.** A function $f : A \to B$ is considered injective, an injection, or one-to-one if it never has the same output twice. Equivalaltenly

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \implies a_1 = a_2.$$

Consider the function

$$f : [0, 2] \to \mathbb{R} : x \mapsto x^2.$$

Graphically it is obvious that for every y-value, there is only a singularlly associated x-value. However, the function f maps to all the real numbers. Consider an output of 16. This would require an input of 4, however that is outside the range. We say that in this case that f is not *surjective*.



Theorem 7 (Function Cardinality)**.** All of the following statements are equivalent.

1. $|A| \leq |B|$
2. $\exists f : A \to B, f$ is injective
3. $\exists f : B \to A, f$ is surjective

Set Theory II

7.1 Cartesian Product

Definition 10 (Cartesian Product)**.** Let A and B be sets. Their Cartesian product is defined as

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

For example, consider the 2-dimensional plane. Each point can be defined in Cartesian coordinates, and therefore as an ordered pair (x, y) where $x, y \in \mathbb{R}$. This means that all elements of the Cartesian plane can be expressed as elements of the set

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}.$$

Theorem 8. If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$

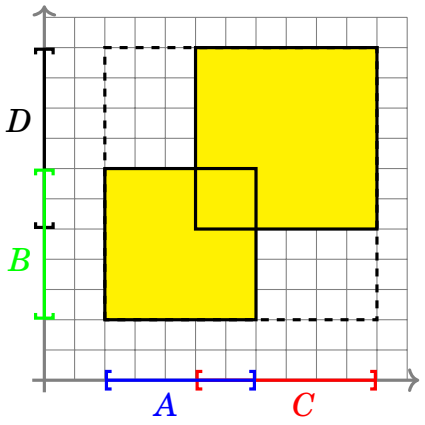
Proof. Let $|A| = m$ and $|B| = n$. Listing out $A \times B$ in a grid pattern results in

$$A \times B = \{ \begin{array}{ccccc} (a_1, b_1) & (a_1, b_2) & (a_1, b_3) & \dots & (a_1, b_n) \\ (a_2, b_1) & (a_2, b_2) & (a_2, b_3) & \dots & (a_2, b_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (a_m, b_1) & (a_m, b_2) & (a_m, b_3) & \dots & (a_m, b_n) \end{array} \}.$$

Every ordered pair is written only once. Since there are m rows and n columns, the number of elements is mn, therefore $|A \times B| = mn$. ∎

Here is a basic set relationship involving the Cartesian product.

Theorem 9. Let A, B, C, D be any sets. Then $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.



Visually, this can be seen as two regions in the Cartesian plane being contained within a larger region where the boundaries are equivalent to the union of the individual region's sides.

Proof. Let $(x, y) \in (A \times B) \cup (C \times D)$. If (x, y) is in $(A \times B)$, then $x \in A$ and $y \in B$. Therefore $x \in A \cup C$ and $y \in B \cup D$, meaning $(x, y) \in (A \cup C) \times (B \cup D)$. If (x, y) is in $(C \times D)$, then $x \in C$ and $y \in D$. Therefore $x \in A \cup C$ and $y \in B \cup D$, meaning $(x, y) \in (A \cup C) \times (B \cup D)$, as required. ■

Here is a proof of a more generalized version of Theorem 8 using induction.

Theorem 10. For all $n \in \mathbb{N}$, if $A_1, \ldots, A_n$ are finite sets, then

$$|A_1 \times \ldots \times A_n| = |A_1| \ldots |A_n|.$$

Proof. Proceed with induction to show that for all $n \in \mathbb{N}$, if $A_1, \ldots, A_n$ are finite sets, then $|A_1 \times \ldots \times A_n| = |A_1| \ldots |A_n|$. Consider the base case when $n = 1$. Then $|A_1| = |A_1|$, hence the base case is true. Assume for a fixed $n \in \mathbb{N}$ that $|A_1 \times \ldots \times A_n| = |A_1| \ldots |A_n|$. Consider then the Cartesian product $A_1 \times \ldots \times A_{n+1}$. This will result in every ordered pair in $A_1 \times \ldots \times A_n$ being repeated with a new element from A_{n+1} added in each time. Hence the number of ordered pairs in the set $A_1 \times \ldots \times A_{n+1}$ will be the same as the number of elements of $A_1 \times \ldots A_n$ multiplied by the number of elements in A_{n+1}. By the induction hypothesis, the number of elements in $A_1 \times \ldots \times A_n = |A_1| \ldots |A_n|$ and the number of elements in A_{n+1} is $|A_n + 1|$. Hence

$$|A_1 \times \ldots \times A_{n+1}| = |A_1| \ldots |A_{n+1}|.$$

Therefore for all $n \in \mathbb{N}$, if $A_1, \ldots, A_n$ are finite sets, then

$$|A_1 \times \ldots \times A_n| = |A_1| \ldots |A_n|.$$

■

7.2 Power Sets

Definition 11 (Power Set)**.** The *power set* of a set A is the set $\mathcal{P}(A)$ of all subsets of A. That is

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

Equivalently $B \in \mathcal{P}(A) \iff B \subseteq A$.

7.3 Indexed Collections

Definition 12 (Indexed Collection)**.** Given a family of indexed sets $\{A_n : n \in I\}$, the union or intersection of the family can be formed as

$$\bigcup_{n \in I} A_n = \{x : x \in A_n \text{ for some } n \in I\}$$
$$\bigcap_{n \in I} A_n = \{x : x \in A_n \text{ for all } n \in I\}.$$

Equivalently,

$$x \in \bigcup_{n \in I} A_n \iff \exists n \in I, x \in A_n$$
$$x \in \bigcap_{n \in I} A_n \iff \forall n \in I, x \in A_n$$

Relations

Relations will serve useful in concretizing the idea of functions and in general how elements of sets are related to each other.

Definition 13 (Relation)**.** A relation $\mathcal{R}$ on a set A is defined as $\mathcal{R} \subseteq A \times A$ with 3 possible properties

Reflexive	$\forall a \in A, (a, a) \in \mathcal{R}$
Symmetric	$\forall a, b \in A, (a, b) \in \mathcal{R} \implies (b, a) \in \mathcal{R}$
Transitive	$\forall a, b, c \in A, (a, b), (b, c) \in \mathcal{R} \implies (a, c) \in \mathcal{R}.$

Consider the relation $\mathcal{R}$ defined as $(\leq, \mathbb{R})$. Which properties of a relation does it satisfy?

Proof. Let ■

If a relation $\mathcal{R}$ obeys all 3 possible properties of a relation, it is called an **Equivalence Relation** often denoted by a $\sim$. Let $\mathcal{R}$ be the relation $\sim$ on $\mathbb{Z}$ such that

$$x \sim y \iff x - y \text{ is even.}$$

Is $\mathcal{R}$ an equivalence relation?

Proof. Proceed to show that $\mathcal{R}$ is an equivalence relation.

(Reflexivity) Let $a \in \mathbb{Z}$. It follows that

$$\begin{aligned} a \sim a &\implies 2 | a - a \\ &\implies 2 | 0 \end{aligned}$$

which is true. Therefore $\mathcal{R}$ is reflexive.

(Symmetry) Let $a, b \in \mathbb{Z}$. It follows that

$$\begin{aligned} a \sim b &\implies a - b = 2k \\ &\implies b - a = 2(-k) \\ &\implies b \sim a \end{aligned}$$

■

hence $\mathcal{R}$ is symmetric.

List of Theorems

List of Definitions