An Introduction to Proofs

Hassium

In higher-level mathematics, such as algebra, students need "mathematical maturity" to understand and apply abstract ideas. There is no obvious way to determine this maturity, nor a clear method to teach someone how to write a proof. These notes are designed to serve as a transition to proof-based mathematics, guiding students in adapting to the way mathematics operates.

This introduction is divided into several sections. The first section introduces the basic logic used in proofs. In the second section, we begin to "formalize mathematics" by studying sets and their relations: union, intersection, and complement. In the third section, we expand this concept in a more complex way, namely, functions. Functions are natural tools for connecting sets while preserving their structure. We shall use facts from these sections in further discussions and revisit these ideas.

Section 4 explains some properties of integers and provides concrete examples for rigorous proofs. Building on the properties of integers, we extend the discussion to infinite sets, exploring questions such as: What is an infinite set? Are these sets countable?

The final section covers $\mathbb{R}$ and $\mathbb{C}$, the real and complex fields, respectively. It begins with their constructions and presents several algebraic and analytic properties to deepen understanding. This section offers students a first taste of a rigorous mathematics course, so it is highly recommended.

During the reading, you may notice that we use different names for the same object. This happens quite often in mathematics. For instance, we can view $\mathbb{R}$ as a set, a group, a ring, a field, a manifold, a topological space, ... Every time we use a word, we are specifying a particular aspect of the same object. As Poincaré said, "Mathematics is the art of giving the same name to different things."

1 Basic Logic

Logic is the formal framework and rules of inference that ensure the validity and coherence of arguments in math.

Remark. We shall accept that sentences can be either true or false.

A *proposition* is a sentence that is either true or false in a mathematical system. The label "true" or "false" assigned to a proposition is called its *truth value*. We use the letters T and F to represent "true" and "false", respectively. An *axiom* is a proposition that is assumed to be true within a mathematical system without requiring proof. Axioms serve as the foundational building blocks of a mathematical theory, from which other propositions can be derived. A *theorem* is a proposition that has been proven to be true using logical reasoning and the accepted axioms and previously established theorems of the mathematical system. The proof demonstrates why the theorem must hold based on these foundations.

Consider the proposition "π is not a rational number", which is trivially true. However, we could always find some false companion of this proposition, such as "π is a rational number". Similarly, we can find a true companion of a false proposition. Let P be a proposition, such companion of P is called the *negation* of P, denoted $\neg P$.

Let P and Q be propositions. Those sentences can be combined using the word "and", denoted $P \wedge Q$, and called the *conjunction* of P and Q. The proposition $P \wedge Q$ is true if both P and Q is true. We can combine the propositions by the word "or", denoted $P \vee Q$, and called the *disjunction* of P and Q. The proposition $P \vee Q$ is true if at least one of P or Q is true. A *truth table* is shown below.

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

Two propositions P and Q are *logically equivalent* if they have the same truth value in every possible combination of truth values for the variables in the statements, denoted $P \equiv Q$.

Example. Let P be a proposition, then $P \equiv \neg(\neg P)$ is logically equivalent. To prove this statement, consider $\neg P$ as a proposition Q, then we obtain the following truth table.

P	$Q \equiv \neg P$	$\neg Q \equiv \neg(\neg P)$
T	F	T
F	T	F

Here P and $\neg Q$ has the same truth value in each case, so $P \equiv \neg(\neg P)$.

Problem 1.1. Let P, Q, and R be propositions. Consider the following statements:

1. $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$;
2. $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$.

Try to prove or disprove the statements.

Problem 1.2. Let P, Q, and R be propositions. Consider the following statements:

1. $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$;
2. $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$;
3. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

Try to prove or disprove the statements. Based on your results, can you find more properties?

Let P and Q be propositions. Consider the proposition "if n is a natural number, then $2n$ is an even number". Let P denotes "n is a natural number" and let Q denotes "$2n$ is an even number", then the sentence becomes "if P,

then Q", denoted $P \implies Q$. This implication called a *conditional proposition*, P is called the *antecedent* and Q is called the *consequent*. The proposition $P \implies Q$ is true if P is true and Q is true. What if P is false? The answer arises from one's intuition.

Example. Imagine your high school teacher say "if you didn't submit your homework, then you haven't completed it". How would you argue against this sentence? The most likely response would be, "I did the homework but I didn't submit it". Whether or not you submitted your homework does not affect the truth value of the implication.

You should convinced by your own intuition (not mine). This case is called a *vacuous truth*. In the proposition $P \implies Q$, when P is false, $P \implies Q$ is true. The truth table of $P \implies Q$ is shown below.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Let P and Q be propositions, $(P \implies Q) \wedge (Q \implies P)$ is called a *biconditional proposition*, denoted $P \iff Q$. We will write this by "P is true if and only if Q is true".

Problem 1.3. Let P and Q be propositions, show $(\neg P \equiv \neg Q) \iff (P \equiv Q)$.

Example. Let P and Q be propositions. Consider the conditional proposition $P \implies Q$. It is false only if P is true and Q is false, that is, $\neg(P \implies Q) \equiv P \wedge (\neg Q)$. Now we take the negation of the right side, $\neg(P \wedge (\neg Q)) \equiv (\neg P) \vee (\neg(\neg Q)) \equiv (\neg P) \vee Q$.

Problem 1.4. Write down the truth table of a biconditional proposition. Based on your truth table and the previous example, try to find a proposition R by "$\vee$", "$\wedge$", and "$\neg$" such that $R \equiv (P \iff Q)$. If $P \iff Q$ is true, does $P \equiv Q$?

Problem 1.5. Let P, Q, R, and S be propositions. Rewrite $P \implies (Q \implies (R \implies S))$ by '$\vee$", "$\wedge$", and "$\neg$". What is the negation of this sentence?

Problem 1.6. Let P, Q, and R be propositions. Try to prove or disprove $P \implies (Q \vee R) \equiv (\neg P) \vee Q \vee R$. What about $P \implies (Q \wedge R)$?

Given a proposition $P \implies Q$, the *converse* is defined as $Q \implies P$ and the *contrapositive* is defined as $(\neg Q) \implies (\neg P)$. The truth table is shown below, and it suffices to conclude that $(P \implies Q) \equiv (\neg Q \implies \neg P)$.

P	Q	$P \implies Q$	$Q \implies P$	$\neg Q \implies \neg P$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Problem 1.7. Let P and Q be propositions, when does $(P \implies Q) \equiv (Q \implies P)$?

Let P be the proposition "x is a natural number". Here x is a *variable*, and the truth value of this proposition depends on x. For instance, if $x = 1$, then P is true; if $x = 0.86$, then P is false. A *propositional function* is a family of propositions depending on one or more variables. The collection of permitted variables is the *domain*. Now we write $P(x)$ instead of P, so $P(1)$ is true and $P(0.86)$ is false.

Propositional functions are often quantified. The *universal quantifier* is denoted by "$\forall$", and the proposition $\forall x(P(x))$ is true if and only if $P(x)$ is true for every x in its domain. The *existential quantifier* is denoted by "$\exists$", and the proposition $\exists x(P(x))$ is true if and only if $P(x)$ is true for at least one x in its domain. Consider the proposition $\forall x(P(x))$, this means all x make $P(x)$ true, so there does not exists some x such that $P(x)$ is false, which is $\neg(\exists x(\neg P(x)))$.

Example. Let $P(x)$ be a proposition, then $\neg(\forall x(P(x))) \iff \neg(\neg(\exists x(\neg P(x)))) \iff \exists x(\neg P(x))$.

Problem 1.8. Let $P(x)$ be a proposition, show that $\neg(\exists x(P(x))) \iff \forall x(\neg P(x))$.

The order of quantifiers does matter the meaning of a proposition. Consider the proposition "for all natural number x, there exists a natural number y such that $y > x$". Pick some x, let $y = x+1$, then $y > x$ and y is a natural number, so the proposition is true. However, switching the order of quantifiers gives "there exists a natural number y, for all natural number x, $y > x$". Suppose there exists such y, then $y + 1$ is a natural number, so let $x = y + 1$, it is trivial that $y < x$, hence the proposition is false.

Example. Let $P(x)$ and $Q(y)$ be propositions. Consider the proposition $\forall x(\exists y(P(x) \vee Q(y)))$. To find its negation, let $R(x) \equiv \exists y(P(x) \vee Q(y))$, now the negation becomes $\exists x(\neg R(x))$. Since P only depends on x, let $S(y) \equiv (P(x) \vee Q(y))$, then we have $\exists x(\neg(\exists y(S(y)))) \equiv \exists x(\forall y(\neg S(y))) \equiv \exists x(\forall y(\neg(P(x) \vee Q(y)))) \equiv \exists x(\forall y((\neg P(x)) \wedge (\neg Q(y))))$.

Problem 1.9. Let $P(x, y, z)$ be a proposition, consider the following propositions.

1. $Q(x, y, z) \equiv \exists x(\forall y(\forall z(P(x, y, z))))$;
2. $R(x, y, z) \equiv \forall x(\exists y(\forall z(P(x, y, z))))$;
3. $S(x, y, z) \equiv \forall x(\forall y(\exists z(P(x, y, z))))$.

What are the negations of those propositions? What is the negation of $Q \vee (R \wedge S)$?

Example. Let $P(x)$ and $Q(x)$ be propositions. Consider the negation of $P(x) \implies Q(x)$, $\neg(P(x) \implies Q(x)) \equiv \neg((\neg P(x)) \vee Q(x)) \equiv P(x) \wedge (\neg Q(x)) \equiv \forall x(P(x) \wedge (\exists x(\neg Q(x)))) \equiv \exists x(P(x) \wedge (\neg Q(x)))$. Notice that taking the negation brings an existential quantifier.

In the following sections, we shall assume readers are familiar with basic logic and use it as a tool to understand or prove propositions. Several expressions and their "translations" are shown below.

$P \implies Q$	$P \iff Q$
P implies Q; if P, then Q	P if and only if Q
P is sufficient for Q; Q is necessary for P	P is necessary and sufficient for Q

Problem 1.10. Given the following propositions, analyze their structures.

1. the number $\sqrt{2}$ is not a rational number;
2. if x is a natural number, then x is an integer;
3. for all natural number x, for all rational number y with $x < y < x + 1$, there exists a real number z such that $y < z < y + 1$ and z is irrational;
4. given a sequence (x_n) of real numbers, we say (x_n) converges to a real number L if, for all real number $\epsilon > 0$, there exists a real number N such that, for all natural number n, $n > N$ implies $|x_n - L| < \epsilon$.

Find the negation of each proposition.

2 Sets

In this section, we begin to investigate sets, the most basic entities in mathematics. It is natural to ask the question: what is a set? There is no precise definition of sets. Intuitively, a *set* is a collection of objects that satisfy a , and those objects are called *elements*.

If S is a set and x is an element in S, then we say x belongs to S, denoted $x \in S$. If x does not belong to S, then we write $x \notin S$. If S has no element, then we call it an *empty set*, denoted $\varnothing$.

Remark. This note is based on ZFC set theory. In this system, every object is a set and sets have heirachy, so there are set of sets.

Axiom of Extensionality. Two sets A and B are equal if and only if they have the same elements.

Elements determine a set, so it is essential to find a way to show the elements in a set. One way to describe a set is to explicitly list the elements. For instance, we can write a set $S = \{6, 7, 8\}$. Another way is to express the elements by some properties they satisfied. We shall come back to give some restrictions on this property.

Example. The set of rational numbers is the set $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$, where $\mathbb{Z}$ is the set of integers.

Example. The set $\{2n \mid n \in \mathbb{N}\}$ is the set of all even numbers.

Problem 2.1. Write out the set of all positive integers, the set of all prime numbers, and the set of all points on a circle with center $(0, 0)$ and radius 1 in 3-dimensional Euclidean space.

Definition 2.1. Let S be a set. A set R is a *subset* of S, denoted $R \subset S$, if for all $x \in R$, $x \in S$. If there exists some $x \in S$ such that $x \notin R$, then R is called a *proper subset* of S, denoted $R \subsetneq S$.

Remark. Some textbooks use "$\subseteq$" for subsets and "$\subset$" for proper subsets.

Example. For all sets A, for all $x \in A$, $x \in A$, so $A \subset A$.

Proposition. Let X and Y be sets, then $X = Y$ if and only $X \subset Y$ and $Y \subset X$.

Remark. For a biconditional proposition $P \iff Q$, we use the notation "$(\Rightarrow)$" in the proof to show $P \implies Q$ and "$(\Leftarrow)$" for $Q \implies P$.

Proof. Let X and Y be sets. $(\Rightarrow)$ For all $x \in X$, since $X = Y$, $x \in Y$, so $X \subset Y$. For all $y \in Y$, since $X = Y$, $y \in X$, so $Y \subset X$. $(\Leftarrow)$ Suppose $X \neq Y$, then there exists $a \in X$ and $a \notin Y$, so $X \not\subset Y$, yet contradiction. □

Proposition. Let A be any set, then $\varnothing \subset A$.

Proof. Suppose $\varnothing \not\subset A$, then there exists $x \in \varnothing$ such that $x \notin A$, since $x \in \varnothing$ is false, contradiction. □

Problem 2.2. If X, Y, and Z are sets such that $X \subset Y$ and $Y \subset Z$, prove that $X \subset Z$.

Axiom of Union. For all

Definition 2.2. Let A and B be sets. The *union* of A and B is the set $\{x \mid x \in A \text{ or } x \in B\}$, denoted $A \cup B$. The *intersection* of A and B is the set $\{x \mid x \in A \text{ and } x \in B\}$. The *complement* of A in B is the set $\{x \mid x \in B \text{ and } x \notin A\}$, denoted B/A.

Some textbooks assume there exists a "universal set", denoted U, which has all objects as elements including itself, so we can define complements of any set S as the set U/S. However, this assumption leads to a paradox.

Example. Consider the set S, defined as the set of all sets that are not members of themselves, that is, $S = \{X \mid X \notin X\}$. Does S belong to S? This is known as the *Russell's Paradox*.

Assume $S \in S$. By the definition of S, it must satisfy $S \notin S$. This is a contradiction. Assume $S \notin S$. By the definition of S, it must satisfy $S \in S$. This is also a contradiction. Thus, the existence of such a set S leads to a logical inconsistency. In ZFC, we add restrictions to the property to collect elements.

Axiom Schema of Separation. L

Alphabetical Index