Chapter 1

Introduction

1.1 Introduction

1.1.1 Objectives of Teaching

To acquire the fundamentals of mathematical reasoning, the foundations of set theory, and the elements of mathematical proof writing.

1.2 Elements of Mathematical Language

Axiom. An axiom is a statement assumed to be true a priori and is not subject to proof.

For example, Euclid formulated five axioms ("Euclid's five postulates"), which he did not attempt to prove and were to form the basis of (Euclidean) geometry. The fifth of these axioms states: "Through a point not on a line, there is exactly one line parallel to that line."

Another example of axioms is provided by the (five) Peano axioms. These define the set of natural numbers. The fifth axiom asserts: "If P is a subset of $\mathbb{N}$ containing 0 and such that the successor of each element of P is in P (the successor of n is $n+1$), then $P = \mathbb{N}$." This axiom is known as the "axiom of induction" or "recurrence axiom."

These statements are commonly accepted as "obvious" by everyone.

Proposition1.1 (or assertion or statement). A proposition is a statement that can be either true or false. For example, "every prime number is odd" and "every square of a real number is a positive real number" are two propositions. It is easy to prove that the first is false and the second is true. The term proposition is clear: something is proposed, but it remains to be proven.

Theorem1.1. A theorem is a true proposition (and in any case, proven as such). In common practice, the term proposition often refers to an intermediate or lesser important theorem, and there is a tendency to refer to most theorems as propositions, reserving the term theorem for the more significant ones (e.g., the Pythagorean Theorem). This is the perspective we will adopt in later chapters (though not in this first chapter, where the term "proposition" would have two different meanings).

Corollary. A corollary to a theorem is a theorem that follows as a consequence of that theorem. For example, in the chapter on "continuity," the intermediate value theorem states that the image of an interval of $\mathbb{R}$ by a continuous real-valued function is an interval in $\mathbb{R}$. A corollary of this theorem asserts that if a function defined and continuous on an interval of $\mathbb{R}$ takes at least one positive value and at least one negative value, then the function must have at least one root in that interval.

Lemma1.1. A lemma is a preparatory theorem used to establish a more significant theorem.

Conjecture. A conjecture is a proposition believed to be true without being proven. Conjectures drive mathematical progress. A mathematician may suspect that an important result is true and state it without being able to prove it, leaving the mathematical community to either confirm it with a convincing proof or disprove it. The following conjectures are famous:

- (Fermat's conjecture) If n is an integer greater than or equal to 3, there are no non-zero natural numbers x, y, and z such that $x^n + y^n = z^n$. (This conjecture dates back to the 17th century and was recently proven true.)

Definition1.1. A definition is a statement that describes the characteristics of an object. It should be noted that the term "axiom" is sometimes synonymous with "definition." For example, when you read "definition of a vector space," you might just as well read "axioms of vector space structure," and vice versa.

1.3 Writing Mathematical Proofs

1.3.1 Deductive Reasoning

The schema of deductive reasoning is as follows:

When P is a true proposition, and $P \Rightarrow Q$ is a true proposition, one can assert that Q is a true proposition.

A result known to be true (i.e., a theorem) can only lead to another true result. This rule is known as "modus ponens." It is the basic reasoning that you will reproduce many times. In fact, you will employ this reasoning so often (or find yourself so frequently in the situation where the hypothesis P is true) that you might eventually confuse the simple phrase "$P \Rightarrow Q$ is true" with the more complete phrase "P is true, and $P \Rightarrow Q$ is true." Only the latter allows you to assert that Q is true.

Given that implication is transitive, a proof often takes the following form: P is true, and $P \Rightarrow Q \Rightarrow R \Rightarrow \ldots \Rightarrow S \Rightarrow T$ is true, and thus we have shown that T is true.

1.3.2 Proof by Contradiction

To show that a proposition P is true, we assume its negation $\bar{P}$ is true and demonstrate that this leads to a false proposition. We then conclude that P must be true (since Q is false, the implication $\bar{P} \Rightarrow Q$ can only be true if $\bar{P}$ is false, or equivalently, if P is true). The structure of proof by contradiction is as follows:

When $\bar{P} \Rightarrow Q$ is a true proposition, and Q is a false proposition, we can assert that P is a true proposition.

Example. Let's prove that $\sqrt{2}$ is irrational. Assume, by contradiction, that $\sqrt{2} \in \mathbb{Q}$. Then, there exist two non-zero natural numbers a and b such that $\sqrt{2} = \frac{a}{b}$, or equivalently $a^2 = 2b^2$. Now, in the prime factorization of the integer a^2 (which is evidently greater than 2), the prime number 2 appears with an even exponent (if $a = 2^{\alpha} \times \ldots$, then $a^2 = 2^{2\alpha}$), while it appears with an odd exponent in $2b^2$ (if $b = 2^{\beta} \times \ldots$, then $2b^2 = 2^{2\beta+1} \times \ldots$). If we accept the uniqueness of prime factorization for natural numbers greater than 2 (a uniqueness that will be demonstrated later in this course), the equality $a^2 = 2b^2$ is impossible. Therefore, the initial assumption ($\sqrt{2} \in \mathbb{Q}$) is absurd, and we have thus proven (by contradiction) that $\sqrt{2} \notin \mathbb{Q}$.

1.3.3 Proof by Contrapositive

The structure is as follows:

To show that $P \Rightarrow Q$ is a true proposition, it (is necessary and) suffices to show that $\bar{Q} \Rightarrow \bar{P}$ is a true proposition.

Example. Let k and k' be two non-zero natural numbers. Let's prove that $(kk' = 1 \Rightarrow k = k' = 1)$. Assume that $k \neq 1$ or $k' \neq 1$. Then, we have $k \geq 2$ and $k' \geq 1$ or $k \geq 1$ and $k' \geq 2$. In both cases, $kk' \geq 2$, and in particular, $kk' \neq 1$. Therefore, $(k \neq 1$ or $k' \neq 1) \Rightarrow (kk' \neq 1)$.

- By contrapositive, we have shown that $(kk' = 1) \Rightarrow (k = 1$ and $k' = 1)$.

1.4 Mathematical Theories

At the foundation of a mathematical theory are axioms and definitions:

Definition1.2 (Axiom) An axiom is a mathematical statement accepted without proof.

Example.

- Euclid's parallel postulate.
- Pasch's axiom on the intersection of a triangle and a line.

- Hilbert's axioms for Euclidean geometry.
- Archimedes' axiom for real numbers.
- Peano's axioms for natural numbers.
- Zermelo-Fraenkel axioms for set theory.
- Zorn's lemma (also known as the axiom of choice).

Definition1.3 A definition is arbitrarily assigned to designate a mathematical object.

Example.

- Definitions of a number.
- Definitions of a function.
- Definitions of a derivative.

In a mathematical theory, one finds propositions (assertions), predicates, theorems, lemmas, and conjectures:

Definition1.4 (Assertion) An assertion is a mathematical statement to which a truth value can be assigned: true (1) or false (0), but never both simultaneously.

Example.

- The statement "Algiers is the capital of Algeria" is true.
- The statement "24 is a multiple of 2" is true.
- The statement "19 is a multiple of 2" is false.

Definition1.5 (Predicate) A predicate is an assertion that contains variables.

Example.

- The following statement: $P(n)$: "n is a multiple of 2" is a predicate because it becomes an assertion when a value is assigned to n.
- $P(10)$: "10 is a multiple of 2" is a true assertion.

- $P(11)$: "11 is a multiple of 2" is a false assertion.
- $Q(x, A)$: "$x \in A$" is a predicate with two variables; $Q(1, \mathbb{N})$ is true, $Q(\sqrt{2}, \mathbb{Q})$ is false.

Definition1.6 (Lemma) A lemma is a result of minor importance.

Definition1.7 (Theorem) A theorem is a result of major importance.

Definition1.8 (Conjecture) A conjecture is a proposition that has been verified in several cases, but has not yet been proven.

Example.

- Fermat's conjecture on the following Diophantine equation with unknowns x, y, and z: $n \in \mathbb{N}, x^n + y^n = z^n$. It asserts that there is no non-trivial solution if the parameter $n > 2$. But it was not until 1996, with the work of the English mathematician Andrew Wiles, that a definitive answer was found.
- The Riemann conjecture on the non-trivial zeros of the zeta function: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ (an unresolved conjecture).
- Bertrand's conjecture on prime numbers within the intervals $[n, 2n]$.

1.5 Logical Connectors

Let P and Q be two propositions:

Statement. not P

Notation. $\neg P$

The assertion $\neg P$ is true means that P is false.

Statement. P and Q

Notation. $P \wedge Q$

The assertion $P \wedge Q$ is true if both P and Q are true; $P \wedge Q$ is false otherwise.

Statement. P or Q

Notation. $P \vee Q$

The assertion $P \vee Q$ is true if at least one of the assertions P or Q is true; $P \vee Q$ is false if both P and Q are false.

Statement. $\left\{ \begin{array}{c} \text{if } P\text{, then } Q \\ P \text{ implies } Q \\ P \text{ is a sufficient condition for } Q \\ Q \text{ is a necessary condition for } P \end{array} \right\}$

Notation. $P \Longrightarrow Q, P \longrightarrow Q$

The assertion $P \Longrightarrow Q$ is true means that it is excluded that P is true without Q being true.

Statement. $\left\{ \begin{array}{c} P \text{ is equivalent to } Q \\ P \text{ if and only if } Q \end{array} \right\}$

Notation. $P \Longleftrightarrow Q, P \longleftrightarrow Q, P \equiv Q$

The assertion $P \Longleftrightarrow Q$ is true means that:

$$(P \Longrightarrow Q) \text{ and } (Q \Longrightarrow P) \text{ are true.}$$

This is summarized in the truth tables below:

$\neg P$	P
0	1
1	0

P	Q	$P \wedge Q$	$P \vee Q$	$P \Longrightarrow Q$	$P \Longleftrightarrow Q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Properties1.1

- $P \wedge (Q \vee Q) \equiv (P \wedge Q) \vee (P \wedge Q)$; double distributivity of "and" and "or."
- $P \vee (Q \wedge Q) \equiv (P \vee Q) \wedge (P \vee Q)$.
- $(P \implies Q) \equiv (\neg Q \implies \neg P)$; contrapositive.
- $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$; De Morgan's law.
- $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$.
- $P \implies Q \equiv \neg P \vee Q$.
- $\neg(P \implies Q) \equiv P \wedge \neg Q$.

1.6 Logical Quantifiers

Statement. For all or for every.

Notation. $\forall \quad (\forall x P(x))$

Statement. There exists at least one or there exists.

Notation. $\exists \quad (\exists x P(x))$

Example.

- The proposition $\forall x \in [-3, 1], x^2 + 2x - 3 \leq 0$ is true.
- The proposition $\forall n \in \mathbb{N}, (n^2 \text{ even }) \implies (n \text{ even })$ is true.
- The proposition $\exists x \in \mathbb{R}, x^2 = 4$ is true.
- The proposition $\exists! x \in \mathbb{R}_+^*, \ln x = 1$ is true.

Remark.

- The proposition $\exists x \in E, P(x)$ means that

$$\exists x((x \in E) \wedge P(x))$$

and is read as follows: "There exists an element x belonging to E such that $P(x)$ is true."

- The proposition $\forall x \in E, P(x)$ means that

$$\forall x(x \in E \Longrightarrow P(x))$$

and is read as follows: "If for all (or every) x belonging to E, $P(x)$ is true."

- If there exists exactly one x in E such that $P(x)$ is true, one can write $\exists! x \in E, P(x)$.

- If $\forall x \in E, P(x)$ is true, then $\exists x \in E, P(x)$ is true.

Remark. (Caution) $\exists!$ does not denote a quantifier. Indeed:

$$(\exists! x \in E, P(x)) \equiv (R_1 \wedge R_2)$$

with $R_1 =$ existence and $R_2 =$ uniqueness.

- Two identical quantifiers can be swapped.
- Do not swap two different quantifiers.

1.6.1 Negation Rules

Let $P(x)$ be a predicate on E. Clearly, we have:

- $\neg(\forall x \in E, P(x)) \equiv \exists x \in E, \neg P(x)$.

- $\neg(\exists x \in E, P(x)) \equiv \forall x \in E, \neg P(x)$.

Example.

- The negation of $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}_+, 1 + nx \leq (1+x)^n$ is $\exists n \in \mathbb{N}, \exists x \in \mathbb{R}_+, 1 + nx > (1+x)^n$.

- The negation of $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 5$ is $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \neq 5$.

Remark. (Caution) We also verify that:

$$\neg(\exists! x \in E, P(x)) \equiv (\neg R_1 \vee \neg R_2)$$

with R_1 = existence and R_2 = uniqueness.

- Identical quantifiers can be swapped.
- Do not swap different quantifiers.

1.7 Proof Methods

To perform a proof (or reasoning), one follows a process that allows the transition from propositions assumed to be true (as hypotheses) to a proposition called the conclusion, using logical rules.