1.12 Proof

A proof is a sequence of logical statements, one implying another, which gives an explanation of why a given statement is true. It is based on a logical consequence of axioms, definitions, lemmas, theorems, etc.previously established. Mathematical proof is absolute, which means that once a theorem is proved, it is proved for ever. Until proven though, the statement is never accepted as a true one.

1.12.1 Basic Terminology.

1. **Axiom** (or postulate) is a statement that is accepted as true without proof. Axioms serve as the foundational building blocks for a mathematical system.

2. **Rule of inference** is a logical rule that is used to deduce one statement from others.

3. **Theorem:** is a proposition that can be proved using definitions, axioms, other theorems, and rules of inference.

4. **Lemma:** is a preliminary result that is proven to assist in proving a larger theorem. It is often a useful intermediate step in a proof. We sometimes prove a theorem by a series of lemmas.

5. **Corollary:** a theorem that can be easily established from a theorem that has been proved.

6. **Proposition:** a proved and often interesting result, but generally less important than a theorem.

7. **Claim**: an assertion that is then proved. It is often used like an informal lemma.

8. **Conjecture:** a statement proposed to be a true statement, usually based on partial evidence, or intuition of an expert.

9. **Paradox** is a mathematical conclusion so unexpected that it is difficult to accept even though every step in the reasoning is valid.

Examples and explanation: The terms "lemma" and "corollary" are just names given to theorems that play particular roles in a theory. Most people tend to think of a theorem as the main result, a lemma a smaller result needed to get to the main result, and a corollary as a theorem which follows relatively easily from the main theorem, perhaps as a special case. For example, suppose we have proved the Theorem: "If the product of two integers m and n is even, then either m is even or n is even." Then we have the Corollary: "If n is an integer and n^2 is even, then n is even." Notice that the Corollary follows from the Theorem by applying the Theorem to the special case in which $m = n$. There are no firm rules for the use of this terminology; in practice, what one person may call a lemma another may call a theorem.

Euclid's Division Lemma: Let a and b two positive integers, then there exist unique integers q and r which satisfies the condition $a = bq + r$ where $0 \leq r < b$.

Goldbach Conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

Use Euclid's division lemma to show that the square of any positive integer is of the form $3p$, $3p + 1$.

Let us consider a positive integer a. Divide the positive integer a by 3, and let r be the reminder and q be the quotient. We know that According to Euclid's Division Lemma

$$a = 3q + r.$$

so r is an integer which lies in between 0 and 3. Hence can be either: $0, 1$ and 2. Case I - When

Case1: When $r = 0$, we obtain $a^2 = (3q)^2 = 9q^2 = 3(3q^2) = 3p$ (where $m = 3q^2$).

Case2: When $r = 1$, we obtain $a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3p + 1$ (where $p = 3q^2 + 2q$).

Case2: When $r = 2$, we obtain $a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3p + 1$ (where $p = 3q^2 + 4q + 1$).

Thus, the square of any positive integer is of form: $3p$, $3p + 1$.

List of Paradox

Grandi's series: The sum of $1 - 1 + 1 - 1 + 1 - 1...$ can be either 1, 0, or $1/2$.

Banach–Tarski paradox: A ball can be decomposed and reassembled into two balls the same size as the original.

Now, Once we have the undefined terms and axioms for a mathematical system, we can begin defining new terms and proving theorems (or lemmas, or corollaries) within the system.

1.12.2 Methods of Proof

Types of Proofs. Suppose we wish to prove an implication $p \Longrightarrow q$. Here are some strategies we have available to try.

• **Trivial Proof:** If we know q is true then $p \Longrightarrow q$ is true regardless of the truth value of p.

• **Vacuous Proof:** If p is a conjunction of other hypotheses and we know one or more of these hypotheses is false, then p is false and so $p \Longrightarrow q$ is vacuously true regardless of the truth value of q.

Example 1.12.1 *Prove the statement: If there are 100 students enrolled in this course this semester, then* $6^2 = 36$.

Proof. The assertion is trivially true, since the conclusion is true, independent of the hypothesis (which, may or may not be true depending on the enrollment). ■

Example 1.12.2 *Prove the statement. If* 6 *is a prime number, then* $6^2 = 30$.

Proof. The hypothesis is false, therefore the statement is vacuously true (even though the conclusion is also false). ■

The first two methods of proof, the "Trivial Proof" and the "Vacuous Proof" are certainly the easiest when they work. Notice that the form of the "Trivial Proof", $q \Longrightarrow (p \Longrightarrow q)$, is, in fact, a tautology. This follows from disjunction introduction, since $p \Longrightarrow q$ is equivalent to $:\neg p \vee q$. Likewise, the "Vacuous Proof" is based on the tautology: $\neg p \Longrightarrow (p \Longrightarrow q)$.

Exercise 1.12.3 *Fill in the reasons for the following proof of the tautology:*$\neg p \Longrightarrow (p \Longrightarrow q)$.

$$\begin{aligned} \neg p \Longrightarrow (p \Longrightarrow q) &\equiv \neg p \Longrightarrow (\neg p \vee q) \\ &\equiv p \vee (\neg p \vee q) \\ &\equiv p \vee \neg p \vee q \\ &\equiv T \end{aligned}$$

In almost every case, the assertions we will be proving are of the form "if p, then q", where p and q are (possibly compound) propositions. The proposition p is the hypothesis and q is the conclusion. It is almost always useful to translate a statement that must be proved into an "if ..., then ..." statement if it is not already in that form.

To begin a proof we assume the hypotheses. For example, consider the argument

Every bounded set has a supremum.

$(0, 1)$ is a bounded set.

Therefore, $(0, 1)$ has a supremum.

The hypotheses of this argument are "Every bounded set has a supremum" and $(0, 1)$ is a bounded set." The conclusion is $(0, 1)$ has a supremum.

1.12.3 Rules of Inference

There are many rules of inference, we list here the most used ones

Modus Ponens or the Law of Detachment	p $p \Longrightarrow q$ $\_\_\_\_\_$ $\therefore q$
Disjunction Introduction	p $\_\_\_\_\_$ $\therefore p \vee q$
Conjunction Elimination	$p \wedge q$ $\_\_\_\_$ $\therefore p$
Modus Tollens	$\neg q$ $p \Longrightarrow q$ $\_\_\_\_\_$ $\therefore \neg p$
Hypothetical Syllogism	$p \Longrightarrow q$ $q \Longrightarrow r$ $\_\_\_\_\_$ $\therefore p \Longrightarrow r$
Disjunctive Syllogism	$p \vee q$ $\neg p$ $\_\_\_\_$ $\therefore q$
Conjunctive introduction	p q $\_\_\_\_\_$ $\therefore p \wedge q$
Constructive Dilemma	$(p \Longrightarrow q) \wedge (r \Longrightarrow s)$ $p \vee r$ $\_\_\_\_\_$ $\therefore q \vee s$

Definition 1.12.4 *An argument is valid if it is uses only the given hypotheses together with the axioms, definitions, previously proven assertions, and the rules of inference, which are listed above.*

The notation used in this course is commonly used in logic to express an argument symbolically. The proposition(s) before the horizontal line are the hypotheses and the proposition below the line is the conclusion. The symbol "$\therefore$" is a common shorthand for "therefore." Each of the rules of inference is a tautology expressed in a different form. For example, the rule of modus ponens, when stated as a propositional form, is the tautology: $[p \wedge (p \Longrightarrow q)] \Longrightarrow q$.

Remark 1.12.5 *An argument of the form*

$$\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ \hline \therefore B \end{array}$$

is valid if and only if the proposition $[A_1 \wedge A_2 \wedge \ldots \wedge A_n] \Longrightarrow B$ *is a tautology.*

Example 1.12.6 *1. If Ahmed doesn't do his homework or he doesn't feel sick, then he will go to the party and he will stay up late.*

2. If he goes to the party, he will eat too much.

3. He didn't eat too much.

4. So Ahmed did his homework.

1. Assign propositional variables to the component propositions in the argument:

p : Ahmed does his homework

q : Ahmed feels sick

r : Ahmed goes to the party

s : Ahmed stays up late

t :Ahmed eats too much

2. Represent the formal argument using the variables:

1. $(\neg p \vee \neg q) \Longrightarrow (r \wedge s)$

2. $r \Longrightarrow t$

3. $\neg t$

4. $\therefore p$

3. Use the hypotheses, the rules of inference, and any logical equivalences to prove that the argument is valid

Assertion	Reason
5. $\neg r$	Modus Tollens, 3 and 2
6. $\neg r \vee \neg s$	Addition and 5
7. $\neg(r \wedge s)$	DeMorgan and 6
8. $\neg(\neg p \vee \neg q)$	Modus Tollens, 7 and 1
9. $p \wedge q$	DeMorgan and 8
10. p	Simplification and 9

1.12.4 Principal rules of inference

Modus Ponens (direct proof)

We say that a proposition$q$ logically follows from a true proposition p if the implication $p \Longrightarrow q$ is true. In this case we write:

$$\begin{array}{l} p \\ p \Longrightarrow q \\ \hline \therefore q \end{array}$$

The proposition p is the hypothesis and q is the conclusion.

The rule of Modus Ponenes is based on the tautology $(p \wedge (p \Rightarrow q)) \Rightarrow q$. In fact we have

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
F	F	T	F	**T**
F	T	T	F	**T**
T	F	F	F	**T**
T	T	T	T	**T**

1.13 Redaction

The writing of a direct proof often takes the following form:
Proposition : if p then q.
Proof : Assume p
Therefore (or consequently) q.

Example 1.13.1 *Show that for any odd natural integer n the integer $3n+7$ is even.*

By transitivity of the logical implication we obtain: $P \Rightarrow P1 \Rightarrow P2 \Rightarrow P3 \Rightarrow Q$ then the proposition $P \Rightarrow Q$ is also true.Then we have:

$$\begin{aligned} &\forall n \text{ entier impair} \\ &\forall n \text{ entier impair } \Rightarrow 3n+7 \text{ is even} \\ &\quad \therefore 3n+7 \text{ is even} \end{aligned}$$

Remark 1.13.2 *In a direct proof we never start with a false proposition otherwise we cannot conclude anything. Indeed if the proposition p is false the proposition $p \Rightarrow q$ is true. We cannot obtain any conclusion on the nature of q which can be true or false.*

Proof by contrapositive

The proof by contrapositive is based on the following tautological equivalence $(p \Rightarrow q) \Longleftrightarrow (\neg q \Rightarrow \neg p)$.

$$\begin{aligned} &\forall n \text{ entier impair } \Rightarrow \exists k \in N : \underset{P1}{n} = 2k+1 \\ &\exists k \in N : \underset{P1}{n} = 2k+1 \Rightarrow \exists k \in N : 3n+7 \underset{P2}{} = 3(2k+1)+7 \\ &\exists k \in N : 3n+7 = 6k+8 = 2(3k+4) \Rightarrow 3n+7 \text{ est } \underset{Q}{\text{pair}} \end{aligned}$$

In some cases, it allows to simplify a demonstration.

Example 1.13.3 *The classic example of the use of the proof by contrapositive concerns the injectivity of an application. Thus to show that a function $f : E \to F$ is injective we can show the logical implication*

$$\forall x_1, x_2 \in E : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

But often it is easy to show the contrapositive

$$\forall x_1, x_2 \in E : f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Proof by contradiction

The proof by contradiction is based on the following tautology

$$(\neg p \Rightarrow F) \Leftrightarrow p : (F : \text{ false proposition (contradiction) })$$

In fact, we have

p	$\neg p$	F	$\neg p \Rightarrow F$	$(\neg p \Rightarrow F) \Leftrightarrow p$
F	T	F	F	T
T	F	F	T	T

It consists of showing that a logical implication having as hypothesis $\neg p$ and as conclusion a contradiction is true. So the only possibility is that proposition $\neg p$ is false which implies that proposition p is true.

This proof generally begins with: "Let us suppose $\neg p$ and look for a contradiction". The contradiction appears in the form of a proposition and its opposite true at the same time.

Example 1.13.4 *Show that $\sqrt{2}$ is an irrational number. Suppose that $\sqrt{2}$ is a rational number. Therefore, there exist two coprime integers m, n such that $\sqrt{2} = \frac{m}{n}$ with $n \neq 0$.*

By squaring, we obtain $2 = \frac{m^2}{n^2}$ then $2n^2 = m^2$ and we deduce that m^2 is even and consequently m is even. Since 2 divide m then 4 divide m^2. Regarding the result of division of m^2 by n^2 is 2 then n is also even.

We therefore conclude that m and n are both even, which is a contradiction with the fact that they are coprime numbers.

Example 1.13.5 *We will review the proof of the previous example in more detail.*

We want to show that $p : \sqrt{2}$ is an irrational number.
$\neg p : \exists (m, n) \in (\mathbb{N} \times \mathbb{N}^*) : (m \wedge n = 1) \wedge \sqrt{2} = \frac{m}{n} \cdot (\sqrt{2}$ is not an irrational number)
$\neg p \Rightarrow \exists (m, n) \in (\mathbb{N} \times \mathbb{N}^*) : \underbrace{(m \wedge n = 1)}_{C} \wedge \sqrt{2} = \frac{m}{n} \wedge \underbrace{(m \text{ and } n \text{ are even })}_{\neg C}$
$\neg p \Rightarrow C \wedge (\neg C)$.

Proof by counter-example.

The proof by counter example is based on the following tautology

$$\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$$

To show that propostion $\forall x : P(x)$ is fausse we have to find x_0 such that $\neg P(x_0)$ is true.

Proof by Cases.

Let the propositions $p_1, p_2, \ldots p_n$. We intend to prove that the proposition q such that the proposition $p_1 \vee p_2 \vee \ldots \vee p_n$ is true. It is then sufficient to prove separately that $\forall 1 \leq i \leq n$ if p_i is true then q is true. The validity of a proof by cases rests on the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \Longrightarrow q] \Leftrightarrow [(p_1 \Longrightarrow q) \vee \cdots \vee (p_n \Longrightarrow q)]$$

Example 1.13.6 *Show that for $n \in \mathbb{N}$ then $1 + (-1)^n(2n - 1)$ is a multiple of 4 .*

Proof : Let $n \in \mathbb{N}$, so n is either even or odd. Consider each case separately.

Case $n°1$: Suppose n is even then there exists an integer k such that $n = 2k$. We then obtain

$$1 + (-1)^n(2n - 1) = 1 + 1(2.2k - 1) = 4k.$$

Case $n°2$: Suppose n is odd then there exists an integer k such that $n = 2k + 1$. We then obtain

$$1 + (-1)^n(2n - 1) = 1 + -(2(2k + 1) - 1) = -4k.$$

1.13.1 Constructive and non-constructive proofs

To prove a statement of the form $\exists x \in S, P(x)$, we give either a constructive or a non-contructive proof. In a constructive proof, one proves the statement by exhibiting a specific $x \in S$ such that $P(x)$ is true. In a non-constructive proof, one proves the statement using an indirect proof such as a proof by contradiction. Thus, one might prove that the negation $\forall x \in S, \neg P(x)$ is false by deriving a contradiction.

Example 1.13.7 *(constructive proof): Suppose we are to prove*

$$\exists n \in \mathbb{N}, n \text{ is equal to the sum of its proper divisors.}$$

Proof. Let $n = 6$. The proper divisors of 6 are $1, 2$, and 3. Since $1+2+3 = 6$, we have proved the statement. ■

Exercise 1.13.8 *Give another proof of this statement by finding a different example. (Hint: The smallest example larger than 6 happens to be a number between 25 and 30.)*

An integer which is equal to the sum of its proper divisors is called a perfect number. An open problem is to prove or disprove the following statement: there exists an odd perfect integer.

Example 1.13.9 *(non-constructive proof) Suppose we are to prove*

$$\forall x \in \mathbb{Q},\ \exists n \in \mathbb{N},\ x \leq n.$$

Proof. *Suppose, by way of contradition, that there exists an $x \in \mathbb{Q}$ such that $x > n$ for every $n \in \mathbb{N}$. Since $1 \in \mathbb{N}$, we have that $x > 1$. Therefore, $x = a/b$ for some $a, b \in \mathbb{N}$ such that $a > b$. Since $a \in \mathbb{N}$, $a/b > a$. This implies that $1/b > 1$ and thus $1 > b$, which is a contradiction (since $b \in \mathbb{N}$).* ■

Exercise 1.13.10 *The statement in the previous example can be proved by giving a construction. Give a constructive proof that*

$$\forall x \in \mathbb{Q},\ \exists n \in \mathbb{N},\ x \leq n.$$

Intermediate Value Theorem. Suppose that $f(x)$ is a continuous function on an interval $[a, b]$. If y is a real number between $f(a)$ and $f(b)$, then there exists $c \in (a, b)$ such that $f(c) = y$.