AN INTRODUCTION TO PROOFS & THE MATHEMATICAL VERNACULAR

Learning Objectives:

By the end of this chapter, students should be able to:

- understand the mathematical vernacular;
- construct direct proofs.

Proofs are the heart of mathematics.

If you are a math major, then you must come to terms with proofs—

you must be able to read, understand and write them.

What is the secret? What magic do you need to know?

The short answer is: there is no secret, no mystery, no magic. All that is needed is some common sense and a basic understanding of a few trusted and easy to understand techniques.

SETTING THE CONTEXT

H2 Mathematics involves mostly solving equations and computing answers to numerical questions. This is in contrast to H3 Mathematics as well as university mathematics which deals with a wider variety of problems. What is common across all these problems is the use of deductive reasoning to find the answers to questions. When solving an equation for x, one uses the information provided to deduce the possible values of x. Similarly, when mathematicians solve other kinds of mathematical problems, they always justify their conclusions with deductive reasoning.

Deductive reasoning in mathematics is usually presented in the form of a proof. A mathematical proof is an argument which convinces other people that something is true. Moreover, there is a specific vocabulary and structure that underlies all mathematical proofs. The vocabulary includes logical words such as ‘or’, ‘if’, etc. These words have very precise meanings in mathematics which can differ slightly from everyday usage. Moreover, there are specific common-sense principles of logic, or proof techniques, which one uses to structure the proofs to establish the validity of mathematical statements.

This chapter provides a very brief introduction to the aforementioned. You will be introduced to the requirements of writing direct proofs and taught to differentiate a correct proof from an incorrect one. In later chapters, you will learn other proving techniques which can be employed to tackle an even wider range of mathematical problems.

§1 Propositional Logic

In mathematics, note that not everything can be proved. What can be proved needs to be a **statement** or **proposition**, an expression that is either **true** or **false** but <u>not both</u>.

For example,

6 is an even integer

and

4 is an odd integer

are statements. (The first one is true, and the second is false.)

§1.1 Simple Logical Operations

In arithmetic, we can combine or modify numbers with operations such as ‘+’, ‘×’, etc. Likewise, in logic, we have certain operations for combining or modifying statements to form compound statements; some of these operations are ‘and’, ‘or’ and ‘not’. In mathematics, these words have precise meanings, which are given below. In some cases, the mathematical meanings of these words differ slightly from, or are more precise than, common English usage.

For ease of reference, we will let letters ‘P’ and ‘Q’ denote statements.

[Not] The simplest logical operation is ‘not’. ‘Not P’ is defined to be

- true, when P is false;
- false, when P is true.

The statement ‘not P’ is called the **negation** of P (denoted as $\neg$P).

[And] The statement ‘P and Q’ is defined to be

- true, when P and Q are both true;
- false, when P is false or Q is false or both P and Q are false.

The statement ‘P and Q’ is called the **conjunction** of P and Q (denoted as $\text{P} \wedge \text{Q}$).

[Or] The statement ‘P or Q’ is defined to be

- true, when P is true or Q is true or both P and Q are true;
- false, when both P and Q are false.

The statement ‘P or Q’ is called the **disjunction** of P and Q (denoted as $\text{P} \vee \text{Q}$).
Note: In English, sometimes “P or Q” means that P is true or Q is true, but not both. However, this is never the case in mathematics. We always allow for the possibility that both P and Q are true, unless we explicitly say otherwise.

We say that two statements P and Q are **equivalent**, denoted by $\text{P} \equiv \text{Q}$, if both have the same truth value i.e. both P and Q are true or both P and Q are false.

Example 1

Let the statements P and Q be as follows:
P: It is raining.
Q: I am wet.

Write down the symbolic representation of the following compound statements.

Compound statements	Symbolic Representation
It is raining and I am wet.	$P \wedge Q$
It is raining or I am wet.	$P \vee Q$
It is raining and I am not wet.	$P \wedge \neg Q$

§1.2 Conditional and Biconditional Statements

[If. . . then. . .] The statement 'if P then Q' is defined to be

- true, when P and Q are both true or P is false;
- false, when P is true and Q is false.

The statement 'if P then Q' is a **conditional statement** where P is the hypothesis and Q is the conclusion (denoted by '$P \Rightarrow Q$').

In words, the statement $P \Rightarrow Q$ also reads:
(a) P *implies* Q.
(b) P is a *sufficient condition* for Q.
(c) Q is a *necessary condition* for P.
(d) P *only if* Q.

Examples of conditional statements:
1) If $|x-1|<4$, then $-3<x<5$.
2) If a function f is differentiable, then f is continuous.

[If and only if] The statement 'P if and only if Q' is defined to be

- true, when P and Q are both true or both false;
- false, when one of P, Q is true and the other is false.

The statement 'if P then Q' is a **biconditional statement** (denoted by $P \Leftrightarrow Q$). We sometimes abbreviate the phrase 'if and only if' by 'iff'. When $P \Leftrightarrow Q$ is true, we say that P and Q are equivalent i.e. $P \equiv Q$.

Examples of biconditional statements:
1) $\dfrac{dy}{dx}=x$ if and only if $y=\dfrac{1}{2}x^2+c$ for some constant c.
2) Triangle ABC is an equilateral triangle if and only if the three angles are congruent.
3) a is a rational number if and only if $2a+4$ is rational.

§1.3 Quantifiers

Consider the sentence

x is even.

This is not what we have been calling a statement as we cannot say whether it is true or false, because we do not know what x is.

There are three basic ways to turn this sentence into a statement.

The first is to say exactly what x is:

When $x = 6$, x is even.

The following two are more interesting ways of turning the sentence into a statement:

For every integer x, x is even.

There exists an integer x such that x is even.

The phrases '*for every*' and '*there exists*' are called quantifiers.

As an example of the use of quantifiers, we can give precise definitions of the terms 'even' and 'odd'.

Definition 1 An integer x is even if there exists an integer y such that $x = 2y$.

Definition 2 An integer x is odd if there exists an integer y such that $x = 2y + 1$.

Remark: Both should technically be "if and only if" statements but are worded as above in line with mathematical conventions for wording definitions. Recap biconditional statements. With reference to Definition 1, the ($\Rightarrow$) direction means that all even integers x can be expressed in the form $x = 2y$ while the ($\Leftarrow$) direction says that if we can find an integer y such that $x = 2y$, then x is said to be even.

§1.3.1 Notation

We will call a sentence such as 'x is even' that depends on the value of x a "statement about x". We can denote the sentence 'x is even' by 'P (x)'; then P (5) is the statement '5 is even', P (72) is the statement '72 is even', and so forth.

If S is a set and P (x) is a statement about x, then the notation

$$(\forall x \in S)\ P(x)$$

means that P (x) is true for every x in the set S.

The notation

$$(\exists x \in S)\ P(x)$$

means that there exists at least one element x of S for which P (x) is true.

§1.3.2 Using Quantifiers

Using the above notation, the definitions of 'x is even' and 'x is odd' given previously becomes

$$(\exists y \in \mathbb{Z})x = 2y,$$

$$(\exists y \in \mathbb{Z})x = 2y + 1 \text{ respectively.}$$

The above is still incomplete as we have yet to quantify what x is.
For instance, if we wish to say that all integers are even, we can write

$$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})x = 2y, \text{which is clearly false.}$$

Example 2
Try to explain what the following statements mean in words

Statement	What it means in words
$(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})x = 2y$	There exists an integer x and an integer y such that $x = 2y$.
$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})x = 2y \quad \text{or} \quad x = 2y + 1$	For all integers x, there exists an integer y such that $x = 2y$ or $x = 2y + 1$.

The **order of quantifiers is very important**, changing the order of quantifiers in a statement will often change the meaning of a statement.

For example, the statement

$$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})x < y$$

is true.

However the statement

$$(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z})x < y$$

is false. (Can you explain why?)

There is no integer y that is larger than all possible integers x. Note that for any largest integer M that I define, I can always find an integer larger than it by considering the integer $M + 1$.

Note: This method of proof is often used in proof by contradiction, by forming up the negation of the statement involved and then showing that the negation is impossible.

§1.4 What are Proofs?

Let us examine the following statements

(a) If $x = 2k,\ k \in \mathbb{Z}$, then x is odd.
(b) Two different lines in a plane are either parallel or they intersect at exactly one point.
(c) If x is an even integer, then x^2 is an even integer.
(d) There exists an infinite number of prime numbers.

Statement (a) is clearly false whereas statement (b) is observed to be true. However, it is perhaps not so easy to see whether statements (c) and (d) are true. We need some method to prove that these statements are true/false.

> **Mathematical proofs are convincing arguments expressed in mathematical language, i.e. a sequence of statements leading logically to the conclusion, where each statement is either an accepted truth, or an assumption, or a statement derived from previous statements.** Occasionally there will be the clarifying remark, but this is just for the reader and has no logical bearing on the structure of the proof.

A well written proof will flow. That is, the reader should feel as though they are being taken on a ride that takes them directly and inevitably to the desired conclusion without any distractions about irrelevant details. Each step should be clear or at least clearly justified. A good proof is easy to follow.

A common type of statement that we try to prove is of the form **"If P is true, then Q is true."**, as we see in statements (a) and (c). "P" is often called the hypothesis and "Q" is often called the conclusion. As discussed earlier, we say **"If P then Q"** or simply **"P implies Q"**. Using mathematical symbols, we write

"P $\Rightarrow$ Q".

For example, "If x is an even integer, then x^2 is an even integer." can be written as "x is an even integer $\Rightarrow x^2$ is an even integer."

People are sometimes confused about what needs to be proved when "if" appears. Here are the three main cases:

> - **"Statement**: If P then Q.**"**
>   means we must prove that whenever P is true, Q is also true.
>
> - **"Statement**: P if and only if Q.**"**
>   means we must prove that P and Q are either both true or both false.
>   In other words, we prove "If P then Q" and "If not P then not Q".
>   Equivalently, we prove "If P then Q" and "If Q then P".
>
> - **"Statement**: P only if Q.**"**
>   is equivalent to "If P then Q", so we prove that whenever P is true, Q is also true.

§1.4.1 Direct Proofs

We will first examine the easiest type of proofs to construct i.e. direct proofs. This is probably the most intuitive technique. In a direct proof, we start from an initial set of assumptions and derive some conclusion through a series of logical steps.

Let us take another look at statement C introduced in the previous section "If x is an even integer, then x^2 is an even integer." and see how we can go about to prove it.

Step 1: Understand the Problem (i.e. delimiting the parameters of the problem)

First note that the hypothesis is "x is an even integer" i.e. starting point and the conclusion is "x^2 is an even integer" i.e. ending point.

Moreover, note that the statement is **applicable to all even integers** so we need to prove that the squares of all even integers are indeed even. Moreover, the statement is **NOT applicable to odd integers** so we are not concerned with the parity of the squares of odd integers i.e. we do not care if 17^2 is even since 17 is an odd integer.

Step 2: Devise a Plan

It is always good to start with concrete examples to help one to formulate a plan to tackle the problem. Consider the integer 46 and its square 2116. By eye-balling the number 2116, it is quite apparent that 2116 is an even integer so we can conclude that $46^2 = 2116$ is even. However it is not feasible to do this for all other even integers so we need a more generic plan.

This is where **definitions come in handy**. We have just defined earlier that an integer x is even if and only if there exists an integer y such that $x = 2y$. So if we are able to find such an integer z such that $x^2 = 2z$, then we will be able to conclude that the squared number is indeed even. Moreover, since x is an even number, we can also express $x = 2y$ for some integer y.

Step 3: Carry out the Plan

Proof:

1.Start with the hypothesis.

2. Apply the definition of even integers.

Let x be an even integer. Then by definition, there exists an integer y such that $x = 2y$.

Consider x^2.

3. Try to work toward the conclusion which involves x^2.

$$\begin{aligned} x^2 &= (2y)^2 \\ &= 4y^2 \\ &= 2(2y^2) \\ &= 2z \text{ where } z = 2y^2 \end{aligned}$$

4. Try to find a integer z such that $x^2 = 2z$,

Since z is an integer, x^2 is even. $\square$

6. Conclude (By applying the definition of even integers.)

5. Must state even if it is obvious

7. Small square to mark the end of a proof to signify Q.E.D (quod erat demonstrandum) i.e. what was to be proven has been proven

Note: Steps 1 and 2 are not required. They are provided to elucidate the thinking process. The same goes for the text bubbles in Step 3.

§1.4.2 More Divisibility Proofs

Example 3

Prove that if x is odd, then x^2 is odd.

Proof: (The first and last lines have been written out for you)
Let x be an odd integer. Then by definition, $x = 2y+1$ for some integer y.
Consider x^2.

$$\begin{aligned} x^2 &= (2y+1)^2 \\ &= 4y^2+4y+1 \\ &= 2\left(2y^2+2y\right)+1 \\ &= 2z+1 \text{ where } z = 2y^2+2y \end{aligned}$$

Since z is an integer, x^2 is odd. $\square$

Theorem 1 Combining the previous two results: i.e. x is even $\Rightarrow x^2$ is even and x is odd $\Rightarrow x^2$ is odd, we have the following result:

For all integers, the parity of x and x^2 are the same.

That is, x is even $\Leftrightarrow x^2$ is even and x is odd $\Leftrightarrow x^2$ is odd.

Notes:

1. Subsequently in the course, we will look at how we can negate compound statements like conjunction, disjunction and implication to form equivalent statements. It will be clearer then how the earlier two results can be combined to form the above theorem.
2. You may freely use the above result unless stated otherwise in questions involving divisibility.

When we consider the parity of integers, we are actually considering the divisibility of numbers by 2 i.e. even integers are integers divisible by 2 and odd integers are integers not divisible by 2.

The strategies we employed earlier to prove the parity of numbers can then be easily extended to proofs of divisibility by other numbers.

Definition 3 For all integers x and y, x divides y if $y = kx$ for some integer k.

We commonly abbreviate "x divides y" by writing $x \mid y$ instead. If x does not divide y, we write $x \nmid y$.
Remarks: Similar to before, the above definition is also an "if and only if" statement.

Example 4

Prove that for all positive integer x, if $3 \nmid x$, then $3 \nmid x^2$.

***Understanding the Problem**:* Note we are going to use the strategy that we employed in earlier examples i.e. to find an expression for x that is easy to work. In this case, we note that for x such that $3 \nmid x$, $x \neq 3k$ for all integers k. But it is not easy to work with $x \neq 3k$ so instead we consider the remainder of x when divided by 3. It is clear that there are two possible remainders in this case: 1 and 2. We will deal with these cases separately.

Proof:

Let x be a positive integer not divisible by 3. Then $x = 3k+1$ or $3k+2$ for some integer k.

Case 1: $x = 3k+1$

$$\begin{aligned} \text{Then } x^2 &= (3k+1)^2 = 9k^2 + 6k + 1 \\ &= 3\left(3k^2 + 2k\right) + 1 \\ &= 3z + 1 \text{ where } z = 3k^2 + 2k \end{aligned}$$

Note that z is an integer, thus x^2 will leave a remainder of 1 when divided by 3 and thus is not divisible by 3.

Case 2: $x = 3k+2$ (Left as an exercise to be completed)

$$\begin{aligned} \text{Then } x^2 &= (3k+2)^2 = 9k^2 + 12k + 4 \\ &= 3\left(3k^2 + 4k + 1\right) + 1 \\ &= 3w + 1 \text{ where } w = 3k^2 + 4k + 1 \end{aligned}$$

Note that w is an integer, thus x^2 will leave a remainder of 1 when divided by 3 and thus is not divisible by 3.

Thus, combining both cases, if $3 \nmid x$, then $3 \nmid x^2$. □

Example 5

Prove that for every integer x and for every integer y, if x and y have the opposite parity, then $x + y$ is odd.

Understanding the Problem: If x and y have the opposite parity, there are two possible cases:

1. x is even and y is odd.
2. x is odd and y is even.

Note that both cases are logically similar i.e. the proof for both cases are going to look structurally identical. So instead of "rewriting" the proof for case 1 to prove case 2, we are going to employ a phrase "without the loss of generality (WLOG)".

This is a very helpful phrase in making proofs more concise and less redundant. We use this when dealing with problems with many logically similar cases. When the argument for all the cases are structurally identical, then it suffices to single out one illustrative example.

Proof: (The first and last lines have been written out for you)
Without loss of generality, let x be an even integer and y be an odd integer.

Then $x = 2s$ and $y = 2t + 1$ for some integer s,t.

$$
\begin{aligned}
x + y &= 2s + 2t + 1 \\
&= 2(s + t) + 1 \\
&= 2z + 1 \text{ where } z = s + t
\end{aligned}
$$

Since z is an integer, $x + y$ is odd. $\square$

Question: Can 'without loss of generality" be applied to Example 4 to consider only case 1? Are the proofs for cases 1 and 2 structurally similar?

Answer:

No. The proofs of both cases are not structurally the same as the expression for x is quite different for both cases.

§1.4.3 Proofs involving Inequalities

In proofs of divisibility, it is to be noted that we relied heavily on basic definitions of numbers and applied basic results regarding equalities.

Another class of proofs that we are commonly asked to produce in addition to divisibility proofs are proofs involving inequalities.

For instance, we may be asked to prove that or all positive integers a and b such that $a < b$, $a^2 < b^2$. This may seem like an obvious result thus there lies the challenge. How can we use only basic results i.e. axioms or definitions to prove such seemingly obvious results?

Below we list some axioms (i.e. basic results assumed to be true) that can be applied to inequalities. Such axioms are to be taken to be true without proof as they form the basic building blocks of all proofs involving inequalities.

Axiom 1 For all real numbers a, b, c, if $a \le b$ and $b \le c$ then $a \le c$.

Axiom 2 For all real numbers a, b, c, if $a \le b$ then $a + c \le b + c$.

Axiom 3 For all real numbers a, b, c, if $a \le b$ and $c \ge 0$, then $ac \le bc$.

Axioms 1 to 3 are also true for strict inequalities as well as equalities.

For the next few examples, try applying only Axioms 1 to 3 in the proofs.

Example 6

Prove that for all positive real numbers a and b such that $a \le b$, $a^2 \le b^2$.

Proof: (The first and last lines have been written out for you)
Suppose that $a \le b$ where a and b are positive real numbers.

Multiplying a to both sides of the given inequality, we have $a^2 \le ab$. (*) since $a > 0$.

Multiplying b to both sides of the given inequality, we have $ab \le b^2$. (**) since $b > 0$.

Combining (*) and (**), we have $a^2 \le ab \le b^2$.

Thus, we have $a^2 \le b^2$. $\square$

Example 7

Prove that for all positive real numbers a, $-a < 0$.

Proof: (The first and last lines have been written out for you)
Let a be a positive real number i.e. $a > 0$.

Adding $-a$ to both sides of the given inequality, we have $a + (-a) > 0 + (-a)$.

Thus, we have $-a < 0$. $\square$

Example 8

Prove that for all negative real numbers a and b such that $a < b$, $a^2 \ge b^2$.
(You may freely use any results proven in earlier examples)

Proof:

Let a and b be negative real numbers such that $0 > b \ge a$.

By applying the result in Example 7, $0 > b \Rightarrow -b < 0$. (*)

Adding $-(a+b)$ to both sides of the inequality $b \ge a$, we have $-a \ge -b$. (**)

Combining (*) and (**), we have $0 < -b \le -a$.

By applying the result in Example 6, we have $0 < (-b)^2 \le (-a)^2$.

Simplifying the inequality, we have $a^2 = (-a)^2 \ge (-b)^2 = b^2$. $\square$

§1.5 Conclusion

This chapter provides a brief introduction to mathematical logic, statements and proofs. We learnt about how to construct a direct proof to prove certain mathematical statements.

However, it is to be noted that not all mathematical statements can be easily proven using direct proofs. For example, it is difficult to prove the statement that "there exists an infinite number of prime numbers" by means of a direct proof. We will learn how to prove such statements using other proving techniques subsequently in the course.

In general, to prove the conditional statement

If P then Q.

some commonly used methods are:

(I) **Direct proof**;
Start from P and prove towards Q. For instance, in H2 Math, to prove that a function is increasing, we differentiate the given function to obtain $f'(x)$ and proceed to show that $f'(x)$ is always positive.

Covered in this intro.

(II) **Proof by contradiction**;
We start by supposing that the statement is not true. We try to deduce a fact that contradicts what is given, usually P.

(III) **Proof by contrapositive**;
Prove if not Q, then not P.
Example:
"If it rained, then the grass is wet." has the contrapositive "If the grass is dry, then it did not rain." Another combination: "If it did not rain, then the grass is dry." (***inverse***) may be false because the grass could have been watered.

(IV) **Proof by mathematical induction**;

(V) **Proof by construction**;
Give an example to show it exists.

(VI) **Proof by pigeonhole principle**;

(VII) **Proof by counter-example**.
Give an example to say that something is false.