SECTION D **INTRODUCTION TO PROOF**

By the end of this section you will be able to

- understand what is meant by 'if and only if'
- establish a truth table for 'if and only if'
- understand and follow a $P \Rightarrow Q$ [P implies Q] proof
- prove a $P \Rightarrow Q$ [P implies Q] proof

D1 **If and Only If**

You need to be very careful in this section because it is easy to be confused with all the similar statements. Read each sentence carefully because it seems as if we keep on repeating the same thing but we are not.

We examine the implication of propositions going both ways, that is $\Rightarrow$ and $\Leftarrow$. In the last section we defined implication of two propositions *P* and *Q* which was denoted by $P \Rightarrow Q$ [P implies Q]. *What was the converse of* $P \Rightarrow Q$*?*

The converse goes the other way $Q \Rightarrow P$ $\left[Q \text{ implies } P\right]$. *Assume* $P \Rightarrow Q$ *is true, then what is the truth value of the converse,* $Q \Rightarrow P$*?*

From the last section we could not conclude whether $Q \Rightarrow P$ is true or false. In some cases $Q \Rightarrow P$ is true and in other cases it is false. If the compound proposition $P \Rightarrow Q$ and $Q \Rightarrow P$ have the same truth value then $P \Rightarrow Q$ and $Q \Rightarrow P$ are equivalent propositions. If $P \Rightarrow Q$ [P implies Q] and $Q \Rightarrow P$ [Q implies P] then this is normally denoted by $P \Leftrightarrow Q$ and we say '*P* if and only if *Q*'.

Hence $P \Leftrightarrow Q$ means $P \Rightarrow Q$ and $Q \Rightarrow P$. The symbol $\Leftrightarrow$, which looks like an equal sign with arrows on both ends, means implication goes both ways.

Example 29

Establish the truth table for $P \Leftrightarrow Q$ [P if and only if Q].

Solution

How do we construct this truth table?

List all the combinations of truth values for *P* and *Q* then find the truth values of

(a) $P \Rightarrow Q$

(b) $Q \Rightarrow P$ and then

(c) $P \Leftrightarrow Q$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$ $\left[P \Rightarrow Q \text{ and } Q \Rightarrow P\right]$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

TABLE 19

From this table what do you notice about $P \Leftrightarrow Q$ *when* P *and* Q *have the same truth value?*

If *P* and *Q* have the same truth value then $P \Leftrightarrow Q$ is true.

In general let P and Q be propositions then $P \Leftrightarrow Q$ means

1. $P \Rightarrow Q$ and $Q \Rightarrow P$ [Implication in both directions]
2. P if and only if Q
3. P and Q are equivalent propositions

An example is

$$x^2 - 3x + 2 = 0 \quad \Leftrightarrow \quad x = 1 \quad \text{or} \quad x = 2$$

What does this statement mean?

$$\text{If } x^2 - 3x + 2 = 0 \quad \text{then} \quad x = 1 \quad \text{or} \quad x = 2$$

Also

$$\text{if} \quad x = 1 \quad \text{or} \quad x = 2 \quad \text{then} \quad x^2 - 3x + 2 = 0$$

The implication goes both ways. Another example is:

The quadratic equation $ax^2 + bx + c = 0$ has real roots if and only if $b^2 - 4ac \geq 0$.

What does this mean?

Remember 'if and only if' and '$\Leftrightarrow$' are the same thing therefore this means that

$$\text{if } ax^2 + bx + c = 0 \text{ has real roots then } b^2 - 4ac \geq 0$$

and also

$$\text{if } b^2 - 4ac \geq 0 \text{ then } ax^2 + bx + c = 0 \text{ has real roots.}$$

The implication goes both ways. We could also say '$ax^2 + bx + c = 0$ has real roots' and '$b^2 - 4ac \geq 0$' are equivalent propositions.

D2 **Introduction to Proof**

This is a very difficult and challenging section. To be able to prove the results in this section you need to thoroughly understand and apply the definitions.

What does the term 'proof' mean?

A mathematical proof is a series of steps of logical reasoning which eventually leads to a conclusion. Each step is a deduction from the previous step by some logical reasoning. In mathematics we are normally asked to prove a proposition or a theorem.

What does the term 'theorem' mean?

A theorem is a mathematical proposition whose truth can be established by proving it. Many mathematical propositions and theorems we want to prove are of the form $P \Rightarrow Q$ [P implies Q] where P and Q are propositions. To prove $P \Rightarrow Q$ we assume P is true and then by steps of logical reasoning we deduce Q. Example 30 below shows how this works.

In example 30 we prove that if n is an even number then n^2 is an even number.

It sounds like an obvious proposition but how do we know it is true?

Just because it works for every number we can think of does **not** mean it is true. We have to prove it.

Before we can prove this we need a definition of what is meant by an even number.

Definition (1.1). An integer n is an **even number** $\Leftrightarrow$ there is an integer m such that

$$n = 2m$$

What does this definition (1.1) mean?

Note that the implication goes both ways, that is:

$$\text{if } n \text{ is an even number then } n = 2m \quad [2 \text{ (An Integer)}]$$

And also

$$\text{if } n = 2m \text{ then } n \text{ is an even number}$$

We can also say that the even number n is a multiple of 2 or 2 divides n.

Can you remember what integer means?

A whole number is called an integer. Examples are $-10,\ -3,\ 0,\ 1,\ 5$ etc

Example 30

Prove the following:

Proposition (1.2). If n is an even number then n^2 is an even number.

Remark. *How do we prove that if n is even then n^2 is even?*

Since we have an 'if and then' statement therefore we need to prove

$$n \text{ is even} \Rightarrow n^2 \text{ is even}$$

The procedure for proving $P \Rightarrow Q$ is to assume that P is true and deduce Q by steps of logical reasoning. Let P be 'n is even' and Q be 'n^2 is even'. Hence we assume n is even and deduce n^2 is even.

Proof. Let n be an even number then by definition (1.1) it can be written as $n = 2m$ where m is an integer. We have

$$\begin{aligned} n &= 2m \\ n^2 &= (2m)^2 \qquad [\text{Squaring Both Sides}] \\ &= 4m^2 \\ n^2 &= 2(2m^2) \qquad [\text{Rewriting } 4 = 2(2)] \end{aligned}$$

Since the bracketed term $2m^2$ is an integer and

$$n^2 = 2(2m^2) \qquad [2 \text{ (An Integer)}]$$

therefore by definition (1.1) we can say n^2 is even.

We have proven the required result that if n is even then n^2 is even.

■

The symbol ■ at the end means that the proof is complete. We have shown what was required.

Note the procedure in proving the proposition 'if n is even then n^2 is even'.

You need to know the definition of an even number and then use this definition to prove 'n is even $\Rightarrow$ n^2 is even.'

In mathematical proof we have to be rigorous, each step follows from the previous step by some logical reasoning. In the above proof it is **not** good enough to say that $n^2 = 2(2m^2)$ is even because we think it is. It needs to follow from some rule, definition, proposition, theorem etc. For the above example we can **only** say n^2 is even because $n^2 = 2(2m^2)$ satisfies definition (1.1). That is

$$n^2 = 2 \text{ (An Integer)} \Rightarrow n^2 \text{ is even}$$

Generally in a $P \Rightarrow Q$ proof we call P the **hypothesis** and Q the **conclusion**. In this kind of proof we assume the hypothesis, P, to be true and deduce the conclusion Q to be true.

Should proofs be learnt by rote?

No but it is worth investing your time in learning and understanding definitions and statements of propositions. Moreover you should be able to use these definitions and statements in unfamiliar circumstances. You can only do this if you are confident in the meaning of these. For example we have used definition (1.1) in both directions,

(1.1) An integer n is an even number $\Leftrightarrow$ there is an integer m such that $n = 2m$

$\Rightarrow$ and $\Leftarrow$, in the proof of proposition (1.2) above. You must know this definition from left to right and right to left to be able to use it.

For proving the next proposition we need to know the definition of an **odd** number.
What is an odd number?

Definition (1.3). An odd number is an integer which is **not** even.
Hence an integer n is odd $\Leftrightarrow$ $n = 2m+1$ where m is an intger.

Example 31

Prove the following:
Proposition (1.4). The sum of two odd numbers is even.

Proof. Another obvious proposition but how do we prove this?
We consider two odd numbers such as m and n and then prove that the sum $m+n$ is even.
Let m and n be odd numbers. By definition (1.3) we can write m and n as

$$m = 2k+1 \quad \text{and} \quad n = 2\ell+1$$

where k and ℓ are integers. Then

$$\begin{aligned} m+n &= \underbrace{2k+1}_{=m} + \underbrace{2\ell+1}_{=n} \\ &= 2k+2\ell+2 \\ &= 2\left(k+\ell+1\right) \qquad \left[\text{Factorizing}\right] \end{aligned}$$

Since $k+\ell+1$ is an integer and

$$m+n = 2\left(k+\ell+1\right) \quad [2 \text{ (An Integer)}]$$

therefore using definition (1.1) in $\Leftarrow$ direction we can conclude that $m+n$ is even.
Hence we have proven that 'the sum of two odd numbers is even'.

■

The proof in Example 31 is more challenging because how are we supposed to know that we consider odd numbers m and n?
Because the given proposition says 'The sum of **two odd** numbers…'
Therefore we write out two arbitrary odd numbers m and n by using definition (1.3).
Why arbitrary odd numbers?
Arbitrary here means random. There was no prejudice in choosing these numbers. Hence if the proof works for arbitrary odd numbers, m and n, then it is valid for all odd numbers. This is a technique used in proving general mathematical results.
By adding these numbers we obtain a multiple of 2, that is $m+n = 2\left(k+\ell+1\right)$. Then by definition (1.1) we conclude that this is even. Again the sole reason why

$$m+n = 2\left(k+\ell+1\right)$$

is even is because it satisfies definition (1.1).
In the above proofs we have been assuming the algebraic properties of real numbers. In general we will assume these but they are given in **Appendix A**. We will use these properties throughout the text.

(1.1) n is an even number $\Leftrightarrow$ there is an integer m such that $n = 2m$

D3 **Divisibility Proofs**

What is meant by a divides b ?

Definition (1.5). Let a and b be integers where $a \neq 0$. Then a divides b $\Leftrightarrow$ there is an integer x such that $ax = b$.

What does this definition (1.5) mean?

Note that implication goes both ways. We have for some integer x:

if a divides b then $ax = b$ $\quad [a(\text{An Integer}) = b]$

and also if $ax = b$ then a divides b

The notation for a divides b is $a \mid b$. If a does **not** divide b then this is denoted by $a \nmid b$.

Example 32

Prove the following:

Proposition (1.6). If $a \mid b$ and $b \mid c$ then $a \mid c$.

Note: To understand mathematics you need to learn the symbolic language of mathematics. If you don't know what is meant by $a \mid b$ then you will not be able to prove the given proposition. From above we have $a \mid b$ means 'a divides b.'

Similarly $b \mid c$ means 'b divides c' and $a \mid c$ means 'a divides c.'

How do we prove the given proposition 'if $a \mid b$ and $b \mid c$ then $a \mid c$?'

Since this is an 'if and then' statement it is equivalent to $(a \mid b \text{ and } b \mid c) \Rightarrow a \mid c$.

It is a $P \Rightarrow Q$ proof where P is the proposition '$a \mid b$ and $b \mid c$' and Q is the proposition '$a \mid c$'. *How do we prove $P \Rightarrow Q$?*

We assume P is true and then deduce Q is true by applying logical reasoning. That is we assume $a \mid b$ and $b \mid c$ is true and from this we deduce that $a \mid c$. *What can we use to prove $a \mid c$ from the assumption $a \mid b$ and $b \mid c$?*

We use definition

(1.5) $a \mid b \Leftrightarrow$ there is an integer x such that $ax = b$

Proof. Assume $a \mid b$ [a divides b]. By definition (1.5) we can say there is an integer x such that

$$ax = b$$

Similarly by applying definition (1.5) on the other assumption, $b \mid c$ [b divides c], we know there is an integer y such that

$$by = c$$

Substituting $ax = b$ into $by = c$ gives

$$(ax)y = c \quad [\text{Substituting } b = ax]$$

$$a(xy) = c$$

Since x and y are integers then so is their multiplication, xy. *Have we proven $a \mid c$?*

Yes because we have an integer, xy, such that

$$a(xy) = c \quad [a(\text{An Integer}) = c]$$

By definition (1.5) we have a divides c or in notation form $a \mid c$. Hence we have proved the required result.

■

Examine the steps in the proof of the above proposition (1.6). We assume the hypothesis $a \mid b$ [a divides b] and $b \mid c$ [b divides c] and by using definition (1.5) in the $\Rightarrow$ direction we have integers x and y such that

$$ax = b \text{ and } by = c$$

By substitution we have $a(xy) = c$. Using definition (1.5) on $a(xy) = c$ in $\Leftarrow$ direction, we conclude that $a \mid c$.

In proving a $P \Rightarrow Q$ proposition we first write down the hypothesis P which we assume to be true. Then we use logical rules, definitions, statements of propositions that have been proven to deduce the conclusion Q. This is why you need to learn the definitions, statements of propositions etc so that you can use them in the proof. Sometimes it is helpful to write down the conclusion Q with a statement like 'required to prove Q'. This helps in the direction of the proof.

Example 32

Prove:

Proposition (1.7). If $a \mid b$ and $a \mid c$ then

$$a \mid (bm + cn)$$

where m and n are arbitrary integers.

Note. Since we have an 'if and then' statement in the proposition therefore this is a $P \Rightarrow Q$ proof. We assume $a \mid b$ and $a \mid c$ and we are required to prove

$$a \mid (bm + cn)$$

How?

Use definition

(1.5) $a \mid b \Leftrightarrow$ there is an integer x such that $ax = b$

Proof. Assume $a \mid b$ then by definition (1.5) there is an integer x such that

$$ax = b$$

Similarly we assume $a \mid c$ so again by definition (1.5) there is an integer y such that

$$ay = c$$

We need to prove $a \mid (bm + cn)$. So consider the number $bm + cn$ where m and n are arbitrary integers. *How are we going to use our deductions,* $ax = b$ *and* $ay = c$*, with* $bm + cn$*?*

Substitute $ax = b$ and $ay = c$ into $bm + cn$:

$$\begin{aligned} bm + cn &= (ax)m + (ay)n \\ &= axm + ayn \\ &= a(xm + yn) \qquad [\text{Factorizing}] \end{aligned}$$

Since m, n, x and y are integers then so is $(xm + yn)$ an integer. Hence there is an

---

(1.5) $a \mid b \Leftrightarrow$ there is an integer x such that $ax = b$

integer $(xm+yn)$ such that

$$a(xm+yn)=bm+cn$$

Hence $a(\text{Integer})=bm+cn$.

Using definition (1.5) on this $a(xm+yn)=bm+cn$ in the $\Leftarrow$ direction we have $a \mid (bm+cn)$ or a divides $bm+cn$. This is what was required.

■

Note that the above proof uses definition (1.5) in both directions, $\Rightarrow$ and then $\Leftarrow$.
You need to thoroughly know
Definition (1.5) $a \mid b \Leftrightarrow$ there is an integer x such that $ax=b$
otherwise how would you prove proposition (1.7)?
You need to learn this definition from left to right and right to left.

SUMMARY
The notation $P \Leftrightarrow Q$ means
1. $P \Rightarrow Q$ and $Q \Rightarrow P$
2. 'P if and only if Q'
3. P and Q are equivalent.

The procedure for $P \Rightarrow Q$ proof is to assume P and then deduce Q by steps of logical reasoning. P is called the **hypothesis** and Q is called the **conclusion**.