SECTION 1.2 ⟹ Introduction to Proof

By the end of this section you will be able to

- understand what is meant by tautology
- understand what is meant by 'if and only if'
- construct a $P \Rightarrow Q$ [P implies Q] proof

I.2.1 Tautology

Tautology is a compound proposition which is *always* true.

Example 12

Construct the truth table for $P \vee \left(\neg P\right)$.

Solution

We have (you were asked to construct this in Exercises **I.1** question 9(b)):

P	$\neg P$	$P \vee \left(\neg P\right)$
T	F	T
F	T	T

Table 10

It doesn't matter what the truth value of P is but $P \vee \left(\neg P\right)$ is *always* true. This is sometimes written as

$$P \vee \left(\neg P\right) \equiv T\,.$$

Hence $P \vee \left(\neg P\right)$ is an example of a tautology. This means P or (not P) is always true.

For example, let P be '$x^2 - 9 = 0$' then '$\underbrace{x^2 - 9 = 0}_{P}$ or $\underbrace{x^2 - 9 \neq 0}_{\neg P}$' is *always* true.

That is $x^2 - 9$ is equal to zero or it is *not* equal to zero is an example of a tautology and therefore is always true.

Example 13

Construct the truth table for $\left(P \Rightarrow Q\right) \wedge \left(Q \Rightarrow R\right)$.

Solution

We first list the combination of truth values for the propositions P, Q and R (in the first three columns). Next, we evaluate

$$P \Rightarrow Q \quad \text{(column 4) and } Q \Rightarrow R \quad \text{(column 5)}.$$

Finally, we find the truth values of $\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)$ in the right-hand column.

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	F
F	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T
F	F	F	T	T	T

Table 11

Example 14

Construct the truth table for $\Big[\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)\Big] \Rightarrow \big(P \Rightarrow R\big)$. *What do you notice about your result?*

Solution

We have already found the truth value of $\Big[\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)\Big]$ in the last column of the previous Table 11. We can copy this into the table below and find the truth values of the remainder of the proposition.

P	Q	R	$\Big[\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)\Big]$	$P \Rightarrow R$	$\Big[\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)\Big] \Rightarrow \big(P \Rightarrow R\big)$
T	T	T	T	T	T
T	T	F	F	F	T
T	F	T	F	T	T
F	T	T	T	T	T
T	F	F	F	F	T
F	T	F	F	T	T
F	F	T	T	T	T
F	F	F	T	T	T

Table 12

By observing the right-hand column of Table 12 we can say

$$\Big[\big(P \Rightarrow Q\big) \wedge \big(Q \Rightarrow R\big)\Big] \Rightarrow \big(P \Rightarrow R\big)$$

is a tautology. (It is always true). It can be written as

$$\left[\left(P \Rightarrow Q\right) \wedge \left(Q \Rightarrow R\right)\right] \Rightarrow \left(P \Rightarrow R\right) \equiv T$$

What does this proposition $\left[\left(P \Rightarrow Q\right) \wedge \left(Q \Rightarrow R\right)\right] \Rightarrow \left(P \Rightarrow R\right)$ *mean?*

It looks horrendous but all it says is:

'If $\underbrace{P \text{ implies } Q \text{ and } Q \text{ implies } R}_{(P \Rightarrow Q) \wedge (Q \Rightarrow R)}$ then $\underbrace{P \text{ implies } R}_{P \Rightarrow R}$'.

For example, let P, Q and R be the following propositions:

$$P\text{: } 2x+1=0\,, \quad Q\text{: } 2x=-1 \quad \text{and} \quad R\text{: } x=-\frac{1}{2}\ .$$

Using $\left[\left(P \Rightarrow Q\right) \wedge \left(Q \Rightarrow R\right)\right] \Rightarrow \left(P \Rightarrow R\right)$ we have:

If

$$P \Rightarrow Q\text{: } 2x+1=0 \ \Rightarrow\ 2x=-1 \quad \text{and} \quad Q \Rightarrow R\text{: } 2x=-1 \ \Rightarrow\ x=-\frac{1}{2}$$

then

$$P \Rightarrow R\text{: } 2x+1=0 \ \Rightarrow\ x=-\frac{1}{2}.$$

This is how we deduce our results in a proof:

If $\underbrace{P \text{ implies } Q \text{ and } Q \text{ implies } R}_{(P \Rightarrow Q) \wedge (Q \Rightarrow R)}$ then $\underbrace{P \text{ implies } R}_{P \Rightarrow R}$'.

I.2.2 Converse

Let P and Q be propositions. We know implication between P and Q is denoted by $P \Rightarrow Q$. If we go the other way, which is $Q \Rightarrow P$ [Q implies P] then this is called the **converse** of $P \Rightarrow Q$ [P implies Q]. For example, let

P : I have two exotic holidays per year.

Q : I am rich.

What is $P \Rightarrow Q$ *?*

If $\underbrace{\text{I have two exotic holidays per year}}_{P}$ then $\underbrace{\text{I am rich}}_{Q}$.

What is $Q \Rightarrow P$ *?*

If $\underbrace{\text{I am rich}}_{Q}$ then $\underbrace{\text{I have two exotic holidays per year}}_{P}$.

Example 15

Construct the truth table for $Q \Rightarrow P$ and compare your solution with $P \Rightarrow Q$. *What do you notice?*

Solution

Remember $Q \Rightarrow P$ is *only* false when Q is true and P is false otherwise $Q \Rightarrow P$ is true. The truth table is given by:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Table 13

What can you conclude about $P \Rightarrow Q$ *and* $Q \Rightarrow P$ *?*

Since the truth values of $P \Rightarrow Q$ and $Q \Rightarrow P$ do *not* match therefore we conclude that $P \Rightarrow Q$ is *not* equivalent to $Q \Rightarrow P$:

$$\big(P \Rightarrow Q\big) \not\equiv \big(Q \Rightarrow P\big) \qquad \text{[Not Equivalent]}.$$

This is an *important* result which many students find difficult to accept especially when proving propositions. They sometimes prove the converse, $Q \Rightarrow P$ [Q implies P], and think they have proven $P \Rightarrow Q$ [P implies Q]. You need to be very careful. Let P be the proposition 'x is an omelette' and Q be the proposition that 'x contains eggs'. Then $P \Rightarrow Q$ is true because if x is an omelette then it contains eggs. However, $Q \Rightarrow P$ is *false* because if x contains eggs then x maybe a cake or something else, it doesn't need to be an omelette.

Consider a mathematical example where P is the proposition '$x = 5$' and Q is the proposition '$x^2 = 25$' then $P \Rightarrow Q$ is given by:

$$x = 5 \quad \Rightarrow \quad x^2 = 25 \quad \text{which is true.}$$

However, the converse $Q \Rightarrow P$

$$x^2 = 25 \quad \Rightarrow \quad x = 5 \quad \text{is } \textit{false} \text{ because } x \text{ could equal } -5.$$

Consider another example where P is the proposition 'a and b are odd' and Q is the proposition '$a + b$ is even' then $P \Rightarrow Q$ is given by:

a and b are odd $\Rightarrow$ $a + b$ is even. [This is true, see Proposition (I.4) on page 18].

But the converse $Q \Rightarrow P$:

$$a + b \text{ is even} \Rightarrow \quad a \text{ and } b \text{ are odd}$$

is *false*. *Why?*

If $a + b = 6$ then a could be 4 and b could be 2. Hence $a + b$ is even but both a and b could also be even.

Hence the converse, $Q \Rightarrow P$ [Q implies P], of the proposition $P \Rightarrow Q$ [P implies Q] may or may *not* true.

I.2.3 If and only If

You need to be very careful in this subsection 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 $\Leftarrow$.

From above we could not conclude whether $Q \Rightarrow P$ is true or false. In some cases, $Q \Rightarrow P$ is true but in other cases it is false. If the compound proposition $P \Rightarrow Q$ and $Q \Rightarrow P$ have the same truth values then $P \Rightarrow Q$ and $Q \Rightarrow P$ are equivalent propositions. If $P \Rightarrow Q$ and $Q \Rightarrow P$ then this is denoted by $P \Leftrightarrow Q$ and we say 'P if and only if Q'. The symbol $\Leftrightarrow$, which looks like an equal sign with arrows on both ends, means implication goes both ways.

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?

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

Also

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

The implication goes both ways.

The Proposition $P \Leftrightarrow Q$ can also be stated as

'P is a necessary and sufficient condition for Q'.

Hence, $P \Leftrightarrow Q$, P if and only if Q and 'P is a necessary and sufficient condition for Q' are *all* equivalent.

I.2.4 Introduction to Proof

This is a challenging subsection. 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 16 below shows how this works.

In Example 16 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 must prove it.

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

Definition (I.1). An integer n is an *even number* $\Leftrightarrow$ there is an integer m such that $n = 2m$.

Can you remember what integer means?

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

What does this Definition (I.1) mean?

Note that the implication goes both ways, that is:

if n is an even number then $n = 2m$ $\left[2 \times \text{integer}\right]$.

And

if $n = 2m$ then n is an even number.

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

Example 16

Prove the following:

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

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

n is even $\Rightarrow$ n^2 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'.

Proof.

Let n be an even number then by Definition (I.1) it can be written as $n = 2m$ where m is an integer. We have

$$n = 2m$$
$$n^2 = (2m)^2 = 4m^2 = 2(2m^2) \quad [\text{Squaring both sides}]$$

The bracketed term $2m^2$ is an integer and

$$n^2 = 2(2m^2) \quad [2 \times \text{integer}]$$

By Definition (I.1) we can say n^2 is even. This completes our proof.

■

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 must 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 (I.1). That is

$$n^2 = 2 \times \text{integer} \Rightarrow n^2 \text{ is even.}$$

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 apply 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 (I.1) in both directions, $\Rightarrow$ and $\Leftarrow$, in the proof of Proposition (I.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 (I.3). An integer n is odd $\Leftrightarrow$ $n = 2m + 1$ where m is an integer.

Example 17

Prove the following:

Proposition (I.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 (I.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

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

We have $k+\ell+1$ is an integer therefore

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

Using Definition (I.1) in $\Leftarrow$ direction we can conclude that $m+n$ is even. We have proven that 'the sum of two odd numbers is even'.

■

The proof in Example 17 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 (I.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 (I.1) we conclude that this is even. Again, the reason why

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

is even is because it satisfies Definition (I.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**.

I.2.5 Divisibility Proofs

What is meant by a divides b?

Definition (I.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 (I.5) mean?

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

$$\text{if } a \text{ divides } b \text{ then } ax = b \qquad \left[a \times (\text{An Integer}) = b\right]$$

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 18

Prove the following:

Proposition (I.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 this proposition. From above we have $a \mid b$ means 'a divides b.'

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 compound 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 $b \mid c$ are 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 the previous Definition:

(I.5) $a \mid b \Leftrightarrow$ there is an integer x such that $ax = b$.

Proof.

Assume $a \mid b$ [a divides b]. By (I.5) we can say there is an integer x such that

$$ax = b.$$

Similarly, by applying Definition (I.5) on the other assumption, $b \mid c$, there is an integer y such that

$$by = c\,.$$

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

$$\begin{aligned} (ax)y &= c \qquad [\text{Substituting } \; b = ax] \\ a(xy) &= c \end{aligned}$$

We have $a(xy) = c$ therefore we conclude by Definition (I.5) that a divides c or in notation form $a \mid c$. This completes our proof.

■

Examine the steps in the proof of the previous Proposition (I.6). We assume the hypothesis $a \mid b$ [a divides b] and $b \mid c$ [b divides c] and by using Definition (I.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 (I.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 before to deduce the conclusion Q. Therefore, you need to learn the definitions, statements of propositions 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 and gives your proof a destination.

Summary

The *converse* of $P \Rightarrow Q$ is $Q \Rightarrow P$. Also, it is important to note that

$$(Q \Rightarrow P) \not\equiv (P \Rightarrow Q) \quad [\text{Not Equivalent}].$$

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