SECTION E **PROOFS**

By the end of this section you will be able to

- understand and construct a 'if and only if' proof
- understand and construct a proof by contrapositive
- understand what is meant by the term "without loss of generality"

E1 **If and Only If Proof**

What is meant by 'If and Only If'?

'If and only if' is related to two propositions such as P and Q. We normally have P if and only if Q and this in symbolic form is given by $P \Leftrightarrow Q$. *But what does* $P \Leftrightarrow Q$ *mean?*

$P \Leftrightarrow Q$ means the implication goes both ways, that is $P \Rightarrow Q$ [P implies Q] and $Q \Rightarrow P$ [Q implies P]. In this subsection we are interested in proving propositions of the form $P \Leftrightarrow Q$. *How do we prove these?*

The proof of these, $P \Leftrightarrow Q$, is done in two parts:

1. Prove $P \Rightarrow Q$ (if P then Q).
2. Prove $Q \Rightarrow P$ (if Q then P).

In part 1 we assume P is true and then deduce Q.
In part 2 we assume Q is true and then deduce P.

Mathematical proof is based on rigour **not** instinct. To prove $P \Leftrightarrow Q$ means you have to prove **both** parts, $P \Rightarrow Q$ and $Q \Rightarrow P$.

The next example shows how this works. In this example we assume that you are familiar with solving quadratic equations. Also we use the following:

$$ab = 0 \quad \Rightarrow \quad a = 0 \text{ or } b = 0$$

where a and b are real numbers. That is if a product such as ab is zero then either $a = 0$ or $b = 0$.

Example 33

Prove that

$$x^2 - 5x + 6 = 0 \quad \Leftrightarrow \quad x = 2 \text{ or } x = 3$$

Comment. *How do we prove this?*

Remember the symbol $\Leftrightarrow$ means the implication goes both ways and in this case we have:

$$x = 2 \text{ or } x = 3 \quad \Rightarrow \quad x^2 - 5x + 6 = 0$$

and

$$x^2 - 5x + 6 = 0 \quad \Rightarrow \quad x = 2 \text{ or } x = 3$$

We can first prove '$x = 2$ or $x = 3 \Rightarrow x^2 - 5x + 6 = 0$'. This is a $P \Rightarrow Q$ proof where we assume P $\left(x = 2 \text{ or } x = 3\right)$ and deduce Q $\left(x^2 - 5x + 6 = 0\right)$.

Proof. Assume $x = 2$ or $x = 3$ then substituting these values into $x^2 - 5x + 6$ gives:

$$2^2 - 5(2) + 6 = 0$$

$$3^2 - 5(3) + 6 = 0$$

Hence $x = 2$ or $x = 3 \quad \Rightarrow \quad x^2 - 5x + 6 = 0$.

The second part of the proof involves going the other way. Assume $x^2-5x+6=0$ and we need to show $x=2$ or $x=3$. *How?*
From the assumption $x^2-5x+6=0$ we need to extract out the values of x.

$$\begin{aligned} & x^2-5x+6=0 \\ \Rightarrow\ & (x-2)(x-3)=0 && [\text{Factorizing}] \\ \Rightarrow\ & x-2=0 \text{ or } x-3=0 \\ \Rightarrow\ & x=2 \text{ or } x=3 && [\text{Solving}] \end{aligned}$$

Hence $x^2-5x+6=0 \Rightarrow x=2$ or $x=3$.
By combining the two parts we have proved that

$$x^2-5x+6=0 \Leftrightarrow x=2 \text{ or } x=3$$

which is what was required.

■

We could have proved '$x^2-5x+6=0 \Rightarrow x=2$ or $x=3$' first and then proved '$x=2$ or $x=3 \Rightarrow x^2-5x+6=0$' in the above example. It does **not** matter which one you prove first. Normally it is simpler to prove the easier part first so that you gain confidence.
In the following 3 examples the lower case letters represent integers.
In the next example we use the notation $a \mid b$ from the last section. *What does $a \mid b$ mean?*
$a \mid b$ means 'a divides b'.

Example 34

Prove the following:
Proposition (1.8). For $c \neq 0$

$$ac \mid bc \Leftrightarrow a \mid b$$

Comment. *What does this proposition say in everyday language?*
For $c \neq 0$ we have 'ac divides bc' if and only if 'a divides b'. *So how do we prove this proposition?*
Since we have the implication sign, $\Leftrightarrow$, going both ways therefore we have to prove both parts, that is

1. $ac \mid bc \Rightarrow a \mid b$
2. $a \mid b \Rightarrow ac \mid bc$

Proof. How do we prove the first part '$ac \mid bc \Rightarrow a \mid b$?'
Actually we have already proven this in Exercise 1(d) Question 1(h). However there is **no** harm in reconstructing the proof. This is a $P \Rightarrow Q$ proof where P is '$ac \mid bc$' and Q is '$a \mid b$'.
We assume $ac \mid bc$. *What can we deduce from $ac \mid bc$?*
By using definition
(1.5) $a \mid b \Leftrightarrow$ there is an integer x such that $ax=b$
on $ac \mid bc$ we have an integer x such that

$$ac(x)=bc$$

Remember we are told that $c \neq 0$ therefore we can divide through by c:

$$a(x) = b$$

We have $a(\text{Integer}) = b$. Again by definition (1.5) we have $a \mid b$.

Have we completed the proof?

No we need to prove the second part, that is $a \mid b \;\Rightarrow\; ac \mid bc$. *How do we prove this?*

We assume $a \mid b$ and then deduce $ac \mid bc$.

By applying definition (1.5) on the assumption $a \mid b$ we have an integer *y* such that

$$ay = b$$

Multiple both sides by c:

$$ayc = bc$$

$$ac(y) = bc$$

We have $ac(\text{Integer}) = bc$. Again by definition (1.5) we have deduced the required result, $ac \mid bc$, for the second part.

Hence we have proved both parts of

$$ac \mid bc \;\Leftrightarrow\; a \mid b \text{ where } c \neq 0$$

which means we have shown the given proposition.

■

E2 **Proof by Contrapositive**

We have already covered what is meant by the term contrapositive. *Do you remember what it means?*

If we have a proposition such as $P \Rightarrow Q$ then the contrapositive of $P \Rightarrow Q$ is

$$(\text{not } Q) \Rightarrow (\text{not } P)$$

Also in the earlier section we showed that

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

Since $P \Rightarrow Q$ and $(\text{not } Q) \Rightarrow (\text{not } P)$ are equivalent therefore if we prove $(\text{not } Q) \Rightarrow (\text{not } P)$ then we have proven $P \Rightarrow Q$. Sometimes it is easier to prove $(\text{not } Q) \Rightarrow (\text{not } P)$ rather than $P \Rightarrow Q$. The following example is such a case.

Example 35

Prove that if n^2 is odd then n is odd.

Comment. Clearly this is a $P \Rightarrow Q$ statement because it has 'if and then' in the statement of the proposition. Let's try proving the given proposition by using the normal procedure for $P \Rightarrow Q$ proof. The procedure is to assume *P* (n^2 is odd) and then deduce *Q* (n is odd).

Assume n^2 is odd. By definition (1.3) we can write n^2 as

$$n^2 = 2m + 1$$

where m is an integer. To find n we take the square root of both sides:

$$n = \sqrt{n^2} = \sqrt{2m+1}$$

(1.3) n is odd $\Leftrightarrow$ $n = 2m + 1$

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

Need to prove that n is odd but we have

$$n = \sqrt{2m+1}$$

How can we prove $n = \sqrt{2m+1}$ *is odd?*

It's going to be impossible to show that $n = \sqrt{2m+1}$ is odd because we do not have any further information. Clearly if we assume P (n^2 is odd) and then deduce Q (n is odd) it leads us to a blind alley.

So how are we going to prove the given proposition

$$n^2 \text{ is odd } \Rightarrow n \text{ is odd ?}$$

Prove the contrapositive of the given proposition.

Proof. What is the contrapositive of 'n^2 *is odd* $\Rightarrow n$ *is odd '?*

We have $P \Rightarrow Q$ where P is 'n^2 is odd' and Q is 'n is odd'. The contrapositive is

$$(\text{not } Q) \Rightarrow (\text{not } P)$$

What is (not Q*) equal to in this case?*

Since Q is 'n is odd' therefore $(\text{not } Q)$ is 'n is **not** odd'. Every integer is even or odd (although we have not proven this result) so if 'n is not odd' then it must be even. Hence

$(\text{not } Q)$ is 'n is even'

What is (not P*) equal to in this case?*

Since P is 'n^2 is odd' therefore $(\text{not } P)$ is 'n^2 is **not** odd'. Hence

$(\text{not } P)$ is 'n^2 is even'

We need to show $(\text{not } Q) \Rightarrow (\text{not } P)$ which is

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

How do we show this?

This was proposition (1.2) in the last section. We have already shown this result. Note that since we have proven the contrapositive, 'n is even $\Rightarrow n^2$ is even', therefore we have proven the given proposition, that is 'n^2 is odd $\Rightarrow n$ is odd'.

■

For the next example we need the following definition.

Definition (1.9). Two integers have the **same parity** means they are both even or both odd.

Example 36

Prove the following:

Proposition (1.10). If $m+n$ is even then m and n have the same parity.

Comment. Again the proposition suggests that we need a $P \Rightarrow Q$ proof. *Why?*

Because the given proposition is a 'if and then' statement. Let P be '$m+n$ is even' and Q be 'm and n have the same parity'. We need to prove

$$m+n \text{ is even } \Rightarrow m \text{ and } n \text{ have the same parity}$$

This is our typical $P \Rightarrow Q$ statement. However it is easier to prove the contrapositive of this, which is

$$(\text{not } Q) \Rightarrow (\text{not } P)$$

What is $(\text{not } Q)$ *equal to in this case?*

Since Q is 'm and n have the **same** parity' therefore

$$(\text{not } Q) \text{ is '}m \text{ and } n \text{ have } \textbf{different} \text{ parity'}$$

What is $(\text{not } P)$ *equal to in this case?*

Since P is '$m+n$ is **even**' therefore

$$(\text{not } P) \text{ is '}m+n \text{ is } \textbf{odd}\text{'}$$

We prove $(\text{not } Q) \Rightarrow (\text{not } P)$ which is

$$m \text{ and } n \text{ have different parity} \Rightarrow m+n \text{ is odd}$$

Proof. Assume m and n have different parity. Let m be odd and n be even. (It does **not** make any difference if it is the other way round). Since m is odd we can write m as

$$m = 2a+1 \quad \text{where } a \text{ is an integer}$$

Since n is even we can write n as

$$n = 2b \quad \text{where } b \text{ is an integer}$$

We need to prove $m+n$ is odd. Consider the addition:

$$m+n = \underbrace{2a+1}_{=m} + \underbrace{2b}_{=n}$$

$$= 2(a+b)+1 \qquad [\text{Factorizing}]$$

Hence $m+n = 2(\text{Integer})+1$ so by definition (1.3) we conclude $m+n$ is odd.

We have shown the contrapositive

$$m \text{ and } n \text{ have different parity} \Rightarrow m+n \text{ is odd}$$

which is equivalent to

$$m+n \text{ is even} \Rightarrow m \text{ and } n \text{ have the same parity}$$

This last statement is the given proposition.

■

E3 **Without Loss of Generality (WLOG)**

This term 'without loss of generality' is often used in mathematical proof. For example in the above proof of proposition (1.10) in the second sentence we can say 'without loss of generality assume m is odd and n is even'. In this example it is used to shorten the proof and make it digestible to the reader. Of course we could have covered both instances:

1. Assume m is odd and n is even.
2. Assume m is even and n is odd.

This would have made the proof longer and really gain nothing from this inclusion. Generally in a mathematical proof we might have to cover a number of choices but the proof is the same for each of these selections. In this case it is smarter to say "without loss of generality assume…"

Without loss of generality abbreviated to WLOG is a simplifying assumption.

Another example is say you want to prove a result concerning real numbers such as x and y. In the proof you might need to know which of the two numbers is larger, x or y. We say "Without loss of generality assume $x < y$ [x is less than y]" and then proceed with the remaining proof.

(1.3) n is odd $\Leftrightarrow$ $n = 2m+1$

The next example uses WLOG and is in the field of inequalities of real numbers. We will discuss inequalities of real numbers in a later chapter but will assume the following properties:

Let a, b and c be real numbers. Then

$$a > b \quad \Rightarrow \quad a + c > b + c \qquad (*)$$

$$c > 0, \quad a > b \quad \Rightarrow \quad ac > bc \qquad (**)$$

Note that (*) is valid for any real number c but (**) is valid for positive c **only**.

Example 37

Prove the following, for all real numbers x and y

$$(x+y)^2 \geq 4xy$$

Proof. First consider real numbers x and y where $x \neq y$. Without loss of generality (WLOG) assume $y > x$. Then

$$y - x > 0$$

Multiplying both sides by $y - x$ and using (**) with $c = y - x$ we have

$$(y-x)(y-x) > 0$$

$$y^2 - 2xy + x^2 > 0 \qquad \left[\text{Expanding } (y-x)(y-x) = y^2 - 2xy + x^2\right]$$

By adding $2xy$ to both sides and using (*) we have

$$y^2 + x^2 \underbrace{-2xy + 2xy}_{=0} > 0 + 2xy$$

$$y^2 + x^2 > 2xy$$

Adding another $2xy$ to both sides we have

$$y^2 + x^2 + 2xy > \underbrace{2xy + 2xy}_{=4xy}$$

$$(x+y)^2 > 4xy \qquad \left[\text{Because } (x+y)^2 = y^2 + x^2 + 2xy\right]$$

Initially we have assumed $x \neq y$ but what about the case when $x = y$?

If $x = y$ then on the Left Hand Side we have

$$(x+y)^2 = (x+x)^2 = (2x)^2 = 4x^2$$

On the Right Hand Side we have

$$4xy = 4xx = 4x^2$$

When $x = y$ we have equality

$$(x+y)^2 = 4xy$$

By combining the two parts ($x = y$ and $x \neq y$) we have the required result,

$$(x+y)^2 \geq 4xy$$

■

SUMMARY

The statement *'P* if and only if *Q'*, $P \Leftrightarrow Q$, statement is proved in two parts:

1. Prove $P \Rightarrow Q$ (if *P* then *Q*)
2. Prove $Q \Rightarrow P$ (if *Q* then *P*)

Sometimes it is easier to prove the contrapositve of $P \Rightarrow Q$ which is

$$(\text{not } Q) \Rightarrow (\text{not } P)$$

Since they are equivalent therefore when you prove $(\text{not } Q) \Rightarrow (\text{not } P)$ means you prove $P \Rightarrow Q$.

WLOG – 'Without loss of generality' is a simplifying assumption which is used in proof. In a proof you may have to cover a number of choices which involves the same proof for each selection. Better to say 'without loss of generality assume…'