SECTION 1.3 ➡ Proofs

By the end of this section you will be able to

- construct a proof by contrapositive
- understand what is meant by the term "without loss of generality"
- construct a proof by contradiction

I.3.1 If and only if Proof

What is meant by 'If and Only If'?

'If and only if' in mathematics is related to two propositions such as P and Q. We have P if and only if Q means P implies Q and Q implies P and is denoted by $P \Leftrightarrow Q$.

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.

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:

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

where a and b are real numbers. (You are asked to prove this in question 8 of Exercises **I.3**.)

Example 19

Prove that

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

How do we prove this?

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

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

and

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

We can first prove '$x = 2 \;\text{ or }\; x = 3 \;\Rightarrow\; x^2 - 5x + 6 = 0$'. 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.

$(\Rightarrow)$. 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 $x=3 \quad\Rightarrow\quad x^2-5x+6=0$.

$(\Leftarrow)$. The second part of the proof involves going the other way. *Conversely* 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 solve for x:

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

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

By combining the two parts we have proved that

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

■

We could have proved '$x^2-5x+6=0 \quad\Rightarrow\quad x=2$ or $x=3$' first and then proved '$x=2$ or $x=3 \quad\Rightarrow\quad x^2-5x+6=0$' 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 proof of Example 19 the word 'Conversely' was used and its purpose is to divide the proof into two parts. It means we have finished the first part and are moving on to the second part of the proof.

In the following example 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' or there is an integer x such that $ax=b$ - See Definition (I.5) on page 19.

Example 20

Prove the following:

Proposition (I.7). For $c \neq 0$,

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

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?*

We have the double implication sign, $\Leftrightarrow$, going both ways therefore we must prove both parts, that is

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

Proof.

How do we prove the first part '$ac \mid bc \Rightarrow a \mid b$'?

$(\Rightarrow)$. We have already proven this in Exercise I(b) Question 5(h).

$(\Leftarrow)$. We need to prove the second part, that is $a \mid b \quad \Rightarrow \quad ac \mid bc$. *How do we prove this?*

We assume $a \mid b$ and then deduce $ac \mid bc$. By applying Definition (I.5):

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

on the assumption $a \mid b$ we have an integer y such that $ay = b$. Multiplying both sides by c gives

$$ayc = bc$$
$$ac(y) = bc$$

We have $ac \times (\text{Integer}) = bc$. Again by Definition (I.5) we have deduced the required result, $ac \mid bc$, for the second part.

Hence, we have proved $ac \mid bc \quad \Leftrightarrow \quad a \mid b$ where $c \neq 0$.

■

I.3.2 Proof by Conrapositive

Let P and Q be propositions then the **contrapositive** of $P \Rightarrow Q$ is the proposition $(\neg Q) \Rightarrow (\neg P)$ that is (not Q) implies (not P). Consider the example

P : I have two exotic holidays per year

Q : I am rich

What is the contrapositive of $P \Rightarrow Q$, that is $(\neg Q) \Rightarrow (\neg P)$, for this example?

$$\text{If } \underbrace{\text{I am not rich}}_{\neg Q} \text{ then } \underbrace{\text{I do not have two exotic holidays per year}}_{\neg P}.$$

Example 21

Construct the truth table for $(\neg Q) \Rightarrow (\neg P)$. *What do you notice about your answer in relation to the proposition* $P \Rightarrow Q$ *?*

Solution

In the first two left hand columns we list all the possible combinations of P and Q. For the next two columns we write down the truth tables for $\neg Q$ (not Q) and $\neg P$ (not P) respectively. In the 5th column we find the truth values of $(\neg Q) \Rightarrow (\neg P)$:

P	Q	$\neg Q$	$\neg P$	$(\neg Q) \Rightarrow (\neg P)$	$P \Rightarrow Q$
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

Table 14

By comparing the last two right-hand columns of Table 14 we can say $(\neg Q) \Rightarrow (\neg P)$ and $P \Rightarrow Q$ are equivalent. That is

$$\big((\neg Q) \Rightarrow (\neg P)\big) \equiv (P \Rightarrow Q) \quad \text{[Equivalent]}.$$

This result, $\big((\neg Q) \Rightarrow (\neg P)\big) \equiv (P \Rightarrow Q)$, is important and is often used to prove $P \Rightarrow Q$. That is, if you prove $(\neg Q) \Rightarrow (\neg P)$ then you have proven $P \Rightarrow Q$ because they are equivalent.

Summarizing from the last section and the above example we have two critical results:

$$(Q \Rightarrow P) \not\equiv (P \Rightarrow Q) \quad \text{[Converse is Not Equivalent]}$$
$$\big((\neg Q) \Rightarrow (\neg P)\big) \equiv (P \Rightarrow Q) \quad \text{[Contrapositive is Equivalent]}$$

These two propositions maybe hard to believe because they tend to be against our intuition.

If you are asked to prove $P \Rightarrow Q$ then you can show $(\neg Q) \Rightarrow (\neg P)$ but *not* $Q \Rightarrow P$. 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 22

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 (I.3)

(I.3) n is odd $\Leftrightarrow$ $n = 2m + 1$

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:

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

We 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 try to deduce Q (n is odd) it leads us down 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'?

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

How do we show this?

This was Proposition (I.2) of Example 16 in the last section. We have already shown this result.

Note 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'. These are equivalent propositions.

■

I.3.3 Without Loss of Generality

Generally, in a mathematical proof we might have to cover several 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.

For example, 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 can say "Without loss of generality assume $x < y$ [x is less than y]" and then proceed with the remaining proof.

The next example uses WLOG and is in the field of inequalities of real numbers. We will examine inequalities more seriously at the end of this chapter.

Let a, b and c be real numbers. We assume the following properties of inequalities:

$$a > b \quad \Rightarrow \quad a - b > 0 \qquad (\dagger)$$

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

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

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

We will prove these in Section I.6 but for the time being assume them to be true.

Example 23

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 by (†) we have

$$y - x > 0\,.$$

Multiplying both sides by $y - x$ and using (**) with $c = y - x > 0$ 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

$$4xy = 4xx = 4x^2\,.$$

Thus when $x = y$ we have equality:

$$\left(x+y\right)^2 = 4xy\,.$$

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

$$\left(x+y\right)^2 \geq 4xy\,.$$

■

I.3.4 Procedure for Proof by Contradiction

'*A chess player may offer the sacrifice of a pawn or even a piece, but the mathematician offers the game.*' G.H. Hardy (1877-1947), who was one of the greatest mathematician of 20th Century England, on proof by contradiction.

A compound proposition which is always false is called a **contradiction**.

Example 24

Construct the truth table for $P \wedge \left(\neg P\right)$. *What do you notice about your result?*

Solution

The truth table can be established as follows (you showed this in question 9(a) of Exercises **I.1**:

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

Table 15

The right-hand column of Table 15 shows that $P \wedge \left(\neg P\right)$ is a contradiction. In words this means P and (not$P$) is always false.

Let P be the statement $x^2 - 1 = 0$. *What is* $\neg P$ *(not P) in this case?*

$$x^2 - 1 \neq 0\,.$$

Hence $P \wedge \left(\neg P\right)$ is given by

$$x^2 - 1 = 0 \quad \text{and} \quad x^2 - 1 \neq 0$$

must *always* be false because you *cannot* have both

$$x^2 - 1 = 0 \quad \left[\text{Equals zero}\right] \quad \text{and} \quad x^2 - 1 \neq 0 \quad \left[\text{Not equal to zero}\right].$$

We say '$x^2 - 1 = 0$ and $x^2 - 1 \neq 0$' is a contradiction.

Suppose we want to prove a proposition P then the procedure for proof by contradiction is as follows:

1. We assume the opposite that is $\left(\text{not } P\right)$ is true.
2. We follow our logical deductions in the proof and this will lead to a contradiction.

3. Since our assumption in part 1 of $(\text{not} \quad P)$ is true leads to a contradiction therefore $(\text{not} \quad P)$ is false.
4. Since $(\text{not} \quad P)$ is false therefore our given proposition P must be true.

This method is called **proof by contradiction**. The tradition name of this proof is "reductio ad absurdum" which means reduction to absurdity.

For example; prove that $\dfrac{x^2+2}{x} = x$ has *no* solution.

Proof. Suppose there is a solution $x = a$ which satisfies the given equation. Then

$$\frac{a^2+2}{a} = a \quad \Rightarrow \quad a^2+2 = a^2 \quad \Rightarrow \quad 2 = a^2 - a^2 = 0\,.$$

Clearly the last statement $2 = 0$ is absurd. Hence our supposition that there is a solution must be wrong, so the given equation has *no* solution.

The challenge in these proofs is stating the negation of the given proposition P that is writing down $(\text{not} \quad P)$ and deducing a contradiction. Before we construct proofs by contradiction, we investigate the negation of a proposition.

I.3.5 Negation of a Proposition

Consider the negation of the following propositions.

Let P be the proposition 'there are an infinitely many primes'.

What is $(\text{not} \quad P)$ *equal to?*

The proposition $(\text{not} \quad P)$ is

'there are a *finite* number of primes'.

Let R be the proposition 'if n^2 is even then n is even'.

What is $(\text{not} \quad R)$ *equal to?*

The proposition $(\text{not} \quad R)$ is more difficult to write down because we have a $P \Rightarrow Q$ proposition where

$$\text{if} \quad \underbrace{n^2 \ \text{ is even}}_{=P} \quad \text{then} \quad \underbrace{n \ \text{ is even}}_{=Q}\,.$$

Why is 'if n^2 is even then n is even' a $P \Rightarrow Q$ proposition?

Because it has an 'if and then' in the statement. Thus proposition R is $P \Rightarrow Q$.

Therefore $(\text{not} \quad R)$ *is* $\text{not}(P \Rightarrow Q)$ *but what is* $\text{not}(P \Rightarrow Q)$ *equal to?*

By constructing the truth table of this we can show that

$$\left[\text{not} \ \ (P \Rightarrow Q)\right] \equiv \left[P \wedge (\text{not} \quad Q)\right] \qquad [\text{Equivalent}].$$

You are asked to prove this result in question 1 of Exercises I.3.

'$P \wedge (\text{not } Q)$' is 'P and $(\text{not } Q)$' which means that $(\text{not } R)$ equals 'P and $(\text{not}\, Q)$'. Hence $(\text{not } R)$ is

$$\text{'}\underbrace{n^2 \text{ is even}}_{P} \quad \text{and} \quad \underbrace{n \text{ is odd}}_{\text{not } Q}\text{'}.$$

Consider another proposition Q given by 'it is *impossible* to find non - zero integers a, b and c such that

$$a^n + b^n = c^n \text{ where } n \geq 3\text{'}.$$

The negation of this, or $(\text{not } Q)$, is

'it is *possible* to find three positive integers a, b and c such that

$$a^n + b^n = c^n \text{ where } n \geq 3\text{'}.$$

This proposition Q is the famous Fermat's Last Theorem. Fermat was a French Lawyer and he did mathematics in his spare time. The reason why Fermat's last theorem is popular is because Fermat stated his theorem around 1630 and added that "I have discovered a proof, but the margin is too small to write the proof".

Figure 2 Pierre de Fermat Andrew Wiles

However, for over 350 years no one could find a proof for this theorem. Eventually in 1993 Andrew Wiles a British mathematician working in Princeton USA provided a proof at Cambridge. Initially his proof had a flaw but it was resolved in 1995. Fermat's last theorem states that the equation

$$a^n + b^n = c^n \text{ for } n \geq 3$$

has *no* non - zero integer solutions. *What does this mean?*

We know there are integer solutions for $n = 2$ because it crops up in Pythagoras's theorem (these numbers are called Pythagorean triples):

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad 8^2 + 15^2 = 17^2, \ldots$$

However, when the index $n \geq 3$ we *cannot* find non – zero integer solutions to the above equation. This means there are no positive or negative integers a, b and c such that

$$a^3 + b^3 = c^3, \quad a^4 + b^4 = c^4, \quad a^5 + b^5 = c^5, \ldots$$

There are some near misses such as $6^3 + 8^3 = 728$ but $9^3 = 729$.

I.3.6 Proof by Contradiction

In this subsection we look at examples of proof by contradiction. The proof is carried out by using the procedure outlined in subsection I.3.4.

An important tool we use to prove results is the Pigeonhole Principle given by:

(I.8) Pigeonhole Principle: If there are $n+1$ or more objects and only n boxes then some box will contain at least two objects.

Proof. (By contradiction).

Suppose each box contains at most one object. Then the largest number of objects is

$$\underbrace{1+1+1+\cdots+1}_{\text{There are } n \text{ ones}} = n.$$

This is a contradiction because the largest number of objects is n but we have $n+1$ or more objects.

■

It is worth learning the Pigeonhole Principle statement.

We need to define the term reciprocal for the next example.

Definition (I.9). Let x be a non-zero real number. The reciprocal of this real number, x, is a real number y which has the property

$$x \times y = xy = 1.$$

For example the reciprocal of 3 is $\frac{1}{3}$, reciprocal of -2 is $-\frac{1}{2}$, reciprocal of π is $\frac{1}{\pi}$ reciprocal of $-\frac{2}{3}$ is $-\frac{3}{2}$.

Example 25

Prove the following:

Proposition (I.10). Every non-zero real number has a *unique* reciprocal.

What does the word 'unique reciprocal' mean?

There is *only* one reciprocal.

We can use proof by contradiction to prove this proposition. *To use this approach, what do we need to do first?*

We need to state the negation of the proposition, which is:

There is a non-zero real number whose reciprocal is *not* unique. *What does this statement mean?*

There is a non-zero real number such that it has more than one reciprocal.

Proof.

Suppose there is a non-zero real number call it x whose reciprocal is *not* unique.

Consider it has two different reciprocals call them y and z.

Then y does *not* equal z, that is $y \neq z$. *Why not?*

Because if $y = z$ then x has the same (one) reciprocal and so that means it is unique and there is nothing left to prove.

Since y and z are the reciprocals of x therefore by Definition (I.9) we have

$$xy = 1 \quad \text{and} \quad xz = 1.$$

Because these, xy and xz, are both equal to 1 so we can equate them

$$xy = xz.$$

Since x is non-zero, we can divide through by x which gives

$$y = z.$$

But above we had $y \neq z$. We cannot have $y = z$ and $y \neq z$. Hence this contradicts our supposition on the first line of the proof, that there is a non-zero real number whose reciprocal is *not* unique. Thus, the given proposition must be true.

■

What exactly is the meaning of the negation of the original proposition in the above proof?

If it is *not* unique means, there must be more than one so we considered two reciprocals (of course we could have considered three or even more, but it just makes the proof untidy and unreadable).

Next, we applied logical mathematical deductions assuming two reciprocals in the above proof and this resulted in a contradiction. Since we had a contradiction this means that our supposition of two reciprocals must have been false. Hence the given proposition 'every non-zero real number has a unique reciprocal' must be true.

Proposition (I.10) is an important result in the mathematics of real numbers. The reciprocal is also called the **multiplicative inverse**. In general, if x is a non-zero real number then the *unique* reciprocal (or unique multiplicative inverse) of x is $\frac{1}{x}$.

In the next example we state a proposition which is called a **lemma**.

A lemma is a proposition or theorem used to prove another proposition or theorem.

Lemma is a stepping stone to prove a more important result.

Example 26

Prove the following:

Lemma (I.11). If n^2 is even then n is even.

Proof. See question 3(a) of Exercises I.3.

■

In the next example we prove that $\sqrt{2}$ is *not* a rational number. *What is a rational number?*

Definition (I.12). A rational (ratio) number is an integer or is written as a fraction of two integers, p and q, denoted by $\frac{p}{q}$ where $q \neq 0$.

For example; $\frac{2}{3}$, $-\frac{1}{3}$, $3 = \frac{3}{1}$, $-\frac{10\,000}{6}$ and $9 = \frac{18}{2}$ are all rational numbers.

We can write each rational number $\frac{p}{q}$ in its simplest form. For example

$$\frac{4}{6} = \frac{2}{3}, \quad \frac{2}{4} = \frac{1}{2}, \quad \frac{9}{6} = \frac{3}{2}, \quad \frac{15}{9} = \frac{5}{3}.$$

A rational number in its simplest form is when it is written with *no* factors in common apart from 1. *What does the term* ***factor*** *mean?*

A factor is a number that divides another (or the same) number. For example $2 \mid 4$ [2 divides 4] and we say 2 is a factor of 4. Clearly 1 is always a factor of every number. However, we want to prove $\sqrt{2}$ is *not* a rational number. *Can you think of where* $\sqrt{2}$ *appears?*

In a right-angled triangle with smaller sides of unit length as shown in Fig. 3:

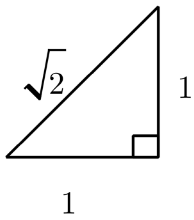

Figure 3

The longest length (hypotenuse) is found by applying Pythagoras theorem:

$$1^2 + 1^2 = 2 \Rightarrow \sqrt{1^2 + 1^2} = \sqrt{2}.$$

Example 27

Prove the following:

Theorem (I.13). $\sqrt{2}$ is *not* a rational number.

Proof. (By contradiction).

Suppose $\sqrt{2}$ is a rational number. By Definition (I.12) we can write $\sqrt{2}$ as

$$\frac{p}{q} = \sqrt{2}$$

where p and q $(\neq 0)$ are integers with *no* factors in common other than 1. We say $\frac{p}{q}$ is in its simplest form. If they do have factors in common, then cancel them down to its simplest form. Multiplying both sides of $\frac{p}{q} = \sqrt{2}$ by q gives

$$p = \sqrt{2}q$$

$$p^2 = 2q^2 \quad \text{[Squaring both sides]}$$

We have $p^2 = 2q^2$ is a multiple of 2 therefore it is even. By Lemma (I.11)

(I.11) n^2 is even $\Rightarrow$ n is even

we have

$$p^2 \text{ is even} \Rightarrow p \text{ is even.}$$

Since p is even, we can write this as

$$p = 2m \quad \text{where } m \text{ is an integer.}$$

Hence $p^2 = (2m)^2 = 4m^2$.

Substituting this, $p^2 = 4m^2$, into the above, $2q^2 = p^2$, gives

$$2q^2 = 4m^2$$

$$q^2 = 2m^2 \quad \text{[Dividing by 2]}$$

We have q^2 is a multiple of 2 therefore q^2 is even. Again, by Lemma (I.11) we have

$$q^2 \text{ is even} \Rightarrow q \text{ is even.}$$

Hence, we have *both* p and q are even. This means that both p and q have a common factor of 2. This is a contradiction. *Why?*

Because at the start of the proof we said that p and q have *no* factors in common (apart from 1) and now we have shown that p and q have a common factor of 2. Our supposition '$\sqrt{2}$ is a rational number' must be false. Hence $\sqrt{2}$ is *not* a rational number.

■

A number which is *not* a rational number is called an **irrational** number. We say $\sqrt{2}$ is an irrational number. $\sqrt{2}$ was the first known irrational number and again it was the Greeks who two thousand years ago produced the first proof of the irrationality of $\sqrt{2}$. Other examples of irrational numbers are

$$\sqrt{2}, \sqrt{3}, \sqrt{5}, \pi \text{ and } e.$$

In fact, square root of a non-square number is irrational therefore

$$\sqrt{6}, \sqrt{7}, \sqrt{8} \text{ and } \sqrt{10} \text{ are } \textit{all} \text{ irrational numbers.}$$

Example 28

Prove the following:

(I.14) Let n be a non - square real number. Then $\sqrt{n}$ is irrational.

Proof.

Suppose $\sqrt{n}$ is rational. Then

$$\sqrt{n} = \frac{p}{q} \text{ where } p \text{ and } q \neq 0 \text{ are integers.}$$

Squaring both sides gives

$$n = \frac{p^2}{q^2} = \left(\frac{p}{q}\right)^2.$$

Hence n is a square number which contradicts our assumption. By contradiction we have our result that $\sqrt{n}$ is irrational provided n is a non – square number.

■

We have the stronger statement:

If n is a non- square number and a and b are integers then

$$a + b\sqrt{n} \text{ is an irrational number.}$$

You are asked to prove this in question 17(ii) of Exercises I.3.

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).

WLOG – 'Without loss of generality' is a simplifying assumption which is used in a proof.

Lemma is a proposition which is used to prove another more important proposition.

The Pigeonhole Principle says:

If there are $n+1$ or more objects and only n boxes, then some box will contain at least two objects.