Introductory Chapter: Mathematical Logic, Proof and Sets

This chapter is a brief introduction to pure mathematics.

At first you will find this a challenging chapter and *not* the kind of mathematics you would have been familiar with. However, to understand this chapter you need to follow each step at a slower pace and become comfortable with the notation used. We will regularly be using the results of this chapter, so it is important that you understand the material thoroughly.

Some sections will seem abstract and lacking in applications, but the practical use of the theory lies in digital electronics, computer science and artificial intelligence.

The proof part of this chapter is particularly challenging because each proof uses different concepts and it is not a handle turning exercise.

SECTION I.1 ⟹ Propositional Logic

By the end of this section you will be able to

- write connectives in symbolic form
- construct truth tables for compound propositions
- show equivalence of propositions using truth tables

I.1.1 Propositions

What does the term proposition mean in mathematics?

It is a statement which has a value of true or false. *Which of the following are propositions?*

(a) Arsenal Football Club won the double in 2002.

(b) $5+3=7$

(c) $x+5=2$

(d) Liz Hurley looks beautiful.

(e) The world ended on 6th June 1984.

(a), (b) and (e) are propositions but (c) and (d) are *not* propositions. *Why not?*

(c) is not a proposition because it contains an unknown, x. Since we do not know the value of x therefore we cannot say whether $x+5=2$ is true or false. 'Liz Hurley looks beautiful' is *not* a proposition because beauty is subjective.

Note that a proposition can be false such as (b) $5+3=7$ and (e) The world ended on 6th June 1984.

We normally denote propositions by the letters P, Q, R, S, … .

Propositions P and Q can only be either true or false. We can write this in a table as:

P	Q
True (T)	True (T)
False (F)	False (F)

Table 1

This kind of table is called a *truth table*.

I.1.2 Negation

What does negation mean?

Generally, means the opposite of something. If P is a proposition then the negation of P is (not$P$) and it is denoted by $\neg P$.

Let P : I weigh more than 75kg. *What is* $\neg P$ *equal to?*

$\neg P$: I do *not* weigh more than 75kg.

Example 1

Write the negations of the following statements:

(1) $a < b$

(2) $2+2 \neq 5$

Solution

(1) $a \geq b$ because the opposite of $a < b$ is a is greater than or equal to b.

(2) $2+2=5$ because the opposite of does not equal $(\neq)$ is equal to $(=)$.

Note the answer to (1) is not $a > b$ but $a \geq b$ because you must cover *all* possibilities.

That is P and $\neg P$ (not P) must include *all* possibilities.

What is the truth value of $\neg P$ *if* P *is true?*

$\neg P$ is false.

What is the truth value of $\neg P$ *if* P *is false?*

$\neg P$ is true.

Putting all this together we have the following truth table of $\neg P$:

P	$\neg P$
T	F
F	T

Table 2

You need to remember the truth values of (not P) which has the opposite truth value to P. We use this throughout this chapter.

Example 2

Negate the following proposition:

P : There are integers a and b such that $\frac{a}{b} = \sqrt{2}$.

Solution

Negate means (not$P$) or in symbolic form $\neg P$.

$\neg P$: There are *no* integers a and b such that $\frac{a}{b} = \sqrt{2}$.

I.1.3 And

Two propositions can be combined by the word 'and' to form a compound proposition.

A **compound proposition** is two or more propositions assembled together.

Let P and Q be propositions then 'P and Q' is denoted by

$$P \wedge Q .$$

The compound proposition $P \wedge Q$ is called the **conjunction** of the original propositions.

Example 3

Let P: Grass is blue

Q: Pigs will fly

Form the sentence which describes $P \wedge Q$.

Solution

The notation $P \wedge Q$ means P and Q.

$P \wedge Q$: $\underbrace{\text{Grass is blue}}_{P}$ $\underbrace{\text{and}}_{\wedge}$ $\underbrace{\text{pigs will fly}}_{Q}$.

We can make the truth table for $P \wedge Q$ by first listing all the combination of truth values for P and Q in the first two columns. $P \wedge Q$ (P and Q) is *only* true if both P is true and Q is true otherwise it is false as shown in Table 3:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 3

I.1.4 Or

Two propositions can also be combined by the word 'or'. Let P and Q be propositions, then 'P or Q' is denoted by

$P \vee Q$.

A sentence of the form 'P or Q' is called a **disjunction**.

Next, we look at the truth table for $P \vee Q$.

Let P and Q be propositions. The compound proposition $P \vee Q$ (P or Q) is true if either one of P or Q is true. It is *only* false when *both* P is false and Q is false:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 4

Example 4

Let $P: 3 < 4$ and $Q: 4 < 3$. Write out the following:

(a) $P \vee Q$ (b) $\neg P$ (c) $(\neg P) \vee (\neg Q)$

Solution

(a) The notation $P \vee Q$ means P or Q:

$P \vee Q$: $3 < 4$ or $4 < 3$.

(b) $\neg P$: $3 \geq 4$ (The opposite of $3 < 4$ is $3 \geq 4$).

(c) $(\neg P) \vee (\neg Q)$: $3 \geq 4$ or $4 \geq 3$.

Example 5

Let P: A natural number is prime.

Q: A natural number is composite.

Write out the following:

(a) $P \vee Q$ (b) $(\neg P) \vee (\neg Q)$

Solution

a) The notation $P \vee Q$ means P or Q.

$P \vee Q$: A natural number is either prime or composite.

b) The notation $(\neg P) \vee (\neg Q)$ means $(\text{not } P)$ or $(\text{not } Q)$.

$(\neg P) \vee (\neg Q)$: A natural number is *not* prime nor composite.

A symbol which combines statements is called a connective. For example, $\wedge$, $\vee$ and $\neg$ are connectives.

From the three connectives $\neg$, $\wedge$ and $\vee$ we can construct more complex propositions. These *three* are the basis or fundamental connectives and you need to know their truth values. The remaining section relies on you knowing the truth values of these connectives.

Example 6

Construct the truth table for $\neg\big(P \vee Q\big)$.

Solution

$\neg\big(P \vee Q\big)$ means the opposite of $P \vee Q$. Hence if $P \vee Q$ is true then $\neg\big(P \vee Q\big)$ is false and vice versa. Therefore, the truth value of $\neg\big(P \vee Q\big)$ is the opposite of the last column of Table 4:

P	Q	$P \vee Q$	$\neg\big(P \vee Q\big)$
T	T	T	F
T	F	T	F
F	T	T	F
F	F	F	T

Table 5

Note that the first three columns are the same as Table 4. The last column gives the truth value of $\neg\big(P \vee Q\big)$.

Example 7

Construct the truth table for $\big(\neg P\big) \wedge \big(\neg Q\big)$.

Solution

Remember $\neg P$ will have truth value opposite to P and similarly $\neg Q$ will have truth value opposite to Q. *How do we find the truth values of* $\big(\neg P\big) \wedge \big(\neg Q\big)$ *?*

Remember the connectives $\wedge$ (and) only gives true if *both* $\neg P$ and $\neg Q$ are true else it is false. We obtain

P	Q	$\neg P$	$\neg Q$	$\big(\neg P\big) \wedge \big(\neg Q\big)$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Table 6

What do you notice about the truth values of $\neg\left(P \vee Q\right)$ *and* $\left(\neg P\right) \wedge \left(\neg Q\right)$*?*

Inspect the last columns of Table 5 and Table 6. Clearly $\neg\left(P \vee Q\right)$ and $\left(\neg P\right) \wedge \left(\neg Q\right)$ have the same truth values. We say the compound propositions $\neg\left(P \vee Q\right)$ and $\left(\neg P\right) \wedge \left(\neg Q\right)$ are **logically equivalent** or just equivalent and it is denoted by $\equiv$.

We write this equivalence as

$$\neg\left(P \vee Q\right) \equiv \left(\neg P\right) \wedge \left(\neg Q\right).$$

Propositions are (logically) equivalent if they have the same truth value for every combination.

Example 8

Show that $P \vee \left(Q \wedge R\right)$ and $\left(P \vee Q\right) \wedge \left(P \vee R\right)$ are logically equivalent.

Solution

We construct the truth table for these propositions.

For the three propositions P, Q and R we need 8 rows covering *all* the possible truth values as shown in the first three columns of Table 7.

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6	Col 7	Col 8
P	Q	R	$Q \wedge R$	$P \vee \left(Q \wedge R\right)$	$P \vee Q$	$P \vee R$	$\left(P \vee Q\right) \wedge \left(P \vee R\right)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	F	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Table 7

Since column 5 has the same truth values as column 8 we conclude that

$$P \vee \left(Q \wedge R\right) \equiv \left(P \vee Q\right) \wedge \left(P \vee R\right) \quad \text{[Equivalent]}.$$

I.1.5 Implication

Let P and Q be two Propositions. The compound statement

'P implies Q'

means 'if P then Q'. Implication is denoted by the symbol $\Rightarrow$. That is

$$P \Rightarrow Q\,,$$

which says P implies Q.

Bertrand Russell made the following statement regarding implication:

"Pure mathematics consists entirely of assertions to the effect that, if such and such a proposition is true of anything, then such and such another proposition is true of that thing."[1]

Example 9

Let P: I am elected.

Q: I will abolish the death penalty.

Form the sentence that describes

(i) $P \Rightarrow Q$ (ii) $Q \Rightarrow P$

Solution

(i) The notation $P \Rightarrow Q$ means 'if P then Q'.

If $\underbrace{\text{I am elected}}_{P}$ then $\underbrace{\text{I will abolish the death penalty}}_{Q}$.

(ii) The notation $Q \Rightarrow P$ means 'if Q then P'.

If $\underbrace{\text{I abolish the death penalty}}_{Q}$ then $\underbrace{\text{I will be elected}}_{P}$.

The truth table for P implies Q, $P \Rightarrow Q$, is given by:

	P	Q	$P \Rightarrow Q$
Row 1	T	T	T
Row 2	T	F	F
Row 3	F	T	T
Row 4	F	F	T

Table 8

You might think there is a misprint in Table 8, with regards to the bottom two rows, which is read as 'if P is false' then '$P \Rightarrow Q$' is true, independent of the truth value of Q. There is *no* misprint, this is correct. *How can we justify these statements?*

Consider Example 9 where P and Q were the following propositions:

P : I am elected.

Q : I will abolish the death penalty.

If P is false that is 'I am not elected' then I am under no obligation to abolish the death penalty. Implication is like a contract or a promise.

[1] https://www.goodreads.com/quotes/577891-pure-mathematics-consists-entirely-of-assertions-to-the-effect-that

The only situation when $P \Rightarrow Q$ is false (I have broken my promise) is

'If I am elected then I do *not* abolish the death penalty.'

This situation is represented in Row 2 of Table 8.

In general the implication $P \Rightarrow Q$ is *only* false if P is true and Q is false, otherwise $P \Rightarrow Q$ is true.

Another example is if you mow my lawn, then I will pay you £25. This is only false, if you mow my lawn and I *don't* pay you £25.

The implication connective is very important in mathematics because when proving results, the proof consists of a sequence of true statements connected by implication. A proof starts with a statement which we know is true and ends with a statement that we are required to prove. Each true statement follows from the previous true statement by implication.

Example 10

Let P: ABC is a right-angled triangle with sides a, b and c where $a \leq b < c$.

Q : The sides of the triangle ABC satisfy $c^2 = a^2 + b^2$.

Write out the following:

(i) $P \Rightarrow Q$ (ii) $Q \Rightarrow P$

Solution

(i) $P \Rightarrow Q$ means if P then Q.

$P \Rightarrow Q$: If ABC is a right-angled triangle with sides a, b and c where $a \leq b < c$ then it satisfies $c^2 = a^2 + b^2$.

(ii) $Q \Rightarrow P$: If the sides of the triangle ABC satisfy $c^2 = a^2 + b^2$ then ABC is a right-angled triangle.

Example 10 is Pythagoras's Theorem.

We can show that $P \Rightarrow Q$ is equivalent to $\left(\neg P\right) \vee Q$ that is (not$P$) or Q.

Example 11

Show that

$$\left(P \Rightarrow Q\right) \equiv \left(\left(\neg P\right) \vee Q\right) \qquad \text{[Equivalent]}$$

We have placed brackets on the left and right of the equivalent sign, $\equiv$, so that it becomes easier to visualize the propositions.

Solution

What does equivalence mean in this context?

It means $\left(\neg P\right) \vee Q$ and $P \Rightarrow Q$ have the same truth values for all possible combinations of truth values of P and Q.

In the first two left hand columns we list the combinations of truth values of P and Q in Table 9. The truth value of $P \Rightarrow Q$ is given in the last column of the previous Table 8. We can work out the truth value of $\left(\neg P\right) \vee Q$. *How?*

First determine the truth values of $\neg P$ (not$P$) and then $\left(\neg P\right) \vee Q$. The truth table is:

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

Table 9

The last two columns agree for all possible combinations of truth values therefore they are equivalent, that is

$$\left(P \Rightarrow Q\right) \equiv \left(\left(\neg P\right) \vee Q\right) \qquad \text{[Equivalent]}.$$

We can also state $P \Rightarrow Q$ as follows:

P is a sufficient condition for Q.

This means the condition P is enough for Q to be true.

Q is a necessary condition for P.

We sometimes use these terms instead of $P \Rightarrow Q$.

P implies Q

sufficient necessary

Summary

A proposition is a statement that is true or false.

Compound propositions can be made by the connectives ‘and’, ‘or’, ‘not’, denoted by $\wedge$, $\vee$, $\neg$ respectively.

Implication of two statements, P and Q, represents ‘if P then Q’ and is denoted by $P \Rightarrow Q$.

Exercises **I.1**

Brief solutions end of Exercises.

Complete solutions at www.oup.co.uk/companion/NumberTheory

1. Which of the following are propositions?

The ones that are propositions state whether they are true or false.

(a) $2+2=4$

(b) $2+2=3$

(c) All Swedish subjects have blonde hair.

(d) She looks beautiful.

(e) $x^2-1=0$

2. Negate the following propositions:

(i) Man can be pregnant.

(ii) Grass is green.

(iii) Lecturers annual salary is over £45 000.

(iv) There are integers a and b such that $\frac{a}{b}=\pi$.

(v) There are integers a and b such that $\frac{a}{b}=e$.

3. Write the following in words:

$$x^2-9=0 \Rightarrow x^2=9$$
$$\Rightarrow x=\sqrt{9}$$
$$\Rightarrow x=\pm 3$$

4. Let $P: x<3, \quad Q: x^2<9$. Write a sentence for

(i) $P \Rightarrow Q$ (ii) $Q \Rightarrow P$

Do you think either of them, (i) and (ii), is true?

5. Let P: ABC is an equilateral triangle.

Q: All the angles inside the triangle ABC are equal.

Write a sentence for

(i) $P \Rightarrow Q$ (ii) $Q \Rightarrow P$

Are both of these, (i) and (ii), true?

6. Let P : n is prime and Q : $2^n - 1$ is prime. Write the following in words:

(i) $P \Rightarrow Q$ (ii) $Q \Rightarrow P$

*Do you think either of them, (i) and (ii), is true?

7. Construct the truth table for $Q \vee P$. Compare your answer with the truth value for $P \vee Q$. What do you notice?

8. Construct the truth table for $Q \wedge P$. What do you notice about your result by comparing with $P \wedge Q$?

9. Construct the truth table for:

(a) $\left(\neg P\right) \wedge P$ (b) $\left(\neg P\right) \vee P$ (c) $\neg\left(\neg P\right)$

10. What are the following compound propositions equivalent to?

(a) $\neg\left(\neg\left(\neg P\right)\right)$ (b) $P \wedge P$ (c) $P \vee P$ (d) $\left(\neg P\right) \wedge \left(\neg P\right)$

11. Show that $\neg\left(P \wedge Q\right)$ and $\neg P \vee \neg Q$ are equivalent.

12. Show that $P \wedge \left(Q \vee R\right)$ and $\left(P \wedge Q\right) \vee \left(P \wedge R\right)$ are equivalent.

13. Devise an equivalence rule to the following compound proposition:

$$\neg\neg \ \ldots \ \left(\neg P\right)$$

[Hint: The rule will depend on the number of $\neg$]

Let P be the proposition 'the cup is full'. By using this devised rule what is $\neg\neg\neg\neg P$ equal to?

14. Construct the truth table for $\left(\neg P\right) \Rightarrow Q$.

15. Construct the truth table for

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

What do you notice about your results?

Brief Solutions to Exercises I.1

1. (a), (b) and (c). 4 and 5. Both Proposition are true. 6. Only (ii) is true.

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 $P \vee (\neg P)$.

Solution

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

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

Table 10

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

$$P \vee (\neg P) \equiv T.$$

Hence $P \vee (\neg P)$ 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 $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$.

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 $Q \Rightarrow P$:

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

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:

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

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) $\quad a \mid b \Leftrightarrow$ 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.

Exercises **I.2**

Complete solutions at www.oup.co.uk/companion/NumberTheory

Throughout this exercise lower case letters such as $a, b, c, \ldots, n, \ldots$ *represent integers.*

1. Show that the following are tautologies.

(a) $\big(\neg P\big) \vee P$

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

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

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

2. Prove the following propositions:

(a) If m and n are even then their sum $n + m$ is even.

(b) If m and n are even then their subtraction $n - m$ is even.

(c) If m and n are odd then their subtraction $n - m$ is even.

(d) If n is an odd number then n^2 is also odd.

(e) If m is even and n is odd then their sum $m + n$ is odd.

(f) If m is odd and n is odd then their product $n \times m = nm$ is odd.

(g) If n is any integer and m is even then their product $n \times m = nm$ is even.

3. Prove the following propositions:

(i) n is odd $\Rightarrow$ $n+1$ is even

(ii) *The product of two consecutive integers is even.

[Hint: Use Proposition (I.4)].

4. Prove that if n is odd then $n^3 - 1$ is even.

[Hint: Use the propositions proved in Question 2].

5. Prove the following propositions:

(a) $a \mid 0$ (b) $a \mid a$ (c) $1 \mid a$ (d) $a \mid a^2$

(e) $a \mid a^n$ where $n \geq 1$ is an integer.

(f) $a \mid b$ and $a \mid c$ $\Rightarrow$ $a \mid \big(b + c\big)$

(g) $a \mid b$ and $a \mid c$ $\Rightarrow$ $a^2 \mid bc$

(h) $ac \mid bc$ $\Rightarrow$ $a \mid b$ where $c \neq 0$.

(i) $a \mid b$ and $c \mid d \Rightarrow ac \mid bd$

The remaining three questions are more difficult.

6. Prove the following proposition:

If n is odd then

(a) $8 \mid \left(n^2 - 1\right)$ (b) $32 \mid \left(n^2 + 3\right)\left(n^2 + 7\right)$

7. Show that if the last digit of an integer n is even then n is even.

[Hint: Write n as

$$n = a_m a_{m-1} a_{m-2} \ldots a_2 a_1 a_0 \quad \left(m > 1\right)$$

where a_m, a_{m-1}, a_{m-2},..., a_2, a_1 and a_0 are the digits of n. Note that a_0 is the last digit. Hence n can be expressed as:

$$n = \left(a_m \times 10^m\right) + \left(a_{m-1} \times 10^{m-1}\right) + \left(a_{m-2} \times 10^{m-2}\right) + \ldots + \left(a_2 \times 10^2\right) + \left(a_1 \times 10^1\right) + a_0]$$

8. Show that if the last digit of an integer n is odd then n is odd.

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:

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

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

Example 19

Prove that

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

How do we prove this?

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

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

and

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

We can first prove '$x = 2$ or $x = 3 \quad \Rightarrow \quad x^2 - 5x + 6 = 0$'. 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:

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

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?

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

Example 21

Construct the truth table for $\left(\neg Q\right) \Rightarrow \left(\neg P\right)$. *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 $\left(\neg Q\right) \Rightarrow \left(\neg P\right)$:

P	Q	$\neg Q$	$\neg P$	$\left(\neg Q\right) \Rightarrow \left(\neg P\right)$	$P \Rightarrow Q$
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 $\left(\neg Q\right) \Rightarrow \left(\neg P\right)$ and $P \Rightarrow Q$ are equivalent. That is

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

This result, $\left(\left(\neg Q\right) \Rightarrow \left(\neg P\right)\right) \equiv \left(P \Rightarrow Q\right)$, is important and is often used to prove $P \Rightarrow Q$. That is, if you prove $\left(\neg Q\right) \Rightarrow \left(\neg P\right)$ 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:

$$\left(Q \Rightarrow P\right) \not\equiv \left(P \Rightarrow Q\right) \quad \text{[Converse is Not Equivalent]}$$

$$\left(\left(\neg Q\right) \Rightarrow \left(\neg P\right)\right) \equiv \left(P \Rightarrow Q\right) \quad \text{[Contrapositive is Equivalent]}$$

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 $\left(\neg Q\right) \Rightarrow \left(\neg P\right)$ but *not* $Q \Rightarrow P$.

Sometimes it is easier to prove $\left(\text{not } \ Q\right) \Rightarrow \left(\text{not } \ P\right)$ 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) $\quad n \text{ is odd} \Leftrightarrow n = 2m+1$

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:

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

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

$$\left(y - x\right)\left(y - x\right) > 0$$

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

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

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

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

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

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

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 '$x^2 - 1 = 0 \quad$ and $\quad x^2 - 1 \neq 0$' 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 $\left(\text{not}\ \ P\right)$ is true leads to a contradiction therefore $\left(\text{not}\ \ P\right)$ is false.
4. Since $\left(\text{not}\ \ P\right)$ 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 $\left(\text{not}\ \ P\right)$ 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 $\left(\text{not}\ \ P\right)$ *equal to?*

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

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

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

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

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

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

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

By constructing the truth table of this we can show that

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

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:

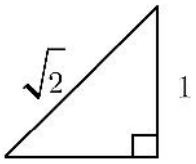


Figure 3 1

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

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

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

(I.11) $\quad n^2$ 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 $p^2=\left(2m\right)^2=4m^2$.

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

$$2q^2=4m^2$$
$$q^2=2m^2 \qquad \left[\text{Dividing by 2}\right]$$

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.

Exercises **I.3**

Brief solutions end of Exercises.

Complete solutions at www.oup.co.uk/companion/NumberTheory

1. By constructing the truth table show that

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

2. Prove the following results:

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

(b) $x^2 - 10x + 21 = 0 \quad \Leftrightarrow \quad x = 3 \text{ or } x = 7$

(c) $x^2 - 1 = 0 \quad \Leftrightarrow \quad x = 1 \text{ or } x = -1$

(d) $x^2 - \left(a + b\right)x + ab = 0 \quad \Leftrightarrow \quad x = a \text{ or } x = b$

(e) $x^2 = y^2 \quad \Leftrightarrow \quad x = y \text{ or } x = -y$

3. Prove the following propositions:

(a) n is even $\Leftrightarrow$ n^2 is even.

(b) mn is odd $\Leftrightarrow$ both m and n are odd.

(c) $m + n$ is odd $\Leftrightarrow$ only m or only n is odd.

(d) mn is even $\Leftrightarrow$ at least one of m or n is even.

4. Let P and Q represent the following mathematical propositions. In each case decide whether $P \Rightarrow Q$ or $Q \Rightarrow P$ or $P \Leftrightarrow Q$. You do *not* have to prove any of these statements:

(a) $P: \ a^2 > 0, \quad Q: \ a > 0$

(b) $P: \ a \neq 0, \quad Q: \ a^2 > 0$

(c) $P: \ x > 3, \quad Q: \ x > 4$

(d) $P: x = 2 \text{ or } x = -1, \quad Q: x^2 - x - 2 = 0$

(e) $P: ax^2 + bx + c = 0$ has two real roots, $\quad Q: \ b^2 - 4ac \geq 0$

(f) $P: \ a \mid \left(b + c\right), \quad Q: \ a \mid b \text{ and } a \mid c$

(g) $P: \ ac \mid bc, \quad Q: \ a \mid b$ where $c \neq 0$.

(h) $P: \ e^x = 1, \quad Q: \ x = 0$

(i) $P:\ \ln(x)=0, \quad Q:\ x=1$

(j) $P:\ 0<a<b, \quad Q:\ a^n<b^n$ where n is a positive integer.

(k) $P:\ 0<x<y, \quad Q:\ 0<\dfrac{1}{y}<\dfrac{1}{x}$

5. Consider the following four cards:

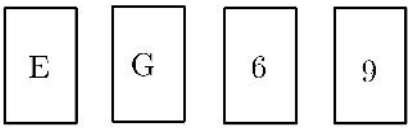


Figure 5

Each card has a letter on one side and a number on the other. You are told that if a card has a vowel on one side then it has an even number on the other. Which two cards should you turn over to test this statement?

6. In a class there are eight students. Prove that at least two of the students were born on the same day of the week.

In each case prove the following statements by applying contradiction. In some cases it may be easier to do a direct proof but this is an exercise in proof by contradiction.

7. Prove the following proposition:

For every real number, x, there is a unique real number y such that

$$x+y=0$$

[y is called the **additive inverse** of x].

8. Let x and y be real numbers. Prove that

$$xy=0 \quad \Rightarrow \quad x=0 \quad \text{or} \quad y=0$$

In the remaining questions lower case letters represents an integer.

9. Prove that n^2 is odd $\Rightarrow$ n is odd.

[We have proved this result by contrapositive in Example 22. This time prove the result by contradiction and compare the two proofs].

10. Prove that n^3 is odd $\Rightarrow$ n is odd.

11. Prove that n^3 is even $\Rightarrow$ n is even.

12. Prove that ab is odd $\Rightarrow$ both a is odd and b is odd.

13. Prove that ab is even $\Rightarrow$ a is even or b is even.

14. Prove that $\sqrt{6}$ is irrational.

15. Prove that $\sqrt[3]{2}$ is irrational.

16. Prove that there are *no* positive integer solutions such that

$$a^2 - b^2 = 1\,.$$

17. (i) Prove that the sum of a rational and irrational number is irrational.

(ii) Prove that $a + b\sqrt{n}$ is irrational if n is a non- square number and a and $b \neq 0$ are integers.

18. Consider the triangle shown in Fig 6. Show that if $\angle B = \angle C$ then $AB = AC$.

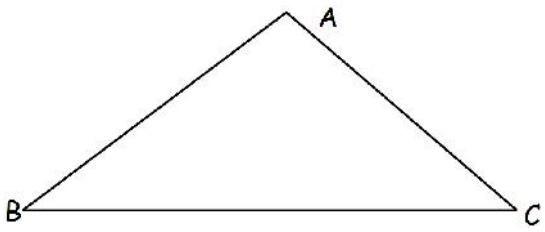


Figure 6

Brief Solutions to Exercises I.3

4. (a) $Q \Rightarrow P$ (b) $P \Leftrightarrow Q$ (c) $Q \Rightarrow P$
(d) $P \Leftrightarrow Q$ (e) $P \Leftrightarrow Q$ (f) $Q \Rightarrow P$
(g) $P \Leftrightarrow Q$ (h) $P \Leftrightarrow Q$ (i) $P \Leftrightarrow Q$
(j) $P \Leftrightarrow Q$ (k) $P \Leftrightarrow Q$

5. Cards E and 9.

SECTION 1.4 ⟹ Principle of Mathematics Induction

By the end of this section you will be able to

- understand the procedure for proof by induction
- construct proofs by induction

In this section we examine propositions concerning positive integers. The positive integers 1, 2, 3, 4, ,… are called **natural numbers** or **counting numbers**. In this section, lower case letters represent natural numbers.

I.4.1 Principle of Mathematics Induction

Mathematical induction is a powerful tool used to prove propositions concerning natural numbers.

Principle of Mathematical Induction (I.15)

For each natural number n, let $P(n)$ be a proposition about n. If $P(n)$ satisfies:

1) $P(1)$ is true,

2) for an arbitrary k, $P(k)$ is true implies $P(k+1)$ is true.

Then for *all* natural numbers, n , we have $P(n)$ is true.

Parts 1) and 2) suggest that

$$P(1) \text{ implies } P(2),\ P(2) \text{ implies } P(3),\ \cdots,\ P(k) \text{ implies } P(k+1),\ldots$$

This is called the domino effect. Once one of the dominos topples it causes the rest to topple as well. You use the k th domino to knock down the $(k+1)$th domino.

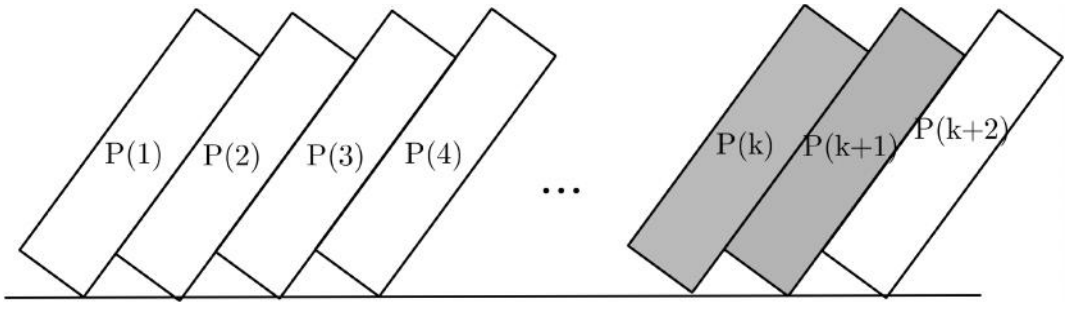


Figure 7 Domino Effect

Another analogy is climbing an infinite rung ladder. Mathematical induction says if you can climb onto the first step of the ladder, and from any (k th) step you can climb to the next ($k+1$)th step, then you can climb to the top of the ladder, although this ladder has an infinite number of rungs.

The process is that we show $P(1)$ is true and by assuming $P(k)$ is true we prove $P(k+1)$ is true. If *both* $P(1)$ is true and $P(k)$ implies $P(k+1)$ then proposition $P(n)$ is true for all natural numbers n.

We can apply this principle of mathematical induction to prove results about natural numbers.

Example 29

For every natural number n prove the proposition $P(n)$ given by

$$1+2+3+4+\ldots+n=\frac{1}{2}n(n+1).$$

What does this proposition mean?

It means that if we add the first n natural numbers then the answer will be $\frac{1}{2}n(n+1)$. For example, if we add the first two numbers we have

$$1+2=\frac{1}{2}(2)(2+1)=3 \qquad \text{[Substituting } n=2 \text{ into the above.]}$$

We need to show this result for all the natural numbers n. *How?*

We use mathematical induction because the proposition concerns the natural numbers.

Proof.

First, we check the proposition for $n=1$:

$$1=\frac{1}{2}(1)(1+1) \qquad \checkmark$$

Hence the proposition is true for $n=1$. Next, we *assume* the given proposition is true for $n=k$, that is $P(k)$. *How do we write this* $P(k)$*?*

By substituting $n=k$ into the given proposition

$$1+2+3+4+\ldots+n=\frac{1}{2}n(n+1)$$

which yields

$$1+2+3+4+\ldots+k=\frac{1}{2}(k)(k+1) \qquad (*)$$

We have labelled this result by (*) because we are going to prove the proposition for $n=k+1$ by using (*). *How do we write the proposition* $P(k+1)$*?*

This is the addition of the first $k+1$ natural numbers, so substituting $n=k+1$ into the given proposition gives:

$$1+2+3+4+\ldots+k+(k+1)=\frac{1}{2}(k+1)\underbrace{(k+1+1)}_{=k+2}=\frac{1}{2}(k+1)(k+2) \qquad (**)$$

This means that *we have to prove* the sum of the first $(k+1)$ natural numbers is equal to $\frac{1}{2}(k+1)(k+2)$. It is critical that you realise we need to prove (**), we have *only* stated $P(k+1)$ *not* proven it yet. The challenge is to show that the left-hand side is equal to the right-hand side of (**). *How?*

By simplifying the left – hand side using (*);

$$1+2+3+\ldots+k+(k+1)=\underbrace{1+2+3+4+\ldots+k}_{=\frac{1}{2}k(k+1)\text{ by (*)}}+(k+1)$$

$$=\frac{1}{2}k(k+1)+(k+1) \qquad [\text{Simplifying}]$$

$$=\frac{1}{2}(k+1)k+\frac{1}{2}(k+1)2 \qquad \left[\text{Rewriting } (k+1)=\frac{1}{2}(k+1)2\right]$$

$$=\frac{1}{2}(k+1)(k+2) \qquad [\text{Factorizing}]$$

The last line is the right-hand side of (**). Hence our result holds by the Principle of Mathematical Induction (I.15) because we have shown (**).

■

Notice how we assume $P(k)$ to be true and then use it to prove $P(k+1)$. The proposition $P(k)$ in the above was (*) and we used this in the derivation of $P(k+1)$. We knock down the first domino $P(1)$ and then we use the k th domino $P(k)$ to knock down the $(k+1)$th domino $P(k+1)$. By mathematical induction we conclude that adding the first n positive integers gives us:

$$1+2+3+4+\ldots+n=\frac{1}{2}n(n+1).$$

We can write the left – hand side $1+2+3+4+\ldots+n$ in compact mathematical notation. In mathematics we use the Greek letter $\sum$, pronounced sigma, for writing this:

$$1+2+3+4+\ldots+n=\sum_{m=1}^{n}m\,.$$

This $\sum_{m=1}^{n}m$ means 'the sum of all positive whole numbers between 1 and n'.

We can write the sum of odd numbers as $1+3+5+\ldots+(2n-1)=\sum_{m=1}^{n}(2m-1)$.

Example 30

For every natural number n prove the proposition $P(n)$ given by

$$1+3+5+7+\ldots+(2n-1)=\sum_{m=1}^{n}(2m-1)=n^2.$$

This proposition says that if we add the first n odd counting numbers then the answer will be the square of n. For example, if we add the first two odd counting numbers, we have

$1+3=2^2=4$ [Substituting $n=2$ into the given proposition.]

Similarly, adding the first five odd counting numbers gives

$\underbrace{1+3+5+7+9}_{5\text{ Terms}}=5^2$ [Adding the first five odd numbers, that is $n=5$.]

and so on.

Proof.

First, we check the proposition for $n=1$:

$$1=1^2 \quad \checkmark$$

The proposition is true for $P(1)$. Next, we *assume* the given proposition is true for $n=k$ that is $P(k)$:

$$\underbrace{1+3+5+7+\ldots+(2k-1)}_{\text{first } k \text{ odd counting numbers}}=k^2 \qquad (\dagger)$$

We have labelled $P(k)$ by $(\dagger)$ because we are going to prove the proposition for $n=k+1$ by using $(\dagger)$. *How do we write the proposition* $P(k+1)$*?*

By adding the first $k+1$ odd counting numbers (substituting $n=k+1$):

$$\underbrace{1+3+5+7+\ldots+(2k-1)}_{\text{First } k \text{ terms}}+\underbrace{(2(k+1)-1)}_{(k+1)\text{th term}}=(k+1)^2 \qquad (\dagger\dagger)$$

We need to prove this, $(\dagger\dagger)$, result. *How?*

We can simplify the sum from 1 to $(2k-1)$ by using $(\dagger)$, we have

$$\underbrace{1+3+5+\ldots+(2k-1)}_{\text{First } k \text{ odd terms}}+(2(k+1)-1)=\underbrace{1+3+5+7+\ldots+(2k-1)}_{=k^2 \text{ by } (\dagger)}+(2k+2-1)$$

$$=k^2+2k+1 \quad [\text{Simplifying}]$$

$$=(k+1)^2 \quad [\text{Factorizing}]$$

The last line is identical to the right-hand side of $(\dagger\dagger)$. By the Principle of Mathematical Induction, we have the sum of first n odd counting numbers is n^2.

■

In the above example, we first showed that the given result was true for $P(1)$:

$1=1^2$ $[n=1]$

Secondly, we assumed it is true for $P(k)$:

$$1+3+5+7+\ldots+(2k-1)=k^2 \qquad [n=k]$$

and finally, we used this assumption to produce the result for $P(k+1)$:

$$1+3+5+7+\ldots+(2k-1)+(2(k+1)-1)=(k+1)^2 \qquad [n=k+1]$$

I.4.2 Divisibility Example

We can apply mathematical induction to divisibility examples.

Remember we can write a divides b by the following notation $a \mid b$ where the vertical line represents division. Recall a divides b means that there is an integer m such that $am=b$ or b is a multiple of a. In mathematical notation we write

$$a \mid b \quad \Leftrightarrow \quad \text{there is an integer } m \text{ such that } am=b.$$

This was Definition (I.5) on page 19.

Example 31

For every natural number n prove the proposition $P(n)$ given by

$$3 \mid (2^{2n-1}+1).$$

What does $3 \mid (2^{2n-1}+1)$ *mean?*

$2^{2n-1}+1$ is divisible by 3 exactly

or there is an integer m such that

$$2^{2n-1}+1=3m.$$

To put it another way, $2^{2n-1}+1$ is a multiple of 3 for every natural number n.

Proof.

How do we prove $3 \mid (2^{2n-1}+1)$ *?*

We apply mathematical induction. *Why?*

Because the given proposition $P(n)$ holds for every natural number n.

First we check the first domino $P(1)$ is knocked over, that is substituting $n=1$ into $2^{2n-1}+1$:

$$2^{2-1}+1=2^1+1=3 \qquad /$$

Clearly 3 divides 3 and this is denoted by $3 \mid (2^{2-1}+1)$. Hence the proposition is true for $P(1)$. Next we assume the given proposition is true for $n=k$ that is 3 divides $2^{2k-1}+1$ or in notation form $3 \mid (2^{2k-1}+1)$. This means there is an integer q such that

$$3q = 2^{2k-1} + 1 \qquad (\$)$$

The challenge is to prove the result for $n = k+1$ by using ($). *How do we write down* $P(k+1)$ *?*

By substituting $n = k+1$ into the given proposition $3 \mid (2^{2n-1}+1)$:

$$3 \mid (2^{2(k+1)-1}+1).$$

That is, we need to prove

$$3 \text{ divides } 2^{2(k+1)-1}+1.$$

Let's examine the right - hand term, $2^{2(k+1)-1}+1$:

$$\begin{aligned}
2^{2(k+1)-1}+1 &= 2^{2k-1+2}+1 && [\text{Rewriting the index of 2}] \\
&= 2^{2k-1}2^2+1 && [\text{Applying the rules of indices } a^{m+n} = a^m a^n] \\
&= (4)2^{2k-1}+1 && [\text{Rewriting } 2^2 = 4] \\
&= (3+1)2^{2k-1}+1 && [\text{Rewriting } 4 = 3+1] \\
&= (3)2^{2k-1}+2^{2k-1}+1 && [\text{Expanding } (3+1)2^{2k-1}]
\end{aligned}$$

By ($) we know the last two terms on the right-hand side, $2^{2k-1}+1$, are equal to $3q$. Therefore, we obtain

$$\begin{aligned}
2^{2(k+1)-1}+1 &= (3)2^{2k-1} + \underbrace{2^{2k-1}+1}_{=3q \text{ by } (\$)} \\
&= (3)2^{2k-1} + 3q \\
&= 3(2^{2k-1}+q) && [\text{Taking out a common factor of 3}]
\end{aligned}$$

Thus the left - hand term $2^{2(k+1)-1}+1 = 3(\text{Integer})$ which means it is a multiple of 3 or 3 divides $2^{2(k+1)-1}+1$. We have proven $P(k) \Rightarrow P(k+1)$, therefore our result follows by induction.

■

I.4.3 Factorization Example

We can apply the principle of mathematical induction to prove general results concerning natural numbers. For example, we can use induction to prove the binomial theorem for positive integers (natural numbers). There is a great deal of algebraic manipulation in proving the binomial theorem, but the procedure of mathematical induction is the same. You are asked to show the binomial theorem in question 18 of Exercise I.4.

Let's first prove a result regarding factorizing of $a^n - b^n$ where a and b are real numbers and n is a natural number. This is a particularly useful result because it can

be employed to factorize expressions which look like $a^n - b^n$. The difficulty is trying to prove the result for $n = k+1$ and we use the 'trick' of writing 0 as $x - x$ or in our Example 32 below as $-a^k b + a^k b\left(= 0\right)$.

Up to now we have been proving results by mathematical induction for all natural numbers 1, 2, 3, 4, …, n, …

Clearly some results may *not* be valid for the first few natural numbers. That is the starting point may *not* be 1 but some other natural number such as n_0 say. In the next example the result is valid for 2, 3, 4, 5,…, n, … so the starting point is $n = 2$ and *not* $n = 1$. In general, the process of mathematical induction is the same apart from the starting point. If the starting point is n_0 then the process of mathematical induction is:

1. We check the result for $n = n_0$ (starting point). Check $P\left(n_0\right)$.
2. Assume it is true for $n = k$. Assume $P\left(k\right)$.
3. Prove $P\left(k\right) \Rightarrow P\left(k+1\right)$.

We use this to show the following identity:

$$a^n - b^n = \left(a-b\right)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}\right)$$

What does the term identity mean?

An **identity** is an algebraic expression which is valid for all values of the unknowns. For example, the following are identities:

$$\left(a+b\right)^2 = a^2 + 2ab + b^2 \text{ is true for all values of } a \text{ and } b.$$
$$a^2 - b^2 = \left(a-b\right)\left(a+b\right) \text{ is true for all values of } a \text{ and } b.$$
$$\sin^2\left(\theta\right) + \cos^2\left(\theta\right) = 1 \text{ is true for all values of } \theta.$$

However $2x + 1 = 0$ is *not* an identity because it is only true when $x = -1/2$.

Example 32

Let a and b be real numbers then for the natural numbers $n \geq 2$ we have the proposition $P\left(n\right)$ given by

(I.16) $$a^n - b^n = \left(a-b\right)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}\right)$$

Prove $P\left(n\right)$.

What does this proposition mean?

An expression of the form $a^n - b^n$ can be factorized into

$$a^n - b^n = \left(a-b\right)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}\right)$$

and of course, we can use this to solve equations of the type $a^n - b^n = 0$. *In any case how do we prove this result?*

Since it is a result concerning natural numbers n therefore, we can use induction.

Proof.

We first show this result for $n = 2$ (Our starting point is $n = 2$). *How?*

By substituting $n = 2$ into the given proposition:

$$a^2 - b^2 = \left(a - b\right)\left(a + b\right)$$

Of course, this is a fundamental identity of algebra, do you remember what it is called?

Difference of two squares. Thus $P\left(2\right)$ is true.

Assume the proposition is true for $n = k$ that is $P\left(k\right)$:

$$a^k - b^k = \left(a - b\right)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}\right) \qquad (*)$$

The difficulty in the process of induction is to prove the result for $n = k + 1$ by employing (*). *What do we need to prove?*

Required to prove $P\left(k+1\right)$, that is:

$$\begin{aligned} a^{k+1} - b^{k+1} &= \left(a - b\right)\left(a^{k+1-1} + a^{k+1-2}b + a^{k+1-3}b^2 + \ldots + ab^{k+1-2} + b^{k+1-1}\right) \\ &= \left(a - b\right)\left(a^k + a^{k-1}b + a^{k-2}b^2 + \ldots + ab^{k-1} + b^k\right) \qquad (**) \end{aligned}$$

We need to show the left-hand side is equal to the right-hand side of (**). Let's consider the left-hand side on its own:

$$\begin{aligned} a^{k+1} - b^{k+1} &= a^{k+1} - a^k b + a^k b - b^{k+1} && \left[\begin{array}{l}\text{Using the above stated trick}\\ \text{of writing } 0 = -a^k b + a^k b\end{array}\right] \\ &= a^k a - a^k b + a^k b - b^k b && \left[\text{Using the rules of indices } a^{m+n} = a^m a^n\right] \\ &= a^k\left(a - b\right) + b\left(a^k - b^k\right) && \left[\text{Factorizing out common terms}\right] \\ &= a^k\left(a - b\right) + b\underbrace{\left(a - b\right)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}\right)}_{\text{by } (*)} \\ &= \left(a - b\right)\left(a^k + b\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}\right)\right) && \left[\text{Factorizing out } \left(a - b\right)\right] \\ &= \left(a - b\right)\left(a^k + a^{k-1}b + a^{k-2}b^2 + a^{k-3}b^3 + \ldots + ab^{k-1} + b^k\right) && \left[\begin{array}{l}\text{Multiplying by } b\\ \text{in the second bracket}\end{array}\right] \end{aligned}$$

Since the last line is the right-hand side of (**) we have shown (**). Hence, we have our factorized result, $a^n - b^n = \left(a - b\right)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}\right)$.

■

Example 32 was a challenging problem but the procedure for mathematical induction is the same apart from the starting point which was $n = 2$.

In the next example we prove a proposition which is a **corollary**.

A corollary is a proposition which follows from one already proved. Normally it is a special case of the already proven proposition.

Example 33

Prove the following:

Corollary (I.17) $a^{rs}-1=\left(a^{r}-1\right)\left(a^{r(s-1)}+a^{r(s-2)}+\cdots+a^{r}+1\right)$

where r and s are integers.

Note that this corollary says that $a^{rs}-1$ factorizes into

$$\left(a^{r}-1\right)\left(a^{r(s-1)}+a^{r(s-2)}+\cdots+a^{r}+1\right)$$

Proof.

Using the rules of indices to rewrite $a^{rs}=\left(a^{r}\right)^{s}$ and the previous proposition:

(I.16) $$a^{n}-b^{n}=\left(a-b\right)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^{2}+\ldots+ab^{n-2}+b^{n-1}\right)$$

with $a=a^{r}$, $b=1$ and $n=s$ gives

$$\begin{aligned}\left(a^{r}\right)^{s}-1^{s}&=\left(a^{r}-1\right)\left(\left(a^{r}\right)^{s-1}+\left(a^{r}\right)^{s-2}1+\left(a^{r}\right)^{s-3}1^{2}+\ldots a^{r}1^{s-2}+1^{s-1}\right)\\&=\left(a^{r}-1\right)\left[a^{r(s-1)}+a^{r(s-2)}+a^{r(s-3)}+\cdots+a^{r}+1\right]\end{aligned}$$

Therefore $a^{rs}-1=\left(a^{r}-1\right)\left(a^{r(s-1)}+a^{r(s-2)}+\cdots+a^{r}+1\right)$. This completes our proof.

■

Note that this corollary is the special case with a being replaced by a^{r}, b being replaced by 1 and n being replaced by s in the previous general proposition (I.16). Also, we did not employ mathematical induction to prove this Corollary (I.17).

Summary

We use mathematical induction to prove propositions involving natural numbers.

The principle of mathematical induction to prove a proposition $P\left(n\right)$ involves:

1. Showing the result for $n=n_{0}$, that is $P\left(n_{0}\right)$. This is the base case.
2. Assuming the result is true for $n=k$ where k is an arbitrary positive integer, that is assuming $P\left(k\right)$ is true.
3. Prove the result for $n=k+1$, that is prove $P\left(k+1\right)$.

Exercises **I.4**

Complete solutions at www.oup.co.uk/companion/NumberTheory

1. Show that for all-natural numbers, n:

$$2+4+6+\ldots+2n=\sum_{m=1}^{n}2m=n\left(n+1\right).$$

2. Prove that for all-natural numbers, n:

$$2+5+8+\ldots+\left(3n-1\right)=\sum_{m=1}^{n}\left(3m-1\right)=\frac{1}{2}n\left(3n+1\right).$$

3. Prove that for all-natural numbers, n:

$$\sum_{m=1}^{n}m^3=\frac{1}{4}n^2\left(n+1\right)^2.$$

4. *Prove that for all natural numbers, n:

$$\sum_{m=1}^{n}m^3=\left(1+2+3+4+\ldots+n\right)^2.$$

[Hint: Use the result of Question 3].

5. Prove that for all natural numbers, n:

$$\left(1\times2\right)+\left(2\times3\right)+\ldots+n\left(n+1\right)=\sum_{m=1}^{n}m\left(m+1\right)=\frac{1}{3}n\left(n+1\right)\left(n+2\right).$$

6. Prove that for all natural numbers, n:

$$\left(1\times2\times3\right)+\left(2\times3\times4\right)+\cdots+n\left(n+1\right)\left(n+2\right)=\frac{1}{4}n\left(n+1\right)\left(n+2\right)\left(n+3\right)$$

7. Show that for all natural numbers, n:

$$\sum_{m=0}^{n}2^m=2^{n+1}-1.$$

8. *Prove that for all natural numbers, n:

$$\sum_{m=1}^{n}\left(2m-1\right)^3=n^2\left(2n^2-1\right).$$

9. Prove that for all natural numbers, n:

$$\sum_{m=1}^{n} m^4 = \frac{n\left(n+1\right)\left(2n+1\right)\left(3n^2+3n-1\right)}{30} .$$

10. Prove that for all natural numbers, n:

$$\sum_{m=1}^{n} m^5 = \frac{n^2\left(n+1\right)^2\left(2n^2+2n-1\right)}{12}.$$

11. Prove that for all natural numbers n, 9 divides $10^n - 1$.

12. Prove that for all natural numbers n:

$$3 \,\Big|\, \left(n^3 - n\right).$$

13. *Show that for every natural number n:

$$3 \,\Big|\, n\left(n+1\right)\left(n+2\right).$$

[This means that 3 divides three consecutive integers.]

14. Prove that for all natural numbers n:

$$n^2 - n \text{ is an even number.}$$

15. (i) Prove that for all natural numbers n:

$$\sum_{m=1}^{n} ar^{m-1} = a + ar + ar^2 + \ldots + ar^{n-1} = \frac{a\left(1-r^n\right)}{1-r} \qquad [\, r \neq 1 \,]$$

where a and r are real numbers.

[This is a geometric series with first term equal to a and common ratio r.]

(ii) Show that for every natural number, n:

$$1 + r + r^2 + \ldots + r^n = \sum_{m=0}^{n} r^m = \frac{1-r^{n+1}}{1-r} \qquad \left(r \neq 1\right)$$

[This is the geometric series with the first term equal to 1.]

16. **Prove that for all natural numbers n we have the following trigonometric identity:

$$\sin(x)+\sin(2x)+...+\sin(nx)=\frac{\cos\left(\frac{x}{2}\right)-\cos\left(\frac{2n+1}{2}x\right)}{2\sin\left(\frac{x}{2}\right)}.$$

where x is a real number such that $\sin\left(\frac{x}{2}\right)\neq 0$. [You will need to know your trigonometric identities to do this question or at least look them up and apply them.]

17. ***Prove the binomial theorem for the natural number n:

If a and b are real numbers, then the binomial theorem says that for all natural numbers n:

$$\left(a+b\right)^n=a^n+na^{n-1}b+\frac{n\left(n-1\right)}{2!}a^{n-2}b^2+\frac{n\left(n-1\right)\left(n-2\right)}{3!}a^{n-3}b^3+...+b^n.$$

SECTION 1.5 ⟹ Joy of Sets

By the end of this section you will be able to

- understand what is meant by a set
- plot Venn diagrams of set operations
- apply the well ordering principle

I.5.1 Introduction to Set Theory

What does the term set mean?

A **set** is a collection of objects and these objects are called **elements** or **members** of the set. The following are examples of sets:

1. The numbers 1, 2, 3 and 4.
2. All the positive odd numbers.
3. European capital cities.
4. The roots of the equation $x^2 - 8x + 7 = 0$.

A set can be described in various ways:

i. By listing *all* the elements of the set. For example, in 1 above the set can be written as $A = \{1,\ 2,\ 3,\ 4\}$. The curly brackets, $\{\ \}$, capture the set and each element in the set is separated by a comma.

ii. By listing the first few elements to give an indication of the pattern of the set. For example, $B = \{1,\ 3,\ 5,\ 7,\ \cdots\}$. Note that the 3 dots (ellipses), $\cdots$, represents the missing members when there is a pattern.

iii. By describing a property of the set such as $C = \{\text{European capital cities}\}$.

iv. By stating a mathematical equation like

$$D = \{x : x^2 - 8x + 7 = 0\}$$

(such that)

What does the set D mean?

The set D consists of the numbers x such that x satisfies the quadratic equation $x^2 - 8x + 7 = 0$. The colon, :, in the set is read as 'such that'. Hence the set D is the set of numbers x such that $x^2 - 8x + 7 = 0$.

Sets are normally denoted by capital letters such as $A,\ B,\ C \ldots\ X,\ Y \ldots$ The elements or objects of the set are denoted by lower case letters $a,\ b,\ c \ldots\ x,\ y \ldots$

Example 34

Determine the elements of the set D given above.

Solution

We need to solve the quadratic equation given in the set $D = \{x : x^2 - 8x + 7 = 0\}$.

The roots of the quadratic equation can be found by factorizing:

$$x^2 - 8x + 7 = 0$$
$$(x-7)(x-1) = 0 \qquad [\text{Factorizing}]$$
$$x - 7 = 0 \text{ or } x - 1 = 0$$
$$x = 7 \text{ or } x = 1$$

We can write the set D as $D = \{1,\ 7\}$ but it can also be written as $D = \{7,\ 1\}$. The order of the elements in a set does *not* matter.

We denote the number 7 is a member of the set D by

$$7 \in D.$$

The symbol $\in$ means 'is a member of'. 2 is *not* a member of this set therefore we denote this by $2 \notin D$ and read it as '2 is *not* a member of the set D'.

In general

$x \in A$ means x is a member of the set A.

What does $x \notin A$ mean?

$x \notin A$ means x is *not* a member of the set A.

Example 35

Let A be the set of *all* even numbers. Write the set A in set notation.

Solution

We can write even numbers as the symbol x such that x is an even number, thus we have $A = \{x : x \text{ is an even number}\}$.

What is the size of the set A?

By size we mean the number of members of the set. A has infinitely many members, so we say the cardinality of A is infinite.

The number of members in a set is called the **cardinality** of the set.

Definition (I.18). Given a set A the **cardinality** of A, denoted $Card\{A\}$ or $|A|$, is defined as the number of elements of the set A.

Can you think of an example of a finite set?

The above set $D = \{1,\ 7\}$ therefore $Card\{D\} = 2$.

If $A = \{a,\ b,\ c,\ d,\ f,\ s,\ z\}$ then what is $Card\{A\}$ equal to?

$$Card\{A\} = |A| = 7 \quad [\text{Because the set } A \text{ has 7 members}].$$

I.5.2 Types of Sets

There may be *no* elements in a set. *What do you think we call a set which has no members?*

The **empty set** or the **null set**. The empty set is normally denoted by $\varnothing$ (The Greek letter phi, pronounced fee). *Can you think of any examples of the empty set?*

$$\{\text{Humans who can walk on water}\}$$

What does the universal set mean?

Universal set is the set of *all* the elements under consideration. For example, if we are discussing prime numbers then the universal set will be the set of *all* prime numbers. The universal set is denoted by U.

There are various types of numbers that we have used throughout our lives, but they have *not* been placed in set form or been given a special symbol. *Can you remember what types of numbers you have used?*

Natural numbers, integers, rational numbers and real numbers. We can give *all* these their own symbol:

$\mathbb{N}$ = the set of all natural numbers 1, 2, 3, 4, … These are sometimes called the counting numbers or positive integers. *What is an integer?*

$\mathbb{Z}$ = the set of all integers $\ldots -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots$ This is the set of all whole numbers.

$\mathbb{Q}$ = the set of all rational numbers. These are numbers which can be written as ratios or fractions such as $\frac{2}{3},\ -\frac{5}{2},\ \frac{100}{2},\ 6,\ -\frac{1}{7}$. Note that all the integers are also in this set because numbers like 6 can be written as $\frac{12}{2}$.

Numbers such as $\pi,\ \sqrt{2},\ e$ *cannot* be written as fractions so these are not rational numbers. These are examples of **irrational numbers**.

$\mathbb{R}$ = the set of all real numbers. This is the set of all rational and irrational numbers. For example, $\pi,\ \frac{22}{7},\ \sqrt{2},\ \frac{41}{29},\ 5,\ -666,\ 2.333\ldots$ are all members of $\mathbb{R}$. The reals come in two different flavours; rationals and irrationals.

$\mathbb{C}$ = the set of all complex numbers. This set contains all the real numbers as well as numbers such as $\sqrt{-1}$ which is *not* a real number. Complex numbers are normally written as $a + bi$ where i denotes an imaginary number and is equal to $\sqrt{-1}$.

Example 36

Determine the members of the set $A = \{x \in \mathbb{N} : (x-3)(2x+1) = 0\}$.

Solution

The already factorized quadratic produces the solutions:

$$(x-3)(2x+1) = 0 \;\Rightarrow\; x = 3 \;\text{ or }\; x = -\frac{1}{2}.$$

Does the set A contain both these elements 3 and $-\frac{1}{2}$?

No, because the set A has the qualification $x \in \mathbb{N}$. *What does this notation $x \in \mathbb{N}$ mean?*

x is a member of the set of natural numbers which means x is a positive whole number. The rational number $-\frac{1}{2}$ is *not* a natural number therefore it *cannot* be a member of the set A. Thus, the set A only has the element 3, that is $A = \{3\}$.

Example 37

Write the following statements in set notation:

(a) The set of positive real numbers excluding 0.

(b) The set of negative integers.

(c) The set of rational numbers between 0 and 1 (inclusive).

Solution

(a) The set of positive real numbers can be written as a symbol x which represents a real number such that it is greater than 0:

$$\{x \in \mathbb{R} : x > 0\}.$$

(b) *What is the symbol for the set of integers?*

$\mathbb{Z}$ represents the set of all integers. The set of negative integers can be written as x which is an integer such that it is less than 0:

$$\{x \in \mathbb{Z} : x < 0\}.$$

(c) *What is the symbol for the set of rationals?*

$\mathbb{Q}$ represents the set of rationals (Q for quotient). The set of rationals between 0 and 1 can be written as:

$$\{x \in \mathbb{Q} : 0 \le x \le 1\}.$$

I.5.3 Venn Diagrams

Venn diagrams are a graphically way of representing sets. Venn diagrams were introduced by John Venn.

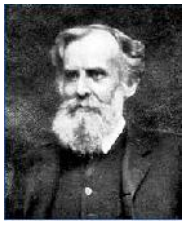


Figure 8 Venn 1834 to 1923

John Venn was born in Hull, England in 1834. His father and grandfather were priests and John was also groomed for a similar post. In 1853 he went to Gonville and Caius College Cambridge and graduated in 1857 becoming fellow of the college. For the next 5 years he went into priesthood and returned to Cambridge in 1862 to teach logic and probability theory.

John Venn is popular known as the person who developed a graphically way to look at sets and this graph become known as a Venn diagram. The sets were represented by oval or circular shape figures but they can be any shape.

It was the Swiss mathematician Euler 1707-83 (pronounced 'oiler') who first discovered Venn diagrams.

Consider the set $A = \{x \in \mathbb{Z} : -3 \leq x \leq 2\}$. *What are the elements of the set A?*

A is the set of integers which lie between -3 to 2. Thus, the elements are $-3,\ -2,\ -1,\ 0,\ 1$ and 2. The Venn diagram of this looks like:

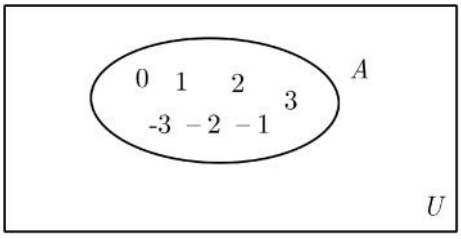


Figure 9

The U in the bottom right hand corner of the rectangle is the universal set which means it includes every element under consideration, which in this case is $U = \mathbb{Z}$. The members of the set A lie within the boundary of the oval shape as shown in Fig. 9.

We can use Venn diagrams to display set operations.

I.5.4 Union and Intersection of Sets

From the age of 7 we have added and multiplied numbers. In a similar fashion we can carry out similar operations on sets. These operations are called **union** and **intersection**.

What is the union of two sets?

The word **union** in everyday language means combining of two or more things. Union of two sets is the combination of all elements in both sets.

Definition (I.19). The **union** of two sets A and B is the set of *all* the elements belonging to set A or set B. The union of two sets A and B is denoted $A \cup B$ and is

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

In terms of a Venn diagram we can draw $A \cup B$ as:

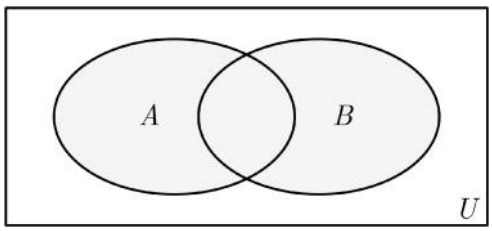


Figure 10 $A \cup B$ (A union B) is shaded

We can also express this $A \cup B$ in terms of mathematical logic discussed in earlier sections. Union $\cup$ is similar to the 'or' symbol which is $\vee$, that is we have

$$x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B)$$

The other operation on sets is intersection. *What does **intersection** mean in everyday language?*

Intersection means crossroads. Intersection of two sets A and B is the set of *all* elements which belong to *both* sets A and B.

Definition (I.20). The **intersection** of two sets A and B, denoted $A \cap B$, is the set of *all* the elements belonging to set A and set B:

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

The Venn diagram of $A \cap B$ is:

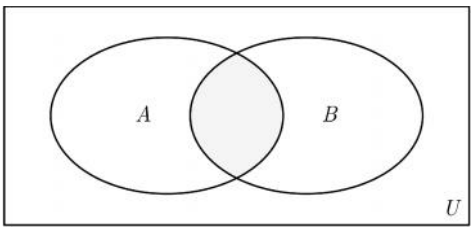


Figure 11 $A \cap B$ (A intersection B) is shaded

Similarly, intersection $\cap$ is similar to the 'and' symbol which is $\wedge$, we have

$$x \in A \cap B \Leftrightarrow (x \in A) \wedge (x \in B).$$

Example 38

Let $A = \{2,\ 3,\ 4,\ 5,\ 6\}$ and $B = \{1,\ 3,\ 7\}$. Determine the sets $A \cup B$ (A union B) and $A \cap B$ (A intersection B). Also draw the Venn diagrams of these sets.

Solution

What does $A \cup B$ mean?

A union B is the set of all elements which are in the set A or B. Thus we have

$$A \cup B = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7\}.$$

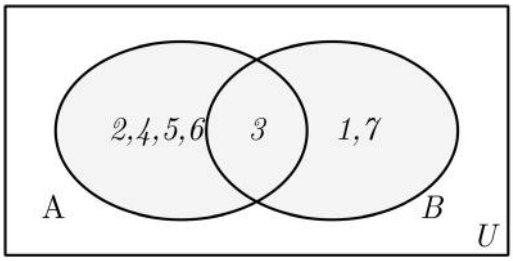
Which members does the set $A \cap B$ have?

All the members which are common to both the sets A and B.

Only the number 3 belongs to both sets A and B. Therefore

$$A \cap B = \{3\}$$

The Venn diagrams of $A \cup B$ and $A \cap B$ are



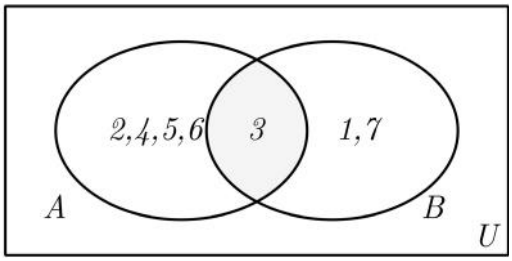


Figure 11 $A \cup B$ is shaded (A or B) $A \cap B$ is shaded (A and B)

I.5.5 Other Set Operations

What does the word ***complement*** *mean in everyday language?*

Complement is something which completes or fills up. In set theory the complement of a set A is the elements which are in the universal set but *not* in set A.

Definition (I.21). The complement of a set A is denoted by A^c and is defined to be

$$A^c = \{x : x \in U,\ x \notin A\}.$$

What does the Venn diagram of A^c *look like?*

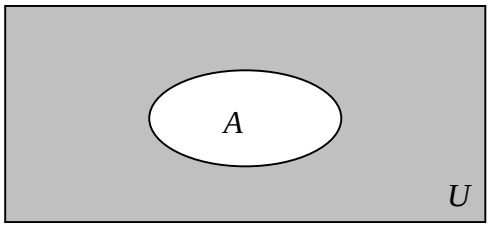


Figure 12 A^c (complement of A) is shaded

Note that $A^C \cup A = U$ where U is the universal set. $A^c \cup A$ fills up U.

We have $x \in A^c \Leftrightarrow x \notin A$. Sometimes A^c is denoted by $\neg A$ or $\sim A$.

Example 39

Let $E = \{2,\ 4,\ 6,\ 8,\ \cdots\}$ and universal set $U = \mathbb{N}$. Determine E^c.

Solution

What does $U = \mathbb{N}$ *mean?*

The universal set U is the set of all the natural numbers 1, 2, 3, 4, … . Note that E is the set of positive even numbers. *What does E^c mean?*

E^c is the set of positive odd natural numbers, that is $E^c = \{1,\ 3,\ 5,\ 7, \cdots\}$.

I.5.6 Introduction to Subsets

*What do you think the term **subset** means?*

The prefix 'sub' normally means contained within a system or structure. Thus, subset is a set contained within another set. The Venn diagram of the set A being a subset of the set B is given by:

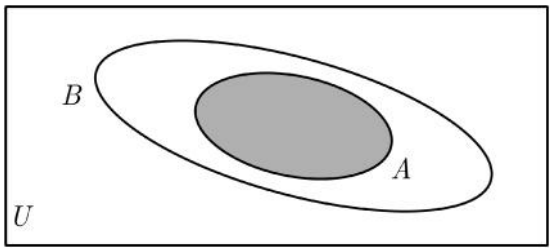


Figure 13 A is a subset of B

What is the definition of a subset?

All the elements of one set are contained within another set. In general, let A and B be two given sets. If every element in set A is also in set B then we say A is a **subset** of B. We also say A is **contained** in B.

How do we denote a subset in mathematical notation?

We denote A is a subset of B by $A \subseteq B$.

An example of a subset is {students} $\subseteq$ {human race}. *Is B a subset of any set in Figure 13?*

The universal set U, that is $B \subseteq U$. Note that set A is also a subset of universal set U. *Is there a set which is the subset of A?*

Yes the empty set $\varnothing$ is a subset of A, that is $\varnothing \subseteq A$. The empty set $\varnothing$ is a subset of *every* set. Also note that A is a subset of itself, that is $A \subseteq A$.

Can you think of any other examples of subsets?

There are an infinitely many examples which you could easily make up such as the following:

1. Let $A = \{\text{Marilyn Munroe, Kim Novak, Michelle Pfeiffer}\}$ and $B = \{\text{women}\}$, then A is a subset of B which we denote by $A \subseteq B$.
2. Let $A = \{\text{Prime Ministers of Britian}\}$ and $B = \{\text{Thatcher, Major, Blair}\}$ then $B \subseteq A$.

3. Let $A=\{a,\ e,\ i,\ o, u\}$ and $B=\{\text{Letters of the alphabet}\}$. Again, we have $A\subseteq B$.

There are many more interesting examples you can create.

The formal definition of subset is:

Definition (I.22). The set A is a **subset** of B if *every* member of set A is also in set B.

I.5.7 Well Ordering Principle

Now we revisit mathematical induction.

Principle of Strong Mathematical Induction (I.23)

For each natural number n, let $P(n)$ be a proposition about n. If $P(n)$ satisfies:

1) $P(n_0)$ is true for base case $n=n_0$ and
2) For all $n\le k$, $P(n)$ is true implies $P(k+1)$ is true.

Then for *all* natural numbers, n, we have $P(n)$ is true.

The difference between strong and ordinary induction can be explained by the ladder analogy:

Ordinary Induction: You are using your present step to prove the next step.

Strong Induction: You have stepped on all the previous steps to get to the current step.

One important property of sets of natural numbers that is often used in proving results is the Well Ordering Principle - WOP:

(I.24) Every non-empty subset of positive integers has a *least* element.

Proof.

We use proof by strong induction.

Let S be a subset of positive integers *without* a least element.

If $1\in S$ then 1 would be the least element in S which is impossible, so $1\notin S$.

We assume by strong induction that $2\notin S,\ 3\notin S,\ \cdots,\ k\notin S$.

Required to prove that $k+1\notin S$.

Suppose $k+1\in S$. However this $k+1\in S$ *cannot* be the case because then $k+1$ would be the least element of S because $2\notin S,\ 3\notin S,\ \cdots,\ k\notin S$ and S has *no* least element.

Therefore, by strong mathematical induction we conclude that S is the empty set, which implies that every non-empty subset of positive integers has a *least* element.

■

The Well Ordering Principle (WOP) is equivalent to Mathematical Induction – you are asked to show this in question 13 of Exercises I.5.

Summary

A set is a collection of objects. The notation $x \in A$ means the element x is a member of the set A.

Let A and B be sets. Then we have the following set operations:

The *union* of two sets is given by $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

The *intersection* of two sets is given by $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

WOP – every non – empty subset of positive integers has a least element.

Exercises **I.5**

Brief solutions end of Exercises.

Complete solutions at www.oup.co.uk/companion/NumberTheory

1. Determine the members of the following sets:

(a) $A = \{x \in \mathbb{R} : 2x + 1 = 0\}$ (b) $B = \{x \in \mathbb{N} : (x-1)(x-2) = 0\}$

(c) $C = \{x \in \mathbb{N} : x^2 - 2x + 1 = 0\}$ (d) $D = \{x \in \mathbb{Z} : x^2 - 4x - 5 = 0\}$

(e) $E = \{x \in \mathbb{Z} : x^2 - 9 = 0\}$ (f) $F = \{x : x \text{ is a prime number less than } 10\}$

2. Determine the elements of the following sets:

(a) $A = \{x \in \mathbb{N} : (x-1)(x+3) = 0\}$ (b) $B = \{x \in \mathbb{N} : 2x + 1 = 0\}$

(c) $C = \{x \in \mathbb{Z} : (x+5)(3x-1) = 0\}$ (d) $D = \{x \in \mathbb{Q} : (x+5)(3x-1) = 0\}$

(e) $E = \{x \in \mathbb{Q} : x - \pi = 0\}$ (f) $F = \{x \in \mathbb{R} : x - \pi = 0\}$

3. Write the following statements in set notation:

(a) The set of negative real numbers.

(b) The set of positive integers.

(c) The set of real numbers between 0 and 2 excluding 0 and 2.

(d) The set of rational numbers less than 1.

(e) The set of natural numbers which are multiples of 10.

4. On a Venn diagram shade in the following regions.

(a) A^c (b) B^c (c) $(A \cap B)^c$ (d) $(A \cup B)^c$ (e) $A^c \cap B^c$

What do you notice about your results to parts (d) and (e).

5. By shading in the appropriate area on a Venn diagram show that $(A^c)^c = A$.

6. Determine in each of the following cases whether $A \subseteq B$ or $B \subseteq A$:

(a) $A = \{x \in \mathbb{R} : 0 \le x \le 10\}$ and $B = \{x \in \mathbb{R} : -10 \le x \le 10\}$.

(b) $A = \{x \in \mathbb{Z} : 0 \le x \le 10\}$ and $B = \{x \in \mathbb{R} : 0 \le x \le 10\}$.

(c) $A = \{x \in \mathbb{R} : 0 \le x \le 10\}$ and $B = \{x \in \mathbb{Z} : 0 \le x \le 10\}$.

(d) $A=\{x\in\mathbb{N}:-10\le x\le 10\}$ and $B=\{x\in\mathbb{Z}:1\le x\le 10\}$.

(e) $A=\{x\in\mathbb{Q}:0\le x\le 10\}$ and $B=\{x\in\mathbb{Q}:0<x<10\}$.

7. Let

$$\varnothing,\ A=\{2,\ 3,\ 5\},\ B=\{x\in\mathbb{Z}:x^2-4=0\}$$
$$C=\{x\in\mathbb{N}:x \text{ is prime and less than } 10\},\ D=\{x\in\mathbb{Z}:0\le x\le 10\}$$

Decide whether the following pairs of sets are subsets or not:

(a) $\varnothing,\ A$ (b) $A,\ A$ (c) $A,\ C$ (d) $C,\ D$ (e) $B,\ C$

8. Consider the following sets:

$$A=\{x\in\mathbb{Z}:0<x<5\},\ B=\{x\in\mathbb{N}:x \text{ is an even number}\}$$
$$C=\{x\in\mathbb{N}:x \text{ is a multiple of } 2\}$$
$$D=\{x\in\mathbb{R}:x\neq x\},\ E=\{x\in\mathbb{N}:x^3\}$$
$$F=\{x\in\mathbb{Z}:0<x<2\}$$

Determine whether the symbol $\square$ in the following is $\subseteq$ or $\nsubseteq$:

(a) $A\square B$ (b) $A\square C$ (c) $B\square C$ (d) $C\square B$ (e) $A\square D$

(f) $D\square A$ (g) $E\square F$ (h) $F\square E$

9. Determine the cardinality, $|A|$, of the following sets:

(a) $A=\varnothing$ (b) $A=\{a,\ b,\ c\}$ (c) $A=\{x\in\mathbb{Z}:3x^2-x=0\}$

(d) $A=\{x\in\mathbb{R}:x=x+1\}$

10. Let $A=\{1,\ 2,\ 3,\ 4,\ 5\}$ and $B=\{x\in\mathbb{N}:x \text{ is a prime number } \le 5\}$. Show that $A\nsubseteq B$ but $B\subseteq A$.

11. Let $A=\{1,\ 3\}$, $B=\{1,\ 3,\ 3,\ 1\}$ and $C=\left\{1,\ 3,\ \frac{3}{1},\ \frac{\pi}{\pi}\right\}$. Determine a set relationship between the given sets $A,\ B$ and C.

12. Use the Well Ordering Principle to prove that for all positive integers n:

$$\sum_{m=1}^{n} m=\frac{n(n+1)}{2}$$

[We proved this result by induction in the last section, Example 29.]

13. *Prove the Induction Principle (I.15) by using the well ordering principle.

This results proves that the Induction Principle and WOP are equivalent because we have already derived the WOP from the Induction Principle.

Brief Solutions to Exercise I.5

1. (a) $A = \left\{-\frac{1}{2}\right\}$ (b) $B = \{1,\ 2\}$ (c) $C = \{1\}$ (d) $D = \{-1,\ 5\}$
(e) $E = \{-3,\ 3\}$ (f) $F = \{2,\ 3,\ 5,\ 7\}$

2. (a) $A = \{1\}$ (b) $B = \varnothing$ (c) $C = \{-5\}$ (d) $D = \left\{\frac{1}{3},\ -5\right\}$
(e) $E = \varnothing$ (f) $F = \{\pi\}$

3. (a) $\{x \in \mathbb{R} : x < 0\}$ (b) $\{x \in \mathbb{Z} : x > 0\}$ or $\mathbb{N}$ (c) $\{x \in \mathbb{R} : 0 < x < 2\}$
(d) $\{x \in \mathbb{Q} : x < 1\}$ (e) $\{10n : n \in \mathbb{N}\}$

6. (a) $A \subseteq B$ (b) $A \subseteq B$ (c) $B \subseteq A$ (d) $A \subseteq B$ and $B \subseteq A$ which means we have $A = B$ (e) $B \subseteq A$

7. (a) $\varnothing \subseteq A$ (b) $A \subseteq A$ (c) $A \subseteq C$ (d) $C \subseteq D$ (e) $B \nsubseteq C$

8. (a) $A \nsubseteq B$ (b) $A \nsubseteq C$ (c) $B \subseteq C$ (d) $C \subseteq B$ (e) $A \nsubseteq D$
(f) $D \subseteq A$ (g) $E \nsubseteq F$ (h) $F \subseteq E$

9. (a) $|\varnothing| = 0$ (b) $|A| = 3$ (c) $|A| = 1$ (d) $|A| = 0$

11. $A = B = C$

SECTION 1.6 ⟹ Inequalities, modulus function and polynomials

By the end of this section you will be able to

- derive properties of inequalities
- understand the modulus function
- examine polynomials

This is a challenging section because we treat inequalities in an abstract manner and many students have difficulty in relating to the results obtained in this section. Additionally, students apply the rules of inequalities as they would for equality, =, because they are comfortable in using them. You need to be a lot more careful with inequalities and *cannot* blindly apply the same rules as you did for equality.

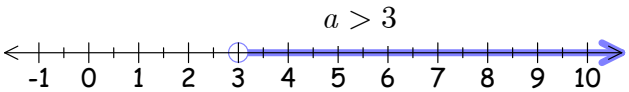
I.6.1 Examples of Inequalities

What does the term 'inequality' mean in the general sense?

We often read in the papers 'inequality of wealth' or 'inequality of women's pay' which implies that the distribution has *not* been equally dispersed.

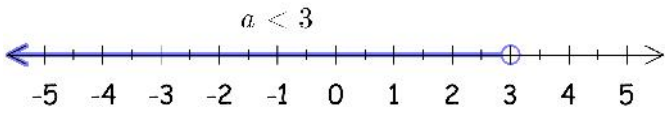
Generally, inequality is opposite to equality which implies that inequality means *not* equal to. For example we can say 'a is greater than 3' and this is denoted by '$a > 3$' meaning that the real number a is to the right of 3 on the real number line:

Figure 14



The real number a is less than 3 is denoted by $a < 3$ and means that a is to the left of 3 on the real number line:

Figure 15



I.6.2 Inequality Properties of Real Numbers

Let a and b be real numbers then *only* one of the following is true:

(i) $a > b$ (a is greater than b).

(ii) $a = b$ (a is equal to b).

(iii) $a < b$ (a is less than b).

Richard Recorde 1512-58 devised the $=$ symbol in 1557. In 1600 Thomas Harriot 1560 – 1621 added the inequality signs $<$ and $>$ and the convention of writing ab for $a \times b$.

The real numbers a and b satisfying $a > b \Leftrightarrow a - b > 0$. For example, in the above case $a > 3 \Leftrightarrow a - 3 > 0$ and $a < 3 \Leftrightarrow a - 3 < 0$.

Also $a > b$ is equivalent to $b < a$. This can be written in mathematical notation as:

$$\big(a > b\big) \equiv \big(b < a\big).$$

For example $5 > 3$ (5 is greater than 3) is equivalent to $3 < 5$ (3 is less than 5).

What is $\pi < 4$ *equivalent to?*

$$4 > \pi$$

We assume the following properties of inequalities of real numbers:

(I.25) If $a > 0$ and $b > 0$ then $a + b > 0$. *What does this notation mean?*

Adding two positive real numbers gives a positive real number.

(I.26) If $a > 0$ and $b > 0$ then $a \times b = ab > 0$. *What does this notation mean?*

Multiplying two positive real numbers gives a positive real number.

(I.27) If $a \in \mathbb{R}$ then *only* one of the following is true: $a > 0$, $a = 0$ or $-a > 0$.

From these we prove other properties of inequalities of real numbers.

Proposition (I.28). Let a, b and c be real numbers. Then the following properties hold:

(a) If $a > b$ then $a + c > b + c$.

(b) If $a > b$ and $b > c$ then $a > c$.

Proof.

(a) Remember $a > b$ means $a - b > 0$. Therefore

$$\begin{aligned} a - b &= a + \underbrace{c - c}_{=0} - b && \big[\text{Rewriting} \quad a - b\big] \\ &= a + c - \big(b + c\big) > 0 && \big[\text{Because} \quad a - b > 0\big] \end{aligned}$$

From $a + c - \big(b + c\big) > 0$ we have $a + c > b + c$. We have proven $a > b \Rightarrow a + c > b + c$.

■

(b) From the given two inequalities, $a > b$ and $b > c$, we have

$$a - b > 0 \text{ and } b - c > 0.$$

Adding these two positive inequalities together gives

$$a \underbrace{-b + b}_{=0} - c > 0$$

$$a - c > 0$$

From $a-c>0$ we have the required result, $a>c$.

■

We can apply the above Proposition (I.28) to concrete examples:

We know $3>2$. Adding $c=5$ does *not* change the inequality:

$$3+5>2+5.$$

Also adding $c=-5$ does *not* change the inequality:

$$3+\big(-5\big)>2+\big(-5\big).$$

Examples of proposition (I.28) (b) (if $a>b$ and $b>c$ then $a>c$) are

$$3>2 \quad \text{and} \quad 2>1 \quad \Rightarrow \quad 3>1$$
$$-3>-4 \quad \text{and} \quad -4>-5 \quad \Rightarrow \quad -3>-5$$

Proposition (I.29). Let a, b and c be real numbers. We have:

(a) If $a>b$ and $c>0$ then $ac>bc$.

(b) If $a>b$ and $c<0$ then $ac<bc$ [The inequality changes].

Proof.

(a) Recall $a>b$ means $a-b>0$. We are given that $c>0$ and so multiplying these two positive inequalities we have

$$\begin{aligned} \big(a-b\big)c &>0 && \big[\text{By (I.26)}\big] \\ ac-bc &>0 && \big[\text{Expanding}\big] \\ ac &>bc \end{aligned}$$

Thus, we have our result.

■

(b) If $c<0$ then $-c>0$ and we are given that $a>b$ so $a-b>0$. Multiplying these two positive inequalities, $a-b>0$ and $-c>0$, we have

$$\begin{aligned} \big(a-b\big)\big(-c\big) &>0 && \big[\text{By (I.26)}\big] \\ -ac+bc &>0 && \big[\text{Expanding}\big] \\ bc &>ac \end{aligned}$$

Note that $bc>ac$ (bc is greater than ac) is equivalent to $ac<bc$ (ac is less than bc) which is our required result.

■

Notice the result of the above proposition (I.29) (b). If we multiply the inequality $a>b$ by a negative real number such as $c<0$ then it changes the inequality sign to $ac<bc$. A negative multiple changes the inequality sign.

If $a<b$ and $c<0$ then what is the inequality between ac and bc?

$$ac>bc$$

Remember a negative multiple *changes* the inequality sign. Note that inequalities such as $<$ and $>$ do *not* behave like equality, $=$. You need to be a lot more careful with inequalities as the following application of Proposition (I.29) shows:

$$5>2 \text{ and } c=3 \Rightarrow (5\times 3)>(2\times 3) \quad [\text{Inequality remains the same}]$$
$$5>2 \text{ and } c=-3 \Rightarrow (5\times(-3))<(2\times(-3)) \quad [\text{Inequality Changes}]$$
$$-2<-1 \text{ and } c=-4 \Rightarrow (-2\times(-4))>(-1\times(-4)) \quad [\text{Inequality Changes}]$$

Proposition (I.30). Let x be a real number. Then $x^2 \geq 0$.

What can x be?

By (I.27), it can be positive, $x>0$, or equal to zero, $x=0$, or negative $x<0$.

We consider each case.

Proof.

If $x=0$ then $x^2=0^2=0\geq 0$ the result holds.

Now consider the positive case, that is let $x>0$ then

$$x\times x>0 \quad [\text{By (I.26)}]$$
$$x^2>0$$

In the last instance we let $x<0$ [Negative], then multiplying this by the same negative real number, $x<0$, we change the inequality because of (I.29) (b):

$$x\times x>0\times x$$
$$x^2>0$$

Combining these three cases we have $x^2\geq 0$.

■

Proposition (I.31).

(a) $1>0$

(b) Let $n\in\mathbb{N}$ then $n>0$.

Proof.

(a) $1=1^2>0$ [With $x=1\neq 0$ in the previous Proposition (I.30).]

■

(b) *What does $n\in\mathbb{N}$ mean?*

This notation $n\in\mathbb{N}$ means that n is a natural number, 1, 2, 3, 4, … . *How do we prove $n>0$ for $n\in\mathbb{N}$?*

By using induction because it is a result concerning the natural numbers. The procedure for induction outlined in Section I.4 is to show the result for $n=1$, assume it is true for $n=k$ and then prove the given result for $n=k+1$.

By part (a) we have $1>0$. Assume $k>0$. Required to prove $k+1>0$. We have

$$\begin{aligned} k &> 0 && \left[\text{By Assumption}\right] \\ 1 &> 0 && \left[\text{By (a)}\right] \\ k+1 &> 0 \end{aligned}$$

Hence by induction we have proven our result, if $n\in\mathbb{N}$ then $n>0$.

■

I.6.3 Introduction to the Modulus Function

Definition (I.32). Let x be a real number then the **modulus** of x is denoted by $|x|$ and is defined as

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

What does this mean?

If x is *positive or zero* then $|x| = x$ and if x is *negative* then $|x| = -x$.

By Definition (I.32) we have $|5| = 5$. *What is the value of* $|-5|$ *?*

By Definition (I.32) we have $|-5| = -(-5) = 5$. *What is the value of* $|-1/2|$ *?*

Similarly, $|-1/2| = -(-1/2) = 1/2$. *What is the value of* $|-\pi|$ *?*

$$|-\pi| = -(-\pi) = \pi.$$

What do you notice about your results?

They are all positive. *What is* $|0|$ *equal to?*

$$|0| = 0.$$

What does the graph of $|x|$ *look like?*

Note that the modulus of negative values of x, $|-x|$, is positive x and for positive and zero x we have $|x| = x$. Therefore, the graph of $y = |x|$ is:

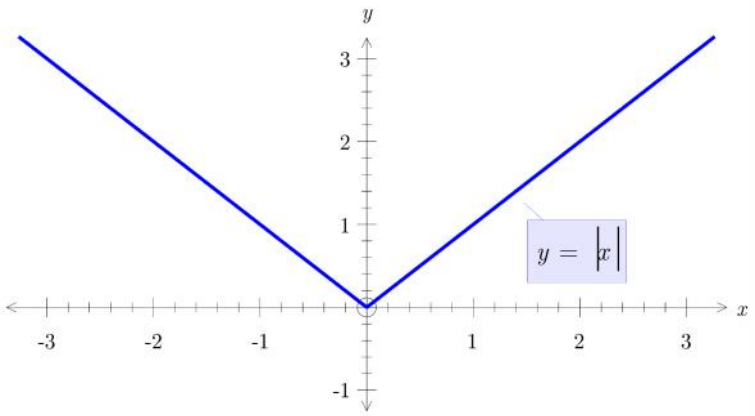


Figure 16

What do you notice about the graph of $y = |x|$ *?*

Symmetrical about the y axis, that is $|-x| = |x|$. *What does the word symmetry mean?*

Symmetry is when two or more parts look alike as they do in the above graph.

Also, the graph of $y = |x|$ is above the x axis and only touches it at $x = 0$. Hence the modulus of a real number is always positive or zero and we can write this as an inequality

(I.33) $$|x| \geq 0$$

What are the values of x *which satisfies* $|x| = 2$ *?*

We have $|x| = 2$ if $x = 2$ or $x = -2$. Therefore $|x| = 2$ has the solutions $x = 2$ or $x = -2$.

The modulus function is also called the **distance** or **absolute function**.

The geometrical interpretation of the modulus function is the distance on the real number line. For example, $|x|$ is the distance from x to zero.

We can visualize $|x| = 2$ as the distance of x from zero is 2 and this is represented by:

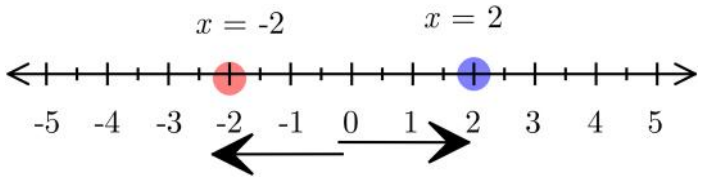


Figure 17

The equation $|x| = a$ has the solution $x = a$ or $x = -a$.

I.6.4 Inequalities of the Modulus Function

Visualizing the modulus function as the distance function is particularly useful for inequalities.

What does $|x| \leq 2$ *represent?*

The distance of x from zero is less than or equal to 2 and can be illustrated as:

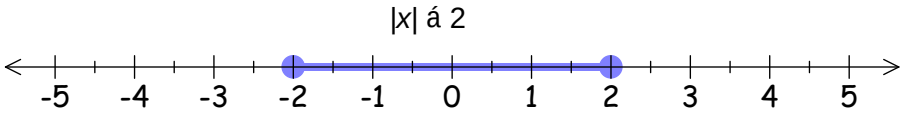


Figure 18

What is the difference between $x \le 2$ *and* $|x| \le 2$ *?*

$x \le 2$ represents all the real numbers less than or equal to 2. The notation $|x| \le 2$ represents all the real numbers between $x = -2$ to $x = 2$. This is the set of all real numbers between -2 to 2 and is denoted by $\{x \in \mathbb{R} : -2 \le x \le 2\}$ which can be written as $-2 \le x \le 2$.

What values of x *satisfy* $|x| < 2$ *?*

$$-2 < x < 2$$

We can solve general inequalities such as $|x| < a$ where $a > 0$ by algebraic means.

What does $|x| < a$ *mean?*

The distance x from zero is less than a and can be illustrated on the real line as:

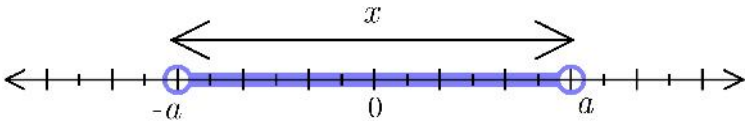


Figure 19

The notation $|x| < a$ means that x lies between $-a$ to a and is denoted by $-a < x < a$ which we can write in symbolic form as

(I.34) $$|x| < a \Leftrightarrow -a < x < a .$$

Example 40

Determine the set of real numbers, x, such that $|x - 3| < 5$.

Solution

How can we interpret $|x - 3| < 5$ *as distance on the real number line?*

This inequality, $|x - 3| < 5$, means that the distance from 3 is less than 5 and we can illustrate this by:

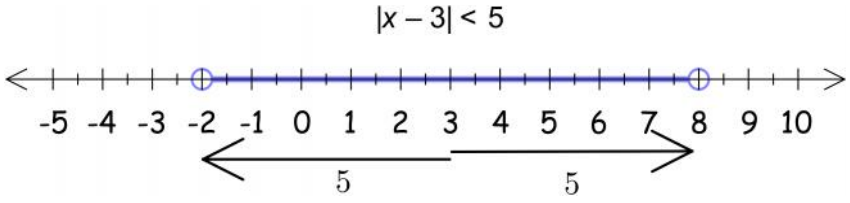


Figure 20

We can also solve this algebraically as follows:

$$\begin{aligned} |x-3| &< 5 \\ -5 < x-3 &< 5 && [\text{By (I.34)}] \\ -5+3 < x &< 5+3 && [\text{Adding } 3] \\ -2 < x &< 8 && [\text{Simplifying}] \end{aligned}$$

Hence all the real numbers between -2 and 8 satisfies the given inequality $|x-3| < 5$.

I.6.5 Properties of the Modulus Function

This subsection is more demanding because the proofs of the results require you to thoroughly understand the definition of the modulus function and inequalities of real numbers as discussed earlier in this section.

Proposition (I.35). For all $x \in \mathbb{R}$ and $y \in \mathbb{R}$ we have

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

Proof. We consider the four possible cases:

(1) If both $x \geq 0$ and $y \geq 0$ then $xy \geq 0$ and we have

$$|x||y| = xy = |xy|.$$

(2) If both $x < 0$ and $y < 0$ then $xy > 0$ and we have

$$\begin{aligned} |x||y| &= (-x)(-y) \\ &= xy = |xy| \end{aligned}$$

Remember by the definition of the modulus function if $x < 0$ and $y < 0$ then $|x| = -x$ and $|y| = -y$ respectively.

(3) If $x > 0$ and $y < 0$ then $xy < 0$ and we have

$$\begin{aligned} |x||y| &= x(-y) && [\text{Because } y < 0 \text{ so } |y| = -y] \\ &= -xy \\ &= |xy| && [\text{Because } xy < 0 \text{ so } |xy| = -xy] \end{aligned}$$

(4) If $x < 0$ and $y > 0$ then $xy < 0$ and we have

$$\begin{aligned} |x||y| &= (-x)y && [\text{Because } x < 0 \text{ so } |x| = -x] \\ &= -xy \\ &= |xy| && [\text{Because } xy < 0 \text{ so } |xy| = -xy] \end{aligned}$$

■

I.6.6 Maximum and Minimum of a Set

Let A be a non – empty set of numbers. Then the minimum m of the set A, denoted $\min A$, satisfies:

I. $m \in A$, that is the m is a member of the set A.

II. For every $a \in A$ we have $m \le a$. This implies that m is less than or equal to every member of A.

Similarly, the maximum M of the set A, denoted $\max A$, satisfies:

I. $M \in A$, that is the M is a member of the set A.

II. For every $a \in A$ we have $M \ge a$. This implies that M is greater than or equal to every member of A.

For example, let $A = \{17, 4, 2019\}$ then $\min A = 4$ and $\max A = 2019$.

For another example let B be the set of non – negative integers. Non– negative integer means $\mathbb{N} \cup \{0\}$, that is all the natural numbers plus zero. Then $\min B = 0$ but it does *not* have a maximum element.

Let C be the set of positive real numbers. Then C has *no* minimum or maximum elements.

I.6.7 Polynomial Expressions

What is a polynomial?

It is an expression of the form

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

where c's are called coefficients and are real numbers. For example

$$2x^4 - x^3 + x^2 + 5x + 7$$

is a polynomial of degree 4 because the highest index of x is 4. A polynomial can be given in factorized form such as

$$y = (x-1)(x-2)(x-3).$$

This is sometimes written in compact form using capital Greek letter pi, $\prod$. The above y can be written as

$$y = (x-1)(x-2)(x-3) = \prod_{j=1}^{3} (x-j)$$

This is like the summation $\sum$ used for summing terms. For example

$$\prod_{j=2}^{7} j = 2 \times 3 \times 4 \times 5 \times 6 \times 7 = 5040.$$

Example 41

Express $y=\prod_{j=1}^{3}\left(x-j\right)$ in $c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ form.

Solution

We have

$$\begin{aligned} y=\prod_{j=1}^{3}\left(x-j\right) &= \left(x-1\right)\left(x-2\right)\left(x-3\right) \\ &= \left(x^2-3x+2\right)\left(x-3\right) \\ &= x^3-3x^2+2x-3x^2+9x-6 \\ &= x^3-6x^2+11x-6 \end{aligned}$$

Now we consider quadratic polynomials. *What are quadratic polynomials?*

It is a polynomial of degree 2 and is generally denoted by ax^2+bx+c where a, b and c are real numbers. Now we convert ax^2+bx+c into another format which can be used to find the maximum and minimum values of this quadratic polynomial.

Example 42

Expand $\left(x+1\right)^2+5$.

Solution

Opening the brackets and simplifying gives

$$\left(x+1\right)^2+5=x^2+2x+1+5=x^2+2x+6.$$

Note that x^2+2x+6 can be written as $\left(x+1\right)^2+5$. In this part we write the expanded expression x^2+2x+6 as $\left(x+1\right)^2+5$. Other examples are

$$x^2+4x+1=\left(x+2\right)^2-3$$

$$x^2-5x+2=\left(x-\frac{5}{2}\right)^2-\frac{17}{4}$$

$$x^2+7x+13=\left(x+\frac{7}{2}\right)^2+\frac{3}{4}$$

Do you notice any relationship between the left and right – hand sides?

The number in the bracket on the right – hand side is half the x coefficient on the left.

Considering the first example $x^2+4x+1=\left(x+2\right)^2-3$. *The 2 is half of 4 but what about the* -3 *?*

Expanding out $\left(x+2\right)^2$ gives

$$\left(x+2\right)^2 = x^2 + 4x + 4$$

Subtracting 4 from both sides yields

$$\left(x+2\right)^2 - 4 = x^2 + 4x$$

Now we have $x^2 + 4x$ but we need $x^2 + 4x + 1$, therefore adding 1 to the above gives

$$x^2 + 4x + 1 = \underbrace{\left(x+2\right)^2 - 4}_{=x^2+4x} + 1 \underset{\text{Simplifying}}{=} \left(x+2\right)^2 - 3$$

This process of converting $x^2 + 4x + 1$ to $\left(x+2\right)^2 - 3$ is called completing the square.

Example 43

Complete the square on (a) $x^2 - 8x + 3$ (b) $x^2 - 5x + 3$ (c) $2x^2 - 5x + 3$

Solution

(a) We have

$$x^2 - 8x + 3 = \left(x-4\right)^2 - 4^2 + 3 \underset{\text{Simplifying}}{=} \left(x-4\right)^2 - 13\,.$$

(b) Similarly, we have

$$\begin{aligned} x^2 - 5x + 3 &= \left(x - \frac{5}{2}\right)^2 - \left(\frac{5}{2}\right)^2 + 3 \\ &= \left(x - \frac{5}{2}\right)^2 - \frac{25}{4} + \frac{12}{4} = \left(x - \frac{5}{2}\right)^2 - \frac{13}{4} \end{aligned}$$

(c) We first take a factor of 2 out:

$$\begin{aligned} 2x^2 - 5x + 3 &= 2\left(x^2 - \frac{5}{2}x + \frac{3}{2}\right) \\ &= 2\left[\left(x - \frac{5}{4}\right)^2 - \left(\frac{5}{4}\right)^2 + \frac{3}{2}\right] \qquad \left[\text{Note } \frac{5}{4} = \frac{1}{2}\left(\frac{5}{2}\right)\right] \\ &= 2\left[\left(x - \frac{5}{4}\right)^2 - \frac{25}{16} + \frac{24}{16}\right] = 2\left[\left(x - \frac{5}{4}\right)^2 - \frac{1}{16}\right] = 2\left(x - \frac{5}{4}\right)^2 - \frac{1}{8} \end{aligned}$$

We can use this completing the square to find the maximum and minimum of a quadratic polynomial as we investigate in the next example.

Example 44

Determine $\min\left\{y \in \mathbb{R} : y = 2x^2 - 5x + 3\right\}$.

Solution

By the previous example part (c) we have

$$2x^2 - 5x + 3 = 2\left(x - \frac{5}{4}\right)^2 - \frac{1}{8}$$

By applying (I.30)

$$z^2 \geq 0$$

to this $2x^2 - 5x + 3 = 2\left(x - \frac{5}{4}\right)^2 - \frac{1}{8}$ we have

$$2x^2 - 5x + 3 = 2\left(x - \frac{5}{4}\right)^2 - \frac{1}{8} \geq 2(0) - \frac{1}{8} = -\frac{1}{8}$$

Therefore $\min\left\{y \in \mathbb{R} : y = 2x^2 - 5x + 3\right\} = -\frac{1}{8}$. By the way the graph of this is:

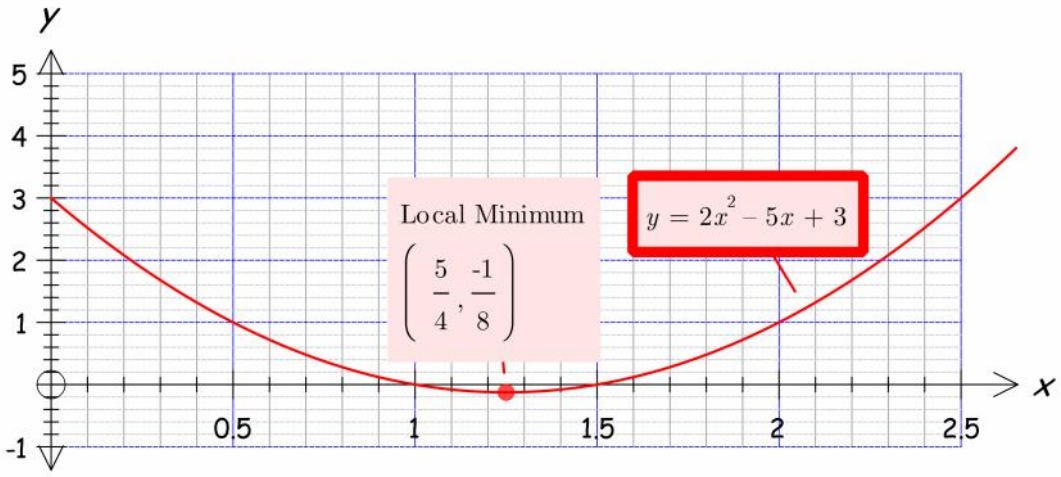


Figure 21

I.6.8 Binomial Expansion

In Exercises I.4 question 18 we proved what is called the binomial expansion:

$$(I.36)\quad \left(a+b\right)^n = a^n + na^{n-1}b + \frac{n\left(n-1\right)}{2!}a^{n-2}b^2 + \frac{n\left(n-1\right)\left(n-2\right)}{3!}a^{n-3}b^3 + \ldots + b^n$$

Note that a and b powers are determined by reducing a by an index of 1, giving $a^n, a^{n-1}, a^{n-2}, \cdots, a, a^0$; and increasing b by an index of 1, giving $b^0 = 1, b^1 = b, b^2, \cdots, b^n$.

We can rewrite the binomial expansion as

$$(I.37)\qquad \left(a+b\right)^n = C_n a^n + C_{n-1}a^{n-1}b + C_{n-2}a^{n-2}b^2 + C_{n-3}a^{n-3}b^3 + \ldots + C_0 b^n$$

where C_{n-j} is the coefficient of $a_{n-j}b^j$. We can also find these coefficients by using Pascal's triangle which is given as follows:

Each row begins and ends with 1.

Every number between these 1's is obtained by adding the two numbers in the row above which are immediately to the left and right of it.

1	$n=0$
1 1	$n=1$
1 2 1	$n=2$
1 3 3 1	$n=3$
1 4 6 4 1	$n=4$
1 5 10 10 5 1	$n=5$
1 6 15 20 15 6 1	$n=6$

Figure 22

For example, the 5 underlined in Fig. 22 is determined by adding 1 and 4. Similarly the 20 in the last line is established by summing 10 and 10. Furthermore each of the rows gives the coefficients for the binomial expansion of the corresponding values of n. For example, $n=4$ gives the coefficients 1, 4, 6, 4 and 1. Hence

$$(8q+r)^4 = (8q)^4 + 4(8q)^3 r + 6(8q)^2 r^2 + 4(8q)r^3 + r^4$$

Example 45

Expand $(2q+r)^6$.

Solution

From Fig. 22 we have the coefficients of $n=6$ are 1, 6, 15, 20, 15, 6 and 1. Applying (I.37) we have

$$\begin{aligned}(2q+r)^6 &= (2q)^6 + 6(2q)^5 r + 15(2q)^4 r^2 + 20(2q)^3 r^3 + 15(2q)^2 r^4 + 6(2q)r^5 + r^6 \\ &= 2^6 q^6 + (6\times 2^5)q^5 r + (15\times 2^4)q^4 r^2 + (20\times 2^3)q^3 r^3 + (15\times 2^2)q^2 r^4 + (6\times 2)qr^5 + r^6 \\ &= 64q^6 + 192q^5 r + 240q^4 r^2 + 160q^3 r^3 + 60q^2 r^4 + 12qr^5 + r^6\end{aligned}$$

Summary

In this section we have established properties of inequalities such as:

If $a>b$ and $c>0$ then $ac>bc$.

If $a>b$ and $c<0$ then $ac<bc$. [The inequality changes].

We discussed the modulus function which is the distance or absolute value function.

We converted the general quadratic polynomial by completing the square.

The binomial expansion is given by

$$(a+b)^n = C_n a^n + C_{n-1}a^{n-1}b + C_{n-2}a^{n-2}b^2 + C_{n-3}a^{n-3}b^3 + \ldots + C_0 b^n$$

where the coefficients C can be found from Pascal's triangle.

Exercises **I.6**

Brief solutions end of Exercises.

Complete solutions at www.oup.co.uk/companion/NumberTheory

Let a, b, c and d be real numbers.

1. Prove that if $a < b$ then $a - c < b - c$.

2. Prove that if $a < b$ and $b < c$ then $a < c$.

3. Prove that if $a < b$ and $c \leq d$ then $a + c < b + d$.

4. Let x be a real number, prove that

(i) if $x > 0$ then $\dfrac{1}{x} > 0$.

(ii) if $x < 0$ then $\dfrac{1}{x} < 0$.

5. Let a and b be real numbers, show that

(a) if $0 < a < b$ then $\dfrac{1}{a} > \dfrac{1}{b}$.

(b) if $b < a < 0$ then $\dfrac{1}{b} > \dfrac{1}{a}$.

6. Let $x \in \mathbb{R}$ and $0 < a < b$. Prove that

(a) $ax^2 \leq bx^2$ (b) $-ax^2 \geq -bx^2$

7. Let $x \in \mathbb{R}$, show that $x^2 - 2x + 1 \geq 0$.

8. Let $x \in \mathbb{R}$, show that $x^2 - 5x + 9 \geq \dfrac{11}{4}$.

9. Prove that $\left(a + b\right)^2 \geq 4ab$.

10. Let x and y be real numbers, prove that

$$\left[\frac{1}{2}\left(x + y\right)\right]^2 \leq \frac{1}{2}\left(x^2 + y^2\right)$$

11. Determine the following: $\left|e\right|$, $\left|-e\right|$, $\left|-\sqrt{2}\right|$, $\left|-6-7\right|$ and $\left|\cos\left(\frac{3\pi}{4}\right)\right|$.

12. Solve the following inequalities:

a. $\left|x\right|<1$ b. $\left|x\right|<\pi$ c. $\left|x-1\right|<1$ d. $\left|x-5\right|\leq 2$

13. Prove that $\left|x-y\right|=\left|y-x\right|$.

14. Prove that $\left|\frac{1}{x}\right|=\frac{1}{\left|x\right|}$ where $x\neq 0$.

15. Prove that $\left|\frac{x}{y}\right|=\frac{\left|x\right|}{\left|y\right|}$ where $y\neq 0$.

16. Prove that if $n\in\mathbb{N}$ then $\left|\frac{1}{n}\right|=\frac{1}{n}$.

17. Let n be a natural number, *disprove* that $\left(n+1\right)^2\geq 2n^2$.

(Challenge: Prove that $\left(n+1\right)^2\leq 2n^2$ for $n\geq 3$).

18. Evaluate $\prod_{j=1}^{5}\left(\frac{2j-1}{2j}\right)\left(\frac{2j+1}{2j}\right)$. Also determine $\left|\frac{2}{\pi}-\prod_{j=1}^{5}\left(\frac{2j-1}{2j}\right)\left(\frac{2j+1}{2j}\right)\right|$. Give your answer correct to 3sf.

Actually $\prod_{j=1}^{\infty}\left(\frac{2j-1}{2j}\right)\left(\frac{2j+1}{2j}\right)=\frac{2}{\pi}$.

19. Complete the square on the following quadratic polynomials:

(i) (a) x^2-4x+3 (b) x^2+7x+1 (c) x^2+3x+5 (d) $x^2+11x-6$

(e) $9+8x-x^2$ (f) $3x^2+7x+1$ (g) $11x^2-5x-7$ (h) $\frac{8}{7}-\frac{7}{5}x-\frac{1}{2}x^2$

Test yourself using the following online questions at

Test on Completing the square

(ii) Determine the following:

(a) $\min\left\{y \in \mathbb{R} : y = x^2 - 4x + 3\right\}$ (b) $\min\left\{y \in \mathbb{R} : y = x^2 + 7x + 1\right\}$

(c) $\min\left\{y \in \mathbb{R} : y = x^2 + 3x + 5\right\}$ (d) $\min\left\{y \in \mathbb{R} : y = x^2 + 11x - 6\right\}$

(e) $\max\left\{y \in \mathbb{R} : y = 9 + 8x - x^2\right\}$ (f) $\min\left\{y \in \mathbb{R} : y = 3x^2 + 7x + 1\right\}$

(g) $\min\left\{y \in \mathbb{R} : y = 11x^2 - 5x - 7\right\}$ (h) $\max\left\{y \in \mathbb{R} : y = \frac{8}{7} - \frac{7}{5}x - \frac{1}{2}x^2\right\}$

20. Expand the following:

(a) $\left(1+x\right)^5$ (b) $\left(2+x\right)^3$ (c) $\left(5-x\right)^4$ (d) $\left(3+2x\right)^5$ (e) $\left(5+x\right)^4$

(f) $\left(2+3x\right)^5$ (g) $\left(4-3x\right)^6$ (h) $\left(2x-y\right)^4$ (i) $\left(x+\frac{1}{x}\right)^5$ (j) $\left(x-\frac{1}{x}\right)^4$

(k) $\left(1+x^2\right)^7$ (l) $\left(\frac{w}{4}-\frac{x}{3}\right)^7$

Test yourself using the following online questions:

Test on the Binomial Expansion using Pascal's triangle

Brief Solutions to Exercise I.6

11. $e, e, \sqrt{2}$, 13 and $\frac{1}{\sqrt{2}}$

12. a. $-1 < x < 1$ b. $-\pi < x < \pi$ c. $0 < x < 2$ d. $3 < x < 7$

18. 0.666 and 0.0296

19. (i) (a) $\left(x-2\right)^2 - 1$ (b) $\left(x+\frac{7}{2}\right)^2 - \frac{45}{4}$ (c) $\left(x+\frac{3}{2}\right)^2 + \frac{11}{4}$ (d) $\left(x+\frac{11}{2}\right)^2 - \frac{145}{4}$

(e) $25 - \left(x-4\right)^2$ (f) $3\left(x+\frac{7}{6}\right)^2 - \frac{37}{12}$ (g) $11\left(x-\frac{5}{22}\right)^2 - \frac{333}{44}$

(h) $\frac{743}{350} - \frac{1}{2}\left(x+\frac{7}{5}\right)^2$

(ii) (a) -1 (b) $-\frac{45}{4}$ (c) $\frac{11}{4}$ (d) $-\frac{145}{4}$ (e) 25 (f) $-\frac{37}{12}$

(g) $-\frac{333}{44}$ (h) $\frac{743}{350}$

20. (a) $1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5$

(b) $8 + 12x + 6x^2 + x^3$

(c) $625 - 500x + 150x^2 - 20x^3 + x^4$

(d) $243 + 810x + 1080x^2 + 720x^3 + 240x^4 + 32x^5$

(e) $625 + 500x + 150x^2 + 20x^3 + x^4$

(f) $32 + 240x + 720x^2 + 1080x^3 + 810x^4 + 243x^5$

(g) $4\ 096 - 18\ 432x + 34\ 560x^2 - 34\ 560x^3 + 19\ 440x^4 - 5\ 832x^5 + 729x^6$

(h) $16x^4 - 32x^3y + 24x^2y^2 - 8xy^3 + y^4$

(i) $x^5 + 5x^3 + 10x + \frac{10}{x} + \frac{5}{x^3} + \frac{1}{x^5}$

(j) $x^4 - 4x^2 + 6 - \frac{4}{x^2} + \frac{1}{x^4}$

(k) $1 + 7x^2 + 21x^4 + 35x^6 + 35x^8 + 21x^{10} + 7x^{12} + x^{14}$

(l) $\frac{w^7}{16384} - \frac{7}{12288}w^6x + \frac{7}{3072}w^5x^2 - \frac{35}{6912}w^4x^3 + \frac{35}{5184}w^3x^4 - \frac{7}{1296}w^2x^5 + \frac{7}{2916}wx^6 - \frac{1}{2187}x^7$