## Contents

How to use this book iv  
Introduction 1  
1 Preliminaries: Proof by contradiction 3  
2 Sets and operations 6  
  2A Defining sets 6  
  2B Operations 12  
  2C Operations on sets 25  
3 Ordered pairs, relations and functions 37  
  3A Ordered pairs 37  
  3B Binary relations and numerical congruence 40  
  3C Classifying relations 43  
  3D Functions 50  
4 Groups and subgroups 67  
  4A Group structure 67  
  4B Group properties and cyclic groups 71  
  4C Subgroups and cosets 79  
  4D Lagrange’s theorem 86  
  4E Frequently encountered groups 89  
  4F Homomorphisms and kernels 101  
  4G Isomorphisms 109  
5 Summary and mixed examination practice 119  
Supplementary sheet: Groups of order 6 125  
Answers 127  
Glossary 134  
Index 141
How to use this book

Structure of the book

This book covers all the material for Topic 8 (Sets, Relations and Groups Option) of the Higher Level Mathematics syllabus for the International Baccalaureate course. It is largely independent of the Core material, although some examples use vectors and complex numbers; the only real prerequisite is familiarity with functions (syllabus topic 2.1), though you will also find it beneficial to cover proof by induction (syllabus topic 1.4) and sets and Venn diagrams (syllabus topics 5.2 and 5.3). We have tried to include in the main text only the material that will be examinable. There are many interesting applications and ideas that go beyond the syllabus and we have tried to highlight some of these in the ‘From another perspective’ and ‘Research explorer’ boxes.

The material is roughly split into three blocks (sets and operations; functions and relations; groups), and those are contained in Chapters 2 to 4. Chapter 1 introduces some methods of mathematical proof that are used throughout the course. Chapter 5 contains a summary of all the topics and further examination practice, with many of the questions mixing several topics – a favourite trick in IB examinations.

Each chapter starts with a list of learning objectives to give you an idea about what the chapter contains. There is an introductory problem at the start of the topic that illustrates what you should be able to do after you have completed the chapter. At the start, you should not expect to be able to solve the problem, but you may want to think about possible strategies and what sort of new facts and methods would help you. The solution to the introductory problem is provided at the end of Chapter 5.

Key point boxes

The most important ideas and formulae are emphasised in the ‘KEY POINT’ boxes. When the formulae are given in the Formula booklet, there will be an icon: if this icon is not present, then the formulae are not in the Formula booklet and you may need to learn them or at least know how to derive them.

Worked examples

Each worked example is split into two columns. On the right is what you should write down. Sometimes the example might include more detail than you strictly need, but it is designed to give you an idea of what is required to score full method marks in examinations. However, mathematics is about much more than examinations and remembering methods. So, on the left of the worked examples are notes that describe the thought processes and suggest which route you should use to tackle the question. We hope that these will help you with any exercise questions that differ from the worked examples. It is very deliberate that some of the questions require you to do more than repeat the methods in the worked examples. Mathematics is about thinking!
Signposts

There are several boxes that appear throughout the book.

Theory of knowledge issues

Every lesson is a Theory of knowledge lesson, but sometimes the links may not be obvious. Mathematics is frequently used as an example of certainty and truth, but this is often not the case. In these boxes we will try to highlight some of the weaknesses and ambiguities in mathematics as well as showing how mathematics links to other areas of knowledge.

From another perspective

The International Baccalaureate® encourages looking at things in different ways. As well as highlighting some international differences between mathematicians these boxes also look at other perspectives on the mathematics we are covering: historical, pragmatic and cultural.

Research explorer

As part of your course, you will be asked to write a report on a mathematical topic of your choice. It is sometimes difficult to know which topics are suitable as a basis for such reports, and so we have tried to show where a topic can act as a jumping-off point for further work. This can also give you ideas for an Extended essay. There is a lot of great mathematics out there!

Exam hint

Although we would encourage you to think of mathematics as more than just learning in order to pass an examination, there are some common errors it is useful for you to be aware of. If there is a common pitfall we will try to highlight it in these boxes. We also point out where graphical calculators can be used effectively to simplify a question or speed up your work.

Fast forward / rewind

Mathematics is all about making links. You might be interested to see how something you have just learned will be used elsewhere in the course, or you may need to go back and remind yourself of a previous topic. These boxes indicate connections with other sections of the book to help you find your way around.

How to use the questions

The colour-coding

The questions are colour-coded to distinguish between the levels.

Black questions are drill questions. They help you practise the methods described in the book, but they are usually not structured like the questions in the examination. This does not mean they are easy, some of them are quite tough.
How to use this book

Each differently numbered drill question tests a different skill. Lettered subparts of a question are of increasing difficulty. Within each lettered part there may be multiple roman-numeral parts ((i), (ii), ...), all of which are of a similar difficulty. Unless you want to do lots of practice we would recommend that you only do one roman-numeral part and then check your answer. If you have made a mistake then you may want to think about what went wrong before you try any more. Otherwise move on to the next lettered part.

- **Green questions** are examination-style questions which should be accessible to students on the path to getting a grade 3 or 4.
- **Blue questions** are harder examination-style questions. If you are aiming for a grade 5 or 6 you should be able to make significant progress through most of these.
- **Red questions** are at the very top end of difficulty in the examinations. If you can do these then you are likely to be on course for a grade 7.
- **Gold questions** are a type that are not set in the examination, but are designed to provoke thinking and discussion in order to help you to a better understanding of a particular concept.

At the end of each chapter you will see longer questions typical of the second section of International Baccalaureate® examinations. These follow the same colour-coding scheme.

Of course, these are just guidelines. If you are aiming for a grade 6, do not be surprised if you find a green question you cannot do. People are never equally good at all areas of the syllabus. Equally, if you can do all the red questions that does not guarantee you will get a grade 7; after all, in the examination you have to deal with time pressure and examination stress!

These questions are graded relative to our experience of the final examination, so when you first start the course you will find all the questions relatively hard, but by the end of the course they should seem more straightforward. Do not get intimidated!

We hope you find the Sets, Relations and Groups Option an interesting and enriching course. You might also find it quite challenging, but do not get intimidated, frequently topics only make sense after lots of revision and practice. Persevere and you will succeed.

The author team.
Introduction

In this Option you will learn:

- about sets and notation for their description, size, exclusions and subsets
- about operations on sets and the qualities of closure, associativity, commutativity and distributivity for operations
- the concept of identity and inverse elements for a given operation
- set operations of union, intersection, set difference and symmetric difference, and the interactions between them
- the Cartesian product of two sets and how to interpret ordered pairs
- about relations as subsets of Cartesian products, the concepts of domain and range for a relation and the qualities of reflexivity, symmetry and transitivity for relations
- equivalence relations, equivalence classes and the specific example of numerical congruence modulo $n$ as an equivalence relation on integers
- about functions as restricted examples of relations, the concepts of domain, range and codomain for a function and the qualities of injectivity, surjectivity and bijectivity for functions
- composition of functions, the inverse of a bijective function and how to determine these
- the four axioms of a group and the additional requirement for an Abelian group
- about cyclic groups and their generator elements
- Lagrange’s Theorem and its corollaries which show how the order of a group can be used to provide information on the orders of elements and subgroups
- about the structures of small groups; specifically cyclic groups, the Klein 4-group and the dihedral group $D_3$
- examples of groups: Functions, symmetries of plane figures and permutations
- about homomorphisms as functions between groups of identical structure which preserve operations; isomorphisms as bijective homomorphisms.

Introductory problem

An automated shuffling machine splits a deck of $n$ cards in half; if $n$ is odd it leaves the extra card in the lower half. It then inverts the lower half and exactly interleaves the two, so that an ordered deck of cards labelled 1, 2, 3, ..., $n$ would, after one shuffle, be in the order $n$, 1, $(n - 1)$, 2, $(n - 2)$, 3, ...
The machine is used on a deck of seven cards.

After how many shuffles would the deck have returned to its original order?

Would it be possible to use the machine to exactly reverse a deck of $n$ cards? If so, for what values of $n$?
In your mathematical studies so far you have learned to take a great many arithmetic rules for granted. Many of these may not have been justified in a meaningful way other than ‘this is just how it works’.

Why, for example, is it logical that $0! = 1$?

Why is it that when adding or multiplying numbers, the order of values is irrelevant (so that $a + b = b + a$ and $a \times b = b \times a$) while for division and subtraction, reversal of order fundamentally alters the result? You also know that in vector multiplication, order does not affect the result of a scalar product, but does impact upon the vector product.

Is there some classification that separates those operations which are or are not affected in this way?

In group theory, we consider mathematical operations in a more abstract way and establish rules and connections between different types of operation. In doing so, it is possible to find links between different types of problem and to transfer conclusions from one branch of mathematics to another.
2 Sets and operations

Since you should have already done some work on sets and Venn diagrams as part of the core syllabus, much of the material in this chapter will be familiar. However, you will see that here we take a slightly different approach as we develop notions of the abstract structure and rules governing sets; the notation is the same, but the use is often more precise.

We shall use this first chapter of the option to familiarise ourselves both with this more structured approach and with the style of proof and working which we shall employ. You will need a clear understanding of the principle of proof by contradiction, which was explained in chapter 1. You may also wish to revise the method of proof by induction that you learned as part of the core syllabus.

2A Defining sets

You should already be familiar with sets and set notation. We shall revise them below, before we apply more formal logic in this option.

A set is a well-defined collection of items; items in a set are referred to as the elements (also sometimes called members) of the set.

The general notation to describe a set by listing its elements is to use braces { } and comma separation. Order is not relevant (though it is useful to list elements in a standard order) and each different element is listed only once.

For example, we could define the sets $A$, $B$ and $C$ by:

$$A = \{1, 2, 3, 4, 5\}$$
$$B = \{1, 3, 5, 2, 4\}$$
$$C = \{5, 4, 3, 2, 1\}$$

Since all contain the same elements, they are equal, each being the set of integers between 1 and 5 inclusive. The order given for $A$ is, of course, the one usually used.
The symbol $\in$ indicates membership of a particular set, while $\notin$ indicates that an item is not an element of a set. For example:

$$1 \in \{1,2,3,4,5\}$$

$$6 \notin \{1,2,3,4,5\}$$

Rather than listing all elements exhaustively, we can also define a set by description:

- \{colours in the US flag\} would indicate the set consisting of the colours red, white and blue
- \{factors of 6\} is the set containing the values 1, 2, 3 and 6.

Alternatively, we can define a set by referring to a predefined set and then imposing restrictions. The restrictions are listed after a colon or vertical bar, using a structure called 'set builder notation'.

Using the set $A = \{1,2,3,4,5\}$, \{x $\in$ A : x is not a factor of 6\} means the set of all elements $x$ in $A$ such that $x$ is not a factor of 6, that is \{4,5\}.

\{x $\in$ A $|$ x$^2$ $\notin$ A\} means the set of elements $x$ of $A$ such that $x^2$ is an element of $A'$, that is \{1,2\}.

You may see either a colon or a vertical bar used in the IB exam questions and in other texts, but in this option a vertical bar will always be used (for consistency).

Exclusions from a set can also be listed, using the slash symbol:

$A \setminus \{1,3\}$

means 'all elements of set $A$, excluding values 1 and 3', that is \{2, 4, 5\}.

**Enumerating a set**

A set with a finite number of elements is termed a 'finite set'. The number of elements of a set $A$ is denoted $n(A)$ or $|A|$, and referred to as the **power, size or cardinality** of set $A$. A set with an infinite number of elements is termed an 'infinite set'.

**Standard number sets**

You should already be familiar with several standard number sets, all of which are infinite:

| $\mathbb{N}$ | represents the set of all Natural numbers | $\mathbb{N} = \{0,1,2,3,\ldots\}$ |
| $\mathbb{Z}$ | represents the set of all Integers | $\mathbb{Z} = \{0,\pm1,\pm2,\pm3,\ldots\}$ |
| $\mathbb{Q}$ | represents the set of all Rational numbers | $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}$ |
| $\mathbb{R}$ | represents the set of all Real numbers |
| $\mathbb{C}$ | represents the set of all Complex numbers | $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$ |
Some texts will define $\mathbb{N}$ without the element zero, but the definition given above is that adopted by the IB.

The set of real numbers cannot easily be written as a list or structure, but can be considered as the set of all values that can be expressed as either terminating or non-terminating decimals.

The Venn diagram below illustrates that each of the five number sets lies entirely within the set(s) below it in the table.

We use a superscript $^+$ to indicate the positive values within a set (so that $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$). You may see in other texts $^\ast$ or $^\times$ used to indicate a number set lacking zero (so that $\mathbb{Z} \setminus \{0\}$ could be alternatively written as $\mathbb{Z}^\ast$ or $\mathbb{Z}^\times$), but we shall not use this notation.

Remember that we use square brackets to indicate intervals on the real line, so that $\{x \in \mathbb{R} \mid a \leq x \leq b\}$ can be written as $[a, b]$ and $\{x \in \mathbb{R} \mid a < x < b\}$ is $(a, b]$.

**Universal and empty sets**

In any given problem involving sets, there will be a limit on which elements are being considered; the set of all these elements is called the **universal set**, denoted as $U$. The universal set may be explicitly defined or may be implicit from context; for example, if a question relates to the factors of integers, it will be clear that $U = \mathbb{Z}^+$. Once the universal set is defined, no elements outside the universal set are considered when listing elements of a set. For example, if we define $U = \{x \in \mathbb{Z} \mid 0 \leq x < 10\}$ then the set $E$ of all even numbers will be $E = \{0, 2, 4, 6, 8\}$. It is not necessary to repeat that we are only interested in integers between 0 and 9 inclusive.

In a Venn diagram, the universal set is indicated by a rectangle which contains any other sets.
A set containing no elements at all is termed the ‘empty set’, and is given by the symbol $\emptyset$:

$$\emptyset = \{ \}$$

**Complementary sets**

Once the universal set is established, every set $A$ has a **complement** set $A'$ within $U$, containing all values in $U$ which are not present in $A$.

$$A' = U \setminus A$$

Necessarily, all elements of $U$ lie exclusively either in $A$ or in $A'$, but never in both.

**Subsets**

If all the elements of a set $A$ are also elements of a set $B$, then $A$ is termed a **subset** of $B$ and $B$ is a **superset** of $A$, written $A \subseteq B$ and $B \supseteq A$, respectively.

If $A \subseteq B$ and there are elements of $B$ which are not present in $A$, then $A$ is a **proper subset** of $B$, written $A \subset B$.

Thus:

$$\{1,2,3\} \subset \{1,2,3,4,5\}$$

$$\{1,2,3\} \subset \{1,2,3,4,5\}$$

$$\{1,2,3\} \subset \{1,2,3\}$$

But:

$$\{1,2,3\} \not\subset \{1,2,3\}$$

$$\{1,2,3\} \not\subset \{1,3,5\}$$

Clearly for any two sets $A$ and $B$, if each is a subset of the other then neither contains any element missing from the other, and hence they must be equal.

*A’ is also sometimes termed the absolute complement to distinguish it from the concept of 'relative complement', which we shall meet in Section 2C of this Option.*
KEY POINT 2.1

\[ A \subseteq B \text{ and } B \subseteq A \text{ if and only if } A = B \]

This fact is frequently used to prove equality of sets. By establishing that any element of B must be an element of A so that \( B \subseteq A \), and also that any element of A must be an element of B so that \( A \subseteq B \), we can demonstrate that A and B are equal.

The empty set is technically a subset of every set. For any set C, \( \emptyset \) fulfils the rule ‘every element of \( \emptyset \) is an element in C’. Similarly, set C is also considered a subset of itself.

Both \( \emptyset \) and C itself are termed ‘trivial subsets’ of C.

So far, we have considered examples of sets whose elements are colours and numbers. It is important to realise that the elements of a set can be any type of object. Importantly, and very usefully, we can consider sets whose elements are also sets.

Worked example 2.1

The set of all possible subsets of a set A is called the power set of A, denoted \( \mathcal{P}(A) \).

Set \( A = \{1,2,3\} \). List the elements of \( \mathcal{P}(A) \).

List the elements systematically by size. Don’t forget the two trivial subsets

\[ \mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \} \]

Notice that in Worked example 2.1, we see the empty set \( \emptyset \) shown as an element of \( \mathcal{P}(A) \). Is it a useful concept to talk about sets containing empty sets?

Exercise 2A

1. List the elements of the sets:
   (a) (i) \( \{a,b,c,d\} \)
      (ii) \( \{2,4,6,8\} \)
   (b) (i) \{vowels in the English alphabet\}
      (ii) \{single digit prime numbers\}
   (c) (i) \( \{x \in \mathbb{N} | x < 5\} \)
      (ii) \( \{x \in \mathbb{R} | x^2 = 4\} \)
2. State the cardinality of the following sets:
   (a) (i) \( \{a, b, c, d\} \)
   (ii) \( \{x, y\} \)
   (b) (i) \( \emptyset \)
   (ii) \( \{\emptyset\} \)
   (c) (i) \{pitches in a chromatic scale\}
   (ii) \{US states\}
   (d) (i) \( \{x \in \mathbb{N} \mid x < 7\} \)
   (ii) \( \{x \in \mathbb{Z} \mid x < 7\} \)
   (e) (i) \( \{x \in \mathbb{Z}^+ \mid \text{lcm}(x, 6) < 20\} \)
   (ii) \( \{x \in \mathbb{Z} \mid x^2 - 8 \leq x\} \)

3. For each of the following sets, state if it is a proper subset of:
   (i) \( \mathbb{N} \)
   (ii) \( \mathbb{Z} \)
   (iii) \( \emptyset \)
   (iv) \( \mathbb{R} \)
   (a) \( \{1, 3, 5\} \)
   (b) \( \{x : x^2 > -1\} \)
   (c) \( \{x + 1 \mid x \in \mathbb{N}\} \)
   (d) \( \left\{ \frac{1}{x} : x \in \mathbb{Z} \setminus \{0\} \right\} \)

4. For each of the following, state whether \( A \subset B, A \supset B \) or \( A = B \). If one is a proper subset of the other, give an example of an element present in the superset and absent from the subset.
   (a) \( A = \mathbb{N}, B = \mathbb{Z} \)
   (b) \( A = \{x^2 \mid x \in \mathbb{N}\}, B = \{x^2 \mid x \in \mathbb{Z}\} \)
   (c) \( A = \mathbb{R}^+, B = \{q^r \mid q \in \mathbb{Q}^+, r \in \mathbb{Q}\} \)
   (d) \( A = \emptyset, B = \{\emptyset\} \)

5. Using the definition given in Worked example 2.1, for each of the following sets \( A \), write down the power set \( \mathcal{P}(A) \):
   (a) \( A = \{0, 1\} \)
   (b) \( A = \{a, b, c, d\} \)

6. Using the definition given in Worked example 2.1, prove that for any finite set \( A \) for which \( n(A) = k \), \( n(\mathcal{P}(A)) = 2^k \).
2B Operations

A binary operation on a set is a well-defined rule for combining two elements of the set to produce a unique result, which may or may not also be an element of the set.

You already know some operations from basic arithmetic, such as addition, subtraction, multiplication, division and exponentiation. We use the symbols $+, - , \times$ and $\wedge$ respectively to indicate each of these operations. When applying an operation to two elements $x$ and $y$ of our number set, we write the operation symbol between its two input values (called operands or arguments):

$$x + y$$
$$x - y$$
$$x \times y$$
$$x \div y$$
$$x \wedge y$$

So far this is familiar, although we are more accustomed to seeing $x \wedge y$ written as $x^y$.

When considering operations in the abstract, we shall generally use non-specific symbols such as $\ast$ and $\circ$ to represent an operation, and define the rules of the operation separately. Where an operation is closely related to one of the standard arithmetic operations, we frequently denote the operation by circling the arithmetic symbol: for example $\oplus$ and $\otimes$.

You know some operations which use only one element (unary operations, such as 'factorial'). There are also operations taking three or more elements; study of these does not come within the syllabus for this option, though you should consider how the rules and considerations given below might be adapted for unary or ternary (three element) operations.

For simplicity we shall from now on refer only to 'operations' rather than 'binary operations'.

Closure

Let us consider the five operations given above when used in the set $\mathbb{Z}^+$. We notice that, although $x \ast y \in \mathbb{Z}^+$ for all $x, y \in \mathbb{Z}^+$ when $\ast$ represents addition, the same is not true when $\ast$ represents subtraction; for example, $2 - 3 \notin \mathbb{Z}^+$. In fact, we can only be fully confident that $x \ast y$ will always be an element of $\mathbb{Z}^+$ for addition, multiplication and exponentiation.

We describe this formally by saying:

' $\mathbb{Z}^+$ is closed under addition, multiplication or exponentiation.'

' $\mathbb{Z}^+$ is not closed under subtraction or division.'
KEY POINT 2.2

For an operation $\ast$ on a set $S$, $S$ is said to be **closed** under $\ast$ if $x \ast y \in S$ for all $x, y \in S$.

Note that the closure property requires this to hold for all elements. It only takes a single exception for closure to be lost.

**Worked example 2.2**

Which of the following sets is closed under the given operation?

(a) $\mathbb{Z}$ under multiplication ($\times$)
(b) $\mathbb{R}$ under division ($\div$)
(c) $\mathbb{Q}\setminus\{0\}$ under division ($\div$)
(d) $\mathbb{Q}^+$ under exponentiation ($^\ast$)
(e) $\mathbb{Z}$ under subtraction ($-$)
(f) $\{-1,0,1\}$ under multiplication ($\times$)

Establish that $x \ast y \in S$ for all $x, y \in S$ or give a counter-example to prove non-closure

(a) Closed: the product of two integers is also an integer
(b) Not closed: $a \div C \notin \mathbb{R}$ for all $a \in \mathbb{R}$
(c) Closed: the ratio of any two non-zero rational values is also a non-zero rational value
(d) Not closed: for example, $2 \times \frac{1}{2} \notin \mathbb{Q}^+$
(e) Closed: the difference of two integers is also an integer
(f) Closed: the product table for this three-element set under multiplication is

<table>
<thead>
<tr>
<th></th>
<th>-1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Notice that the most direct approach to answering part (f) of Worked example 2.2 was to show all the possible results of the operation in a table as there was a (very small) finite set of elements. This is an example of a 'Cayley table', named after mathematician Arthur Cayley.
For an operation \( \ast \) on a finite set \( S = \{a_1, a_2, \ldots, a_n\} \), the Cayley table is laid out as follows:

\[
\begin{array}{cccc}
  a_1 & a_2 & \cdots & a_n \\
  a_1 \ast a_1 & a_1 \ast a_2 & \cdots & a_1 \ast a_n \\
  a_2 \ast a_1 & a_2 \ast a_2 & \cdots & a_2 \ast a_n \\
  \vdots & \vdots & \ddots & \vdots \\
  a_n \ast a_1 & a_n \ast a_2 & \cdots & a_n \ast a_n \\
\end{array}
\]

Each cell of the grid is the result of the operation taking its first operand from the row title and its second operand from the column title.

**Worked example 2.3**

Operators \( \ast \) and \( \circ \) are defined on the set \( S = \{0,1,2,3\} \) by

\[
a \ast b = a^{a+b} \quad b \ast a = \frac{1}{2} (a - 2b + |2b - a|).
\]

Draw out the Cayley tables for \( \ast \) on \( S \) and \( \circ \) on \( S \), and state whether each is closed.

For each cell, combine the row title with the column title according to the formula given. So, for example

\[
0 \ast 2 = 0^{0+2} - 2^{0} = 0 - 2 = -2
\]

**Complete the Cayley table.**

The set is closed under the operation if all elements in the cells of the table are elements of the original set.

A single example is sufficient to demonstrate an operation is not closed.

As shown in the table, \( \ast \) is not closed on \( S \); for example, \( 0,1 \in S \) but \( 0 \ast 1 \notin S \)

As shown in the table, \( \circ \) is closed on \( S \), since \( a \circ b \in S \) for all \( a, b \in S \).
Commutativity

We know that for the operations addition and multiplication, the order of the two operands makes no difference to the result, whether we are using elements from \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) or \( \mathbb{C} \).

\[
\begin{align*}
    x + y &= y + x \quad \text{for all } x, y \\
    x \times y &= y \times x \quad \text{for all } x, y
\end{align*}
\]

Subtraction, division and exponentiation do not have this property, since the order cannot be reversed for every pair of elements in the number set.

Any operation for which the order of operands chosen makes no difference to the result is said to be **commutative** in that set.

**KEY POINT 2.4**

An operation \( \star \) on a set \( S \) is said to be commutative in \( S \) if

\[
x \star y = y \star x \quad \text{for all } x, y \in S.
\]

If the row and column titles of a Cayley table are laid out in the same order then, for a commutative operation, that table will be symmetrical about the leading diagonal.

**Worked example 2.4**

Which of the following operations is commutative for the given set?

(a) \( x \star y \) is defined in \( \mathbb{Z} \) as \( x \star y = xy + x + y \)

(b) \( x \circ y \) is defined in \( \mathbb{R} \) as \( x \circ y = 2^x - 2^y \)

(c) \( x \mathbin{\hat{\Delta}} y \) is defined in \( \{1, 2, 3, 4, 5\} \) as \( x \mathbin{\hat{\Delta}} y = 2 \times \min(x, y) - \max(x, y) \)

**Demonstrate** \( x \star y = y \star x \) or find a counter-example

**Demonstrate** \( x \circ y = y \circ x \) or find a counter-example

**Demonstrate** \( x \mathbin{\hat{\Delta}} y = y \mathbin{\hat{\Delta}} x \) or find a counter-example

(a) Commutative

\[
\begin{align*}
    x \star y &= xy + x + y \\
    &= yx + y + x \\
    &= y \star x
\end{align*}
\]

(b) Not commutative. For example,

\[
\begin{align*}
    2^1 \mathbin{\hat{\Delta}} 2^2 &= 2^1 - 2^2 = 2 \\
    2^2 \mathbin{\hat{\Delta}} 2^1 &= 2^2 - 2^1 = -2
\end{align*}
\]

(c) Commutative

\[
\begin{align*}
    x \mathbin{\hat{\Delta}} y &= 2 \times \min(x, y) - \max(x, y) \\
    &= 2 \times \min(y, x) - \max(y, x) \\
    &= y \mathbin{\hat{\Delta}} x
\end{align*}
\]
Identity element

An identity element for a given operation has the property that it leaves unchanged every other element in the given set under the operation. The identity element for an arbitrary operation is usually represented by the letter $e$. (Note that this is different from the real constant, $e \approx 2.718\ldots$)

**KEY POINT 2.5**

For an operation $*$ on a set $S$, an element $e$ is said to be the identity element if it is both a left-identity and a right-identity for the operation in $S$:

$e \ast x = x \ast e = x$ for all $x \in S$

The row of the identity element $e$ in the Cayley table will match the title row, and the column of $e$ will match the title column.

Not every operation on a set will have an identity element within the set, and some operations may not have an identity element at all.

**EXAM HINT**

If the operation is not commutative, we must check both that $e \ast x = x$ and also that $x \ast e = x$ for all $x$. For an operation $*$ on a set $S$, an element $e_1 \in S$ is said to be a left-identity element if $e_1 \ast x = x$ for all $x \in S$. For an operation $*$ on a set $S$, an element $e_2 \in S$ is said to be a right-identity element if $x \ast e_2 = x$ for all $x \in S$. It is perfectly possible for an operation to have several left-identity elements and right-identity elements, but there can only be one two-sided identity element.

**Worked example 2.5**

Prove that an operation $*$ in a set $S$ can have at most one identity element.

Proof by contradiction:

Suppose that there are two such elements $e_1, e_2 \in S$.

Demonstrate logically that they must be exactly equal.

Suppose $e_1, e_2 \in S$ are both identity elements for $*$ in $S$.

Then $e_1 \ast e_2 = e_1$ (1)

because $e_2$ is an identity

and $e_1 \ast e_2 = e_2$ (2)

because $e_1$ is an identity

$\Rightarrow e_1 = e_2$ (from (1) and (2))

$\therefore$ There can never be two distinct identity elements for an operation in a given set.
Worked example 2.6

For each of the following operations, determine the identity element, if there is one, within the given set.

(a) Multiplication in $\mathbb{R}$
(b) Addition in $\mathbb{Z}$
(c) $\dagger$ in $\{3, 4, 5, 6, 7\}$ where $\dagger$ is given by $x \dagger y = \max(x, y)$
(d) $\ast$ in $\mathbb{Q}$ where $\ast$ is given by $x \ast y = y$

Find an identity or demonstrate that no such element can exist

(a) $e = 1$
\[1 \times x = x \times 1 = x \text{ for all } x \in \mathbb{R}\]
(b) $e = 0$
\[U + x = x + U = x \text{ for all } x \in \mathbb{Z}\]
(c) $e = 3$
Since $x \geq 3$ for all $x \in \{3, 4, 5, 6, 7\}$,
\[\Rightarrow 3 \dagger x = x \dagger 3 = x \text{ for all } x \in \{3, 4, 5, 6, 7\}\]
(d) No identity element
Every element in the set is a left-identity, but there is no right-identity, and hence no identity element.
Proof by contradiction:
Suppose there is an identity element $e$.
There are at least two elements in $\mathbb{Q}$; hence there exists an element $a \in \mathbb{Q}, a \neq e$
\[a \ast e = e \text{ by the definition of } \ast\]
\[\Rightarrow a \neq e \text{ since } e \neq a\]
This contradicts the right-identity requirement on $e$.
There is no identity element

Inverse elements

If a given operation $\ast$ in a set $S$ has an identity, then we can also introduce the concept of inverse elements.

KEY POINT 2.6

For an operation $\ast$ on a set $S$ with identity $e$, an element $y \in S$ is said to be the inverse of $x \in S$ if $x \ast y = y \ast x = e$.
In such a case, $y$ may be written as $x^{-1}$.

We must take care. We are now considering abstract operations; the superscript ‘$-1$’ should not be interpreted as an exponent in the normal arithmetic sense.

Take for example the set $\mathbb{Z}$ under addition. As demonstrated in Worked example 2.6, the identity for addition (called the additive identity) is 0.
So for \( a \) to be the inverse of 2, we require that \( 2 + a = a + 2 = 0 \).

Hence, under the operation addition in \( \mathbb{Z} \), \( 2^{-1} = -2 \), a statement that in other contexts would seem utterly false!

More generally, in \( \mathbb{Z} \) under addition, \( x^{-1} = -x \) for all \( x \in \mathbb{Z} \).

Not all elements need have an inverse within the set.

For example, in \( \mathbb{R} \) under multiplication, the identity element is 1 (the multiplicative identity) so for every element \( x \in \mathbb{R} \) with \( x \neq 0 \), \( x^{-1} = \frac{1}{x} \).

However, the element 0 has no inverse, as there is no element in \( \mathbb{R} \) whose product with 0 is 1.

**Worked example 2.7**

(a) Find the inverse, if it exists, of 3 in \( \mathbb{Q} \) under multiplication.

(b) Find the inverse, if it exists, of 7 in \( \mathbb{N} \) under \( \dagger \), where \( \dagger \) is given by \( x \dagger y = \max(x, y) \).

(c) Find the inverse of \( x \) in \( \mathbb{N} \) under \( \ast \), where \( \ast \) is given by \( x \ast y = x + y \) and state which values of \( x \) have no inverse under \( \ast \).

(d) Find the inverse of \( x \) in \( \mathbb{R} \) under \( \ast \), where \( \ast \) is given by \( x \ast y = x + y + x + y \) and state which values of \( x \) have no inverse under \( \ast \).

**First find the identity element for the operation. Standard identities (multiplicative and additive) may be quoted. Others should be established.**

**State and prove an inverse.**

**Find the identity element for the operation.**

**Either state and prove an inverse, or demonstrate rigorously the absence of any possible inverse.**

(a) **Multiplicative identity \( e = 1 \)**

\[
\frac{1}{3} \times \frac{1}{3} = \frac{1}{3} \times \frac{1}{3} = 1 \\
\therefore \frac{1}{3}^{-1} = \frac{1}{3}
\]

(b) \( \max(x, 0) = \max(0, x) = x \) for all \( x \in \mathbb{N} \)

\[ \Rightarrow e = 0 \]

\[ \max(x, 7) \geq 7 \text{ for all } x \in \mathbb{N} \]

\[ \therefore \text{there is no element } x \in \mathbb{N} \text{ such that } \max(x, 7) = 0 \]

\[ \text{there is no inverse for the element 7} \]

(c) \( x \ast 0 = x \ast x = x \) for all \( x \in \mathbb{N} \)

\[ \Rightarrow e = 0 \]

Let \( y = x^{-1} \) under \( \ast \)

\[ \Rightarrow x \ast y = y \ast x = 0 \]

\[ \Rightarrow \max(x, y) = 0 \]

\[ \Rightarrow y = x \]

\[ \therefore x^{-1} = x \text{ for all } x \in \mathbb{N} \]
Notice that in Worked example 2.7c, we found that every element was equal to its own inverse; that is, every element in the set is 'self-inverse'.

**KEY POINT 2.7**

For an operation $*$ on a set $S$ with identity $e$, an element $x \in S$ is said to be **self-inverse** if $x * x = e$.

**Associativity**

Consider adding three numbers together:

$$4 + 3 + 1$$

We have two operations to perform (both addition). Does it matter which we choose first? In other words, will we get a different answers from $(4 + 3) + 1$ and $4 + (3 + 1)$?

We know that the answer is no, and so we are quite happy to write the original expression using no brackets at all.

However, in the case of subtraction, we do get different results from $(4 - 3) - 1$ and $4 - (3 - 1)$.

We say that an operation applied repeatedly in this way is **associative** if the position of parentheses makes no difference and 'not associative' if parentheses are significant.

Addition is associative in $\mathbb{R}$, and we can simply drop the parentheses and write:

$$x + y + z$$

when adding three elements together.

Subtraction is not associative in $\mathbb{R}$, because parentheses are required to specify which calculation is to be performed first.

**KEY POINT 2.8**

An operation $*$ on a set $S$ is said to be associative in $S$ if and only if $x * (y * z) = (x * y) * z$ for all $x, y, z \in S$. 

(d) $x * U = U * x = x$ for all $x \in \mathbb{R}$

$\Rightarrow e = 0$

Let $y = x^{-1}$ under $*$

$\Rightarrow x * y = y * x = 0$

$\Rightarrow x * y + x + y = 0$

$\Rightarrow y(x + 1) = -x$

$\Rightarrow y = \frac{-x}{x + 1}$ when $x \neq -1$

Since no such element exists in $\mathbb{R}$ when $x = -1$, every element except $-1$ has an inverse under $*$. 
If an operation is associative, the position of brackets makes no difference to the end result. We can, for simplicity, not write them at all:

\[ x \ast (y \ast z) = (x \ast y) \ast z = x \ast y \ast z \]

In particular, it is convenient to use the shorthand form

\[ x \ast x = x^2 \]
\[ x \ast x \ast x = x^3 \]
\[ x \ast x \ast \ldots \ast x = x^n \]

_in terms_.

---

**Worked example 2.8**

Which of the following operations is associative in the given set?

(a) \( x \ast y \) is defined in \( \mathbb{Z} \) as \( x \ast y = xy + x + y \)

(b) \( x \ast y \) is defined in \( \mathbb{R} \) as \( x \ast y = 2^x - 2^y \)

(c) \( x \ast y \) is defined in \( \{1, 2, 3, 4, 5\} \) as \( x \ast y = 2 \times \min(x, y) - \max(x, y) \)

---

Demonstrate \( x \ast (y \ast z) = (x \ast y) \ast z \) or find a counter-example

(a) Associative

\[ x \ast (y \ast z) = x \ast (yz + y + z) = x(yz + y + z) + x + y + z \]

(b) Not associative: for example,

\[ 1 \ast (2 \ast 3) = 1 \ast (2^1 - 2^3) = 1 \ast -6 \]
\[ (1 \ast 2) \ast 3 = (2^1 - 2^3) - 2^3 = -8 \]

(c) Not associative: for example,

\[ 1 \ast (5 \ast 5) = 1 \ast (2 \times \min(5, 5) - \max(5, 5)) = -1 \ast 5 \]
\[ (1 \ast 5) \ast 5 = (2 \times \min(1, 5) - \max(1, 5)) \ast 5 = -3 \ast 5 \]
Be aware that the indices \( \omega^2, \omega^3 \) and \( \omega^n \) used here are not necessarily the same as exponents in arithmetic, which specifically indicate repeated applications of multiplication.

However, the following familiar rules of exponents do still hold.

**KEY POINT 2.9**

For an associative operation \( \ast \) acting on a set \( S \) with \( x, y \in S \) and for any positive integers \( m \) and \( n \):

\[
\begin{align*}
\ast^m \ast^m &= \ast^{m+n} \\
(x^m)^n &= x^{mn}
\end{align*}
\]

If the inverse element \( x^{-1} \) exists:

\[
x^{-n} = (x^n)^{-1}
\]

However, only if \( \ast \) is commutative can we assert that:

\[
x^m \ast y^n = (x \ast y)^n
\]

Finally we can consider the interaction of two different operations.

**Distributivity**

Put simply, this is the quality which allows us to expand brackets. More formally:

**KEY POINT 2.10**

For two operations \( \ast \) and \( \circ \) acting on a set \( S \), \( \ast \) is **distributive** over \( \circ \) if \( x \ast (y \circ z) = (x \ast y) \circ (x \ast z) \) for all \( x, y, z \in S \).

You are already familiar with an example of this property in basic algebra:

In all standard number sets, multiplication is distributive across addition, since:

\[
x \ast (y + z) = (x \ast y) + (x \ast z)
\]

However, the reverse is not true. Addition is not distributive across multiplication, since we cannot say that:

\[
x + (y \ast z) = (x + y) \ast (x + z)
\]
Worked example 2.9

For which of the following operations is \( \ast \) distributive over \( \circ \)?

(a) In \( \mathbb{R} \): \( x \ast y = x(y + 1) \), \( x \circ y = x - y \)
(b) In \( \mathbb{Z} \): \( x \ast y = \max(x, y) \), \( x \circ y = x + y \)
(c) In \( \mathbb{Q} \): \( x \ast y = 3xy \), \( x \circ y = 2x - y \)

Evaluate \( x \ast (y \circ z) \) and \( (x \ast y) \circ (x \ast z) \).

\[
(\ast) \quad x \ast (y \circ z) = x \ast (y - z) \\
\quad \quad = x(y - z + 1) \\
\quad \quad = xy - x + x \\
\quad \quad = xy - xz + x \\
(x \ast y) \circ (x \ast z) = (x + y) \circ (xz + x) \\
\quad \quad = xy + x - (xz + x) \\
\quad \quad = xy - xz + x \\
\quad \quad \Rightarrow x \ast (y \circ z) \neq (x \ast y) \circ (x \ast z) \text{ only if } x = 0 \\
\quad \quad \Rightarrow \ast \text{ is not distributive over } \circ \text{ in } \mathbb{R}
\]

(b) \( x \ast (y \circ z) = x \ast (y + z) \\
\quad \quad = \max(x, y + z) \\
(x \ast y) \circ (x \ast z) = \max(x, y) \circ \max(x, z) \\
\quad \quad = \max(x, y) + \max(x, z)

Take \( x = 3, y = 2, z = 1 \):
\[
\ast \cdot (2 \ast 1) = 3 \\
(3 \ast 2) \ast (2 \ast 1) = 3 + 3 = 6 \\
\therefore 3 \ast (2 \ast 1) \neq (3 \ast 2) \ast (2 \ast 1) \\
\Rightarrow \ast \text{ is not distributive over } \circ \text{ in } \mathbb{Z}
\]

(c) \( x \ast (y \circ z) = x \ast (zy - z) \\
\quad \quad = 6xy - 3xz \\
(x \ast y) \circ (x \ast z) = (3xy) \circ (3xz) \\
\quad \quad = 6xy - 3xz \\
\therefore x \ast (y \circ z) = (x \ast y) \circ (x \ast z) \text{ for all } x, y, z \in \mathbb{Q} \\
\Rightarrow \ast \text{ is distributive over } \circ \text{ in } \mathbb{Q}
\]

The scalar triple product of three vectors \( \mathbf{a}, \mathbf{b} \) and \( \mathbf{c} \) is given as \( \mathbf{a} \ast (\mathbf{b} \times \mathbf{c}) \). This is an example of a ternary operation as it takes three elements to produce a result. Investigate the properties of the scalar triple product, and consider how the concepts of closure, commutativity and associativity, as defined above for binary operations, might be interpreted for ternary operations.

\[ \lim_{n \to \infty} a_n = \alpha \]

\[ P(\mathbf{A} | \mathbf{B}) = P(\mathbf{A} \cap \mathbf{B}) \]

\[ \log \alpha \]
Exercise 2B

1. Binary operations * and \( \circ \) are defined in \( \mathbb{R} \) by:
   \[ x \ast y = x - y + 3, \quad x \circ y = 3 - xy \]

   (a) Find:
   (i) \( 3 \ast 2 \)   (ii) \( 7 \ast 2 \)
   (iii) \( -2 \ast 1 \)   (iv) \( -4 \circ 3 \)

   (b) (i) Show that * has no identity element.
   (ii) Show that \( \circ \) is commutative.

   (c) Solve for \( x \):
   (i) \( x \ast 2 = 6 \)   (ii) \( x \circ 2 = 7 \)

2. State which of the qualities
   (A) closure
   (B) commutativity
   (C) associativity

   apply to each of the following operations:

   (a) * in \( \mathbb{Q} \) where \( xy = \frac{x + y}{2} \)
   (b) * in \( \mathbb{Z} \) where \( xy = 3x - 2y \)
   (c) * in \( \mathbb{R} \setminus \{0\} \) where \( xy = \frac{xy}{x + y} \)
   (d) * in \( \{2^n \mid n \in \mathbb{Q}\} \) where \( xy = x + y \)

3. Where it exists, state the identity of the following and find the general form of an inverse to element \( x \):

   (a) (i) \( \mathbb{R} \) under * where \( xy = x + y + 1 \)
       (ii) \( \mathbb{R} \) under * where \( xy = 2xy \)

   (b) (i) The set of non-zero vectors of three-dimensional space under vector product.

   (ii) The set of vectors of three-dimensional space under vector addition.

   (c) (i) \( \mathbb{Q} \) under * where \( xy = \frac{|y - x|}{1 + xy} \)

   (ii) \( \mathbb{C} \setminus \{0\} \) under * where \( v \ast w = |v| \text{cis} \left( \text{arg}(w) \right) \)

4. Draw the Cayley table, determine closure and identify the identity element (if it exists) for:
   (a) \( \{0,1,2,3, \} \) under * where \( xy = |xy - x - y| \)
   (b) \( \{0,2,4,6, \} \) under * where \( xy = \frac{xy}{4} \)
   (c) \( \{7,8,9, \} \) under * where \( xy = \max(x, y) \)
5. Operations $\ast$ and $\circ$ are defined on a set $S \subseteq \mathbb{Z}$ by:

$$a \ast b = \max(a - b, b - a)$$

$$a \ast b = ab - a - b + 2$$

(a) Which of the following is true?
(i) $\ast$ is closed on $\mathbb{Z}$
(ii) $\ast$ is closed on $\mathbb{N}$
(iii) $\circ$ is closed on $\{0, 1, 2, 3\}$
(iv) $\circ$ is closed on $\mathbb{N}$

(b) Which of the following is true?
(i) $\ast$ is commutative
(ii) $\circ$ is commutative

(c) Which of the following is true?
(i) $\ast$ is associative
(ii) $\circ$ is associative

(d) Determine the identity element, if one exists, for:
(i) $\ast$ in $\mathbb{Z}^+$
(ii) $\circ$ in $\mathbb{Z}$

(e) Determine for which $x \in \mathbb{Z}$ there is an inverse $x^{-1}$ and express $x^{-1}$ in terms of $x$.
(i) $\ast$ in $\mathbb{Z}$
(ii) $\circ$ in $\mathbb{Z}$

6. Operations $\ast$ and $\circ$ are defined on $\mathbb{R}^+$ by:

$$x \ast y = xy \quad \text{and} \quad x \circ y = y^x$$

Show that $\circ$ is distributive over $\ast$.

7. For $k \in \mathbb{Z}$, the binary operation $\ast_k$ is defined for $x, y \in \mathbb{Z}^+$ by:

$$x \ast_k y = x + y + k$$

Determine whether or not $\ast_k$ is:
(a) closed
(b) commutative
(c) associative

Find:
(d) the identity element of $\ast_k$
(e) the subset of $\mathbb{Z}^+$ having an inverse under $\ast_k$

8. For an operation $\ast$ on a set $A$, an absorbing element $z$ is defined as any element such that $a \ast z = z \ast a = z$ for all $a \in A$.

(a) Prove that:
(i) There can be at most one absorbing element for an operation $\ast$.
(ii) An absorbing element can have no inverse under $\ast$. 
(b) Find an absorbing element for:
(i) \( \mathbb{Q} \) under multiplication
(ii) \( \mathbb{Z}^+ \) under gcd (greatest common divisor)
(iii) \( \mathbb{R} \) under \( * \) where \( x * y = xy - 2x - 2y + 6 \)

2C Operations on sets

Now we have some general terminology for operations, we can consider the various operations which act upon subsets of \( U \).

Union of sets

\( A \cup B \) is the union of \( A \) and \( B \), a set containing all elements of \( A \) and all elements of \( B \); for example
\[
\{1,2,3\} \cup \{1,3,5\} = \{1,2,3,5\}
\]
Notice that elements 1 and 3 were present in both sets on the left side, but are only listed once in the union because elements are not repeated within a set.

\[
A \cup B
\]

Properties of union: for any sets \( A, B, C \subseteq U \)

\[
\begin{array}{|l|}
\hline
A \cup B = B \cup A & \text{Union is commutative} \\
A \cup (B \cup C) = (A \cup B) \cup C & \text{Union is associative} \\
A \cup \emptyset = A & \emptyset \text{ is the identity for union} \\
A \cup A' = U & \text{The union of complementary sets is } U \\
\hline
\end{array}
\]

Intersection of sets

\( A \cap B \) is the intersection of \( A \) and \( B \), a set containing only those elements present in both \( A \) and \( B \); for example,
\[
\{1,2,3\} \cap \{1,3,5\} = \{1,3\}
\]

\[
A \cap B
\]
Any two sets whose intersection is the empty set are termed **disjoint** sets; for example,

\[ \{1,2,3\} \cap \{4,5\} = \emptyset \]

Hence \{1,2,3\} and \{4,5\} are disjoint sets.

Properties of intersection: for any sets \( A, B, U \subseteq U \)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A \cap B = B \cap A )</td>
<td>Intersection is commutative</td>
</tr>
<tr>
<td>( A \cap (B \cap C) = (A \cap B) \cap C )</td>
<td>Intersection is associative</td>
</tr>
<tr>
<td>( A \cap U = A )</td>
<td>( U ) is the identity for intersection</td>
</tr>
<tr>
<td>( A \cap A' = \emptyset )</td>
<td>Complementary sets are disjoint</td>
</tr>
</tbody>
</table>

Now that we have a clear definition of union and intersection, we can make a formal definition of the idea of a partition, which we introduced in Section 2A:

**KEY POINT 2.11**

The set \( A \) is **partitioned** by non-empty subsets \( B_1, B_2, \ldots \) if

\[ B_i \cap B_j = \emptyset \quad \text{for any} \quad i \neq j \] (the subsets are disjoint)

\[ B_1 \cup B_2 \cup \ldots = A \] (the union of all the subsets equals \( A \))

We have already met a very simple example of a partition: \( A \) and \( A' \) partition \( U \), as illustrated in the diagram for complementary sets in Section 2A.

Properties of distributivity for intersection and union: for any sets \( A, B, U \subseteq U \),

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) )</td>
<td>Intersection is distributive over union</td>
</tr>
<tr>
<td>( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) )</td>
<td>Union is distributive over intersection</td>
</tr>
</tbody>
</table>
Set difference

$A \setminus B$ has already been loosely described in Section 2A of this chapter; it is called the relative complement or set difference of $A$ and $B$ and can now be formally defined as:

$A \setminus B = A \cap B'$

e.g. $\{1, 2, 3\} \setminus \{1, 3, 5\} = \{2\}$

Notice that set difference is not commutative: $A \setminus B$ is not equivalent to $B \setminus A$:

e.g. $\{1, 3, 5\} \setminus \{1, 2, 3\} = \{5\}$

Some texts may use the alternative notation $A - B$, since we begin with the elements in $A$ and then remove any elements which also appear in $B$. 

Set difference

$A \setminus B = (A \cap B) \cup (A \cap C)

A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Properties of set difference: for any sets $A, B \subseteq U$

- $(A \setminus B) \cap (B \setminus A) = \emptyset$ : Reversed set differences are disjoint
- $A \setminus A = \emptyset$ : Self-difference is the empty set
- $A \setminus \emptyset = A$ : $\emptyset$ is the right-identity for set difference

Set difference is not generally commutative or associative.

**Symmetric difference**

$A \Delta B$ is the symmetric difference of $A$ and $B$, and is the set of those elements which are members of exactly one of $A$ and $B$, but do not lie in their intersection; for example,

$$\{1,2,3\} \Delta \{1,3,5\} = \{2,5\}$$

Notice that we could define this either as the union without the intersection,

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

or as the union of the two relative complements

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Properties of symmetric difference: for any sets $A, B, C \subseteq U$

- $A \Delta B = B \Delta A$ : Symmetric difference is commutative
- $A \Delta (B \Delta C) = (A \Delta B) \Delta C$ : Symmetric difference is associative
- $A \Delta \emptyset = A$ : $\emptyset$ is the identity for symmetric difference
- $A \Delta A = \emptyset$ : Every set is self-inverse under symmetric difference
Worked example 2.10

Let \( U = \{x \in \mathbb{N} | x < 8\}, \ A = \{1, 2, 3, 4, 5\} \) and \( B = \{1, 2, 4, 6\}. \)

List the elements of the following sets:

- (a) \( A' \)
- (b) \( A \setminus B \)
- (c) \( A \cup B \)
- (d) \( A \cap B \)
- (e) \( A \Delta B \)

It helps to list the elements of the universal set \( U = \{0, 1, 2, 3, 4, 5, 6, 7\} \):

- (a) \( A' = \{0, 6, 7\} \)
- (b) \( A \setminus B = \{3, 5\} \)
- (c) \( A \cup B = \{1, 2, 3, 4, 5, 6\} \)
- (d) \( A \cap B = \{1, 2, 4\} \)
- (e) \( A \Delta B = \{3, 5, 6\} \)

De Morgan’s laws

We have already seen that union and intersection are distributive over each other.

We can also show, using Venn diagrams, that the complement of an intersection is the union of complements, and that the complement of a union is the intersection of complements:

**Key point 2.12**

**De Morgan’s laws** state that:

\[
\begin{align*}
(\overline{A \cup B}) & = A' \cap B' \\
(\overline{A \cap B}) & = A' \cup B'
\end{align*}
\]

**Exam hint**

You may be asked for proofs using set algebra. In most cases, you should expect to use either De Morgan’s laws or the rules of distributivity of union and intersection, both of which can be quoted. You should never be required to prove De Morgan’s laws algebraically.
Worked example 2.11

Prove that \( A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \).

Proof that two sets equal each other:

Prove that each is a subset of the other

Take an arbitrary element in the left-hand set and show it must be an element of the right-hand set

Suppose \( x \in A \setminus (B \cup C) \)
\[ \Rightarrow x \in A \text{ and } x \notin (B \cup C) \]
\[ \Rightarrow x \in A \text{ and } x \in B' \cap C' \text{ by De Morgan's law} \]
\[ \Rightarrow x \in A \text{ and } x \in B' \text{ and } x \in C' \]
\[ \Rightarrow x \in A \text{ and } x \in A \cap (B' \cap C') \]
\[ \therefore A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C) \]

(1)

Then repeat, showing that an element of the RHS must be an element of the LHS

Suppose \( x \in (A \setminus B) \cap (A \setminus C) \)
\[ \Rightarrow x \in A \cap B' \text{ and } x \in A \cap C' \]
\[ \Rightarrow x \in A \text{ and } x \in B' \text{ and } x \in C' \]
\[ \Rightarrow x \in A \text{ and } x \in (B \cup C)' \text{ by De Morgan's law} \]
\[ \therefore (A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C) \]

(2)

Having established each is a subset of the other, we can conclude the sets are equal

\[ (1) \& (2) \Rightarrow A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \]

Worked example 2.12

Prove that for any sets \( A \) and \( B \), \( A \cup B = A \cap B \) if and only if \( A = B \).

Proofing if and only if: Prove each direction separately

Proving if and only if:

Prove each direction separately

Proof that two sets equal each other:

Prove that each is a subset of the other

Assume \( A \cup B = A \cap B \)

Proof that \( A \cup B = A \cap B \Rightarrow A = B \):

Assume \( A \cup B = A \cap B \)

Proof that \( A \cup B = A \cap B \Rightarrow A = B \):
Exercise 2C

1. If \( U = \{a, b, c, d, e, f, g, h\}, A = \{a, b, c\}, B = \{c, d, e\}, C = \{b, g, h\} \)
   (a) Find: (i) \( A \cup B \) (ii) \( A \cup C \)
       (iii) \( A \cup B' \) (iv) \( B' \cup C \)
   (b) Find: (i) \( A \cap B \) (ii) \( B \cap C \)
       (iii) \( A' \cap C \) (iv) \( A' \cap B' \cap C' \)
   (c) Find: (i) \( A \setminus B \) (ii) \( A' \setminus C \)
       (iii) \( B' \setminus C' \) (iv) \( B \cup (A' \setminus C') \)
   (d) Find: (i) \( A \Delta B \) (ii) \( A \Delta C \)
       (iii) \( A' \Delta C' \) (iv) \( (A' \Delta B') \Delta C' \)

2. Draw Venn diagrams showing \( A, B, C \subset U \), shading the area representing:
   (a) \( A \cup B \) (b) \( A \cup (C \cap B) \)
   (c) \( A \cap B \cap C' \) (d) \( A \cap (B \Delta C) \)
   (e) \( A \cup (B' \Delta A') \)
3. For an operation \( * \) on a set \( A \), a left-absorbing element \( z \) is defined as any element such that \( z \cdot a = z \) for all \( a \in A \), and a right-absorbing element \( z \) is defined as any element such that \( a \cdot z = z \) for all \( a \in A \).

For the following operations in \( U \), identify the left- and right-absorbing elements of \( U \), if they exist.
(a) Union
(b) Intersection
(c) Set difference
(d) Symmetric difference

4. Prove that for any sets \( A \) and \( B \):
\[
A \cup B = A \iff B \subseteq A
\]

5. Prove that for any sets \( A \) and \( B \):
\[
A \cap B = A \iff A \subseteq B
\]

6. Prove that for any set \( A \subseteq U \):
\[
A \Delta U = A'
\]

7. Define the operation \( * \) on the sets \( A \) and \( B \) by \( A \cdot B = A' \cup B' \).
Show algebraically that:
(a) \( A \cdot A = A' \)
(b) \( (A \cdot A) \cdot (B \cdot B) = A \cup B \)
(c) \( (A \cdot B) \cdot (A \cdot B) = A \cap B \)

8. (a) Use a Venn diagram to show that \( (A \cup B)' = A' \cap B' \).
(b) Prove that \( (A' \cup B') \cap (A \cup B) = (A' \cap B) \cup (A \cap B) \).

9. For each \( n \in \mathbb{Z}^+ \), a subset of \( \mathbb{Z}^+ \) is defined by:
\[
S_n = \{ x \in \mathbb{Z}^+ \mid n \text{ divides } x \}
\]
(a) Express in simplest terms the membership of the following sets:
(i) \( S_1 \)
(ii) \( S_2 \)
(iii) \( S_3 \cap S_2 \)
(iv) \( S_5 \setminus S_6 \)
(b) Prove that \( (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B) \).
Summary
In this chapter we formally examined the structure and rules surrounding sets, and encountered the algebraic concept of a binary operation, which combines two elements of a set under a defined rule to produce a new element.

For a set $A$:

- $B$ is a subset of $A$ if all elements of $B$ are also elements of $A$.
- $A \subseteq B$ and $B \subseteq A$ if and only if $A = B$.
- $A'$, the absolute complement of $A$, contains all elements not in $A$.

An operation $*$ on a set $A$:

- $*$ is closed on $A$ if $x \ast y \in A$ for all $x, y \in A$.
- $*$ is commutative on $A$ if $x \ast y = y \ast x$ for all $x, y \in A$.
- $*$ is associative on $A$ if $(x \ast y) \ast z = x \ast (y \ast z)$ for all $x, y, z \in A$.
- For an associative operation $\ast$ acting on a set $S$ with $x, y \in S$ and for any positive integers $m$ and $n$: $x^m \ast x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$.
- $e$ is the identity element of $\ast$ if $e \ast a = a \ast e = a$ for all $a \in A$ and is unique.
- If $\ast$ has an identity then for a given element $a \in A$, its inverse element $a^{-1}$ is the unique element such that $a \ast a^{-1} = a^{-1} \ast a = e$.
- For an operation $\ast$ on a set $S$ with identity $e$, any element $x \in S$ is said to be self-inverse if $x \ast x = e$.

For sets $A$ and $B$:

- $A \cup B$, the union of $A$ and $B$, contains all elements of $A$, $B$ or both.
- $A \cap B$, the intersection of $A$ and $B$, contains all elements in both $A$ and $B$.
- $A$ and $B$ are disjoint whenever $A \cap B = \emptyset$.
- $A \setminus B$, the set difference of $A$ with $B$, contains all elements in $A$ not in $B$.
- $A \Delta B$, the symmetric difference of $A$ and $B$, contains all elements in one of $A$ and $B$ but not both.

- Union and intersection are mutually distributive:
  
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- De Morgan's laws state that:
  
  $(A \cap B)' = A' \cup B'$

  $(A \cup B)' = A' \cap B'$
• To prove $A = B$, prove both $A \subseteq B$ and $B \subseteq A$.
• Subsets $B_1, B_2, \ldots$ **partition** $A$ if
  
  $B_i \cap B_j = \emptyset$ for $i \neq j$ (subsets are pairwise disjoint)
  
  and

  $B_1 \cup B_2 \cup \ldots = A$ (the collective union of the subsets equals $A$)
Mixed examination practice 2

1. Use a Venn diagram to show that for any two sets \( A, B \subset U \), the three sets \( A \Delta B, A \cap B' \) and \( A \cap B \) partition \( U \).

2. Use Venn diagrams to show that:
   (a) \( A \cup (B \cap A') = A \cup B' \)
   (b) \( (A \cap B)' \cup B = \emptyset \)

3. Set \( V_2 \) is the set of vectors with non-zero elements in two-dimensional space, and operation \( * \) on \( V_2 \) is given by:

\[
\begin{pmatrix} a \\ b \end{pmatrix} * \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ bd \end{pmatrix}
\]

(a) Show that \( V_2 \) is closed under \( * \).
(b) Find the identity element for \( * \) and determine the inverse of the general element \( \begin{pmatrix} a \\ b \end{pmatrix} \in V_2 \).
(c) Establish whether \( * \) is associative or commutative in \( V_2 \).

4. The binary operation \( a * b \) is defined by \( a * b = \frac{ab}{a + b} \) where \( a, b \in \mathbb{Z}^+ \).
   (a) Prove that \( * \) is associative.
   (b) Show that this binary operation does not have an identity element.
   \[11 \text{ marks}\]
   \( \text{(© IB Organization 2005)} \)

5. Prove that symmetric difference \( * \) is distributive across intersection \( \cap \).

6. Let \( X \) be a set containing \( n \) elements, where \( n \) is a positive integer. Show that the set of all subsets of \( X \) contains \( 2^n \) elements.

7. Define the operation \( # \) on the sets \( A \) and \( B \) by \( A # B = A' \cup B' \). Show algebraically that
   (a) \( A # A = A' \);
   (b) \( (A # A) # (B # B) = A \cup B \);
   (c) \( (A # B) # (A # B) = A \cap B \).
   \[6 \text{ marks}\]
   \( \text{(© IB Organization 2005)} \)
8. A binary operation is defined on \( \mathbb{Q} \setminus \{0\} \) by:

\[
\begin{cases}
  x * y = xy & \text{if } x > 0 \\
  x * y = \frac{x}{y} & \text{if } x < 0
\end{cases}
\]

(a) Determine the identity element for *, if one exists.
(b) Establish whether * is associative, commutative and closed in \( \mathbb{Q} \setminus \{0\} \).

9. For any positive integer \( a \), define set \( K_a \subset \mathbb{Q}_+^* \) by \( K_a = \{a^n \mid n \in \mathbb{Z}\} \).

(a) Show that \( K_a \) is closed under multiplication and division, but not addition or subtraction.
(b) Prove that \( n(K_a \cap K_b) > 1 \) if and only if \( a = bq^r \) for some \( q \in \mathbb{Q}_+^* \).