OXFORD IB DIPLOMA PROGRAMME

MATHEMATICS HIGHER LEVEL: SETS, RELATIONS AND GROUPS

COURSE COMPANION

Josip Harcet
Lorraine Heinrichs
Palmira Mariz Seiler
Marlene Torres-Skoumal

OXFORD

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford OX2 6DP

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide in

Oxford New York

Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in

Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan South Korea Poland Portugal
Singapore Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trade mark of Oxford University Press
in the UK and in certain other countries

First published 2015

British Library Cataloguing in Publication Data

Data available

ISBN 978-0-19-830486-9
10 9 8 7 6 5 4 3 2 1

Printed in Great Britain by Bell and Bain Ltd, Glasgow

Paper used in the production of this book is a natural, recyclable product made from wood grown in sustainable forests.
The manufacturing process conforms to the environmental regulations of the country of origin.

Acknowledgements

The publisher would like to thank the following for permission to reproduce photographs:

p3: Trajano Paiva/Alamy; **p11:** Diego Cervo/Shutterstock; **p12l-r:** Eric Pradel; **p14t:** Eric Pradel; **p14b:** OUP; **p47:** Private Collection/Archives Charmet/Bridgeman Images; **p88:** snig/Shutterstock; **p126:** Science Photo Library.

Course Companion definition

The IB Diploma Programme Course Companions are resource materials designed to support students throughout their two-year Diploma Programme course of study in a particular subject. They will help students gain an understanding of what is expected from the study of an IB Diploma Programme subject while presenting content in a way that illustrates the purpose and aims of the IB. They reflect the philosophy and approach of the IB and encourage a deep understanding of each subject by making connections to wider issues and providing opportunities for critical thinking.

The books mirror the IB philosophy of viewing the curriculum in terms of a whole-course approach; the use of a wide range of resources, international mindedness, the IB learner profile and the IB Diploma Programme core requirements, theory of knowledge, the extended essay, and creativity, activity, service (CAS).

Each book can be used in conjunction with other materials and indeed, students of the IB are required and encouraged to draw conclusions from a variety of resources. Suggestions for additional and further reading are given in each book and suggestions for how to extend research are provided.

In addition, the Course Companions provide advice and guidance on the specific course assessment requirements and on academic honesty protocol. They are distinctive and authoritative without being prescriptive.

IB mission statement

The International Baccalaureate aims to develop inquiring, knowledgable and caring young people who help to create a better and more peaceful world through intercultural understanding and respect.

To this end the IB works with schools, governments and international organizations to develop challenging programmes of international education and rigorous assessment.

These programmes encourage students across the world to become active, compassionate, and lifelong learners who understand that other people, with their differences, can also be right.

The IB learner Profile

The aim of all IB programmes is to develop internationally minded people who, recognizing their common humanity and shared guardianship of the planet, help to create a better and more peaceful world. IB learners strive to be:

Inquirers They develop their natural curiosity. They acquire the skills necessary to conduct inquiry and research and show independence in learning. They actively enjoy learning and this love of learning will be sustained throughout their lives.

Knowledgable They explore concepts, ideas, and issues that have local and global significance. In so doing, they acquire in-depth knowledge and develop understanding across a broad and balanced range of disciplines.

Thinkers They exercise initiative in applying thinking skills critically and creatively to recognize and approach complex problems, and make reasoned, ethical decisions.

Communicators They understand and express ideas and information confidently and creatively in more than one language and in a variety of modes of communication. They work effectively and willingly in collaboration with others.

Principled They act with integrity and honesty, with a strong sense of fairness, justice, and respect for the dignity of the individual, groups, and communities. They take responsibility for their own actions and the consequences that accompany them.

Open-minded They understand and appreciate their own cultures and personal histories, and are open to the perspectives, values, and traditions of other individuals and communities. They are accustomed to seeking and evaluating a range of points of view, and are willing to grow from the experience.

Caring They show empathy, compassion, and respect towards the needs and feelings of others. They have a personal commitment to service, and act to make a positive difference to the lives of others and to the environment.

Risk-takers They approach unfamiliar situations and uncertainty with courage and forethought, and have the independence of spirit to explore new roles, ideas, and strategies. They are brave and articulate in defending their beliefs.

Balanced They understand the importance of intellectual, physical, and emotional balance to achieve personal well-being for themselves and others.

Reflective They give thoughtful consideration to their own learning and experience. They are able to assess and understand their strengths and limitations in order to support their learning and personal development.

A note on academic honesty

It is of vital importance to acknowledge and appropriately credit the owners of information when that information is used in your work. After all, owners of ideas (intellectual property) have property rights. To have an authentic piece of work, it must be based on your individual and original ideas with the work of others fully acknowledged. Therefore, all assignments, written or oral, completed for assessment must use your own language and expression. Where sources are used or referred to, whether in the form of direct quotation or paraphrase, such sources must be appropriately acknowledged.

How do I acknowledge the work of others?

The way that you acknowledge that you have used the ideas of other people is through the use of footnotes and bibliographies.

Footnotes (placed at the bottom of a page) or endnotes (placed at the end of a document) are to be provided when you quote or paraphrase from another document, or closely summarize the information provided in another document. You do not need to provide a footnote for information that is part of a 'body of knowledge'. That is, definitions do not need to be footnoted as they are part of the assumed knowledge.

Bibliographies should include a formal list of the resources that you used in your work. The listing should include all resources, including books, magazines, newspaper articles, Internet-based resources, CDs and works of art. 'Formal' means that you should use one of the several accepted forms of presentation. You must provide full information as to how a reader or viewer of your work can find the same information. A bibliography is compulsory in the extended essay.

What constitutes misconduct?

Misconduct is behaviour that results in, or may result in, you or any student gaining an unfair advantage in one or more assessment component. Misconduct includes plagiarism and collusion.

Plagiarism is defined as the representation of the ideas or work of another person as your own. The following are some of the ways to avoid plagiarism:

- Words and ideas of another person used to support one's arguments must be acknowledged.
- Passages that are quoted verbatim must be enclosed within quotation marks and acknowledged.
- CD-ROMs, email messages, web sites on the Internet, and any other electronic media must be treated in the same way as books and journals.
- The sources of all photographs, maps, illustrations, computer programs, data, graphs, audio-visual, and similar material must be acknowledged if they are not your own work.
- Words of art, whether music, film, dance, theatre arts, or visual arts, and where the creative use of a part of a work takes place, must be acknowledged.

Collusion is defined as supporting misconduct by another student. This includes:

- allowing your work to be copied or submitted for assessment by another student
- duplicating work for different assessment components and/or diploma requirements.

Other forms of misconduct include any action that gives you an unfair advantage or affects the results of another student. Examples include, taking unauthorized material into an examination room, misconduct during an examination, and falsifying a CAS record.

About the book

The new syllabus for Mathematics Higher Level Option: Sets is thoroughly covered in this book. Each chapter is divided into lesson-size sections with the following features:

- Did you know?
- History
- Extension
- Advice

The Course Companion will guide you through the latest curriculum with full coverage of all topics and the new internal assessment. The emphasis is placed on the development and improved understanding of mathematical concepts and their real life application as well as proficiency in problem solving and critical thinking. The Course Companion denotes questions that would be suitable for examination practice and those where a GDC may be used.

Questions are designed to increase in difficulty, strengthen analytical skills and build confidence through understanding.

Where appropriate the solutions to examples are given in the style of a graphics display calculator.

Mathematics education is a growing, ever changing entity. The contextual, technology integrated approach enables students to become adaptable, lifelong learners.

Note: US spelling has been used, with IB style for mathematical terms.

About the authors

Lorraine Heinrichs has been teaching mathematics for 30 years and IB mathematics for the past 16 years at Bonn International School. She has been the IB DP coordinator since 2002. During this time she has also been senior moderator for HL Internal Assessment and workshop leader of the IB; she was also a member of the curriculum review team.

Palmira Mariz Seiler has been teaching mathematics for over 25 years. She joined the IB community in 2001 as a teacher at the Vienna International School and since then has also worked as Internal Assessment moderator in curriculum review working groups and as a workshop leader and deputy chief examiner for HL mathematics. Currently she teaches at Colegio Anglo Colombiano in Bogota, Colombia.

Marlene Torres-Skoumal has taught IB mathematics for over 30 years. During this time, she has enjoyed various roles with the IB, including deputy chief examiner for HL, senior moderator for Internal Assessment, calculator forum moderator, workshop leader, and a member of several curriculum review teams.

Josip Harcet has been involved with and teaching the IB programme since 1992. He has served as a curriculum review member, deputy chief examiner for Further Mathematics, assistant IA examiner and senior examiner for Mathematics HL as well as a workshop leader since 1998.

Contents

1 The development of Set Theory

CHAPTER OBJECTIVES:

8.1 Finite and infinite sets; subsets; Operations on sets: union, intersection, complement, set difference, symmetric difference; Venn diagrams; De Morgan's laws: distributive, associative and commutative laws for union and intersection.

8.2 Ordered pairs: the Cartesian product of two sets; relations: equivalence relations, equivalence classes and partitions.

Before you start

You should know how to:

1 Given that α, β are the roots of the equation $z^2 - 4z + 13 = 0$, find the value of $\alpha(1 - \alpha) + \beta(1 - \beta)$, without solving the quadratic equation.

Using Viete's formulas for sum and difference of roots:

$\alpha + \beta = 4$, $\alpha\beta = 13$

$\alpha(1 - \alpha) + \beta(1 - \beta)$

$= \alpha - \alpha^2 + \beta - \beta^2$

$= \alpha + \beta - (\alpha^2 + \beta^2)$

$= \alpha + \beta - ((\alpha + \beta)^2 - 2\alpha\beta)$

$= 4 - (16 - 26) = 14$

Skills check:

1 **a** Given that α, β are the roots of the equation $z^2 - 4z + 1 = 0$,

find the value of $\left(\alpha - \frac{1}{\alpha}\right)^2 + \left(\beta - \frac{1}{\beta}\right)^2$.

b If α and β are the roots of $2x^2 + 3x + 4 = 0$, show that the roots of the equation $8z^2 + 7z + 8 = 0$ are $\frac{\alpha}{\beta}$ and $\frac{\beta}{\alpha}$ **without** solving either of the two given equations.

The language of sets

In this chapter we will be looking at the basic elements of set theory. Georg Cantor, 19th century German mathematician who is best known for his creation of the language of sets, explained the notion of a set as *"... the taking together into a whole of distinct well-defined objects of our intuition or thought".* He went on to study the relation between sets, and to do this he associated with each set a cardinal number which would help him compare sizes, not only of finite sets but also infinite ones. Stated simply, by comparing different infinite sequences Cantor discovered that there are different sizes of infinity. The infinite size of the set of Natural numbers, made up of discrete elements, is smaller than the infinite size of the set of real numbers, which is continuous. The Natural numbers, Integers and Rational numbers are all said to be countable, infinite and have the same size (cardinality). He called the size of the countable infinite sets $\aleph_0$ whereas the infinity associated with the uncountable real numbers was $\aleph_1$. He further made a conjecture that became known as the Continuum Hypothesis. In his conjecture Cantor says that there is no set whose size is between $\aleph_0$ and $\aleph_1$. Cantor never proved this, and the Continuum Hypothesis was the first on the famous David Hilbert list of unsolved problems at the turn of the 20th century. Kurt Gödel and Paul Cohen worked extensively on this conjecture between 1930 and 1966. Their work changed the focus of mathematics in the second half of the 20th century and opened doors to many other theories.

? A cardinal number is one which denotes quantity or an amount of something.

The Hilbert Hotel: Hotel Infinity is a thought experiment created by the German mathematician David Hilbert. When Hotel Infinity first opened, it advertised itself as the hotel that always has room for one more guest! Initially everything was fine, as there were more than enough rooms for anyone wanting to stay. One week, however, it was an especially busy time, and an infinite number of people were staying in the hotel, so it was full! How does the hotel live up to its promise, that there is always room for one more? At this point, Hilbert asked his friend Cantor for help in solving his hotel problem. Cantor said that each guest should move to the room number that was twice the room number they originally occupied. This way all the odd numbered rooms became available. Cantor however did warn Hilbert that there were situations when it would be very difficult to find a way of allocating rooms. For example, suppose an infinite number of buses show up at the hotel, with an infinite number of people in each bus? You might want to research this intriguing problem, and all its different aspects!

Georg Cantor is known as the founder of Set Theory. His doctoral thesis was titled, "In mathematics the art of asking questions is more valuable than solving problems" David Hilbert (1862–1943) said Cantor's work was, "*the finest product of mathematical genius and one of the supreme achievements of purely intellectual human activity*."

1.1 Set definitions and operations

Much of the first part of this chapter you will have already encountered, since sets is the basic language of most of the mathematics you have studied, and is also included in the Prior Learning of the Higher Level syllabus.

A set S is a collection of objects, and if x is one of these objects we say that x is an element of S. We denote this by $x \in S$.

For example, the subjects offered in the IB diploma form a set.

The number of elements in a set S is called the ***cardinality*** of the set and we will denote it by $n(S)$. In some books it is denoted by $card\,(S)$ or $|S|$.

A finite set is one with a finite number of elements, i.e. a finite set is one whose cardinality is a natural number. If a set has an infinite number of elements then we say that the set is infinite.

The set $A = \{1, 3, 5, 7, 9\}$ is finite whereas the set $B = \{2, 4, 6, 8, ...\}$ is infinite.

There is exactly one set that has no elements and we call this the **empty set**, denoted by $\varnothing = \{\}$.

Set builder notation is a mathematical notation used to describe sets, whether finite or infinite. The following examples illustrate this:

$A = \{1, 3, 5, 7, 9\}$ in set builder notation becomes

$A = \{x \mid x = 2n - 1, n \in \mathbb{Z}^+, n \le 5\}$

$B = \{2, 4, 6, 8, \ldots\}$ in set builder notation becomes

$B = \{x \mid x = 2n, n \in \mathbb{Z}^+\}$

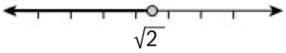
Set builder notation consists of three parts within curly brackets: a variable, a vertical line (or a colon) and any restrictions on the variable.

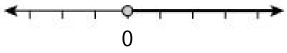
You have been using a number of infinite sets in your mathematical journey so far. Here is a list of them using the IB symbols for the sets:

The natural numbers	$\mathbb{N} = \{0, 1, 2, 3\ldots\}$
The integers	$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$
The positive integers	$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
The negative integers	$\mathbb{Z}^- = \{-1, -2, -3, \ldots\}$
The rational numbers	$\mathbb{Q} = \left\{ \frac{p}{q} \middle\| p, q \in \mathbb{Z}, q \neq 0 \right\}$
The positive rational numbers	$\mathbb{Q}^+ = \left\{ \frac{p}{q} \middle\| p, q \in \mathbb{Z}^+ \right\}$

Note that $\mathbb{Q}^+$ can also be described as $\mathbb{Q}^+ = \left\{ \frac{p}{q} \middle| p, q \in \mathbb{Z}^- \right\}$

The real numbers, denoted by $\mathbb{R}$, are often represented by a number line.





The positive real numbers	$\mathbb{R}^+ = \{x \mid x \in \mathbb{R}, x > 0\}$
The complex numbers	$\mathbb{C} = \left\{ a + ib \mid a, b \in \mathbb{R}, i = \sqrt{-1} \right\}$

Well-defined sets, equal sets and set difference

Definition

A set S is said to be **well-defined** if for any given x, we can determine if x belongs to the set.

For example, $P = \left\{ n \middle| n \in \mathbb{Z}^+, n < 50, n \text{ is a prime number} \right\}$ is a well-defined set because given any number $n \in \mathbb{Z}^+$ we can determine whether $n \in P$ or $n \notin P$.

So for the set P, $5 \in P$, $1 \notin P$, $59 \notin P$. Although 59 is a prime number it is greater than 50 and therefore not in P.

The set $T = \{x \mid x \in \mathbb{Z}^+, x \text{ is a prime number}\}$ is well-defined even though it is infinite, because we know that any positive integer is either prime or non-prime.

The set L = {numbers which are lucky} is not well-defined because we do not know which numbers are lucky and which are not. The definition of a lucky number depends on the context.

Given two sets A and B, if every element in B is also an element of A, we say that B is a subset of A and denote this by $B \subseteq A$. If all the elements of B are in A and there is at least one element in A which is not in B then we say that B is a proper subset of A, denoted by $B \subset A$.

Definitions

If $x \in B \Rightarrow x \in A$ for all $x \in B$, then $B \subseteq A$.
If $x \in B \Rightarrow x \in A$ for all $x \in B$, and there is $y \in A$ such that $y \notin B$, then $B \subset A$.

Axiom

If a set B is a subset of A, and A is also a subset of B, then it follows that the two sets are equal. The converse of this is also true, i.e. if A and B are equal sets then A is a subset of B, and B is a subset of A.

Using set notation: $B \subseteq A$ and $A \subseteq B \Leftrightarrow A = B$

$\Leftrightarrow$ is the notation used for "if and only if". Whenever we need to prove a statement containing $\Leftrightarrow$ we need to prove both ways, i.e. $\Rightarrow$ and $\Leftarrow$.

The empty set $\varnothing$ is a subset of any given set. We say that $\varnothing$ is a trivial subset. Another trivial subset of any given set is the set itself.

Definitions

A set containing all the elements under discussion is called the **universal set** and is denoted by U.

If set $S \subseteq U$, then the **complement of S**, denoted by S', consists of all those elements that are in U but not in S,

i.e. $S' = \{x \in U \mid x \notin S\}$.

The **intersection of two sets** A and B, denoted by $A \cap B$, is made up of those elements which are in both A and in B,

i.e. $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

Since for all $x \in A \cap B$, $x \in A$ it follows that $A \cap B \subseteq A$.

Similarly $A \cap B \subseteq B$.

The **union of two sets** A and B, denoted by $A \cup B$, is made up of those elements which are either in A, in B, or in both A and B,

i.e. $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

If $A \cap B = \varnothing$ then A and B are said to be **disjoint sets**.

The set consisting of those elements that are in set A but not in set B is called the **set difference** B from A denoted by $A \setminus B$,

i.e. $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$.

In Example 4 you will find the proof that $A \setminus B = A \cap B'$.

The **symmetric difference** of two sets A and B is denoted by $A \Delta B$ and consists of those elements which are either in A, in B, but not in both A and B,

i.e. $A \Delta B = \{x \mid x \in A \text{ or } x \in B, x \notin A \cap B\} = (A \setminus B) \cup (B \setminus A)$.

The following example demonstrates the application of set operations on two finite sets.

Example 1

Consider the sets $U = \{n \mid n \in \mathbb{N}, n \leq 65\}$, $A = \{2, 4, 6, 8, 10, 12, 14, 16\}$, and $B = \{2, 4, 8, 16, 32, 64\}$.

Find:

a $A \cup B$

b $A \cap B$

c $A \setminus B$

d $A \Delta B$

e $(A \cup B)\setminus(A \cap B)$

Comment upon your results.

a $A \cup B = \{2, 4, 6, 8, 10, 12, 14, 16, 32, 64\}$	*List all elements that are in A or in B.*
b $A \cap B = \{2, 4, 8, 16\}$	*List the elements that are in both A and B.*
c $A \setminus B = \{6, 10, 12, 14\}$	*List the elements which are in A but not in B.*
d $A \Delta B = \{6, 10, 12, 14, 32, 64\}$	*List the elements that are in A or B, but not in both A and B.*
e $(A \cup B)\setminus(A \cap B) = \{6, 10, 12, 14, 32, 64\}$ From the results of parts **d** and **e**, we see that: $A \Delta B = (A \cup B)\setminus(A \cap B)$	*List the elements that are in* $A \cup B$ *but not in* $A \cap B$.

In the next example the sets are described using set builder notation.

Example 2

$A = \{x \mid x \in \mathbb{Z}^+, x < 10\}$, $B = \{y \mid y \in \mathbb{Z}, |y| \leq 5\}$, $C = \{z \mid z \in \mathbb{N}, z \leq 15\}$.

List the elements in the following sets:

a $A \cap B$

b $A \cup C$

c $C \setminus B$

d $A \Delta B$

$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ $B = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$ $C = \{0, 1, 2, 3, 4, \ldots, 15\}$	*List the elements of the given sets.*
a $A \cap B = \{1, 2, 3, 4, 5\}$ **b** $A \cup C = \{0, 1, 2, 3, \ldots, 15\} = C$ **c** $C \setminus B = \{6, 7, 8, \ldots, 15\}$ **d** $A \Delta B = \{-5, -4, -3, -2, -1, 0, 6, 7, 8, 9\}$	*Since all the elements of A are in C this means that* $A \subset C$.

The next example deals with subsets of a finite set.

Example 3

Given that $S = \{x \mid x = 2n - 1, n \in \mathbb{Z}^+, n \le 4\}$, list all the proper subsets of S.

$S = \{1, 3, 5, 7\}$	*List all the elements of S.*
The proper subsets of S are: $\{1\}, \{3\}, \{5\}, \{7\}$, $\{1, 3\}, \{1, 5\}, \{1, 7\}, \{3, 5\}, \{3, 7\}, \{5, 7\}$, $\{1, 3, 5\}, \{1, 3, 7\}, \{1, 5, 7\}, \{3, 5, 7\}$	*List all the proper subsets of S. Note that the empty set and {1, 3, 5, 7} are* ***not*** *proper subsets of S.*

Investigation

The **power set**, $P(S)$, of a finite set S with n elements is the set of all subsets of S including the empty set $\varnothing$ and S itself.

a Find the number of sets in the power set of S when $n(S) = 0$ to 4.

b Make a conjecture about the number of sets in the power set of S.

c Check that your conjecture works for $n(S) = 5$.

One method to show that two sets A and B are equal is called the containment method, or the double inclusion method.

To show that two sets A and B are equal we need to show both containment conditions, i.e. $A \subseteq B$ and $B \subseteq A$.

The following example illustrates how to use the double inclusion method to show that two statements are equal.

Example 4

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

Let $x \in A \setminus B$	*Use the double inclusion method.*
$\Rightarrow x \in A$ and $x \notin B$	*Working from left to right.*
$\Rightarrow x \in A$ and $x \in B'$	*Definition of set difference.*
$\Rightarrow x \in A \cap B'$.	*Definition of complement.*
Therefore $A \setminus B \subseteq A \cap B'$.	*Definition of intersection.*
Let $x \in A \cap B'$	*Working from right to left.*
$\Rightarrow x \in A$ and $x \in B'$	*Definition of intersection.*
$\Rightarrow x \in A$ and $x \notin B$	*Definition of complement.*
$\Rightarrow x \in A \setminus B$	*Definition of set difference.*
$\Rightarrow A \cap B' \subseteq A \setminus B$	
Since $A \setminus B \subseteq A \cap B'$ and $A \cap B' \subseteq A \setminus B$,	
it follows that $A \setminus B = A \cap B'$.	

Example 5 illustrates how to use the double inclusion method to show that two sets are equal.

Example 5

$A = \{n \mid n = 5k + 2, k \in \mathbb{Z}\}$ and $B = \{n \mid n = 5k - 3, k \in \mathbb{Z}\}$
Show that $A = B$.

Let $x \in A$ — *Use the double inclusion method.*
$\Rightarrow x = 5m + 2, m \in \mathbb{Z}$.
Let $m = k - 1$. — *Since m is an integer, k is also an integer.*
Then $x = 5(k - 1) + 2 = 5k - 3$.
Therefore $A \subseteq B$.

Let $x \in B$
$\Rightarrow x = 5m - 3, m \in \mathbb{Z}$.
Let $m = k + 1$. — *Since m is an integer, k is also an integer.*
Then $x = 5(k + 1) - 3 = 5k + 2$.
Therefore $B \subseteq A$.

Since $A \subseteq B$ and $B \subseteq A$ it follows that $A = B$.

Example 6 proves the conjecture suggested by the investigation on page 9.

Example 6

Prove that the power set of a finite set S with n elements has exactly 2^n elements.

Method I
By definition, the power set of S is the set of all subsets of S including the empty set and S itself. We can count these subsets as follows: The number of subsets containing no elements is given by $\binom{n}{0}$.

The number of subsets containing only one element is given by $\binom{n}{1}$.

The number of subsets containing only 2 elements is given by $\binom{n}{2}$, etc.

The total number of subsets is therefore given by:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n.$$

Use the binomial expansion of $(1 + x)^n$ with $x = 1$.

Method II Let $P(S_n)$ denote the power set of a set S with n elements and let $\lvert P(S_n)\rvert$ denote the order of $P(S_n)$, i.e. the number of elements in the power set.	
Proof by induction: $P_n: \lvert P(S_n)\rvert = 2^n$	
When $n = 0$, $S_0 = \varnothing$ which has only one subset.	*Write down the statement.*
$\Rightarrow$ LHS $= \lvert P(S_0)\rvert = 1$	*Prove that the statement is true for n = 0.*
RHS $= 2^0 = 1$	
So P_0 is true.	
Assume that P_k is true for some $k \geq 0$, since we have started with 0, i.e. $\lvert P(S_k)\rvert = 2^k$. When we add another element to S, $n = k + 1$. Then S_{k+1} consists of all those subsets that do not contain the new element, i.e. 2^k subsets, and all those other subsets which contain it, i.e. another 2^k possible subsets. This gives us a total of $2 \times 2^k = 2^{k+1}$ subsets.	*Assume that statement is true for n = k.* *Show using assumption that the statement is true for n = k + 1.*
Since we proved that P_0 is true and we showed that if P_k is true P_{k+1} is also true it follows by the principle of mathematical induction that $P_n: \lvert P(S_n)\rvert = 2^n$ for all $n \geq 0$.	*Write final statement.*

Russell's Paradox: The development of set theory in the early 20th century was plagued by some thorny questions, the most famous of these posed by the eminent philosopher Bertrand Russell, and known as Russell's Paradox. The problem he posed was to find the set of all sets that do not contain themselves as members. The reason it is a paradox is easy to see in the well-known Barber's paradox, which poses the question: "Suppose there is one barber in town and he shaves all the men in town, except for those who shave themselves. Who shaves the barber?"

If he shaves himself, then he contradicts his job description. If he doesn't shave himself, he goes against his mandate to shave all those men who do not shave themselves. This paradox arises because Russell tries to find the set containing all sets. Such paradoxes led to a formal axiomatic system of sets.

Exercise 1A

1 Given that $A = \{a, b, c, d, e\}$, $B = \{a, e, i, o, u\}$ and $C = \{b, c, d, f, g\}$, list the elements of the following:

a $A \setminus B$ **b** $B \setminus A$ **c** $A \Delta B$

d $(A \cap B)\setminus(A \cap C)$ **e** $A \cap (B \cup C)$.

2 Use the double inclusion method to prove that:

a $A \cup B = B \cup A$ **b** $A \cap B = B \cap A$.

3 Prove that for three non-empty sets A, B and C $(C \setminus A) \cap (C \setminus B) = C \setminus (A \cup B)$.

4 Given that $A \subset B$ and $B \subset C$, prove that $A \subset C$.

5 Prove that $(A \cup B)\setminus(A \cap B) = A \Delta B$.

1.2 Partitions and Venn diagrams

The picture on the left above shows a collection of seashells. On the right, the seashells have been organized by type. All the seashells from the left-hand picture are in the right-hand picture but each seashell belongs to only one subset determined by its type. The seashells have been partitioned into sets which are disjoint but together make up the whole set.

Definition

Let A be a non-empty set.
A **partition** of a set A is another set P made up of non-empty subsets of A which are disjoint and whose union makes up the whole set.

i.e. $P = \{A_i \mid A_i \subseteq A$, if i is not equal to j $A_i \cap A_j = \varnothing, \cup A_i = A\}$

$\cup A_i = A$ means the union of all A_i

For example, one partition of $\{1, 2, 3\}$ would be $P = \{\{1\}, \{2, 3\}\}$.
Another partition would be $P = \{\{1, 2\}, \{3\}\}$.
In fact there are only five partitions of the set $\{1, 2, 3\}$, the other partitions being $\{\{1, 3\}, \{2\}\}$, $\{\{1\}, \{2\}, \{3\}\}$ and $\{\{1,2,3\}\}$.

If A = {all the countries of the world}, one partition would be P = {all the continents} provided we assume that each country belongs to only one continent.

Example 7

Let W = {all the countries of the world}.
Determine which of the following subsets of W form a partition:

a A = {countries in Africa}
B = {countries in N and S America}
C = {countries in Europe}
D = {countries in Asia}
E = {countries in Australasia}

b A = {any country whose name begins with a vowel}
B = {any country whose name contains the letter "a"}
C = {any country whose name starts with a consonant}

a The given sets form a partition of W.

The sets represent all the continents and each country belongs to one continent only.

b The given sets do not form a partition. Armenia, for example, is in both set A and set B.

The sets in a partition must be disjoint.

Example 8

Let S = {all subjects that can be chosen for an Extended Essay}.
Consider the sets A = {all subjects in group 1} D = {all subjects in group 4}
B = {all subjects in group 2} E = {all subjects in group 5}
C = {all subjects in group 3} F = {all subjects in group 6}
Determine whether the sets A to F partition the set S.

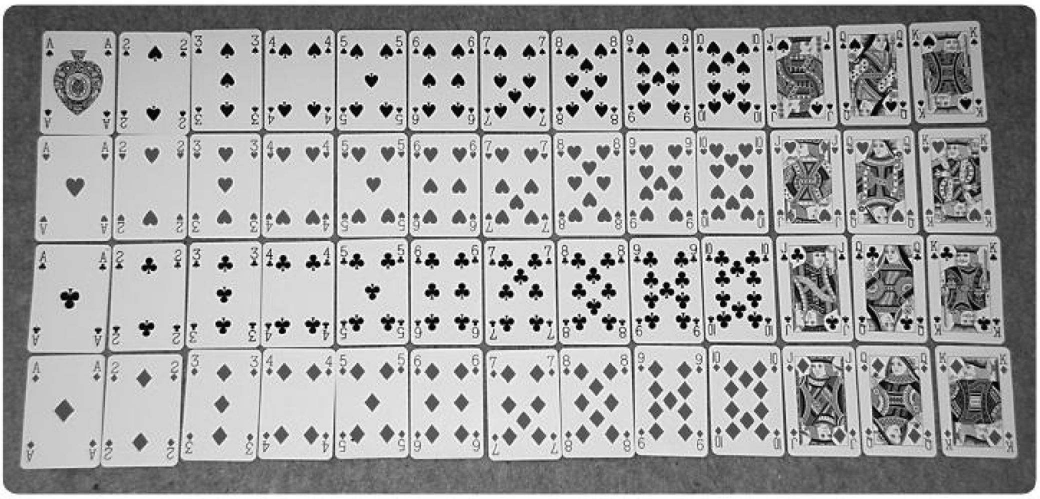
The given sets do not partition S because the subject Environmental Systems and Societies falls into group 3 and group 4.

The sets in a partition must be disjoint.

Exercise 1B

1 A deck of playing cards contain 52 cards. These are divided into two red suits (hearts and diamonds) and two black suits (spades and clubs). Each suit contains 13 cards representing the numbers 1 to 10 plus three picture cards (Jack, Queen and King). The picture on the next page shows a deck of cards partitioned into 4 suits.

List a further two ways in which you could partition a deck of cards.



2 Let $S = \{1, 2, 3, \ldots, 9\}$. Determine whether each of the following is a partition of S.

a $P = \{\{1, 2, 3, 9\}, \{4, 5, 6\}, \{7, 8\}\}$

b $Q = \{\{x \mid x \in S, x \text{ is even}\}, \{y \mid y \in S, y \text{ is a multiple of } 3\}, \{1, 5, 7\}\}$

c $B = \{\{x \mid x \in S, x \text{ is a prime number}\}, \{1, 2, 4, 6, 8, 9\}\}$

3 Which of the following collections of subsets are partitions of $\mathbb{Z}$?

a $\{\{x \mid x = 2n, n \in \mathbb{Z}\}, \{x \mid x = 2n + 1, n \in \mathbb{Z}\}\}$

b $\{\{x \mid x = 4n, n \in \mathbb{Z}\}, \{x \mid x = 4n + 1, n \in \mathbb{Z}\}, \{x \mid x = 4n + 2, n \in \mathbb{Z}\}, \{x \mid x = 4n + 3, n \in \mathbb{Z}\}\}$

c $\{\{x \mid x \in \mathbb{Z}, x < -50\}, \{x \mid x \in \mathbb{Z}, |x| \le 50\}, \{x \mid x \in \mathbb{Z}, x > 50\}\}$

4 Give examples with the given properties of a partition P on the set $\mathbb{R}$.

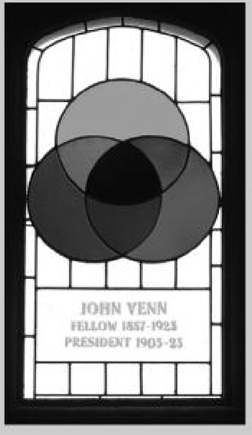
a P divides $\mathbb{R}$ into a finite and an infinite set.

b P divides $\mathbb{R}$ into two infinite sets.

c P divides $\mathbb{R}$ into an infinite number of sets.

1.3 Venn diagrams and set properties

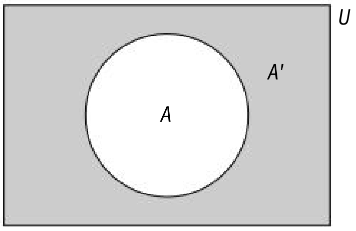
Venn diagrams are named after the logician and philosopher John Venn. It may well be that these types of diagram were used earlier than his time. In fact Venn diagrams are very similar to Euler diagrams which were first used by Leonhard Euler a century earlier.



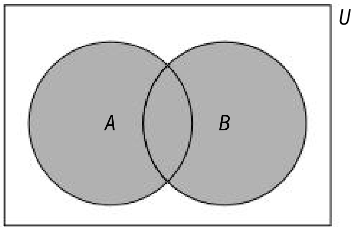
Venn diagram stained glass window from Gonville and Caius College, Cambridge.

Venn diagrams are very useful for showing relationships between different sets. A Venn diagram consists of a rectangle representing the universal set *U*, and circles inside the rectangle to represent the sets under consideration. The following Venn diagrams represent the operations and relationships described above them. You should remember that a correct Venn diagram provides an illustration of a statement but does not constitute a formal proof.

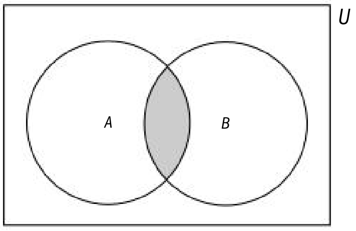
A' is the complement of A



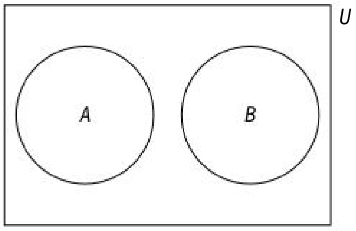
$A \cup B$



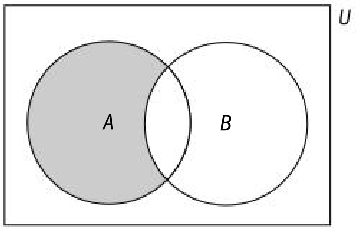
$A \cap B$



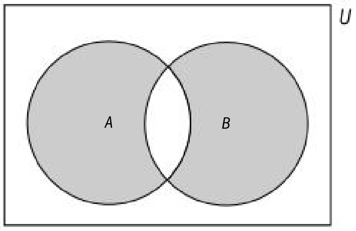
Disjoint sets have no intersection
$A \cap B = \varnothing$



The difference of sets $A \setminus B$



The symmetric difference $A \bigtriangleup B$



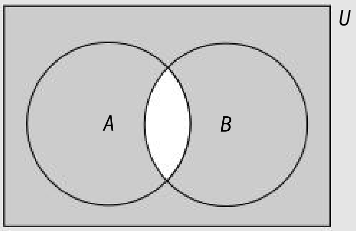
As previously seen, one way of showing that two sets are equal is by the containment or double inclusion method. Example 9 involves using the double inclusion method, which means establishing that if *x* is an element of the set on the LHS, then it is also an element of the set on the RHS, and vice versa.

Before you start with the formal proof it is useful to draw a Venn diagram. This will help you visualize what you are aiming to prove.

Example 9

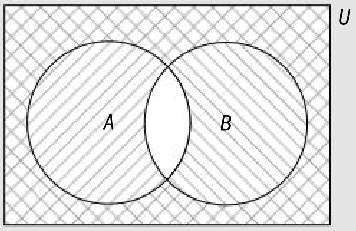
Show that $(A \cap B)' = A' \cup B'$

$(A \cap B)'$



Draw Venn diagrams of both the left hand side and right hand side of the equation to help illustrate what you are asked to prove.

$A' \cup B'$



Let $x \in (A \cap B)'$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \notin A$ and B

$\Rightarrow x \in A'$ or $x \in B'$

$\Rightarrow x \in A' \cup B'$

Therefore $(A \cap B)' \subseteq A' \cup B'$

Show both containment conditions.
Start by showing that $(A \cap B)' \subseteq A' \cup B'$.
Since $A \cap B$ is made up of elements that are in both A and in B it follows that an element which is not in this set is either not in A or not in B or not in both.

Let $x \in A' \cup B'$

Now we must show that $A' \cup B' \subseteq (A \cap B)'$.

$\Rightarrow x \in A'$ or $x \in B'$

$\Rightarrow x \notin A$ and B

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \in (A \cap B)'$

Since x is missing from A or B or both it cannot be in the intersection.

Therefore $A' \cup B' \subseteq (A \cap B)'$

Thus we conclude that $A' \cup B' = (A \cap B)'$

$(A \cap B)' = A' \cup B'$ is one of **De Morgan's Laws.** The other one of De Morgan's laws states that $(A \cup B)' = A' \cap B'$. The proof is left as an exercise.

Set properties

Before we move on, we need to prove some properties of sets that will be used in the rest of the book. The following theorem concerns properties that may seem trivial. These basic properties will be required for proofs of less obvious results.

Theorem 1

For any non-empty set $A \subseteq U$ the following statements hold:

i $A \cap A = A$ **ii** $A \cap \varnothing = \varnothing$

iii $A \cup A' = U$ **iv** $A \cap A' = \varnothing$

v $A \cup A = A$ **vi** $A \cup U = U$

vii $A \cap U = A$ **viii** $A \cup \varnothing = A$

Proofs:

i For all x in $A \Leftrightarrow x \in A$ and $x \in A$, it follows that $A \cap A = A$.

ii By the definition of intersection we know that $A \cap B \subseteq B$.

If we let $B = \varnothing$ then this becomes $A \cap \varnothing \subseteq \varnothing$.
But by definition $\varnothing \subseteq A \cap \varnothing$, since the empty set is a trivial subset of any set.
It therefore follows that $A \cap \varnothing = \varnothing$ (double inclusion).

iii $x \in A \cup A'$
$\Rightarrow x \in A \cup (U \setminus A)$, by definition of complement
$\Rightarrow x \in A$ or $x \in U \setminus A$, by definition of union
$\Rightarrow x \in U$, by definion of the universal set
$\therefore A \cup A' \subseteq U$

By definition of the universal set
$x \in U \Rightarrow x \in A$ or $x \notin A$
$\Rightarrow x \in A$ or $x \in A'$, by definition of complement
$\Rightarrow x \in A \cup A'$, by definition of union
$\therefore U \subseteq A \cup A'$

Since $A \cup A' \subseteq U$ and $U \subseteq A \cup A'$ it follows that $A \cup A' = U$.

The proofs of the last five properties are left as exercises.

You proved the next theorem in question 2 of Exercise 1A.

Theorem 2: Commutative property

For any two sets A and B the following statements are true:

i $A \cup B = B \cup A$ **ii** $A \cap B = B \cap A$

We shall now look at a very important property of sets, namely the **associative property** for intersection and union. Again this property is very useful when proving other relations between sets.

Theorem 3: Associative property

For any three non-empty sets A, B and C, the following statements are true:

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

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

Proof of i: This proof is carried out using double inclusion.

i LHS:

$x \in A \cap (B \cap C)$

$\Rightarrow x \in A$ and $x \in (B \cap C)$, by definition of intersection

$\Rightarrow x \in A$ and $x \in B$ and $x \in C$, by definion of intersection

$\Rightarrow (x \in A$ and $x \in B)$ and $x \in C$

$\Rightarrow x \in A \cap B$ and $x \in C$

$\Rightarrow x \in (A \cap B) \cap C$

$\therefore A \cap (B \cap C) \subseteq (A \cap B) \cap C$

RHS:

$x \in (A \cap B) \cap C$

$\Rightarrow x \in (A \cap B)$ and $x \in C$, by definition of intersection

$\Rightarrow x \in A$ and $x \in B$ and $x \in C$, by definition of intersection

$\Rightarrow x \in A$ and $(x \in B$ and $x \in C)$

$\Rightarrow x \in A$ and $x \in (B \cap C)$

$\Rightarrow x \in A \cap (B \cap C)$

$\therefore (A \cap B) \cap C \subseteq A \cap (B \cap C)$

Since $A \cap (B \cap C) \subseteq (A \cap B) \cap C$ and
$(A \cap B) \cap C \subseteq A \cap (B \cap C)$,

it follows that $A \cap (B \cap C) = (A \cap B) \cap C$.

The proof of **ii** is left as an exercise.

There are similarities between these properties and the associative and distributive properties of addition and multiplication of real numbers.
For all $a, b, c \in \mathbb{R}$:

$a + b = b + a$

$ab = ba$

$a + (b + c) = (a + b) + c$

$a(bc) = (ab)c$

$a(b + c) = ab + bc$

With set operations, both intersection and union behave like addition and multiplication. For this reason we have two distributive properties, one for union over intersection and one for intersection over union. This is important for the study of algebraic structures where the focus is on the similarities (and differences) of properties of different operations acting on different sets.

Another useful property when establishing further relations between sets is the distribution of intersection over union and vice versa. Proof of the distributive law is found in the next theorem.

Theorem 4: Distributive property

For any three non-empty sets A, B and C the following statements are true:

i $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Intersection is distributive over union.

ii $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Union is distributive over intersection.

Proof: *(Once more we shall use the double inclusion method for part **i**. Part **ii** is included in the next exercise.)*

i For all $x \in A \cap (B \cup C)$

$\Rightarrow x \in A$ and $x \in B \cup C$ Definition of intersection

$\Rightarrow x \in A$ and $(x \in B$ or $x \in C)$ Definition of union

$\Rightarrow (x \in A$ and $x \in B)$ or $(x \in A$ and $x \in C)$ Rearranging within context

$\Rightarrow x \in A \cap B$ or $x \in A \cap C$

$\Rightarrow x \in (A \cap B) \cup (A \cap C)$

Therefore $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

For all $x \in (A \cap B) \cup (A \cap C)$,

$x \in A \cap B$ or $x \in A \cap C$. Definition of union

$\Rightarrow (x \in A$ and $B)$ or $(x \in A$ and $C)$ Definiton of intersection

$\Rightarrow x \in A$ and $(x \in B$ or $x \in C)$

$\Rightarrow x \in A$ and $x \in B \cup C$

$\Rightarrow x \in A \cap (B \cup C)$

Therefore $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Hence by the double inclusion principle
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

? There are different set theories. The one we cover in the HL syllabus is Naive Set Theory. This set theory is defined informally using natural language and properties of Boolean Algebra rather than the formal axioms of Symbolic Logic.

Sometimes it is easier to prove a statement by using set properties than by using the double inclusion method. The previous theorems are essential when proving complex results, especially when the double inclusion method becomes too cumbersome. This is illustrated in the next example.

Example 10

Given two non-empty sets A and B, show that:

a $A \cap (A \cup B)' = \varnothing$

b $(A \setminus B) \cup (B \setminus A) = (A \cup B) \cap (A \cap B)'$

a $A \cap (A \cup B)' = A \cap (A' \cap B')$	*De Morgan's Law*
$= (A \cap A') \cap B'$	*Associative property.*
$= \varnothing \cap B'$ $= \varnothing$	*With the addition of the proposed statements in Theorem 1, we can state that: $A \cap A' = \varnothing$.*
b RHS	
$= (A \cup B) \cap (A \cap B)' = (A \cup B) \cap (A' \cup B')$	*De Morgan's Law.*
$= \left[(A \cup B) \cap A'\right] \cup \left[(A \cup B) \cap B'\right]$	*Distributive property.*
$= [(A \cap A') \cup (B \cap A')] \cup [(A \cap B') \cup (B \cap B')]$	*Distributive property.*
$= [\varnothing \cup (B \cap A')] \cup [(A \cap B') \cup \varnothing]$	*Definition of intersection.*
$= (B \cap A') \cup (A \cap B')$	*Definition of union.*
$= (A \cap B') \cup (B \cap A')$	*Commutative property.*
$= (A \setminus B) \cup (B \setminus A)$ $=$ LHS	*Alternative form of symmetric difference.*

Here is a list of rules you should remember because you will need to use them for proving more complex properties:

- $A \cup A' = U$
  $A \cap A' = \varnothing$
  $A \cup A = A$
  $A \cap A = A$
- $A \cup (A \cap B) = A$
  $A \cap (A \cup B) = A$
- $(A')' = A$
- $\varnothing' = U$
  $U' = \varnothing$
- $A \cup \varnothing = A$
  $A \cap U = A$
- $A \cap \varnothing = \varnothing$
  $A \cup U = U$
- Commutative Laws $A \cup B = B \cup A$
  $A \cap B = B \cap A$
- Distributive Laws $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Associative Laws $A \cup (B \cup C) = (A \cup B) \cup C$
  $A \cap (B \cap C) = (A \cap B) \cap C$
- De Morgan's Laws $(A \cup B)' = A' \cap B'$
  $(A \cap B)' = A' \cup B'$

Exercise 1C

1 Prove that:

a $(A \cup B) \cap C \subseteq A \cup (B \cap C)$

b $A \cap (B \cup C) \subseteq (A \cap B) \cup C$

(You may first want to draw Venn diagrams to help visualize what you are trying to prove.)

2 Prove that $(A \cup B)' = A' \cap B'$.
(*Hint: Use the double inclusion method used in Example 4.*)

3 Prove that for all sets A, B and C:
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

This is the second part of the distributive law, i.e. union is distributive over intersection.

4 Given that A and B are subsets of a universal set U, use De Morgan's laws to prove that:

a $(A' \cup B)' = A \cap B'$ **b** $(A \cap B)' \cup B = U$

c $(A \cup B)' \cap B = \varnothing$

5 Use the double inclusion method shown in Example 4 to prove that $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

6 **a** Use a Venn diagram to illustrate that $A \Delta B = A' \Delta B'$.

b Prove this result using the double inclusion method and the result of question 5.

7 Prove that $((A \cap C) \cup (B \cap C'))' = (A' \cap C) \cup (B' \cap C') \cup (A' \cap B')$

8 Use mathematical induction to prove De Morgan's laws for n sets, i.e.

a $(A_1 \cup A_2 \cup A_3 \ldots \cup A_n)' = A_1' \cap A_2' \cap A_3' \ldots \cap A_n'$

b $(A_1 \cap A_2 \cap A_3 \ldots \cap A_n)' = A_1' \cup A_2' \cup A_3' \ldots \cup A_n'$

1.4 The Cartesian product of two sets

In mathematics, a Cartesian product is a method which allows us to construct a new set of multiple dimensions by combining multiple sets. For example if we take the Cartesian product of the sets $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ we obtain a three-dimensional set we are familiar with, namely the three-dimensional set of ordered triplets which was used when studying vectors in three dimensions. In general, if we take the Cartesian product of n sets, we obtain a representation of an n-dimensional space.
René Descartes first came up with this concept when he formulated analytic geometry by using a "Cartesian plane".

> It was thanks to a common housefly that the "Cartesian plane" came about. René Descartes, a French philosopher and mathematician, was in bed and noticed a fly on the ceiling of his bedroom. He wondered whether he would be able to describe the exact position of the fly to someone not in the room. Looking at a corner in the ceiling he saw three lines and three planes which intersected at the corner. He imagined dividing the lines into equal segments, calling the corner the 'origin' and giving it the value (0,0,0) and numbering the segments along each line 1, 2, 3 ...
> The position of the fly in the room could then be described by three numbers. Descartes had created a system to describe 3D space. If he used only one plane, the ceiling, and two perpendicular lines, then the position of the fly on the ceiling would be described by just two numbers. This was the birth of the 3D Cartesian coordinate system as well as the Cartesian plane in 2D.

The following two examples illustrate how new sets are constructed using the Cartesian product.
If Fabienne has three blouses: plain, flowered and striped, and four pairs of jeans: blue, red, white and green, then the total number of ways of combining these would be the Cartesian product of the sets {blouses} and {jeans}.

$B = \{\text{blouses}\} = \{p, f, s\}$

$J = \{\text{jeans}\} = \{b, r, w, g\}$

$B \times J = \{(p, b), (p, r), (p, w), (p, g), (f, b), (f, r), (f, w), (f, g), (s, b), (s, r), (s, w), (s, g)\}$

Note that in the set denoting the Cartesian product $B \times J$, each pair is **ordered** so that the first item is a blouse and the second is a pair of jeans.

Another example of the Cartesian product would be coordinates used to locate positions on a globe, i.e. Latitude × Longitude.

Valletta, the capital city of the island of Malta, would be located at (35° 53′ 58″ N, 14° 30′ 52″ E).

Definition

The **Cartesian product** of two non-empty sets A and B denoted by $A \times B$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

In set-builder notation, $A \times B = \{(a, b) \mid a \in A, b \in B\}$

So if $A = \{1, 3\}$ and $B = \{2, 4, 6\}$,

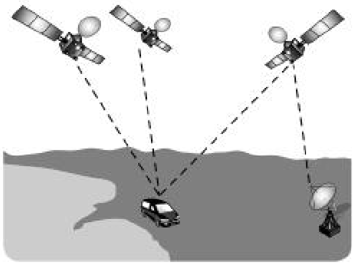
$A \times B = \{(1, 2), (1, 4), (1, 6), (3, 2), (3, 4), (3, 6)\}$

$B \times A = \{(2, 1), (2, 3), (4, 1), (4, 3), (6, 1), (6, 3)\}$

Clearly you can see that $A \times B \neq B \times A$.

With this definition it becomes evident that the Cartesian product $\mathbb{R} \times \mathbb{R}$ represents the Euclidean plane, also referred to as the Cartesian plane. The Cartesian product $\mathbb{Z} \times \mathbb{Z}$ is made up of the points on this plane whose coordinates are integers. It is usual to denote the Cartesian product of a set A with itself as A^2. So $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ and $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$. Since the Cartesian product is a set, the number of ordered pairs in a Cartesian product is its cardinality. The three dimensional Cartesian coordinate system, also known as Euclidean space, is represented by $\mathbb{R} \text{ x } \mathbb{R} \text{ x } \mathbb{R} = \mathbb{R}^3$.

? Global Positioning Systems calculate our longitude and latitude in real time. Differential GPS is an enhancement of some GPS units that, in addition to orbiting satellites, uses ground stations on the Earth to calculate a position more accurate than satellite-only GPS. Differential GPS can improve the accuracy of readings from about 50 feet to within 10 feet of the actual location.



Example 11

The Cartesian product of two sets A and B consists of six elements. Three of these are (a, a), (b, b) and (c, a). Find the sets:

i A

ii B

iii $A \times B$

i $a, b, c \in A$ $a, b \in B$ $A = \{a, b, c\}$	*Since they are the first elements in the three ordered pairs given.*
ii $B = \{a, b\}$	*They are the second elements in the ordered pairs.*
iii $A \times B = \{(a, a), (a, b), (b, a), (b, b), (c, a), (c, b)\}$	*Since* $n(A \times B) = 6$

1.5 Relations

You should have noticed from the previous examples the following points:

1 The Cartesian product of two sets is a set.

2 The elements of the set are ordered pairs.

3 In each ordered pair, the first element comes from the first set and the second element comes from the second set.

Now that you understand what a Cartesian product is we can move on to appreciate how this product allows us to construct other sets.

Definition

A **relation**, R, between two non-empty sets A and B is a subset of $A \times B$ and is usually governed by a rule connecting the ordered pair in the relation, commonly denoted by aRb.

Actually a relation does not have to be governed by a rule. Any random subset of $A \times A$ is a relation on A whether or not it describes a rule.

For example if $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and we define the relation $aRb \Leftrightarrow b = a^2$, then $R = \{(1, 1), (2, 4), (3, 9)\}$.

Example 12

Given a set A, prove that a relation R on A is a subset of $A \times A$.

Let $(a, b) \in R$	
$\Rightarrow aRb$	
$\Rightarrow a \in A$ and $b \in A$	
$\Rightarrow (a, b) \in A \times A$	*Since R is a relation on A.*
Therefore $R \subseteq A \times A$.	

Definition

Let R be a relation from set A to set B. The **inverse** of relation R, denoted by R^{-1}, is the set of ordered pairs $\{(b, a) \mid (a, b) \in R\}$.

Example 13

Given that $A = \{1, 2, 3, \ldots, 10\}$ and $R \subseteq A \times A$ such that $aRb \Rightarrow \frac{b}{a} = 2$, find R^{-1}.

$R = \{(1, 2), (2, 4), (3, 6), (4, 8), (5, 10)\}$	*List all the elements of R.*
$\Rightarrow R^{-1} = \{(2, 1), (4, 2), (6, 3), (8, 4), (10, 5)\}$	*Use the definition of R^{-1} to list its elements.*

In other words, $bR^{-1}a \Leftrightarrow aRb$.

Exercise 1D

1 If $A = \{1, 2, 3\}$ and $B = \{p, q\}$, find $A \times B$ and $B \times A$.
Are the two products equal?

2 A tetrahedral die A and a normal six-sided die B are tossed simultaneously, thus $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3, 4, 5, 6\}$.

a **i** List the elements of the Cartesian product $A \times B$.

ii Show that $A \times A \subset A \times B$.

b Write down the sets that represent the following relations:

i If $a \in A$ and $b \in B$, $aRb \Leftrightarrow a + b$ is a prime number.

ii If $a \in A$ and $b \in B$, $aRb \Leftrightarrow b = a^2$.

iii If $a \in A$ and $b \in B$, $aRb \Leftrightarrow b - a$ is a prime number.

iv If $a, b \in A$, $aRb \Leftrightarrow a + b \in B$.

3 Given set $A = \{a, b\}$ and set $B = \{p, q\}$, list all the elements of $A \times B$ and find the number of subsets in the power set of $A \times B$.

4 Let $A = \{a, b\}$, $B = \{1, 2, 3\}$ and $C = \{3, 4\}$. Find:

a $(A \times B) \cap (A \times C)$

b $A \times (B \cap C)$

c What can you conclude from the answers to *a* and *b*?

5 Let A, B and C be three non-empty sets. Prove that if $A \subset B$ then $A \times C \subset B \times C$.

6 Let $S = \{0, 2, 4, 6, 8\}$. Write out the elements of set R which is a subset of $S \times S$ given by $aRb \Rightarrow a \leq b$.

7 Prove that for three non-empty sets A, B and C: $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

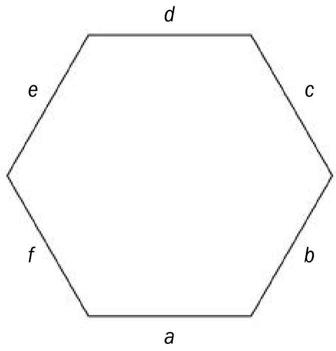
8 Let A, B, C and D be four non-empty sets such that $A \subseteq C$ and $B \subseteq D$.
Show that $A \times B \subseteq C \times D$.

9 For three non-empty sets A, B and C show that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

10 Given that $A = \mathbb{R}^+$ and $B = \{x \mid x \in \mathbb{Z}^+, x \leq 10\}$, define the relation R on $A \times B$ as follows: $aRb \Rightarrow a = 2^b$. List all the elements that make up the relation R. Find R^{-1}. What is the cardinality of R^{-1}?

Equivalence relations

Among all the relations that can be established in sets there is a special class, namely equivalence relations.



As just discussed, a relation on a set A is a collection of ordered pairs (a, b) which are governed by this relation. As such, a relation R on a set A is a subset of $A \times A$.
For example, $A = \{a, b, c, d, e, f\}$,
the sides of a regular hexagon, and R_1 is the relation defined by $xR_1y \Leftrightarrow$ 'x is parallel to y', where, $x, y \in A$.
Then we can say that segment a is parallel to itself and also to d.
Segment b is parallel to itself and also to e, etc.
Thus $R_1 = \{(a, a), (a, d), (b, b), (b, e), (c, c), (c, f), (d, d), (d, a), (e, e), (e, b), (f, f), (f, c)\}$ which is a subset of $A \times A$.

Note that in the hexagon example, for all elements $a \in A$, we have the ordered pair (a, a) in R. Therefore we say that xR_1x for all $x \in A$, i.e. the relation is **reflexive**.
Also in this example we notice that if (x, y) is in R_1 then (y, x) is in R_1, for example (a, d) and (d, a).
i.e. $xR_1y \Rightarrow yR_1x$ for all $x, y \in A$. The relation is said to be **symmetric**.

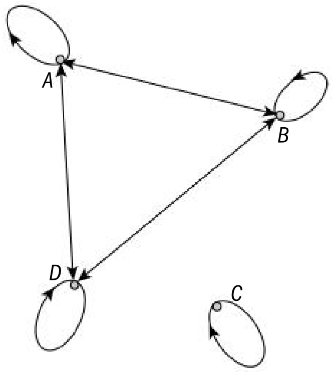
Now consider a different example, the set of all polygons P.
Let R be the relation on $P \times P$ defined by $xRy \Rightarrow$ 'x and y are similar polygons'.

R is **reflexive** since any polygon is similar to itself.
R is **symmetric** since if polygon x is similar to polygon y, then y is also similar to x.
Now consider $xRy \Rightarrow$ 'x is similar to y' and $yRz \Rightarrow$ 'y is similar to z'.
Then by properties of similarity it follows that x is similar to z.
Since xRy and $yRz \Rightarrow xRz$ we say that the relation R is **transitive**.

Definition

A relation R defined on a set A is said to be an **equivalence relation** if the following three conditions are true:

- R is reflexive, i.e. aRa for all $a \in A$
- R is symmetric, i.e. $aRb \Rightarrow bRa$ for all $a, b \in A$
- R is transitive, i.e. aRb and $bRc \Rightarrow aRc$ for all $a, b, c \in A$



The diagram on the right illustrates an equivalence relation on the set $S = \{A, B, C, D\}$. The arrows indicate the relation between individual elements of S, which are represented by the vertices. Note that although C is related only to itself, the relation is still symmetric and transitive.

In simple cases like the next example, it may be useful to draw a similar diagram.

Example 14

Let $A = \{1, 2, 3, 4\}$ and $R \subseteq A \times A$ such that
$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4)\}$.
Is R an equivalence relation?

For all $a \in A$, aRa R is reflexive	*We see that* *1R1, 2R2, 3R3 and 4R4*
For all $a, b \in A$, if aRb then bRa R is symmetric	*We can see that* *1R2 and 2R1, 1R3 and 3R1, 2R3 and 3R2*
Also for $a, b, c \in A$, aRb and $bRc \Rightarrow aRc$ R is transitive	*We see that* *1R2 and 2R3 and 1R3* *1R3 and 3R2 and 1R2* *2R3 and 3R1 and 2R1* *2R1 and 1R3 and 2R3* *3R2 and 2R1 and 3R1*
Thus, R is an equivalence relation.	*3R1 and 1R2 and 3R2*

Example 15

Let $A = \{1, 2, 3, 4\}$ and $R_i \subseteq A \times A$.
Construct the following relations:

a A relation R_1 that is reflexive and symmetric but not transitive.

b A relation R_2 that is reflexive and transitive but not symmetric.

c A relation R_3 that is symmetric and transitive but not reflexive.

The following working shows three examples to illustrate the relations. There are other examples that you might be able to come up with.

a $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (2, 3), (3, 2)\}$
Reflexive because
$1R1$, $2R2$, $3R3$ and $4R4$.

Symmetric because
$1R2$ and $2R1$ and $2R3$ and $3R2$.
Not transitive because
$1R2$ and $2R3$ but $1 \not{R} 3$.

$a \not{R} b$ means that a is not related to b.

b $R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2)\}$
Reflexive because
$1R1$, $2R2$, $3R3$ and $4R4$.

Transitive because, for example
$1R1$ and $1R2$ and $1R2$.
Not symmetric because $1R2$ but $2 \not{R} 1$

c $R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$
Symmetric because
$1R2$ and $2R1$, $1R3$ and $3R1$, $2R3$ and $3R2$
Transitive because
$1R3$ and $3R2$ and $1R2$
$1R2$ and $2R3$ and $1R3$
$2R1$ and $1R3$ and $2R3$
$2R3$ and $3R1$ and $2R1$
$3R2$ and $2R1$ and $3R1$
$3R1$ and $1R2$ and $3R2$
Not reflexive because $4 \not R 4$

Example 16

$A = \{3, 4, 5, 9, 10, 11, 13\}$ and $aRb \Leftrightarrow |a - b|$ is divisible by 5.
Show that R is an equivalence relation.

$R = \{(3, 3), (4, 4), (5, 5), (9, 9), (10, 10), (11, 11), (13, 13),$
$(3, 13), (4, 9), (5, 10), (13, 3), (9, 4), (10, 5)\}$

$|a - a| = 0 = 0 \times 5$, for all a, therefore R is **reflexive**

$|a - b| = |b - a| \Rightarrow aRb \Rightarrow bRa$, therefore R is **symmetric**

$|a - b|$ is divisible by 5 $\Rightarrow a - b = 5m, m \in \mathbb{Z}$

$|b - c|$ is divisible by 5 $\Rightarrow b - c = 5n, n \in \mathbb{Z}$

Combining these two we obtain
$a - c = 5(m + n)$
$\Rightarrow |a - c| = 5|m + n| \Rightarrow aRc$. Therefore R is **transitive**.
R satisfies all three conditions necessary to qualify as an equivalence relation.

Modular Congruence

The following is a common example of equivalence relations. It generates all the $\mathbb{Z}$ sets that will later be used to define groups of every single order n.

$x, y \in \mathbb{Z}$ are said to be congruent modulo n if $|x - y|$ is divisible by n.
We denote this by $x \equiv y (\text{mod } n)$.

Consider the following lists of numbers from 1 to 60:

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30
31	32	33	34	35
36	37	38	39	40
41	42	43	44	45
46	47	48	49	50
51	52	53	54	55
56	57	58	59	60

These tables are another way of writing the congruences modulo 6 (≡ (mod 6)) and modulo 5 (≡ (mod 5)). Note that the first column of each table represents $x \equiv 1 \pmod 6$ and $y \equiv 1 \pmod 5$ respectively. Another way of expressing these numbers would be to say that all the numbers in the first column leave a remainder of 1 when divided by 6 and by 5 respectively. Similarly the second column of each table represents the numbers that leave a remainder of 2, and so on. So each column would represent a relation on all the positive integers if we were to continue building up the tables.

It is also easy to see from the tables that congruence modulo 6 and modulo 5 are equivalence relations.

Let's look at the first table only. Since each column represents $x \pmod 6$ with $x \in \{0, 1, 2, 3, 4, 5\}$ with 0 representing 6 since 0(mod 6) represents all the multiples of 6, we see that $x \equiv x \pmod 6$ since these are the numbers in the first row. Any two numbers in the same column are congruent to each other modulo 6.
For example, $28 \equiv 4 \pmod 6$ and $52 \equiv 4 \pmod 6$

$\Rightarrow 28 \equiv 52 \pmod 6$ and $52 \equiv 28 \pmod 6$ i.e. symmetric.

We can do this for any pair of numbers in the same column; this leads to the conclusion that the relation 'congruence modulo 6' is symmetric.

Similarly if we take any three numbers in a column, we realize that they are all related to each other. e.g. $\left.\begin{matrix} 59 \equiv 35 \pmod 6 \\ 35 \equiv 11 \pmod 6 \end{matrix}\right\} \Rightarrow 59 \equiv 11 \pmod 6$.

Again we can do this for any three numbers in a particular column, thus we can deduce that congruence modulo 6 is a transitive relation on the positive integers.

We can now list the first table as follows:

1(mod 6)	**2(mod 6)**	**3(mod 6)**	**4(mod 6)**	**5(mod 6)**	**0(mod 6)**
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60

Each column represents the different congruences modulo 6 and the columns have divided the numbers into distinct, disjoint subsets (equivalence classes). Although the table represents only the integers 1 to 60, it is clear that we could continue to build up the table endlessly. All the positive integers could be included in such an endless table, and they would all be separated into distinct equivalence classes representing the particular congruence.

We say that $\equiv$ (mod 6) partitions the positive integers into six equivalence classes.

Repeat the process above with $\equiv$ (mod 5) and show that this is an equivalence relation.

We are now in a position to explain the properties of modular arithmetic in a more rigorous manner.

Definition

a is **congruent** to b modulo n if n divides $(a - b)$, i.e. $(a - b) = kn$, $k \in \mathbb{Z}$.

$a \equiv b(\text{mod } n) \Rightarrow n \mid (a - b) \Rightarrow (a - b) = kn,\ k \in \mathbb{Z}$.

So, $14 \equiv 0(\text{mod } 7)$ since $7 \mid 14$.

But $13 \not\equiv 5(\text{mod} 7)$ since $7 \nmid (13 - 5)$.

$34 \equiv 6(\text{mod } 7)$ since $7 \mid (34 - 6)$.

Theorem 5

The relation R which is defined as : $aRb \Leftrightarrow a \equiv b(\text{mod } n),\ n \in \mathbb{Z}^+$, is an equivalence relation on $\mathbb{Z}$.

Note that congruence (mod 0) does not exist since we cannot divide by 0.

Proof:

$a \equiv a(\text{mod } n)$ since $n \mid 0$ for all $a \in \mathbb{Z}$

Therefore R is reflexive.

$$\begin{aligned} a \equiv b(\text{mod } n) &\Rightarrow a - b = kn,\ k \in \mathbb{Z} \\ &\Rightarrow b - a = -kn,\ -k \in \mathbb{Z} \\ &\Rightarrow n \mid b - a \Rightarrow b \equiv a(\text{mod } n) \end{aligned}$$

Therefore R is symmetric.

$a \equiv b(\text{mod } n) \Rightarrow a - b = pn, p \in \mathbb{Z}$

$b \equiv c(\text{mod } n) \Rightarrow b - c = qn, q \in \mathbb{Z}$

Adding $\Rightarrow a - c = n(p + q), p + q \in \mathbb{Z}$

$\Rightarrow a \equiv c(\text{mod } n)$

Therefore R is transitive. Q.E.D.

Example 17

For each given set S and associated relation R, determine whether or not R is an equivalence relation.

a S is the set of all people in Asia,
$aRb \Leftrightarrow a$ and b have the same parents.

b S is the set of all people in Australia,
$aRb \Leftrightarrow a$ and b live within 100 km of each other.

c S is the set of straight lines in a plane,
$aRb \Leftrightarrow a$ is parallel to b.

a It is clear that $aRa \Rightarrow R$ is reflexive.
$aRb \Rightarrow bRa$ since both have the same parents. R is symmetric
$aRb \Rightarrow a$ and b have the same parents.
$bRc \Rightarrow b$ and c have the same parents.
It follows that a, b and c have the same parents so
aRc and R is transitive.
R is an equivalence relation.

b Clearly aRa. R is reflexive.
$aRb \Rightarrow a$ and b live within 100 km of each other $\Rightarrow bRa$. R is symmetric.
Let b live 90 km due east of a and c 80 km due east of b.
aRb and bRc but a is not related to c because
c lives 170 km due east of a. R is not transitive.
Therefore it is not an equivalence relation.

c By definition of parallel lines in a plane aRa.
Similarly $aRb \Rightarrow bRa$. So R is symmetric.
$aRb \Rightarrow a$ is parallel to b
$bRc \Rightarrow b$ is parallel to c
By definition of parallel lines, aRc which means
R is transitive, so R is an equivalence relation.

Example 18

Let the relation R on $\mathbb{N}$ be defined as $xRy \Leftrightarrow 2x - y = 5n,\ n \in \mathbb{Z}$.
Determine if the relation is:

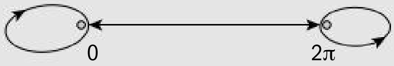
a reflexive
b symmetric
c transitive

a When $x = 1$, $2 \times 1 - 1 \neq 5n$ Therefore $x \not{R} x$ R is not reflexive.	*Proof by counter-example* *Substitute $x = 1$ into $2x - x$.* *(We could also have chosen any other non-zero natural number for x.)*
b Let $xRy \Rightarrow 2x - y = 5n,\ n \in \mathbb{Z}$ $\Rightarrow 2y - x = 4x - 10n - x = 3x - 10n$ $\Rightarrow 3x - 10n \neq 5k,\ k \in \mathbb{Z}$ Therefore $y \not{R} x$ R is not symmetric.	*Proof by counter-example* *Substitute $y = 2x - 5n$ into $2y - x$*
c $8R11$ $11R2$ $8 \not{R} 2$ R is not transitive.	*Proof by counter-example* $16 - 11 = 5$ $22 - 2 = 5 \times 4$ $16 - 2 = 14$ *and 14 is not a multiple of 5.*

A counter-example is a valid method to show that a property does not hold; in fact it is the most common method to disprove "for all" statements.

Example 19

Let $S = \{0, 2\pi\}$ and the relation $R = \{(0, 0), (0, 2\pi), (2\pi, 0), (2\pi, 2\pi)\}$.
Determine if R is an equivalence relation.

 R is reflexive because $0R0$ and $2\pi R 2\pi$ R is symmetric because $0R2\pi$ and $2\pi R0$. R is also transitive because: $0R2\pi$, $2\pi R2\pi$ and $0R2\pi$ $0R2\pi$, $2\pi R0$ and $0R0$ R is an equivalence relation of S.	*Draw a diagram to illustrate the relation.*

Note that when a relation includes all the elements of S × S the relation is an equivalence relation.

Exercise 1E

In questions 1 to 5 determine whether or not the given relation is an equivalence relation on the defined set.

1 For $a, b \in \mathbb{Z}$, $aRb \Leftrightarrow |a| = |b|$.

2 For $m, n \in \mathbb{Z}^+$, $mRn \Leftrightarrow$ "m and n have the same number of digits".

3 For $x, y \in \mathbb{R}$, $xRy \Leftrightarrow |x - y| \leq 3$.

4 For $x, y \in \mathbb{R}$, $xRy \Leftrightarrow x + y \in \mathbb{Z}$.

5 For $p, q \in \mathbb{Q}$, $pRq \Leftrightarrow p - q \in \mathbb{Z}$.

6 Let $S = \{f_i(x) | f_i(x) = m_i x + c_i$, where $m_i, c_i \in \mathbb{R}\}$. The relation R is defined on S such that $f_i(x) R f_j(x) \Leftrightarrow m_i = m_j$.
Show that R is an equivalence relation on S.

7 Let $S = \{f_i(x) | f_i(x) = m_i x + c_i$, where, $m_i, c_i \in \mathbb{R}\}$. The relation R is defined on S such that $f_i(x) R f_j(x) \Leftrightarrow m_i m_j = -1$.
Show that R is symmetric but not reflexive or transitive.

8 The relation R is defined on $\mathbb{Z}$ such that $mRn \Leftrightarrow m^2 \equiv n^2 (\text{mod}\, 4)$.
Show that R is an equivalence relation.

9 The relation R is defined on $\mathbb{R} \times \mathbb{R}$ such that
$(a, b)R(c, d) \Leftrightarrow a^2 + b^2 = c^2 - d^2$.
Determine whether or not R is an equivalence relation.

10 Let $S = \left\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\right\}$. The relation R is defined on S such that $\frac{a}{b} R \frac{c}{d} \Leftrightarrow ad = bc$. Determine whether or not R is an equivalence relation.

1.6 Equivalence classes and partitions

Refer back to Example 14 where we had $A = \{1, 2, 3, 4\}$ and $R \subseteq A \times A$ such that $R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4)\}$.

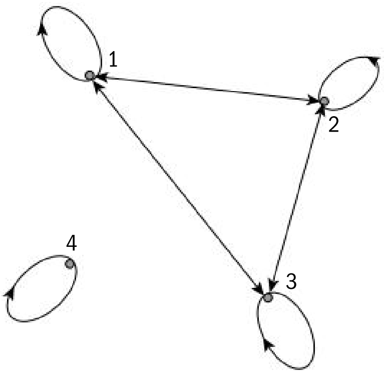
We create the set of those elements related to 1, i.e. $\{1, 2, 3\}$.

Similarly the set of those elements related to 2, i.e. $\{1, 2, 3\}$.

And the set of elements related to 3 would also be $\{1, 2, 3\}$.

Then the set of elements related to 4 is $\{4\}$.

We can also illustrate this by sketching a diagram.



This diagram shows the division of a set into 6 partitions by a given relation

Note that the equivalence relation R has separated A into two distinct subsets, $\{l, 2, 3\}$ and $\{4\}$. We call these the equivalence classes of the elements of A under the relation R. The relation has induced a partition of the set A into two disjoint subsets.

Now consider the relation $x \equiv y(\text{mod } 6)$ on $\mathbb{Z}^+$. We saw on page 28 that this relation distributes the positive integers into 6 distinct sets of integers as follows:

$[1] = x \equiv l(\text{mod}6) \Leftrightarrow x \in \{l, 7, 13, 19, \ldots\}$

$[2] = x \equiv 2(\text{mod}6) \Leftrightarrow x \in \{2, 8, 14, 20, \ldots\}$

$[3] = x \equiv 3(\text{mod}6) \Leftrightarrow x \in \{3, 9, 15, 21, \ldots\}$

$[4] = x \equiv 4(\text{mod}6) \Leftrightarrow x \in \{4, 10, 16, 22, \ldots\}$

$[5] = x \equiv 5(\text{mod}6) \Leftrightarrow x \in \{5, 11, 17, 23, \ldots\}$

$[0] = x \equiv 0(\text{mod}6) \Leftrightarrow x \in \{6, 12, 18, 24, \ldots\}$

Notice that the equivalence classes form a partition of the set A.

In some text books equivalence classes are denoted by $\bar{x}$ or $\dot{x}$.

We say that congruence modulo 6 divides $\mathbb{Z}^+$ into 6 distinct sets denoted by $\mathbb{Z}_6$. The relation has broken up the infinite set $\mathbb{Z}$ into a set of six infinite sets, each one called an equivalence class. These equivalence classes constitute a partition of the original set. Hence we say that an equivalence relation induces a partition of the set.

Definition

An **equivalence class** $[x]$ under an equivalence relation R on a set A is the set of all elements related to x in A,

i.e. $[x] = \{a \mid a \in A, aRx\}$.

Let's refer back to Example 16 where $A = \{3, 4, 5, 9, 10, 11, 13\}$ and $aRb \Leftrightarrow |a - b|$ is divisible by 5.

$R = \{(3, 3), (4, 4), (5, 5), (9, 9), (10, 10), (11, 11), (13, 13), (3, 13), (4, 9), (5, 10), (13, 3), (9, 4), (10, 5)\}$

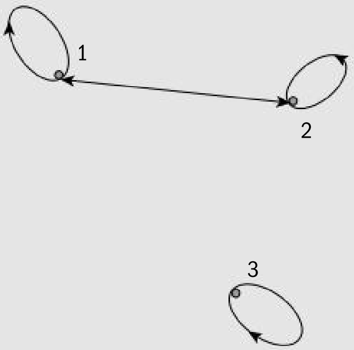
The equivalence classes induced by this relation are
$[3] = \{3, 13\}$, $[4] = \{4, 9\}$, $[5] = \{5, 10\}$ and $[11] = \{11\}$

[3] is an equivalence class consisting of {3, 13} because $3R3$ and $3R13$. No other element in A is related to 3.

Example 20

Let $S = \{1, 2, 3\}$.
The relation $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$.Show that R is an equivalence relation and find the partition of the set S induced by R.

It is easy to check that R is reflexive, symmetric and transitive. So R is an equivalence relation on S.
We can illustrate the relation on a diagram.



A diagram helps us visualize the equivalence classes.

Under the relation R, $[1] = \{1, 2\}$ and $[2] = \{1, 2\}$ and $[3] = \{3\}$.
Since $[1] = [2]$, $\{[1], [3]\}$ or $\{[2], [3]\}$ are partitions of S.

Example 21

$T = \{\text{triangles}\}$ and R is defined on T such that for $a, b \in T$, $aRb \Leftrightarrow a$ is similar to b. Determine whether R is an equivalence relation and explain the equivalence classes of T under R.

Any triangle is similar to itself.
$aRa \Rightarrow R$ is reflexive

Check the properties for an equivalence relation.

Triangles whose angle measures are the same are similar to each other.
$aRb \Rightarrow bRa \Rightarrow R$ is symmetric

Check the properties for an equivalence relation.

Similar triangles are triangles of the same shape.

Check the properties for an equivalence relation.

$$\left.\begin{array}{l} aRb \Rightarrow a \text{ is similar to } b \\ bRc \Rightarrow b \text{ is similar to } c \end{array}\right\} a \text{ is similar to } c$$

$aRc \Rightarrow R$ is transitive

Hence, R induces the partition of T into those triangles which are similar to each other.

Note that in all the examples seen so far the equivalence classes formed by a particular relation are disjoint. In the following theorem we will prove that an equivalence relation generates a collection of disjoint subsets whose union is the set itself.
In other words, we will now formally prove that an equivalence relation R on a set A induces a partition of A.

Theorem 6

Equivalence classes formed by an equivalence relation on a set A are disjoint, and their union is A.

Proof:

First we need to prove that $[x_i]$ are disjoint for different values of i.

Assume that two equivalence classes $[x_i]$ and $[x_j]$ are not disjoint. Then there must be some $a \in A$ such that $a \in [x_i]$ and $a \in [x_j]$.
By definition of equivalence classes this means that aRx where $x \in [x_i]$ and aRy where $y \in [x_j]$.

Because of the symmetric and transitive properties, this can be true only if $[x_i] \subseteq [x_j]$ and $[x_j] \subseteq [x_i] \Rightarrow [x_i] = [x_j]$.

That is, if aRx then xRa since R is symmetric, and xRa together with aRy implies that xRy because R is transitive. Hence $[x_i] = [x_j]$.

Therefore equivalence classes are disjoint.

Now we need to prove that the equivalence classes are exhaustive, i.e. all of set A is partitioned by the set of equivalence classes.

Since R is an equivalence relation we know that it is reflexive:

xRx for all $x \in R$

The most trivial case of the partition would be when each equivalence class has only one element.

So at least one element $x \in [x]$, which means that there is no element in A which does not belong to an equivalence class.
This means that the equivalence classes $[x_i]$ partition the set A.

We say that an equivalence relation *induces* a partition of a set. Q.E.D.

In the following example you will see how an equivalence relation on $\mathbb{R}^2$ divides the plane into equivalence classes that can be described geometrically.

Example 22

A relation R is defined on $\mathbb{R} \times \mathbb{R}$ as follows: $(a, b)\,R\,(c, d) \Leftrightarrow 2a - b = 2c - d$

a Show that R is an equivalence relation.

b Find the equivalence classes and explain them geometrically.

a $(a, b)R(a, b)$

$2a - b = 2a - b$ *for all* $a, b \in R$

Therefore R is reflexive.

$(a, b)R(c, d) \Leftrightarrow 2a - b = 2c - d$

$\Rightarrow 2c - d = 2a - b$

$\Rightarrow (c, d)R(a, b)$

Therefore R is symmetric.

$(a, b)R(c, d) \Leftrightarrow 2a - b = 2c - d$

$(c, d)R(p, q) \Leftrightarrow 2c - d = 2p - q$

$\Rightarrow 2a - b = 2p - q$

$\Rightarrow (a, b)R(p, q)$

Therefore R is transitive, hence R is an equivalence relation.

Show that the properties of equivalence relations are satisfied.

b Let $(x, y) \in [(a, b)]$

$2x - y = k$ where $k = 2a - b$

$\Rightarrow y = 2x - k$

This represents the set of lines parallel to $y = 2x$.

One of these lines would be the line $y = 2x \Rightarrow (x, y) \in [(1, 2)]$

In the following example we will look at a relation that categorizes the integers into odd and even numbers.

Example 23

The relation R is defined on $\mathbb{Z}$ such that $aRb \Rightarrow a + b$ is even.

a Show that R is an equivalence relation.

b Find the partitions of $\mathbb{Z}$ under R.

a aRa

$a + a = 2a \Rightarrow aRa \in \mathbb{Z}$

Therefore R is reflexive.

Show that the properties of equivalence relations are satisfied.

$aRb \Rightarrow a + b$ is even

$\Rightarrow b + a$ is even $\quad \Rightarrow bRa$

Addition is commutative in $\mathbb{Z}$.

Therefore R is symmetric.

$aRb \Rightarrow a + b = 2p \qquad p \in \mathbb{Z}$

$bRc \Rightarrow b + c = 2q \qquad q \in \mathbb{Z}$

$\Rightarrow a + c = 2(p + q - b) \quad \Rightarrow aRc$

Therefore R is transitive.

If a is odd then c must be odd and if a is even then c must also be even.

b Let $x \in [a]$

$\Rightarrow xRa \Rightarrow x + a = 2n$

Therefore R partitions $\mathbb{Z}$ into two equivalence classes [1] and [2] which represent the odd and even numbers respectively.

Under R

$\mathbb{Z} = \{\mathbb{Z}_1 \cup \mathbb{Z}_2\}$ *since*

$\mathbb{Z}_1 = 1(\text{mod } 2) = \{\text{odd numbers}\}$

$\mathbb{Z}_2 = 0(\text{mod } 2) = \{\text{even numbers}\}$

The next relation organizes ordered pairs of integers along lines passing through the origin.

Example 24

The relation R is defined on $\mathbb{Z}^+ \times \mathbb{Z}^+$ such that $(a, b)R(c, d) \Rightarrow ad = cb$. Show that this is an equivalence relation and give a geometric description of the equivalence classes.

$(a, b)R(a, b)$

$ab = ab$

Therefore R is reflexive

Show that the properties of an equivalence relation hold.

$(a, b)R(c, d) \Rightarrow ad = cb$

$\Rightarrow cb = ad$

$\Rightarrow (c, d)R(a, b)$

Therefore R is symmetric

$(a, b)R(c, d) \Rightarrow ad = cb \Rightarrow adq = cbq$

$(c, d)R(p, q) \Rightarrow cq = dp \Rightarrow cqb = dpb$

$\Rightarrow adq = cbq = dpb \Rightarrow aq = pb$

$\Rightarrow (a, b)R(p, q)$

Therefore the relation is transitive.

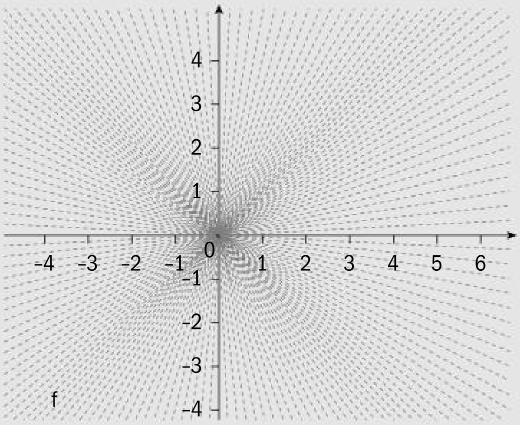
Let $(x, y) \in [(a, b)]$

$\Rightarrow xb = ay$

$\Rightarrow y = \frac{b}{a}x$

The equivalence class $[(a, b)]$ represents ordered pairs of positive integers which lie on the straight lines passing through the origin with gradient $\frac{b}{a}$.

This is illustrated on the diagram below:



Example 25

The relation R is defined on $S = \{x \mid x \in \mathbb{Z}^+, x \leq 15\}$ by $aRb \Leftrightarrow a(a-1) \equiv b(b-1) (\text{mod } 7)$.

a Show that R is an equivalence relation.

b Show that the equivalence R can be written in the form $(a-b)(a+b-1) \equiv 0 (\text{mod } 7)$.

c Hence, or otherwise, determine the equivalence classes.

a $a(a-1) \equiv b(b-1)(\text{mod } 7)$ $\Rightarrow a(a-1) - b(b-1) = 7n, n \in \mathbb{Z}$	*We need to confirm the properties of an equivalence relation.*
Reflexive: $aRa \Rightarrow a(a-1) \equiv a(a-1)(\text{mod } 7)$ $a(a-1) - a(a-1) = 0n = 0$	
Symmetric: $aRb \Rightarrow a(a-1) - b(b-1) = 7n$ $\Rightarrow b(b-1) - a(a-1) = 7(-n) \Rightarrow bRa$	
Transitive: $aRb \Rightarrow a(a-1) - b(b-1) = 7n$	
$bRc \Rightarrow b(b-1) - c(c-1) = 7m$	*Add the two equations.*
$\Rightarrow a(a-1) - c(c-1) = 7(n+m)$ $\Rightarrow aRc$	
b $a(a-1) - b(b-1) = 7n$	
$\Rightarrow a^2 - a - b^2 + b = 7n$	*Expand.*
$\Rightarrow (a-b)(a+b-1) = 7n \equiv 0(\text{mod } 7)$	*Rearrange and factorize.*
c $\Rightarrow (a-b)(a+b-1) = 7n.$	
$a - b = 7n$ or $a + b - 1 = 7n, n \in \mathbb{Z}$ Therefore the equivalence classes are:	*Since the product is divisible by 7* *$b = a - 7n$ or $b = 7n - a + 1$*
$[1] = \{1, 7, 8, 14, 15\}$	*substitute $a = 1$ and $n = 0, 1, 2$*
$[2] = \{2, 6, 9, 13\}$	*substitute $a = 2$ and $n = 0, 1, 2$*
$[3] = \{3, 5, 10, 12\}$	*substitute $a = 3$ and $n = 0, 1, 2$*
$[4] = \{4, 11\}$	*substitute $a = 4$ and $n = 0, 1, 2$*

The next example illustrates how the infinite set $\mathbb{Z}^2$ is partitioned into six equivalence classes.

Example 26

The relation R is defined on $\mathbb{Z} \times \mathbb{Z}$ such that $(a, b)R(c, d)$ if and only if $a - c$ is divisible by 2 and $b - d$ is divisible by 3.

a Show that R is an equivalence relation.

b Find the equivalence class for (1, 3).

c Write down the five remaining equivalence classes.

a Reflexive: $(x, y)R(x, y)$
since $x - x = 0$ and $y - y = 0$
which are both divisible by 2 and 3
so R is reflexive.

We need to confirm the properties of an equivalence relation.

Symmetric:
$(x, y)R(a, b)$

$\Rightarrow x - a = 2m,\ m \in \mathbb{Z}$

$\Rightarrow a - x = -2m$

$y - b = 3n,\ n \in \mathbb{Z}$

$\Rightarrow b - y = -3n$ so R is symmetric.

Transitive:

$(x, y)R(a, b)$ and $(a, b)R(c, d)$

$$\left.\begin{aligned} x - a &= 2p \\ a - c &= 2p \end{aligned}\right\} \Rightarrow x - c = 2(p + q)$$

$$\left.\begin{aligned} y - b &= 3m \\ b - c &= 3n \end{aligned}\right\} \Rightarrow y - c = 3(m + n)$$

$(x, y)R(c, d)$ so R is transitive.

Therefore R is an equivalence relation.

b $(x, y)R(1, 3)$

Let $x - 1 = 2m \Rightarrow x = 2m + 1$

$y - 3 = 3n \Rightarrow y = 3n + 3 = 3n$

Since n is any integer we can write 3n.

So

$[(1, 3)] = \{(x, y) \mid x = 2m + 1, y = 3n,$
m, n *elements of Z*$\}$

c The other equivalence classes will be

$\{(x, y) \mid x = 2m, y = 3n\}$ i.e. $[(2,3)]$

$\{(x, y) \mid x = 2m, y = 3n + 1\}$ i.e. $[(2,1)]$

$\{(x, y) \mid x = 2m, y = 3n + 2\}$ i.e. $[(2,2)]$

$\{(x, y) \mid x = 2m + 1, y = 3n + 1\}$ i.e. $[(1,1)]$

$\{(x, y) \mid x = 2m + 1, y = 3n + 2\}$ i.e. $[(1,2)]$

Example 27

The relation R is defined on cubic polynomials P of the form
$P_n(z) = z^3 + az^2 + bz$ where $a, b \in \mathbb{R}, z \in \mathbb{C}$.
The relation R is defined by P_1RP_2 if and only if the
sum of the three zeros of P_1 is equal to the sum of the three zeros of P_2.

a Show that R is an equivalence relation.

b Determine the equivalence class containing $z^3 - 2z^2 + 8z$.

---

a Let the zeros of $P_n(z)$ be $\alpha_n, \beta_n, \gamma_n$

Since $P_n(z) = z(z^2 + az + b)$
We know that $\alpha_n = 0$ for all n
So sum of roots becomes $\beta_n + \gamma_n = -a$

Using Viete's theorem about sum and product of roots.

Reflexive:
$P_n(z)RP_n(z)$
The sum of the zeros of $P_n(z)$ is equal to the sum of the zeros of $P_n(z)$.

Symmetric:

$P_1(z)RP_2(z) \Rightarrow \beta_1 + \gamma_1 = \beta_2 + \gamma_2 = -a$
$\Rightarrow P_2RP_1$

Coefficient of z^2 is the same in both cubic polynomials.

Transitive:

$P_1(z)RP_2(z) \Rightarrow \beta_1 + \gamma_1 = \beta_2 + \gamma_2 = -a$
$P_2RP_3 \Rightarrow \beta_2 + \gamma_2 = \beta_3 + \gamma_3 = -a$

Coefficient of z^2 is the same in all three cubic polynimials.

$\Rightarrow \beta_1 + \gamma_1 = \beta_3 + \gamma_3$
$\Rightarrow P_1(z)RP_3(z)$

Using Viete's theorem.

Therefore R is an equivalence relation.

b The equivalence class containing $z^3 - 2z^2 + 8z$ consists of cubic polynomials of the form $z^3 - 2z^2 + bz$

One of the roots is zero and the sum of roots must be two. The product of the two remaining zeros could be any number.

Exercise 1F

1 Consider the set of words:
$W = \{$set, table, chair, car, tennis, bike, stairs, sea, wave, sun$\}$.
In **a** and **b**, show that R is an equivalence relation and list the equivalence classes induced by each relation on W.

a R is the relation on W, "has the same number of letters".

b R is the relation on W, "starts with the same letter of the alphabet".

2 **a** Let $L = \{l_i | l_i$ is a line segment of length $|l_i|\}$. Let R be a relation on L such that $l_i \, R \, l_j \Leftrightarrow |l_i| = |l_j|$. Show that this is an equivalence relation on L and describe the partition induced by R.

b Let $P = \{$polygons$\}$ and R be a relation on P such that $aRb \Leftrightarrow$ 'a has the same number of sides as b'. Show that R is an equivalence relation and describe the partitions induced by R.

3 Let $P = \{f(x) | f(x) = ax^2 + bx + c$, with $a, b, c \in \mathbb{R}\}$. The relation R on P is such that $f(x)Rg(x) \Leftrightarrow f(0) = g(0)$. Show that R is an equivalence relation and describe the partition induced by R on P.

4 Let $S = \{(x, y) | \; x, y \in \mathbb{R}\}$. Let R be a relation on S such that $aRb \Rightarrow a^2 + b^2 = r^2$ where $r \in \mathbb{R}^+$.
Show that R is an equivalence relation and give a geometric meaning of the partitions of $\mathbb{R} \times \mathbb{R}$ under this relation.

5 Let R be a relation on $\mathbb{Z}^+$ such that $aRb \Leftrightarrow a + 2b$ is divisible by 3. Show that R is an equivalence relation and list the equivalence classes of $\mathbb{Z}^+$ under this relation.

6 Let R be a relation defined on $\mathbb{Z}^+$ such that $aRb \Leftrightarrow a^2 = b^2 \pmod 3$. Show that R is an equivalence relation and list the equivalence classes of $\mathbb{Z}^+$ under this relation.

7 Show that the relation R defined on $\mathbb{R}^2$ such that $(a, b)R(c, d) \Leftrightarrow a = c$ is an equivalence relation and give a geometrical description of the equivalence class $[(a, b)]$.

8 Show that the relation R defined on $(\mathbb{Z}^+)^2$ such that $(a, b)R(c, d) \Leftrightarrow ad = cb$ is an equivalence relation. Describe the equivalence class $[(1, 2)]$. Hence or otherwise describe the partition induced by R on $(\mathbb{Z}^+)^2$.

9 Let R be a relation defined on $\{\mathbb{R}^2 \setminus (0, 0)\}$ such that $(a, b)R(c, d) \Leftrightarrow ab = cd$. Show that R is an equivalence relation on $\{\mathbb{R}^2 \setminus (0, 0)\}$. Describe the equivalence class $[(1, 1)]$. Hence or otherwise describe the partition induced by R.

10 Consider the relation R on $\mathbb{Q}$ such that $xRy \Rightarrow x - y \in \mathbb{Z}$.

a Show that this is an equivalence relation.

b Determine the equivalence class [0] for this relation.

c Determine the equivalence class $\left[\frac{3}{4}\right]$ for this relation.

d Describe the partition induced by R on the rational numbers.

Review exercise

EXAM-STYLE QUESTIONS

1 A, B and C are subsets of the universal set U.

a Use Venn diagrams to illustrate

i $A \backslash B = A \cap (U \setminus B)$

ii $(A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$

b Use double inclusion to prove that $A \backslash B = A \cap (U \setminus B)$.

c Use De Morgan's laws to prove that $(A \backslash B) \cup (B \backslash A)$
$= (A \cup B) \backslash (A \cap B)$.

2 A, B and C are subsets of the universal set U. Use Venn diagrams to illustrate the distributive laws. Use these properties and De Morgan's laws to show that $(A' \cap B) \cup C' = (A \cap C)' \cap (B' \cap C)'$

3 The relation R on $\mathbb{C} \setminus \{0\}$ is defined as: $z_1 R z_2 \Leftrightarrow \arg z_1 = \arg z_2$ for $z_1, z_2 \in \mathbb{C} \setminus \{0\}$.

a Show that R is an equivalence relation on $\mathbb{C}$.

b Describe the equivalence classes under the relation R.

4 Sets A, B, C, D and E are subsets of $\mathbb{Z}$:

$A = \{n \mid 0 < n < 20, n \text{ is a prime number}\}$

$B = \{n \mid |n - 2| \le 1\}$

$C = \{n \mid n^2 - 3n - 4 < 0\}$

$D = \{n \mid n^5 = 16n\}$

$E = \{n \mid (n - 1)^2 \le 4\}$

a List the elements of each of these sets.

b Determine, giving reasons, which of the following statements are true and which are false.

i $n(A) = n(D) + n(E)$

ii $n(D \cap A') = 1$

iii $B \subset E$

iv $(D \setminus B) \cap A = \varnothing$

v $C \Delta E = \varnothing$

5 Let R be a relation on $\mathbb{Z}$ such that $aRb \Leftrightarrow 5ab \leq 0$.

a Determine whether R is

i reflexive

ii symmetric

iii transitive.

b Write down whether or not R is an equivalence relation and give a reason for your answer.

6 The relation R is defined on the set $\mathbb{N}$ such that for $a, b \in \mathbb{N}$, $aRb \Leftrightarrow a^3 \equiv b^3 \pmod 5$.

a Show that R is an equivalence relation.

b Denote the equivalence class containing n by C_n.

i Find C_0.

ii List the first six elements of C_1.

iii Prove that $C_n = C_{n+5}$ for all $n \in \mathbb{N}$.

7 P is the set of polynomials of the form $P(z) = z^2 + bz + c$ where $b, c \in \mathbb{R}$ and $z \in \mathbb{C}$.

a The relation S on the set P is such that $P_1RP_2 \Leftrightarrow$ the sum of the zeros of P_1 is equal to the sum of the zeros of P_2.

i Show that S is an equivalence relation.

ii Determine the equivalence class containing the polynomial $P = z^2 - 3z + 4$.

b The relation R on the set P is such that $P_1RP_2 \Leftrightarrow$ the product of the zeros of P_1 is equal to the product of the zeros of P_2.

i Show that R is an equivalence relation.

ii Determine the equivalence class containing the polynomial $P = z^2 - 3z + 4$.

8 The relation R is defined on $\mathbb{Z}^+$ such that $aRb \Leftrightarrow 5^a \equiv 5^b \pmod 8$.

a Show that R is an equivalence relation.

b Identify the two equivalence classes formed by this relation.

c Find the value of $5^{355} \pmod 8$.

9 The relation R is defined on $\mathbb{Z} \times \mathbb{Z}$ such that $(a, b)R(c, d)$ if and only if $a = c$ and $b - d$ is divisible by 5.

a Prove that R is an equivalence relation.

b Describe the equivalence classes induced by R.

10 The relation S is defined on quadratic polynomials P of the form:

$P(z) = z^2 + az + b$, where $a, b \in \mathbb{R}, z \in \mathbb{C}$.

The relation S is defined by P_1SP_2 if and only if P_1 and P_2 have at least one zero in common. Determine whether or not S is transitive.

11 The points in a plane or space are given. $\overrightarrow{AB}$ is a directed line segment where A is the starting point and B is the terminal point.

$\overrightarrow{AB}\ R\ \overrightarrow{CD}$ if line segments $[AD]$ and $[BC]$ have a common midpoint.

a Show that R is an equivalence relation.

b Give a geometrical description of the partition of all the directed line segments in a plane or space.

Chapter 1 summary

A set S is a collection of objects. If x is one of these objects we say $x \in S$.

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

The **empty set** denoted by $\varnothing = \{\ \}$.

$B \subseteq A$ and $A \subseteq B \Leftrightarrow A = B$. The converse of this is also true, i.e. if A and B are equal sets then A is a subset of B and B is a subset of A.

If set $S \subseteq U$, then the **complement** of S is denoted by S' where $S' = \{x \in U \mid x \notin S\}$.

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

The **union** of two sets A and B is denoted by $A \cup B$ where $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

If $A \cap B = \varnothing$ then A and B are said to be **disjoint** sets.

The set consisting of those elements that are in set A but not in set B is called the **set difference** B from A denoted by $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\} = A \cap B'$.

The **symmetric difference** of two sets A and B is denoted by $A \Delta B$ and consists of those elements which are either in A or in B but not in both A and B. $A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$.

The power set of a finite set S with n elements is the set of all subsets of S including the empty set $\varnothing$ and S itself. The total number of distinct subsets of a finite set S with n elements is 2^n. $n(P(S)) = 2^n$

Commutative Laws

$A \cup B = B \cup A$

$A \cap B = B \cap A$

Distributive laws

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, i.e. intersection is distributive over union
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, i.e. union is distributive over intersection

Associative laws

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

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

De Morgan's Laws

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

Cartesian product

$A \times B = \{(a, b) : a \in A, b \in B\}$

A relation R defined on a set A is said to be an **equivalence relation** if the following three conditions are true:

- R is **reflexive**, i.e. aRa for all $a \in A$
- R is **symmetric**, i.e. $aRb \Rightarrow bRa$ for all $a, b \in A$
- R is **transitive**, i.e. aRb and $bRc \Rightarrow aRc$ for all $a, b, c \in A$

a is **congruent** to b **modulo** n if n divides $(a - b)$, i.e. $a - b = kn, k \in \mathbb{Z}$.

Notation: $a \equiv b(\text{mod } n) \Leftrightarrow n|a - b$

An **equivalence class** $[x]$ under an equivalence relation R on a set A is the set of all elements related to x in A, i.e. $[x] = \{a \,|\, a \in A, aRx\}$.

A **partition** of a set A consists of another set P made up of non-empty subsets of A which are disjoint and whose union makes up the whole set.

Equivalence classes are mutually exclusive and the set A is partitioned into equivalence classes by an equivalence relation R on A.

2 Extension of the concept of function

CHAPTER OBJECTIVES:

8.3 Functions: injections, surjections, bijections; composition of functions and inverse functions.

8.4 Binary operations and operation tables (Cayley tables).

8.5 Binary operations: associative, distributive and commutative properties.

8.6 The identity element *e*.
The inverse a^{-1} of an element *a*.
Proof that left-cancellation and right-cancellation by an element *a* hold, provided that *a* has an inverse.
Proofs of the uniqueness of the identity and inverse elements.

Before you start

You should know how to:

1 Find the intervals for which the function $f(x) = \frac{10x}{x-2}$, $x \neq 2$ is increasing or decreasing. Find the derivative:

$$f'(x) = \frac{(x-2)(10) - 10x}{(x-2)^2} = \frac{-20}{(x-2)^2}$$

Since $f'(x) < 0$ for all values of x in the domain, it follows that $f(x)$ is a strictly decreasing function.

2 Find the inverse of the function $f(x) = \frac{x+1}{x-1}$, where $x \in \mathbb{R}$, $x \neq 1$ and state its domain.

Interchange y and x, and make x the subject of the formula:

$$x = \frac{y+1}{y-1} \quad \Rightarrow x(y-1) = y+1$$

$$\Rightarrow xy - y = x + 1$$

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

$f^{-1}(x) = \frac{x+1}{x-1}$ where $x \in \mathbb{R}$, $x \neq 1$

Skills check:

1 When a certain drug is administered, the concentration of medication in the bloodstream t hours after the drug is administered is given by: $A(t) = \frac{4t}{3t^2 + 27}$

a Over which interval of time is the concentration of medication increasing?

b Over which interval is the concentration decreasing?

2 Find the inverse function for each of the following:

a $f : x \mapsto \frac{x+3}{x+2}$, $x \neq -2$

b $f : x \mapsto 2^x$

c $f : x \mapsto e^x - 2e^{-x}$

Evolution of the function concept

So far you have studied functions as formulas defined on real number sets where every ordered pair $(x, y) \in \mathbb{R}^2$ represented a dependent variable $y \in \mathbb{R}$ which was a function of $x \in \mathbb{R}$, the independent variable. You learned that, for any given function, there is a rule that determines the unique value of y for any value of x and this could be illustrated by a graph of this function, e.g. the ordered pair (–1, 5) would be a point on the graph of $f(x) = 2x^2 + 3$.

The term "function" first appeared in a letter written by Leibniz in 1673. He used it to describe quantities related to curves. In 1755 Euler introduced a more general concept when he wrote *"When certain quantities depend on others in such a way that they undergo a change when the latter change, then the first are called functions of the second."*

In the 19th century more emphasis was placed on rigour in mathematics. The notion of function continued to evolve with the development of Set Theory by Cantor. Cauchy was the first to consider the fact that a function may have a restricted domain. This eventually led to the definition of functions by Dedekind in 1888 that said a function is a single-valued relation between two non-empty sets. However the most accurate definition of a function was given by Nicolas Bourbaki in 1939 which described a function as a possibly infinite set of ordered pairs (x, y) in which each x is paired with only one y.

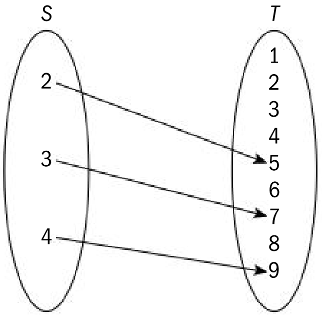
? The name Nicolas Bourbaki does not represent just a single mathematician. A small group of French mathematicians used this name as a pseudonym in the mid 1930's. The group was originally formed to write rigorous textbooks based on Set Theory initiated by Cantor. However their work included studies of many branches of mathematics including Topology.

2.1 Functions as relations

A **relation** that associates each element in a non-empty set S with a unique element in a non-empty set T is called a function from S to T.

A function from S to T is a subset M of $S \times T$ such that for every $s \in S$ there is a unique $t \in T$ such that $(s, t) \in M$.

For example: $S = \{2, 3, 4\}$, $T = \{1, 2, 3, \dots, 9\}$ and $M = \{(2, 5), (3, 7), (4, 9)\}$. We can represent this pictorially as shown here.



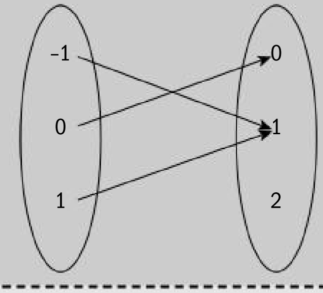
2 is mapped onto 5 so we say that 5 is the image of 2 under this function. The function has a rule that enables us to find the image of every element of S under f. In this case the rule is $f(s) = 2s + 1$.
We denote this function by $f : S \to T$ such that $s \mapsto 2s + 1$ for all $s \in S$.

The set S is called the **domain** and T, the target set, is called the **co-domain**. The set $f(S) = \{t \mid t \in T, t = f(s) \text{ for some } s \in S\}$ is called the **range**. It is the set containing all the images of S under the function f. In the above example the range is the set $\{5, 7, 9\}$.

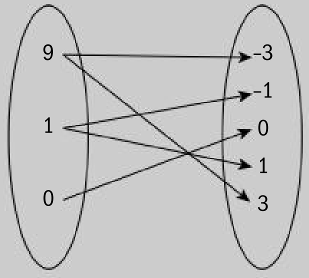
Example 1

Determine which of the following relations are functions, and state the domain and the range for those which are functions.

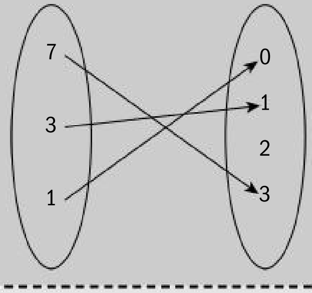
a



b



c



a This is a function.
Domain $\{-1, 0, 1\}$, Range $\{0, 1\}$

Each element on the domain has a unique image in the co-domain.

b This is not a function.
In this relation 9 and 1 are mapped to ± 3 and ± 1 respectively, hence 9 and 1 are not mapped to unique elements.

c This is a function.
Domain $\{1, 3, 7\}$, Range $\{0, 1, 3\}$

Each element is mapped to a unique image.

Example 2

Determine which of these relations are functions:

a R on $\mathbb{Z}$ such that $aRb \Leftrightarrow a^2 = b^2$

b R on $\mathbb{R}^+$ such that $aRb \Leftrightarrow a^2 = b^2 - 1$

a This is not a function.	
$1R1$ since $1^2 = 1^2$	
$1R\,(-1)$ since $1^2 = (-1)^2$	
Therefore 1 is mapped to two distinct elements so it is not a function.	
b Suppose this is not a function. Then:	
$aRb \Rightarrow a^2 = b^2 - 1$	*Subtraction of the two equations yields:*
$aRc \Rightarrow a^2 = c^2 - 1$	$0 = b^2 - c^2$
$\Rightarrow b^2 = c^2$	
$b = c$	*Since R is defined on* $\mathbb{R}^+$
Therefore R is a function.	*Proved by contradiction.*

There are two rules governing functions as follows:

- $f(s)$ must specify an element of T for every $s \in S$
- if $s = s'$ and both $s, s' \in S$ then $f(s) = f(s')$

Although the above rules may look trivial, they actually have strong implications. They make sure that there are no contradictory or ambiguous connotations. Let's take the example of a function defined on the rational numbers as follows:

Let $f : \mathbb{Q} \rightarrow \mathbb{Q}$ such that $f\left(\frac{p}{q}\right) = \frac{q}{p}$.

Because the domain of this function is $\mathbb{Q}$, every element of $\mathbb{Q}$ must have an image in $\mathbb{Q}$. However by the definition of this function it is clear that 0 does not have an image because division by zero is undefined. In other words the first rule ensures that we do not have any singularities.

> You have met and discussed singularities in the core book, when discussing limits and graphs of functions. At a singularity the mathematical function is not defined or is not "well-behaved", e.g. $f(x) = \frac{x^2 - 1}{x + 1}$, has a singularitiy at $x = -1$ and the graph is a straight line with a 'hole' at $x = -1$. Similarly the function $f(x) = \frac{1}{x}$ is not defined when $x = 0$ and so this is a vertical asymptote. The function also has a singularity at $x = 0$. The function $f(x) = |x - 1|$ is continuous but it is not differentiable at $x = 1$. Once more there is a singularity at $x = 1$. The function is said to be "not well-behaved" at $x = 1$.

The second rule ensures that the function is well-defined. In other words, it ensures that each element of the domain has only one image in the co-domain. This is illustrated by the following example in which the rule is violated.

Suppose that $f:\mathbb{Q}\to\mathbb{Q}$ such that $f\left(\frac{p}{q}\right)=\frac{1}{q}$.

But $f\left(\frac{2}{5}\right)=\frac{1}{5}$ and $f\left(\frac{10}{25}\right)=\frac{1}{25}$ which violates the second rule governing functions.

Equality of functions

Two functions $f:S\to T$ and $g:P\to Q$ are equal if and only if $S=P$, $f(S)=g(P)$ and $f(a)=g(a)$ for all values of $a\in S$.

We can illustrate this property by looking at some functions.

Consider the functions $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}\setminus\{0\}$ such that $f(x)=\frac{x}{x^2}$,

and $g:\mathbb{R}\setminus\{0\}\to\mathbb{R}\setminus\{0\}$ such that $g(x)=\frac{1}{x}$.

These two functions are equal because they both have the same domain which excludes $x=0$ and for all values of x in the domain, $f(x)=g(x)$.

Now let us define another two functions as follows:

$f(x)=x$ with domain $x\in\mathbb{R}$
$g(x)=\arccos(\cos x)$ with domain $x\in\mathbb{R}$

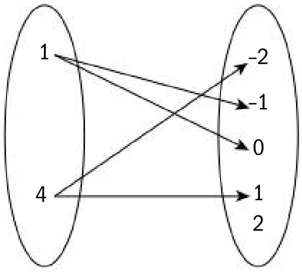
If we compare these two functions we see that $f(2\pi)=2\pi$, but $g(2\pi)=\arccos(\cos 2\pi)=\arccos(1)=0$. The image of 2π under f is different to the image of 2π under g, so the functions are not equal. These two functions are equal only if we restrict both domains to $x\in\mathbb{R}$, $0\le x<2\pi$.

Definition

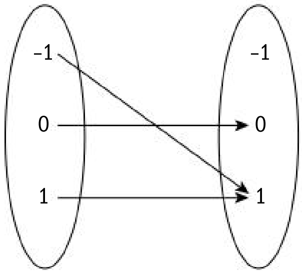
A function is said to be injective if it preserves distinctness. In other words, every element of the co-domain is mapped to by no more than one element in the domain. A function $f:S\to T$ for which each element of the range, $f(S)$, corresponds to exactly one element of the domain, S, is said to be **injective**. In other words, if $f(a)=f(b)\Rightarrow a=b$ for $a,b\in S$. A logically equivalent statement would be: $a\ne b\Rightarrow f(a)\ne f(b)$.

We say that an injective function is one in which each element of $f(S)$, the range of the function, is the image of only one element of S, the domain of the function. An injective function is therefore a one-to-one function.

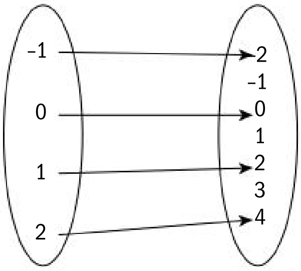
For a function to be injective we can state that if *a* is not equal to *b* in the domain, then *f*(*a*) is not equal to *f*(*b*) in the co-domain. The **contrapositive** statement of this is that if *f*(*a*) = *f*(*b*) then *a* = *b*. Contrapositive statements are useful when it is difficult to examine all the different elements of the domain to check for unique images in the co-domain. Then it is much easier to check by using the logically equivalent contrapositive statement.



One-to-many : not a function



Many-to-one : is a function



One-to-one : injective function

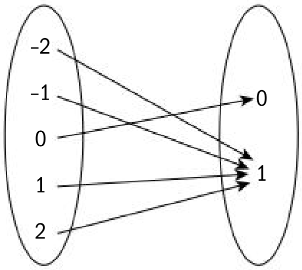
The diagrams above illustrate three types of mapping.

- The first mapping is not a function because elements 1 and 4 both have two images in the co-domain.
- The second mapping is a function because each element in the domain is mapped onto a unique element in the co-domain. It is not injective because $1 \in$ co-domain is the image of -1 and 1 in the domain. Alternatively we can say that two different elements 1 and -1 from the domain don't have two different images in the co-domain but have the same image of 1. The function doesn't preserve distinctness.
- The third mapping is a function because each element in the domain is mapped onto a unique element in the co-domain. It is also injective because each element in the range is the image of only one element in the domain.

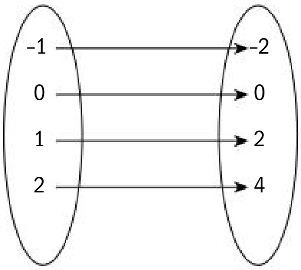
Definition

If every element in the co-domain of a function is the image of at least one element in the domain we say that the function is a **surjection**, i.e. for all b in the co-domain there exists an a in the domain such that $f(a) = b$. A surjection is also called an **onto** function.

None of the previous three examples represent surjections. The two examples below illustrate surjections.



Many-to-one : surjection



One-to-one correspondence : injection and surjection

To check for injection we look at the elements in the domain and check that different elements have different images in the co-domain. We can establish a relationship between the cardinality of sets S and T as follows: $n(S) \le n(T)$. For a surjection we look at the elements in the co-domain and check that they are all images. So for a surjection, $n(T) \le n(S)$. If a function is both surjective and injective then $n(S) = n(T)$. This is the case in the second mapping above.

Definition

A function is a **bijection** if it is an injection and a surjection.
A bijection is also called a one-to-one correspondence.

In the core book we studied functions of real variables, i.e. when the domain was a subset of $\mathbb{R}$. It is good to remember that a graph that did not pass the vertical line test did not represent a function. This is a one-to-many relation. If a function passed the horizontal line test then the function is an injective function. Graphically speaking, if a horizontal line drawn in any region of the co-domain crosses the graph exactly once then the function is a bijection. We also say that the function is surjective if any horizontal line drawn in any region of the co-domain crosses the graph at least once.

Example 3

$A = \{1, 2, 3, 4\}$ and $B = \{5, 6, 7, 8, 9\}$. Given that $f : A \to B$ such that $f(x) = x + 4$, determine whether f is an injection, a surjection or both.

$f(a) = f(b)$ $\Rightarrow a + 4 = b + 4$ $\Rightarrow a = b$ So f is an injection.	*Assume two elements in the co-domain are equal. Prove that they are the images of the same element in the domain.*
Let $y \in B \Rightarrow y = x + 4, x \in A$ $\Rightarrow x = y - 4$ $y = 9 \Rightarrow x = 5 \quad 5 \notin A$ So f is not a surjection.	*Given any element in the co-domain try to find an element in the domain which maps onto it. It is sufficient to find one such element for which the statement is not true.*

Example 4

Given $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = x + 4$, determine whether f is an injection, a surjection or both.

$f(a) = f(b)$ $\Rightarrow a + 4 = b + 4$ $\Rightarrow a = b$	*Use the contrapositive statement of injective functions.*
So f is an injection. Let $y \in \mathbb{Z} \Rightarrow y = x + 4, x \in \mathbb{Z} \Rightarrow x = y - 4$ since for all $y \in \mathbb{Z}$, $y - 4 \in \mathbb{Z}$, f is a surjection.	*Check that each element in the co-domain is the image of an element in the domain.*

Examples 3 and 4 involve discrete functions. In Example 3 the functions were mappings between finite sets, and in Example 4 they were mappings between infinite sets. We now look at examples with functions as mappings between infinite continuous sets.

Example 5

The function f is defined by $f : \mathbb{R}^+ \to \mathbb{R}^+$ where $f(x) = e^{\cos 2x} + 1$.

a Find the exact range, A, of f.

b **i** Explain why f is not an injection.

ii Giving a reason, state whether or not f is a surjection.

a The range of $\cos 2x$ is the interval $[-1, 1]$, so $A = [e^{-1} + 1, e + 1]$	*Find the minimum and maximum values that $\cos 2x$ can take to find the range of f.*
b **i** **Method I** For f to be an injection or one-to-one function, $x \neq y \Rightarrow f(x) \neq f(y)$ $f(0) = f(n\pi) = e + 1,\ n \in \mathbb{Z}$ Therefore f is not an injection.	*We know from the core syllabus that f is a periodic function. Use a counter example to show that f is not injective.*
Method II $f(x) = e^{\cos 2x} + 1$ $\Rightarrow f'(x) = -(2\sin 2x)e^{\cos 2x}$ $\Rightarrow f'(x) < 0$ for $0 < x < \frac{\pi}{2}$ and $f'(x) > 0$ for $\frac{\pi}{2} < x < \pi$ Since $f(x)$ is not strictly increasing or decreasing over the whole domain it is not injective.	*Since the function is continuous and differentiable over the whole domain we can use the derivative.*
ii The co-domain of f is $\mathbb{R}^+$ but the range of f is $A = [e^{-1} + 1, e + 1]$ i.e. for $y \in \mathbb{R}^+$, $y \notin A$ there is no $x \in \mathbb{R}^+$ such that $f(x) = y$. Therefore f is not surjective.	*Use the result of part **a** to show that f is not a surjection.*

Note that the derivative test shown in the second method can be used only for functions that are continuous and differentiable on the given domain. It is not valid for functions that are discrete, like the ones in Examples 3 and 4.

Example 6

Consider the following functions:
$f :]2, +\infty[\to \mathbb{R}^+$ where $f(x) = (x - 2)(x + 1)$
$g : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ where $g(x, y) = (\cos(x - y), x - y)$

a Show that f is bijective.

b Determine, with reasons, whether

i g is injective

ii g is surjective.

a Method I

Injective: $f(a) = f(b)$

$\Rightarrow (a - 2)(a + 1) = (b - 2)(b + 1)$

$\Rightarrow a^2 - a - b^2 + b = 0$

Use quadratic formula to solve for a:

Solve for a.

$$a = \frac{1 \pm \sqrt{1 - 4(b - b^2)}}{2}$$

$$= \frac{(1 \pm |1 - 2b|)}{2}$$

$$= \frac{(1 - 1 + 2b)}{2}$$

$\sqrt{x^2} = |x|$ and since $b > 2$ we have $|1 - 2b| = -1 + 2b$. The second solution is discarded because it is out of the domain.

$\Rightarrow a = b$

So $f(x)$ is an injection.

Surjective: Let $f(x) = y$

Show that for all possible values of y in the co-domain, there is a value of x in the domain.

$\Rightarrow y = x^2 - x - 2 \Rightarrow x^2 - x - 2 - y = 0$

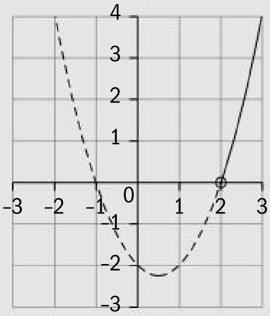
$$\Rightarrow x = \frac{1 + \sqrt{9 + 4y}}{2}$$

For all $y \in \mathbb{R}^+$, $\sqrt{9 + 4y} > 3$, so $x > 2$.

Therefore for all $y \in \mathbb{R}^+$ there is $x \in]2, +\infty[$ such that $f(x) = y$.
Therefore f is a surjection.
Since f is injective and surjective it is a bijection.

Method II

Sketch the graph of f:



Use the graph of f with the horizontal line test.

The graph of *f* passes the horizontal line test, therefore *f* is injective. From the graph it is clear that the range of *f* is equal to the co-domain so *f* is surjective.	*Compare range and co-domain on graph.*
Since *f* is both an injection and a surjection it is a bijection.	
b **i** $g(2\pi, \pi) = g\left(\frac{5\pi}{4}, \frac{\pi}{4}\right)$	*Find a counterexample.*
Therefore it is not injective.	
ii The range of *g* is contained in $[-1, 1] \times \mathbb{R} \neq \mathbb{R} \times \mathbb{R}$ so *g* is not surjective.	$-1 \leq \cos(x - y) \leq 1$

In all the examples above the domains are real numbers or ordered pairs. However by our definitions of functions we may have domains or co-domains that are not subsets of $\mathbb{R}$ or $\mathbb{R}^2$. The following example illustrates this.

Example 7

Let $P = \left\{ p(x) | p(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0, a_i \in \mathbb{R}, n \in \mathbb{N} \right\}$ and $f : P \to P$ such that $f(p_n) = p_n'$. Determine whether *f* is an injection, a surjection or both.

$f(p_i) = f(p_j) \Leftrightarrow p_i' = p_j'$ This is true even when $p_i = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ $p_j = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + b_0$, $a_0 \neq b_0$	*Use the contrapositive statement of injective functions.*
So *f* is not injective.	
Let $p_i \in P$ such that $f(p_i) = p$ $\Rightarrow p = p_i'$	
Then $p_i = \int p dx$ and there are infinitely many $p_i \in P$ that satisfy this condition. Therefore *f* is surjective.	*Since* $\int p dx = q + c$ *where q is a polynomial of degree n + 1 and c can take any real value.*

In Chapter 1 you learned that the cardinality of a set *S*, denoted by $n(S)$, is the number of elements in the set *S*. In the following theorem we are going to use the cardinality of finite sets to obtain two results for injection and surjection of functions with finite domains and co-domains.

Theorem 1

Let $f : S \to T$ where *S* and *T* are finite sets.

Then **a** f is injective $\Leftrightarrow n(f(S)) = n(S)$

b f is surjective $\Leftrightarrow n(f(S)) = n(T)$

Proof:

a f is injective $\Leftrightarrow n(f(S)) = n(S)$

$\Rightarrow$ For any function we know that $n(f(S)) \leq n(S)$ since we cannot have more images than we have elements in the domain.

Let's assume that $n(f(S)) < n(S)$. Then there must be at least one pair of different elements in S that have the same image, which is in contradiction with the fact that f is injective. Therefore $n(f(S)) = n(S)$.

$\Leftarrow$ If $S = \{x_1, x_2, \ldots, x_n\}$ then $\{f(x)\} = \{f(x_1), f(x_2), \ldots, f(x_n)\}$. If $f(x_i) = f(x_j)$ for some $i \neq j$ then $n(f(S)) \leq n - 1$, which is a contradiction. Therefore, f is injective. Q.E.D.

b f is surjective $\Leftrightarrow n(f(S)) = n(T)$.

$\Rightarrow$ Suppose f is surjective.

Then each $y \in T$ is the image of an element $x \in S$.

Therefore $T \subseteq f(S)$.

But by definition of range and co-domain, $f(S) \subseteq T$.

Therefore, by double inclusion, $T = f(S) \Rightarrow n(T) = n(f(S))$.

$\Leftarrow$ Suppose that $n(f(S)) = n(T)$.

We know that $f(S) \subseteq T$.

But since both $f(S)$ and T have the same number of elements it follows that $f(S) = T \Rightarrow y = f(x)$ for each $y \in T \Rightarrow$ surjection. Q.E.D.

In the core syllabus you studied functions on real numbers. Consider the function $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x$. We can easily see that this is a bijection.

$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ so it is an injection.

For every $x \in \mathbb{R}$, there is an $x \in \mathbb{R}$, such that $f(x) = x$, therefore it is a surjection. This function is called the **identity function** because it assigns every element to itself.

Example 8 is another illustration of how the derivative can be used to check injectivity; parts **a** and **c** are a little more challenging.

Example 8

Determine which of the following functions are injective given that in each case $f:\mathbb{R}\to\mathbb{R}$.

a $f(x) = 3x^2 + 7x - 2$

b $f(x) = x^5$

c $f(x) = \mathrm{e}^{3x} - \dfrac{1}{\mathrm{e}^{2x}}$

a $f(x) = 3x^2 + 7x - 2$ is continuous over $\mathbb{R}$.

Check for continuity and use derivative.

$f'(x) = 6x + 7$

$\Rightarrow f'(x) \geq 0$ when $x \geq -\dfrac{7}{6}$

and $f'(x) < 0$ when $x < -\dfrac{7}{6}$

Since $f(x)$ has a turning point, i.e. $f(x)$ is not strictly increasing or decreasing, it is not injective.

b $f(x) = x^5$ is continuous over $\mathbb{R}$.

$f'(x) = 5x^4 \geq 0$ for all $x \in \mathbb{R}$.

Hence $f(x)$ is increasing for all $x \in \mathbb{R}$ which means that it is injective.

c $f(x) = \mathrm{e}^{3x} - \dfrac{1}{\mathrm{e}^{2x}}$ is continuous over $\mathbb{R}$.

$f'(x) = 3\mathrm{e}^{3x} + 2\mathrm{e}^{-2x} > 0$ for all $x \in \mathbb{R}$.

Hence since $f(x)$ is increasing for all $x \in \mathbb{R}$, it must be injective.

Exercise 2A

1 A and B are two non-empty sets, $X,\ Y \subset A$, and $f: A \to B$.
Show that:

a $f(X \cup Y) = f(X) \cup f(Y)$

b $f(X \cap Y) \subseteq f(X) \cap f(Y)$

2 Determine which of these mappings are functions:

a $f:\mathbb{Q}\to\mathbb{Q}$ such that $f\left(\dfrac{m}{n}\right) = \dfrac{1}{mn}$

b $f:\mathbb{Q}\to\mathbb{Q}$ such that $f\left(\dfrac{m}{n}\right) = \dfrac{1}{m} + \dfrac{1}{n}$

c $f:\mathbb{N}\to\mathbb{Q}$ such that $f(m) = \dfrac{1}{m}$

3 Let G denote the set of citizens of Germany. Determine which of the following statements correctly specify a function.

a $f: G \to G, f(x)$ is "the mother of x"

b $g: G \to G, g(x)$ is "the daughter of x"

c $h: G \to G, h(x)$ "the sister of x"

4 The function $f: \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+ \times \mathbb{R}^+$ is defined by $f(x, y) = (x + 2y, \frac{x}{y})$. Show that f is a bijection.

5 P is the set of all polynomials: $P = \left\{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_i \in \mathbb{R}\right\}$.

Let $g: P \to P, g(p) = x^2 p$. Determine whether g is

a surjective **b** injective.

6 Determine which of the following functions are

a injective **b** surjective.

i $f: \mathbb{R} \to [0, \infty[, f(x) = \mathrm{e}^x$ **ii** $f: [0, 1] \to \mathbb{R},\ f(x) = \tan x$

iii $f: \mathbb{Z} \to \mathbb{Z},\ f(n) = \begin{cases} n+1 \text{ if } n \text{ is odd} \\ n-1 \text{ if } n \text{ is even} \end{cases}$

7 Let $f: (\mathbb{R}^+)^2 \to (\mathbb{R}^+)^2$, such that $f(x, y) = \left(xy^2, \frac{x}{y}\right)$.

Show that f is a bijection.

8 Determine which of the following functions, $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$, are

a injective **b** surjective

i $f(n, m) = nm$ **ii** $f(n, m) = \frac{nm(m+1)}{2}$

iii $f(n, m) = 3n + 7m$

9 The function $f: \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = \frac{1 - 2\mathrm{e}^{-x}}{1 + 2\mathrm{e}^{-x}}$.

a Find the range of f.

b Sketch the graph of f.

c Prove that f is an injection.

10 Consider the functions f and g, defined by

$f: \mathbb{Z} \to \mathbb{Z}$ where $f(n) = 5n + 4$

$g: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ where $g(x, y) = (x + 2y, 3x - 5y)$

Determine whether:

a the function f is surjective

b the function f is injective

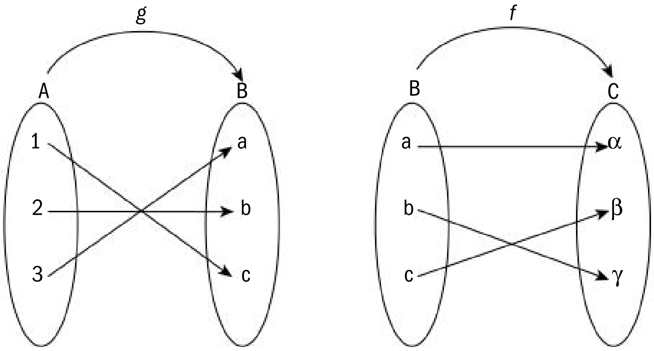
c the function g is surjective

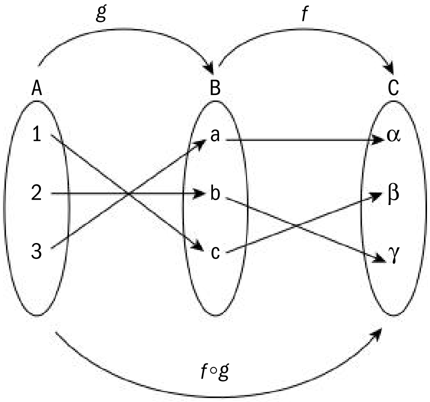
d the function g is injective.

Composition of functions

If the co-domain of a function g is equal to the domain of a second function f, the two functions can be combined. The composition of the functions g and f is denoted by $f \circ g$. The diagram below illustrates this.

The composite function $(f \circ g)(x)$ is also denoted by $f(g(x))$





Note that $g(3) = a$ and $f(a) = \alpha \Rightarrow (f \circ g)(3) = \alpha$.

We can show that given two functions f and g such that the domain of f is the co-domain of g, their composition $h = f \circ g$ is also a function.

Theorem 2

If $g: A \to B, f: B \to C$ are functions, then $f \circ g : A \to C$ is also a function.

Proof:

Since g is a function we know that for every $a \in A$ there is an element $b \in B$ such that $g(a) = b$.

Since f is a function and b is in the domain of f, we know that there is an element $c \in C$ such that $f(b) = c$.

Combining the two we obtain that for every $a \in A$ there is a $c \in C$ such that $(f \circ g)(a) = f(g(a)) = f(b) = c$, making it a function. Q.E.D.

Example 9

Given that $f:\mathbb{R} \to \mathbb{R}$ such that $f(x) = e^x$ and $g:\mathbb{R} \to \mathbb{R}$ such that $g(x) = x^2$.

a Find

i $(f \circ g)(x)$ **ii** $(g \circ f)(x)$

b Comment about your results to **a i** and **a ii**.

c Check each of the composite functions for injective and surjective properties.

a i $(f \circ g)(x) = f(g(x)) = f(x^2) = e^{x^2}$

ii $(g \circ f)(x) = g(f(x)) = g(e^x) = (e^x)^2 = e^{2x}$

Remember the correct order when working out composite functions.

b $e^{x^2} \neq e^{2x}$ for every x element of $\mathbb{R}$. Composition of functions is not commutative.

c **Method I**

Using the result in **a i**

$$(f \circ g)(x_1) = (f \circ g)(x_2)$$
$$\Rightarrow e^{x_1^2} = e^{x_2^2}$$
$$\Rightarrow x_1^2 = x_2^2$$
$$\Rightarrow x_1 = \pm x_2$$

So $(f \circ g)(x)$ is not an injection.

Method II

$(f \circ g)'(x) = 2xe^{x^2}$

$\Rightarrow (f \circ g)'(x) \geq 0$ when $x \geq 0$

and $(f \circ g)'(x) < 0$ when $x < 0$

When the function is continuous and differentiable it is easier to check by taking the derivative.

Hence $(f \circ g)(x)$ is not continuously increasing or decreasing since there is a turning point so it is not injective.

Let $y \in \mathbb{R}$ such that $(f \circ g)(x) = y \Rightarrow y = e^{x^2} > 0$
Then for all $y \leq 0$ there is no $x \in \mathbb{R}$ such that $(f \circ g)(x) = y$
Therefore $(f \circ g)(x)$ is not a surjection.

Using the result in **a ii**:

$(g \circ f)(x) = e^{2x}$

$\Rightarrow (g \circ f)'(x) = 2e^{2x} > 0$

$\Rightarrow g \circ f$ is a strictly increasing function.

Therefore $(g \circ f)(x)$ is an injection.

Let $y \in \mathbb{R}$ such that $(g \circ f)(x) = y \Rightarrow y = e^{2x} > 0$
Then for all $y \leq 0$ there is no $x \in \mathbb{R}$ such that $(g \circ f)(x) = y$
Therefore $(g \circ f)(x)$ is not a surjection.

Example 9 illustrates that composition of functions is not always commutative, i.e. $(f \circ g)(x) \neq (g \circ f)(x)$ for all $f(x)$, $g(x)$.

Inverse functions

Let $f: S \to T$ be a bijection. Since it is a surjection, each element in T is the image of some element in S. But f is also an injection, so every element in T is the image of a unique element in S. We can therefore define a new function from T to S that reverses the mapping from S to T as follows:

Definition

Let $f: S \to T$ be a bijection from S to T. The **inverse function of f**, denoted by $f^{-1}: T \to S$, is a function such that $f \circ f^{-1} = I = f^{-1} \circ f$ where I is the identity function.

Note that f has to be a bijection. If f is not injective then there is some element in T that is the image of more than one element in S. Let us say that $f(x_i) = y_i = f(x_j)$. In this case we cannot assign a unique element in S such that $f^{-1}(y_i) = x$ since y_i is the image of two elements in S. If f is not surjective then there is some element $y_i \in T$ for which there is no element in S such that $f(x) = y_i$.

Theorem 3

a A function $f: A \to B$ is bijective $\Leftrightarrow$ it has an inverse.
b A function $f: A \to B$ is bijective $\Leftrightarrow$ its inverse is also a bijection.

Proof:

a $\Rightarrow$: Let $f: A \to B$ be a bijection. Then f is injective and f is surjective.
Since f is injective, $f(a) = f(b) \Rightarrow a = b$ for all $a, b \in A$.
Since f is surjective, for every $y \in B$, there is an $a \in A$ such that $f(a) = y$.

Taking these together we have:
f is bijective $\Rightarrow$ for every $y \in B$ there is a unique $a \in A$ such that $f(a) = y$.

If we define a mapping $g: B \to A$, such that $g(f(a)) = a$ for all $f(a) \in B$, this is a well-defined function because every element in B may be written in the form $f(a)$ and its image a under g is a unique element of A.

Hence we have $(g \circ f)(a) = a \Rightarrow g$ is a left inverse of f.
Also for all $f(a) \in B$, $f(g(f(a)) = f(a) \Rightarrow f \circ g(f(a)) = f(a)$.
Therefore g is also a right inverse of f.
Since g is a left and right inverse of f, we can say that f has an inverse.
$\Leftarrow$: Let g be the inverse of f and let us suppose that f is not injective.
$\Rightarrow$ there are $a, b \in A$ such that $a \neq b$ but $f(a) = f(b)$.

$$\begin{aligned} \Rightarrow a &= g(f(a)) \\ &= g(f(b)), \text{ since } f(a) = f(b) \\ &= b \end{aligned}$$

This is a contradiction since we started by saying that $a \neq b$.
Therefore f must be injective.

Let us now suppose that f is not a surjection.
Then there must be some element $y \in B$ that is not the image of any $a \in A$
i.e. $f(a) \neq y$ for all $a \in A$.
On the other hand $f(g(y)) = y$ by definition of inverse.
It follows that there must be an $a \in A$ whose image under f is y in B.
This is a contradiction, therefore f is a surjection.
Since f is both an injection and a surjection it follows that f is a bijection.

b To show that $f^{-1} : B \to A$ is a bijection we need to show that it is an injection and a surjection.

Let $x_1, x_2 \in B$ such that $f^{-1}(x_1) = f^{-1}(x_2)$.

Then by the definition of inverse we know that
$x_1 = (f \circ f^{-1})(x_1) = f(f^{-1}(x_1)) = f(f^{-1}(x_2)) = (f \circ f^{-1})(x_2) = x_2$
Therefore $f^{-1} : B \to A$ is injective.

Since $f : A \to B$ is a surjection we know that for each $y \in B$ there is $x \in A$ such that $f(x) = y$
$\Rightarrow f^{-1} \circ f(x) = x = f^{-1}(y)$

Therefore since for all $x \in A$ there is $y \in B$ such that $f^{-1}(y) = x$ it follows that $f^{-1} : B \to A$ is a surjection.

Since $f^{-1} : B \to A$ is injective and surjective, it follows that it is a bijection.

Example 10

Determine whether f is an injection, and/or a surjection and find the inverse function f^{-1} where applicable:

a $f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ and $f(x) = x^2$

b $f : \mathbb{R}^+ \to \mathbb{R}^+$ and $f(x) = x^2 + 1$

c $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = x^3 + 1$

a **Method I**

Let $f(x_1) = f(x_2)$
$\Rightarrow x_1^2 = x_2^2$
$\Rightarrow x_1 = \pm x_2$
Therefore f is not an injection.

Method II

$f(x) = x^2 \Rightarrow f'(x) = 2x$
$\Rightarrow f'(x) < 0$ when $x < 0$
$f'(x) = 0$ when $x = 0$
and $f'(x) > 0$ when $x > 0$
$\Rightarrow$ is not continuously increasing or decreasing over $\mathbb{R}$.

	Therefore f is not an injection.	
	For every $y \in \mathbb{R}^+$ there is $x \in \mathbb{R}$ such that $x^2 = y$. Therefore f is a surjection.	*$f(x) > 0$ for all $x \in \mathbb{R}^+$.*
	Since f is not a bijection it does not have an inverse.	
b	Let $f(x_1) = f(x_2)$ $\Rightarrow x_1^{\ 2} + 1 = x_2^{\ 2} + 1$ $\Rightarrow x_1 = x_2$ Therefore f is an injection.	*Use contrapositive statement for injection.*
	Let $y \in \mathbb{R}^+$, $y < 1$ There is no $x \in \mathbb{R}^+$ such that $f(x) = y$. Therefore f is not a surjection. Since f is not a bijection it does not have an inverse.	*Use definition of surjection.*
c	Let $f(x_1) = f(x_2)$ $\Rightarrow x_1^{\ 3} + 1 = x_2^{\ 3} + 1$ $\Rightarrow x_1 = x_2$ Therefore f is an injection.	
	For every $y \in \mathbb{R}$, $\sqrt[3]{y-1} \in \mathbb{R} \Rightarrow f\left(\sqrt[3]{y-1}\right) = y$ So f is a surjection. The inverse function is given by $f^{-1}(x) = \sqrt[3]{x-1}$	

As mentioned previously, functions are not restricted to having the domain or co-domain as subsets of $\mathbb{R}$. In Example 7 the domain and co-domain were the set of polynomial functions with real coefficients. In the next examples you will see work on functions that have a Cartesian product as domain and co-domain.

Example 11

Given $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ such that $f(x, y) = (y - 2x, x + y)$,

a show that f is a bijection

b find $f^{-1}(x, y)$.

a	Let $f(x, y) = f(a, b)$ $\Rightarrow (y - 2x, x + y) = (b - 2a, a + b)$	*First show that f is an injection.*
	$\Rightarrow y - 2x = b - 2a$ and $y + x = b + a$	*Equate corresponding elements.*
	$\Rightarrow -3x = -3a$ $\Rightarrow x = a$	*Subtract the second equation from the first.*
	Since $y + x = b + a$ then $y = b$. Therefore f is injective.	*Show that $(x, y) = (a, b)$*

Let $(a, b) \in \mathbb{R} \times \mathbb{R}$.	*Now show that f is a surjection.*
If $f(x, y) = (a, b)$, $(y - 2x, y + x) = (a, b)$	
$\Rightarrow y - 2x = a$ and $y + x = b$	*Equate corresponding elements.*
$\Rightarrow -3x = a - b$	*Subtract second equation from the first.*
$\Rightarrow x = \dfrac{b-a}{3} \in \mathbb{R}$	
$y + x = b$	
$\Rightarrow y = b - x$	*Substitute for x*
$\Rightarrow y = b - \dfrac{b-a}{3}$	
$\Rightarrow y = \dfrac{2b+a}{3} \in \mathbb{R}$	
Therefore $(x, y) \in \mathbb{R} \times \mathbb{R}$.	
So f is a surjection, and therefore f is a bijection.	
b Let $(a, b) = f(x, y)$	
$\Rightarrow (a, b) = (y - 2x, y + x)$	
$\left.\begin{aligned} \Rightarrow a &= y - 2x \\ b &= y + x \end{aligned}\right\} \Rightarrow x = \dfrac{b-a}{3},\ y = \dfrac{2b+a}{3}$	*Replace a and b by x and y respectively to write the inverse function.*
Therefore $f^{-1}(x, y) = \left(\dfrac{y-x}{3}, \dfrac{2y+x}{3}\right)$	*You need to write the inverse function using $f^{-1}(x, y)$.*

Example 12

Given that $\begin{aligned} &g : \mathbb{R}^2 \to \mathbb{R}^2,\ g(x, y) = (x - y, 2x + y) \\ &h : \mathbb{R}^2 \to \mathbb{R}^2,\ h(x, y) = (xy, 2x - y) \end{aligned}$

a Show that g has an inverse and find it.

b Determine whether $(g \circ h)$ is a bijection.

a For g to have an inverse it has to be a bijection.	
Let $g(x, y) = g(a, b)$	
$(x - y, 2x + y) = (a - b, 2a + b)$	
$\Rightarrow x - y = a - b$	*Equate elements of ordered pairs.*
and $2x + y = 2a + b$	*Add the equations.*
$\Rightarrow 3x = 3a \Rightarrow x = a$	*Show that $(x, y) = (a, b)$.*
$x - y = a - b \Rightarrow y = b$	
Therefore g is an injection.	
Let $(a, b) \in \mathbb{R}^2$	
If $f(x, y) = (a, b)$ then	
$(x - y, 2x + y) = (a, b)$	

$\left.\begin{array}{l}\Rightarrow \quad x-y=a\\ \text{and } \; 2x+y=b\end{array}\right\}\Rightarrow x=\frac{a+b}{3}\in\mathbb{R}$ and $y=\frac{b-2a}{3}\in\mathbb{R}$	*Equate elements of ordered pairs and add to solve for x and y.*
Therefore g is a surjection. Since g is bijective it has an inverse. Let $(a, b) = g(x, y)$ Then $(a, b) = (x - y, 2x + y)$	
$\left.\begin{array}{l}\Rightarrow \quad a=x-y\\ \text{and } b=2x+y\end{array}\right\}\Rightarrow x=\frac{a+b}{3},\ y=\frac{b-2a}{3}$	*Equate elements of ordered pairs and add to solve for x and y.*
$g^{-1}(x, y)=\left(\frac{x+y}{3}, \frac{y-2x}{3}\right)$	*Again we need to write it out using inverse notation.*
b $(g\circ h)(x, y)=g(h(x, y))=g(xy, 2x-y)$ $=(xy-2x+y, 2xy+2x-y)$ Let $(g\circ h)(x, y)=(g\circ h)(a, b)$ $\Rightarrow (xy-2x+y, 2xy+2x-y)=(ab-2a+b, 2ab+2a-b)$	
$\left.\begin{array}{l}\Rightarrow xy-2x+y=ab-2a+b\\ 2xy+2x-y=2ab+2a-b\end{array}\right\} xy=ab$ $xy=ab\Rightarrow x=\frac{ab}{y}, y\neq 0$	*Equate elements of ordered pairs and add to write x in terms of a, b and y*
$\Rightarrow \cancel{ab}-\frac{2ab}{y}+y=\cancel{ab}-2a+b$	*Substitute for x in the first equation.*
$\Rightarrow -2ab+y^2=-2ay+by$ $\Rightarrow y^2+(2a-b)\,y-2ab=0$	
$\Rightarrow y=\frac{-(2a-b)\pm\sqrt{(2a-b)^2+8ab}}{2}$ $\Rightarrow y=\frac{-(2a-b)\pm\sqrt{4a^2-4ab+b^2+8ab}}{2}$ $\Rightarrow y=\frac{-(2a-b)\pm\sqrt{(2a+b)^2}}{2}$ $\Rightarrow y=b$ or $y=-2a$ When $y=b$, $x=a$ and when $y=-2a,\ x=\frac{-b}{2}$ We have $(g\circ h)(x, y)=(g\circ h)(a, b)$	*Solve the quadratic equation for y.*
$\Rightarrow (g\circ h)(2, 6)=(g\circ h)(-3, -4)$ $(g\circ h)$ is not injective therefore it is not a bijection.	*It is sufficient to find two different elements that have the same image.* *e.g. $a=2$, $b=6$*

2.2 Properties of functions

We will now consider some properties of functions by looking at the three functions:

$f : \mathbb{R} \to \mathbb{R}, f(x) = 3x + 2$

$g : \mathbb{R} \to \mathbb{R}^+,\ g(x) = e^{x^2}$

$h : \mathbb{R}^+ \to \mathbb{R}^+,\ h(x) = \dfrac{1}{x}$

First we find $f \circ (g \circ h)(x)$ as follows

$$f \circ (g \circ h)(x) = f \circ g(h(x)) = f \circ g\left(\frac{1}{x}\right) = f\left(g\left(\frac{1}{x}\right)\right)$$

$$= f\left(e^{\left(\frac{1}{x}\right)^2}\right) = f\left(e^{x^{-2}}\right) = 3e^{x^{-2}} + 2$$

Now let us compute $(f \circ g) \circ h(x)$.

$$(f \circ g)(x) = f(g(x)) = f(e^{x^2}) = 3e^{x^2} + 2$$

$$\Rightarrow (f \circ g) \circ h(x) = (f \circ g)\left(\frac{1}{x}\right) = 3e^{\left(\frac{1}{x}\right)^2} + 2 = 3e^{x^{-2}} + 2$$

Therefore for the given functions we have shown that
$((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$.
In the next theorem we will prove that this result is true for any three well-defined functions.

Theorem 4

Composition of functions is associative; in other words, given three functions $f : C \to D$, $g : B \to C$ and $h : A \to B$, it follows that $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$.

Proof:

LHS $= ((f \circ g) \circ h)(x) = (f \circ g)\ (h(x)) = f(g(h(x))$

RHS $= (f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))$

The domains and co-domains of $((f \circ g) \circ h)$ and $(f \circ (g \circ h))$ are the same and since $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$ for all $x \in A$, it follows that $((f \circ g) \circ h) = (f \circ (g \circ h))$. Q. E. D.

Investigation

Before we look at the next properties you should justify whether the following statements are true or false. A formal proof is not necessary at this stage and you may use diagrams to help you decide on an answer.

$f : A \to B$ and $g : B \to C$

a **i** Given that both f and g are injective functions then $g \circ f$ is also injective.
ii Given that both f and g are injective functions then $f \circ g$ is also injective.
iii If $g \circ f$ is injective and g is also injective then f is injective.
iv If $g \circ f$ is injective and f is also injective then g is injective.

b **i** Given that both f and g are surjective functions then $g \circ f$ is also surjective.
ii Given that both f and g are surjective functions then $f \circ g$ is also surjective.

c If f is injective and g is surjective then:
i $g \circ f$ is injective
ii $g \circ f$ is surjective.

d If f is surjective and g is injective then
i $g \circ f$ is injective
ii $g \circ f$ is surjective.

Theorem 5

a If $f: A \to B$ and $g: B \to C$ are injective functions then $g \circ f: A \to C$ is also injective.

b If $f: A \to B$ and $g: B \to C$ are surjective functions then $g \circ f: A \to C$ is also surjective.

c If $f: A \to B$ and $g: B \to C$ are bijections then $g \circ f: A \to C$ is also a bijection.

Proof:

a Let $(g \circ f)(x_1) = (g \circ f)(x_2)$
$\Rightarrow g(f(x_1)) = g(f(x_2))$
$\Rightarrow f(x_1) = f(x_2)$ since g is injective
$\Rightarrow x_1 = x_2$ since f is injective
Therefore $(g \circ f)$ is also injective.

b Let $q \in C$, then, since g is surjective, there is some $y \in B$ such that $g(y) = q$.
For this y there is some $x \in A$ such that $f(x) = y$ since f is surjective.
So $q = g(y) = g(f(x)) = (g \circ f)(x)$
Therefore $(g \circ f)$is also surjective.

c Since it was shown in **a** and **b** that $(g \circ f)$ is both injective and surjective, then by definition of bijection it follows that if f and g are both bijective then $(g \circ f)$ is a bijection. Q.E.D.

Properties of composite functions

- Associative $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$
- If $f : S \to T$ and $g : T \to S$ are injections, then $(f \circ g)(x)$ and $(g \circ f)(x)$ are injective.
- If $f : S \to T$ and $g : T \to S$ are surjections, then $(f \circ g)(x)$ and $(g \circ f)(x)$ are surjective.

Exercise 2B

1 A and B are two non-empty sets, and $A, B \subset \mathbb{R}$. The functions f and g are defined as follows: $f : A \times B \to B \times A$, $f(a, b) = (b, a)$ and $g : B \times A \to B$, $g(b, a) = b$. Find $g \circ f$.

2 Explain why the function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x - x^2$ is neither injective nor surjective.

3 Given that $f : \mathbb{R} \to \mathbb{R}^+$, $f(x) = e^{2x}$ and $g : \mathbb{R}^+ \to \mathbb{R}$, $g(x) = \ln x$, find:

a **i** $(f \circ g)(x)$

ii $(g \circ f)(x)$

b Check each of the composite functions in **a** for injection and surjection.

4 Two functions f and g are defined as follows:
$f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $f(n) = (n - 1, 1)$ and
$g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $g(m, n) = m + n$

a Show that f is a bijection and find its inverse.

b Show that g is not a bijection, but a surjection.

c Find $f \circ g$ and $g \circ f$.

5 Consider the two functions $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ such that $f(x, y) = (xy, x + y)$.

a Determine whether or not f is a bijection.

b Find $(f \circ f)(x, y)$.

6 Let $f : \mathbb{R} \setminus \{0, 1\} \to \mathbb{R} \setminus \{0, 1\}$ such that $f(x) = \dfrac{1}{x}$ and

$g : \mathbb{R} \setminus \{0, 1\} \to \mathbb{R} \setminus \{0, 1\}$ such that $g(x) = 1 - x$

a Show that f and g are both bijections.

b Find $f \circ g$ and $g \circ f$.

c Show that $(f \circ g) \circ (g \circ f)(x) = (g \circ f) \circ (f \circ g)(x)$.

d What can you say about f and g?

e What can you say about $f \circ g$ and $g \circ f$?

7 The function $f:(\mathbb{R}^+)^2 \to (\mathbb{R}^+)^2$ is defined by $f(x, y) = \left(\frac{y}{x}, x^2 y\right)$.

a Show that f is a bijection.
b Find the inverse f^{-1}.

8 The function $f:[0, \infty[\to [1, \infty[$ is defined by $f(x) = 4e^{2x} - 3$.

a Find $f'(x)$ and hence show that f is a bijection.
b Find an expression for $f^{-1}(x)$.

9 The function $f:\mathbb{R} \to \mathbb{R}$ is defined by

$$f(x) = \begin{cases} \frac{x}{e} & \text{for } x \le e \\ \ln x & \text{for } x > e \end{cases}$$

a Sketch the graph of f.
b By referring to your graph, show that f is a bijection.
c Find f^{-1}.

10 Three functions mapping $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ are defined by
$f_1(m, n) = m - n - 1$, $f_2(m, n) = |n|$ and $f_3(m, n) = m^2 - n^2$.
Two functions mapping $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ are defined by
$g_1(p) = (2p + 1, p)$ and $g_2(p) = (|p|, p)$.

a Find the range of
i $f_1 \circ g_1$
ii $f_3 \circ g_2$
b Find all the solutions of $f_1 \circ g_2(p) = f_2 \circ g_1(p)$.
c Find all the solutions of $f_3(m, n) = k$ in each of the cases $k = 1$ and $k = 2$.

11 Consider the functions

$$f:\mathbb{Z} \to \mathbb{Z} \text{ where } f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ n + 1 & \text{if } n \text{ is odd} \end{cases}$$

$g:\mathbb{Z} \to \mathbb{Z}$ where $g(n) = 16 - n$
$h:\mathbb{Z} \to \mathbb{Z}$ where $h(n) = n(\text{mod } 8)$
$k:\mathbb{Z} \to \mathbb{Z}$ where $k(n) = |n - 8|$
Find:

a $(h \circ g)(n)$ **b** $(k \circ f)(n)$ **c** $(f \circ g)(n)$
d $(f \circ h \circ g)(n)$ **e** $(k \circ h \circ g)(n)$ **f** $(k \circ f \circ g)(n)$

12 Given that $f:[1, \infty[\to \mathbb{R}, f(x) = \ln(2x - 1)$, $g:\mathbb{R} \to \mathbb{R}^+$, $g(x) = e^{x^2}$ and $h:\mathbb{R} \to \mathbb{R}$, $h(x) = 2x$, find the following functions:

a $(g \circ f)(x)$ **b** $(f \circ g)(x)$ **c** $(h \circ f)(x)$

d $(g \circ h \circ f)(x)$ **e** $(h \circ g \circ f)(x)$

Identity functions

In this section we will be focusing on identity functions. An identity function is one whose output is the same as the original input.

Definition

The **identity function** for a set S is a bijection $I_S : S \rightarrow S$ such that $I_S(x) = x$ for all $x \in S$.

Theorem 6

Let $f : S \rightarrow S$ be any function.
Then $(I_S \circ f)(x) = (f \circ I_S)(x) = f(x)$ for all $x \in S$.

Proof:

Let $x \in S$.
Then $(I_S \circ f)(x) = I_S(f(x)) = f(x)$ and $(f \circ I_S)(x) = f(I_S(x)) = f(x)$.
Therefore $(I_S \circ f)(x) = (f \circ I_S)(x) = f(x)$. Q.E.D.

Theorem 7

For a bijection $f : S \rightarrow T$ such that $f(x) = y$, $x \in S$ and $y \in T$, the inverse function $f^{-1} : T \rightarrow S$ is such that $(f^{-1} \circ f)(x) = I_S$ and $(f \circ f^{-1})(y) = I_T$.

Proof:

$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_S$

$(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = I_T$ Q.E.D.

Notice that one composition gives an identity on the domain and the other one gives an identity on the co-domain.

Example 13

Show that if $f : B \rightarrow C$ and $g : A \rightarrow B$ are both bijections then $(f \circ g)^{-1}(x) = (g^{-1} \circ f^{-1})(x)$.	
$(f \circ g) \circ (g^{-1} \circ f^{-1})(x)$ $= (f \circ (g \circ g^{-1}) \circ f^{-1})(x)$ $= (f \circ (I_B \circ f^{-1}))(x)$ $= (f \circ f^{-1})(x) = I_C$ Similarly $(g^{-1} \circ f^{-1}) \circ (f \circ g)(x)$ $= (g^{-1}(f^{-1} \circ f) \circ g)(x)$ $= (g^{-1}(I_B \circ g))(x)$ $= (g^{-1} \circ g)(x) = I_A$	*Composition of functions is associative.*

Example 14

Given that $f:\mathbb{Z}\setminus\{0\}\to\mathbb{Z}^{+}$ such that $f(x)=\dfrac{4x|x|-x+|x|}{2x}$, show that $f(x)$ is a bijection.

When $x>0$, $|x|=x$ and $f(x)=\dfrac{4x^2-x+x}{2x}=2x$

So $f(x_1)=f(x_2)\Rightarrow x_1=x_2$.

When $x<0$, $|x|=-x$ and $f(x)=\dfrac{-4x^2-2x}{2x}=-2x-1$

and $f(x_1)=f(x_2)\Rightarrow x_1=x_2$.

Moreover, if $x<0$ then $f(x)$ is even, while if $x>0$ then $f(x)$ is odd. So if $x_1>0$ and $x_2<0$ then $f(x_1)\neq f(x_2)$. Therefore $f(x)$ is an injection.

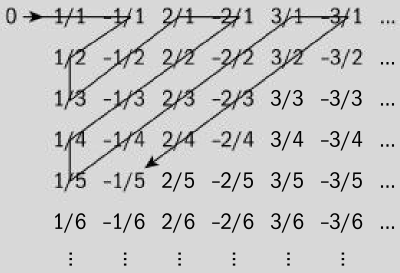
$f(\mathbb{Z}^{+})=\{2,4,6,\ldots\}$
$f(\mathbb{Z}^{-})=\{1,3,5,\ldots\}$
$f(\mathbb{Z})=\{2,4,6,\ldots\}\cup\{1,3,5,\ldots\}=\mathbb{Z}$

Therefore $f(x)$ is a surjection.
Since the function is both an injection and a surjection it follows that it is a bijection.

Show that f is both injective and surjective.

Although $\mathbb{R}$ and $\mathbb{R}^{+}$ have the same cardinality and are both infinite they are uncountable, unlike $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{Z}$, which are countably infinite.

Cantor came up with an ingenious yet very simple method to show that the rational numbers are countable. A set is said to be countable if a one-to-one correspondence can be found between the elements of the set and the set of positive integers. Cantor constructed a table that enables all the rational numbers, both positive and negative, to be included and hence allows a one-to-one correspondence to be found. The table is on the right, with the lines showing the order of pairing up the fractions with the positive integers.



0	1/1	−1/1	2/1	−2/1	3/1	−3/1	…
	1/2	−1/2	2/2	−2/2	3/2	−3/2	…
	1/3	−1/3	2/3	−2/3	3/3	−3/3	…
	1/4	−1/4	2/4	−2/4	3/4	−3/4	…
	1/5	−1/5	2/5	−2/5	3/5	−3/5	…
	1/6	−1/6	2/6	−2/6	3/6	−3/6	…
	⋮	⋮	⋮	⋮	⋮	⋮	

Having understood what we mean by a bijection it should be clear that if we have a bijection $f:S\to T$ where S and T are finite sets it follows that $n(S)=n(T)$.

What if $g:\mathbb{R}\to\mathbb{R}^{+}$ such that $g(x)=2^x$? You have shown in Exercise 2B that this is a bijection. In this case we say that the two sets $\mathbb{R}$ and $\mathbb{R}^{+}$ have the same cardinality because there is a bijection $g:\mathbb{R}\to\mathbb{R}$

Exercise 2C

1 For each of the following questions find $(f \circ g)(x)$ and $(g \circ f)(x)$ and determine whether f and g are mutual inverses.

a $f : \mathbb{R} \to \mathbb{R},\ f(x) = 1 - 3x$

$g : \mathbb{R} \to \mathbb{R},\ g(x) = 1 - \dfrac{x}{3}$

b $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{-4\},\ f(x) = \dfrac{1}{x} - 4$

$g : \mathbb{R} \setminus \{-4\} \to \mathbb{R} \setminus \{0\},\ g(x) = \dfrac{1}{x + 4}$

c $f : \mathbb{R} \to \mathbb{R},\ f(x) = \sqrt[3]{kx - 1},\ k \in \mathbb{Z}^+$

$g : \mathbb{R} \to \mathbb{R},\ g(x) = \dfrac{1}{k}(x^3 + 1)$

2 Show that the following functions are bijective and describe the respective inverse functions:

a $f : \mathbb{R}^+ \to \mathbb{R}, f(x) = \ln x$

b $f : \mathbb{R} \to \mathbb{R}, f(x) = \begin{cases} x \text{ if } x \text{ is rational} \\ -x \text{ if } x \text{ is irrational} \end{cases}$

3 **a** Given that $f : \mathbb{R} \to \mathbb{R}, f(x) = e^x$ and $g:[0, \pi] \to [-1, +1], g(x) = \cos x$ find:

i $(f \circ g)^{-1}(x)$

ii $(g^{-1} \circ f^{-1})(x)$

b Prove that for invertible functions f and g, $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

If a function is invertible it means that it has an inverse.

2.3 Binary operations

You are familiar with the operations of addition and multiplication of numbers, the dot product of two vectors, the union and intersection of sets and earlier in this chapter we looked at the composition of functions. All of these are operations. Other operations you are familiar with include:

$n!$	factorial
$\lvert z \rvert$	modulus
A'	the complement of set A

There is a difference between $n!$ and the product of two numbers. In order to find $n!$ we need to know only the value of n. So when $n = 4$, $4! = 24$. We call these unary operations (operations that have only one input). However, in order to perform multiplication we need two numbers. We need two sets to find a union or intersection but we only need set A to identify its complement.

Definition

A **binary operation** $*$ on a non-empty set S is a rule for combining any two elements $x, y \in S$ to give a unique element c of a set. This is denoted by $x * y = c$.

In this book we mostly use $*$ to denote binary operations. However, we sometimes also use other notations, for example: $\circ, \otimes, \#, \odot, \ldots$

Division on $\mathbb{R}$ is not a binary operation because $x \div 0$ is not defined. However division on $\mathbb{R} \setminus \{0\}$ is a binary operation.

Multiplication on $\mathbb{Z}$ produces another integer. The dot product of two vectors is not a closed binary operation since it produces a scalar quantity. The vector product however is a closed binary operation since it produces another vector.

Consider a set S with binary operation $*$. We say that S is **closed** under $*$ if for every $x, y \in S$, $x * y \in S$.

The set of vectors, V, is closed under the vector product because for all $(a, b) \in V$, $a \times b = c \in V$.

The set of real numbers, $\mathbb{R}$, is closed under multiplication because for all $x, y \in \mathbb{R}$, $xy \in \mathbb{R}$.

When testing for closure on finite sets it is useful to illustrate the operation using a Cayley table. This is a square grid which shows all the possible elements obtained by the binary operation. We can represent the operation $*$ on the set $A = \{a, b, c, d\}$ as follows:

$A \times A$	a	b	c	d
a	$a*a$	$a*b$	$a*c$	$a*d$
b	$b*a$	$b*b$	$b*c$	$b*d$
c	$c*a$	$c*b$	$c*c$	$c*d$
d	$d*a$	$d*b$	$d*c$	$d*d$

Arthur Cayley (1821–1895) was the first mathematician to define the concept of a group (which you will first study in Chapter 3) as a set together with a binary operation that satisfies certain conditions.

Note that order is important when filling out a Cayley table. The element in the third row and second column above is $c*b$ and not $b*c$.

Consider the binary operation multiplication on the set $S = \{-1, 0, 1\}$. The operation table is shown below.

$S \times S$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

We can see from the Cayley table that every product is a member of S.

We can therefore say that S is closed under multiplication.

Example 15

Determine which of the following operations are binary operations on the given sets and for those which are, state whether or not they are closed.

a Addition on the set $S = \{-1, 0, 1\}$

b Multiplication on the set of complex numbers $\mathbb{C}$

c Addition on the set $A = \left\{x \mid x = 2n,\ n \in \mathbb{Z}^+\right\}$

d Multiplication on the set $B = \left\{x \mid x = 2n + 1,\ n \in \mathbb{Z}^+\right\}$

e Division on the set of rational numbers $\mathbb{Q}$

a

+	−1	0	1
−1	−2	−1	0
0	−1	0	1
1	0	1	2

It is a binary operation since each addition gives a unique element. Not closed, since $-2, 2 \notin S$

b It is a binary operation which is closed.
$(a + ib)(c + id) = (ac - bd) + i(bc + ad) \in \mathbb{C}$

c It is a binary operation which is closed on the set of positive even integers. $2m + 2n = 2(m + n)$, which belongs to A since $(m + n)$ is an element of $\mathbb{Z}^+$.

d It is a binary operation which is closed on the positive odd integers.
$(2n + 1)(2m + 1) = 2(2mn + m + n) + 1 = 2k + 1 \in B$

e It is not a binary operation since $0 \in \mathbb{Q}$, and division by 0 is not defined

Check whether it is a binary operation and for closure.

Example 16

The operations $*$ and $\circ$ on the set $S = \{1, 2, 3\}$ are defined as follows:

$a * b = a^b - b^a$ and $a \circ b = \dfrac{|a - 2b| + a}{2}$

Draw a Cayley table for each operation and determine whether the set is closed under these operations.

$*$	1	2	3
1	0	−1	−2
2	1	0	−1
3	2	1	0

Fill out the table by working out the operation, e.g. $2 * 1 = 2^1 - 1^2 = 1$.

The set is not closed under $*$ since −2 and −1 are not in S.

$\circ$	0	1	2	3
0	0	1	2	3
1	1	1	2	3
2	2	1	2	3
3	3	2	2	3

Work out the operations to fill out the table, e.g.

$$3 \circ 2 = \frac{|\ 3 - 4|\ +\ 3}{2} =\ 2.$$

The set is closed under $\circ$.

Exercise 2D

1 Determine which of the following operations are binary operations on the given sets and for those which are, state if they are closed.

a $*$ on $S = \{0, 1, 2, 3\}$, where $a * b = a + b$

b $*$ on $\mathbb{Z}^+$, where $a * b =$ the smaller of a or b, or the common value if $a = b$

c $*$ on $\mathbb{Z}^+$, where $a * b = (ab + 1)$

d $\circ$ on $\mathbb{Z}^+$, where $a \circ b = b^a$

2 Let $S = \{z | z = a + bi$, where $a, b \in \mathbb{R}, b \neq 0, i = \sqrt{-1}\}$. Show that the following operations are binary operations on S and determine whether or not they are closed.

a addition **b** multiplication **c** division

3 Determine whether or not the following sets are closed under

a addition

b multiplication

i $A = \{m | m = 2n, n \in \mathbb{Z}^+\}$ **ii** $B = \{m | m = 2n - 1, n \in \mathbb{Z}^+\}$

4 The operations $*$ and $\circ$ on the set $S = \{0, 1, 2, 3\}$ are defined as follows: $a * b = a + b(\text{mod}4)$ and $a \circ b = ab(\text{mod}4)$.
Draw a Cayley table for each operation and determine whether or not the set is closed under these operations.

5 Let $X = \{f \,|\, f: \mathbb{R} \to \mathbb{R}, f \text{ is a function}\}$. Show that the following operations are binary operations on X and determine whether or not they are closed.

a addition of functions **b** subtraction of functions

c composition of functions

6 Let $S = \{-1, 1, i, -i\}$ where $i = \sqrt{-1}$. Draw a Cayley table to show that S is closed under multiplication.

7 The binary operation $*$ is defined for $a, b \in \mathbb{Z}^+$ by $a * b = 2a + b + ab$.
Show that $*$ is a binary operation and determine whether or not $\mathbb{Z}^+$ is closed under $*$.

8 The operations $*$ and $\circ$ on the set $S = \{1, 2, 3\}$ are defined as follows:

$a * b = a^b - b^a + ab$ and $a \circ b = \dfrac{a!b!}{ab}$

Draw a Cayley table for each operation and determine whether or not the set is closed under these operations.

9 Let $S = \{n^2 | n \in \mathbb{Z}^+\}$. Determine whether or not S is closed under

a addition **b** multiplication.

10 Let $S = \{1, 2\}$. The binary operation $*$ is defined on S as follows.
For $a, b \in S$, $a * b = 3ab$ and the binary operation $\circ$ is defined on $S \times S$ is defined as $(x_1, y_1) \circ (x_2, y_2) = (x_1 * x_2, y_1 * y_2)$.

a Write the elements of $S \times S$.

b Construct the Cayley table for the operation $*$ on S. Is S closed under $*$?

c Construct the Cayley table for the operation $\circ$ on $S \times S$.

Properties of binary operations

Definition

A binary operation $*$ on a non-empty set S is said to be **associative** if for all $a, b, c \in S, a * (b * c) = (a * b) * c$.

The operation addition on $\mathbb{R}$ is associative but subtraction is not since $(6 - 2) - 3 = 1$ and $6 - (2 - 3) = 7$.

Also the operation multiplication on $\mathbb{R}$ is associative but division on $\mathbb{R} \setminus \{0\}$ is not associative because $8 \div (12 \div 3) \neq (8 \div 12) \div 3$.

Definition

A binary operation $*$ on a non-empty set S is said to be **commutative** if for all $a, b \in S, a * b = b * a$.

Addition and multiplication are commutative on $\mathbb{R}$ but the operation division on $\mathbb{R} \setminus \{0\}$ is not commutative because it is not the case that $a \div b = b \div a$, for all $a, b \in \mathbb{R}\setminus\{0\}$.

Also the operation subtraction on $\mathbb{R}$ is not commutative since it is not the case that $a - b \neq b - a$, for all $a, b \in \mathbb{R}\setminus\{0\}$.

Example 17

The binary operation $\circ$ on $\mathbb{C}$ is defined as follows $z \circ w = |z + w|$. Determine whether $\circ$ is:

a commutative **b** associative.

a $z = a + ib, w = c + id$

$\Rightarrow |z + w| = \sqrt{(a+c)^2 + (b+d)^2}$

$= |w + z|$

$z \circ w = |z + w|$

$w \circ z = |w + z| = |z + w|$

The operation is commutative.

Check whether *$z \circ w = w \circ z$*

b **Method I**

$(-1) \circ ((-1) \circ 1) = (-1) \circ 0 = 1$, but $((-1) \circ (-1) \circ 1 = 2 \circ 1 = 3$

Method II

$|z + |w + v|| = \left|\left(a + \sqrt{(c+e)^2 + (d+f)^2}\right) + ib\right|$

$||z + w| + v| = \left|\left(\sqrt{(a+c)^2 + (b+d)^2} + e\right) + if\right|$

$|z + |w + v|| \neq ||z + w| + v|$

$z \circ (w \circ v) = z \circ (|w + v|) \neq (|z + w|) \circ v$

The operation is not associative.

Check whether *$z \circ (w \circ v) = (z \circ w) \circ v$*

Definition

Given two binary operations $*$ and $\circ$ on a set S, $*$ is said to be **distributive** over $\circ$ if $a * (b \circ c) = (a * b) \circ (a * c)$ and $(a \circ b) * c = (a * c) \circ (b * c)$ for all $a, b, c \in S$.

The following example illustrates this property.

Example 18

Given the operations $*$ and $\circ$ on $\mathbb{Z}$, such that $a * b = 3ab$ and $a \circ b = a + 3b$, determine whether:

a $*$ is distributive over $\circ$ **b** $\circ$ is distributive over $*$

a $a * (b \circ c) = a * (b + 3c) = 3a(b + 3c) = 3ab + 9ac$

Check if $*$ is distributive over $\circ$

$(a * b) \circ (a * c) = (3ab) \circ (3ac) = 3ab + 3(3ac)$

$= 3ab + 9ac$

Therefore $*$ is distributive over $\circ$

b $a \circ (b * c) = a \circ (3bc) = a + 9bc$

Check if is $\circ$ is distributive over $*$

$(a \circ b) * (a \circ c) = (a + 3b) * (a + 3c)$

$= 3(a + 3b)(a + 3c)$

$a \circ (b * c) \neq (a \circ b) * (a \circ c)$

For example, $5 \circ (5 * 5) = 5 \circ 75 = 230$, but $(5 \circ 5) * (5 \circ 5) = 1200$.

Therefore $\circ$ is not distributive over $*$.

Exercise 2E

1 For the binary operations defined below determine whether $*$ is

i commutative **ii** associative

a $*$ is defined on $\mathbb{Z}$ by $a * b = a - b$

b $*$ is defined on $\mathbb{Q}$ by $a * b = 2ab + 1$

c $*$ is defined on $\mathbb{N}$ by $a * b = 2^a 3^b$

2 $*$ is a commutative and associative binary operation on a set S.

Show that $(a * b) * (c * d) = \big((d * c) * a\big) * b$.

3 Let f_1, f_2, f_3 and f_4 be functions defined on $\mathbb{R} \setminus \{0\}$ such that $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$ and $f_4(x) = -\frac{1}{x}$. The binary operation $\circ$ on $S = \{f_1, f_2, f_3, f_4\}$ is defined as the composition of functions.

Draw a Cayley table to illustrate this operation. Determine whether

a S is closed under composition of functions

b the operation composition of functions is commutative in S.

4 The binary operation $*$ is defined on $\mathbb{R}$ such that for all $a, b \in \mathbb{R}$, $a * b = a + 2b - 1$. Determine whether the binary operation $*$ is

a commutative **b** associative.

5 The operation $*$ is defined on $\mathbb{R} \setminus \{1\}$ by $a * b = ab - a - b + 2$ for all $a, b \in \mathbb{R} \setminus \{1\}$. Show that:

a $\mathbb{R} \setminus \{1\}$ is closed under the operation $*$

b the operation $*$ is commutative

c the operation $*$ is associative.

The identity element *e*

Definition

Let $*$ be a binary operation on S. If there is an element $e \in S$ such that for every element $x \in S$, $e * x = x = x * e$, then we say that e is the **identity element** of S under the operation $*$.

Theorem 8

The identity element of a binary operation $*$ on S is unique.

Proof:

Let $e, f \in S$, $e \neq f$ such that for every element $x \in S$:

$e * x = x = x * e$ and $f * x = x = x * f$

$e * x = x = x * e \Rightarrow e * f = f = f * e$ (replacing x by f since $f \in S$)

$f * x = x = x * f \Rightarrow f * e = e = e * f$ (replacing x by e since $e \in S$)

Combining the two we obtain the result that $e = f$ and so the identity is unique. Q.E.D.

In general we could say that an element $e \in S$ is the left identity if for every $x \in S$, $e * x = x$, and $f \in S$ is the right identity if for every $x \in S$, $x = x * f$. We can show that $e = f$ as follows. (i.e. if there is a left identity and there is also a right identity, then they are equal.)

Since e is a left identity we know that $e * x = x$.
But since $f \in S$ we can replace x by f to obtain $e * f = f$.
But f is a right identity so $e * f = e$.
Therefore $e = f$.

Example 19

Let the binary operation $*$ be defined on set of numbers S such that for $a, b \in S$, $a * b = \frac{ab}{2}$.
Determine whether or not an identity exists and if it does, find it.

Suppose an identity exists, i.e. $e * b = b$ for $b \in S$.

First we find the left identity.

$e * b = b$ and $e * b = \frac{eb}{2}$

Therefore $b = \frac{eb}{2} \Rightarrow e = 2$

Now we find the right identity.

$b * e = b$ and $b * e = \frac{be}{2}$

$b = \frac{be}{2} \Rightarrow e = 2$

Since the left identity is equal to the right identity the identity exists and $e = 2$.

Example 20

Let the binary operation $*$ be defined on $\mathbb{Z}^+$ such that for $a, b \in S$, $a * b = 2a + 3b$. Determine whether or not an identity exists and if it does, find it.

Suppose an identity exists, i.e. $e * b = b$ for $b \in S$

$e * b = b$ and $e * b = 2e + 3b$

$\Rightarrow b = 2e + 3b$

$\Rightarrow e = -b$

First look for the left identity.

We can show that the right identity is not equal to the left identity as follows:

$b * e = b$ and $b * e = 2b + 3e$

$\Rightarrow b = 2b + 3e$

$$\Rightarrow e = -\frac{b}{3}$$

Since the left identity is not equal to the right identity and neither left identity nor right identity are elements of $\mathbb{Z}^+$ it follows that the operation does not have an identity in S.

Exercise 2F

In Questions 1 to 5 below, determine whether the binary operation $*$ is:

a commutative

b associative.

Determine whether or not an identity element exists and if it does, find it.

1 The binary operation $*$ is defined on $\mathbb{Q}$ such that for all $a, b \in \mathbb{Q}$, $a * b = a + b - ab$.

2 The binary operation $*$ is defined on $\mathbb{N} \times \mathbb{N}$ such that for all $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$, $(m, n) * (p, q) = (mp, nq)$.

3 The binary operation $*$ is defined on $\mathbb{N} \times \mathbb{N}$ such that for all $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$, $(m, n) * (p, q) = (m + p, n + q)$.

4 The binary operation $*$ is defined on $\mathbb{Q} \times \mathbb{Q}$ such that for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$, $(a, b) * (c, d) = (ac, ad + b)$.

5 The binary operation $*$ is defined on $\mathbb{Z}^+ \times \mathbb{Z}^+$ such that for all $(m, n), (p, q) \in \mathbb{Z}^+ \times \mathbb{Z}^+$, $(m, n) * (p, q) = (mq + np, nq)$.

The inverse of an element

Definition

Let $*$ be a binary operation on S with identity e. Then for all $x \in S$ if there exists an element $y \in S$ such that $x * y = e = y * x$ then we call y the **inverse** of x, and we write $y = x^{-1}$.

It is easy to understand this concept with some operations that you are familiar with. The identity of addition in $\mathbb{R}$ is 0 because $x + 0 = x = 0 + x$ for all $x \in \mathbb{R}$. Since $-x \in \mathbb{R}$ and $x + (-x) = (-x) + x = 0$ we conclude that for addition in $\mathbb{R}$, $e = 0$ and $x^{-1} = -x$.

Similarly for multiplication in $\mathbb{R}\backslash\{0\}$, the identity $e = 1$ since $1 \times x = x = x \times 1$ and the inverse is given by $x^{-1} = \frac{1}{x}$ since $x \times \left(\frac{1}{x}\right) = \left(\frac{1}{x}\right) \times x = 1$.

Note that x^{-1} here is the notation for inverse, not the reciprocal notation for numbers, which happens to be the same.

Theorem 9

For an associative binary operation $*$ in S with identity e, the inverse is unique.

Proof:

Let a, b be inverses of x.

$a = e * \mathrm{a}$	by definition of identity
$= (b * x) * a$	since b is an inverse of x
$= b * (x * a)$	by associativity
$= b * e$	since a is an inverse of x
$= b$	by definition of identity Q.E.D.

You should remember that you cannot discuss an inverse without first establishing that an identity exists. We also need to assume the associativity property but **not commutativity**.

Example 21

For multiplication in $\mathbb{C} \setminus \{0\}$ determine whether or not the identity element exists and if it does find the inverse of $z \in \mathbb{C} \setminus \{0\}$.

We know that for $z \in \mathbb{C} \setminus \{0\}$, $1 \times z = z \times 1 = z \Rightarrow e = 1 + 0i$. For $z \in \mathbb{C} \setminus \{0\}$, $z \times \frac{1}{z} = \frac{1}{z} \times z = 1$.	*Establish whether there is an identity.*
$z = a + bi$ $\Rightarrow \frac{1}{z} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{z^*}{zz^*}$ Therefore the inverse $z^{-1} = \frac{z^*}{zz^*}$.	*Find the inverse.*

Example 22

Let $*$ be a binary operation on $\mathbb{Q} \times (\mathbb{Q}\backslash\{0\})$ such that $(a, b) * (c, d) = (a + c, bd)$.

a Show that the operation is

i associative **ii** commutative.

b Show that the identity exists and find the inverse $(a, b)^{-1}$ under $*$ in $\mathbb{Q} \times (\mathbb{Q}\backslash\{0\})$.

a i Associativity:

$(a, b) * ((c, d) * (m, n)) = ((a, b) * (c, d)) * (m, n)$

LHS

$$= (a, b) * \big((c, d) * (m, n)\big)$$
$$= (a, b) * (c + m, dn)$$
$$= (a + (c + m), b(dn))$$
$$= ((a + c) + m, (bd)n)$$
$$= ((a + c), bd) * (m, n)$$
$$= ((a, b) * (c, d)) * (m, n) = \text{RHS}$$

Therefore $*$ is associative in $\mathbb{Q} \times (\mathbb{Q}\backslash\{0\})$.

ii Commutativity:

$$(a, b) * (c, d) = (a + c, bd)$$
$$= (c + a, db)$$
$$= (c, d) * (a, b)$$

Therefore $*$ is commutative in $\mathbb{Q} \times (\mathbb{Q}\backslash\{0\})$.

b Since we have shown that $*$ is commutative there is no need to find both left and right identities since they will be equal.

Let $(x, y) \in \mathbb{Q} \times (\mathbb{Q}\backslash\{0\})$ such that $(x, y) * (a, b) = (a, b)$
$\Rightarrow (x + a, yb) = (a, b) \Rightarrow x + a = a \Rightarrow x = 0$ and $yb = b \Rightarrow y = 1$
So the identity is $(0, 1)$.

Let $(m, n) \in \mathbb{Q} \times (\mathbb{Q}\backslash\{0\})$ such that $(m, n) * (a, b) = (0, 1)$.
$(m + a, nb) = (0, 1)$

$$\Rightarrow m = -a, n = \frac{1}{b}$$

Therefore $(a, b)^{-1} = \left(-a, \frac{1}{b}\right)$.

When checking the properties you should first define them and then prove that the RHS = LHS.

The cancellation laws

The cancellation laws are very important in abstract algebra and will be used extensively in the next chapters.

An invertible binary operation on S is one where for every x element of S, there exits an inverse also in S.

Theorem 10

Let $*$ be an invertible associative binary operation on a non-empty set S with identity e. Then the operation satisfies

i the **left cancelation law**, i.e. $a * b = a * c \Rightarrow b = c$

ii the **right cancelation law**, i.e. if $a * b = c * b \Rightarrow a = c$

Proof:

Let $a * b = a * c$, where $a, b, c \in S$.

$a^{-1} * (a * b) = a^{-1} * (a * c)$, since a has a unique inverse in S

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$, since the operation is associative

$\Rightarrow e * b = e * c$ by definition of the inverse element

$\Rightarrow b = c$ by definition of the identity element Q.E.D.

The proof of the right cancellation law is left as an exercise.

Example 23

Show that both right and left cancellation laws are satisfied for the composition of bijective functions.

Let f, g, h be bijections. We need to show that	
a if $f \circ g = f \circ h$ then $g = h$	
b if $f \circ g = h \circ g$ then $f = h$	
Since f is a bijection it is invertible, i.e. there exists a bijection f^{-1} such that $f \circ f^{-1} = I = f^{-1} \circ f$	
$f \circ g = f \circ h$	
$\Rightarrow f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ h)$	
$\Rightarrow (f^{-1} \circ f) \circ g = (f^{-1} \circ f) \circ h$	*Composition of functions is associative.*
$\Rightarrow I \circ g = I \circ h$	*Inverse property.*
$\Rightarrow g = h$	*Identity property.*
Therefore the left cancellation law holds.	
It is left as an exercise to prove part **b**.	

Exercise 2G

1 The binary operation $*$ is defined on $\mathbb{R}$ as follows. For any $a, b \in \mathbb{R}$
$a * b = a + b + 1$

a Show that $*$ is commutative. **b** Find the identity element.

c Find the inverse of the element a.

2 Consider the binary operation multiplication on the set $\mathbb{C} \setminus \{0\}$.

a Show that multiplication is commutative.

b Show that multiplication is associative.

c Find the identity element under multiplication.

d Find the inverse of the element $a + bi$ under multiplication.

3 Consider the set $A = \{0, 1, 2, 3\}$ under the binary operation $*$ such that for $a, b \in A$, $a * b = a + b \pmod 4$. Construct a Cayley table to illustrate this binary relation and show that the relation is commutative. Identify the identity element and hence find the inverse of each element in A.

4 For each of the following sets, $*$ represents a closed binary operation defined on the given set S. Determine whether or not the identity element exists. If it does, find it and the inverse of $a \in S$.

a $S = \{2, 4, 6, 8\}$, $a * b = ab \pmod{10}$

b $S = \mathbb{Q} \setminus \{0\}$, $a * b = \dfrac{ab}{2}$ **c** $S = \mathbb{Z}^+$, $a * b = 2 + ab$

5 Consider the binary operation multiplication on the set $S = \{2^n \mid n \in \mathbb{Z}\}$.

a Show that

i S is closed under multiplication

ii multiplication is associative

iii an identity exists

iv every element in S has an inverse in S

6 Given the set $S =]-1, 1[$ and the operation $a * b = \dfrac{a+b}{1+ab}$,

a show that

i S is closed under $*$

ii $*$ is associative

iii an identity exists.

b Find the inverse of $a \in S$ under $*$.

Review exercise

EXAM-STYLE QUESTIONS

1 $S = \{1, 2, 3, 4, 5, 6\}$ and the function $f : S \to S$ is defined by $f(x) = 6x \pmod 7$

a Prove that f is a bijection.

b Show that f is its own inverse.

2 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** $(A * B) * (A * B) = A \cap B$.

3 Let $f : A \to B$ where $A = [0,\infty[\times \left[0, \dfrac{\pi}{2}\right[$, $B = [0, \infty[\times [0, 1[$ and $f(x, y) = (x \cos y, \sin y)$. Determine whether f is a bijection.
If it is, find the inverse function f^{-1}.

4 The operation $*$ is defined on $\mathbb{Z} \times \mathbb{Z}$ as
$(a, b) * (c, d) = (ac + bd, ad + bc)$, where $a, b, c, d \in \mathbb{Z}$.
Find the identity element for this operation.

5 Consider three sets S, T and U.
f and g are two mappings such that $f : S \to T$, and $g : T \to U$.

i If $g \circ f$ is surjective, prove that g is surjective

ii If $g \circ f$ is injective, prove that f is injective.

6 The function $f:\mathbb{R}\to\mathbb{R}$ is defined by $f(x)=3^{\cos x}+\frac{1}{6}$.

a Determine whether or not the function is injective or surjective, giving reasons.

b If the domain is restricted to $[0, \pi]$, what are the restrictions on the co-domain that would make f invertible? Find the inverse function.

7 Let $*$ be the binary operation on the set $S=\left\{x\middle|-1<x<1,\ x\in\mathbb{R}\right\}$ defined by $x*y=\dfrac{x+y}{1+xy}$, for any $x,\ y\in S$.

a Determine whether or not the operation $*$ is

i commutative **ii** associative.

b Establish whether or not an identity exists and if so find it.

8 The function $f:\mathbb{R}\to\mathbb{R}$ is defined by $f(x)=\mathrm{e}^{2\cos x}+1$

a Find the exact range of f.

b **i** Explain why f is not an injection.

ii Giving a reason, state whether or not f is a surjection.

c A new function g is now defined as follows:
$g:[0,k]\to A$ where $g(x)=\mathrm{e}^{2\cos x}+1$ and $k\geq 0$.

i Find the maximum value of k for which g is an injection.
For this value of k, what values can A take to make $g(x)$ a bijection?

ii Find an expression for $g^{-1}(x)$.

iii Write down the domain of g^{-1}.

Chapter 2 summary

A relation that associates each element in a non-empty set S with a unique element in a non-empty set T is called a function from S to T.

We denote this function by $f: S\to T$.

The set S is called the **domain** and T, the target set, is called the **co-domain**.
The set $f(S)=\{t|t\in T, t=f(s)\}$, subset of T, is called the **range**.

A function $f: S\to T$ for which each element of the range, $f(S)$, corresponds to exactly one element of the domain, S, is said to be an **injection**, i.e. if $f(a)=f(b)\Rightarrow a=b$ for $a,b\in S$.

If every element in the co-domain of a function is the image of at least one element in the domain we say that the function is a **surjection**, i.e. for all b in the co-domain there exists an a in the domain such that $f(a)=b$.

A function is a **bijection** if it is an injection and a surjection.

Given $f: S\to T$ where S and T are finite sets, then:

a f is injective $\Leftrightarrow n(f(S))=n(S)$

b f is surjective $\Leftrightarrow n(f(S))=n(T)$

Composite functions

If $g : A \to B,\ f : B \to C$ are functions, then $f \circ g : A \to C$ is also a function.

A function $f : A \to B$ is bijective $\Leftrightarrow$ it has an inverse.

A function $f : A \to B$ is bijective $\Leftrightarrow$ its inverse is also a bijection.

Properties of composite functions:

- Associativity $\left(\left(f \circ g\right) \circ h\right)(x) = \left(f \circ \left(g \circ h\right)\right)(x)$
- If f: $S \to T$ and g: $T \to S$ are injections, then $\left(f \circ g\right)(x)$ and $\left(g \circ f\right)(x)$ are injective.
- If f: $S \to T$ and g: $T \to S$ are surjections, then $\left(f \circ g\right)(x)$ and $\left(g \circ f\right)(x)$ are surjective.

The **identity function** for a set S is a bijection $I_S : S \to S$ such that $I_S(x) = x$ for all $x \in S$.

Let f: $S \to S$ be any function, then $\left(I_S \circ f\right)(x) = \left(f \circ I_S\right)(x) = f(x)$ for all $x \in S$.

For a bijection f: $S \to T$ such that $f(x) = y,\ x \in S$ and $y \in T$, the inverse function $f^{-1} : T \to S$ is such that $\left(f^{-1} \circ f\right)(x) = I_S$ and $\left(f \circ f^{-1}\right)(y) = I_T$

A **binary operation** $*$ on a non-empty set S is a rule for combining any two elements $x, y \in S$ to give a unique element c. This is denoted by $x * y = c$. A binary operation on a non-empty set S is said to be closed if for all $a, b \in \mathrm{S}$, $a * b \in S$.

A binary operation on a non-empty set S is **closed** if for all $a, b \in S$, $A * B \in S$.

A binary operation $*$ on a non-empty set S is said to be **associative** if for all $a, b, c \in S$, $a * (b * c) = (a * b) * c$.

A binary operation $*$ on a non-empty set S is said to be **commutative** if for all $a, b \in S$, $a * b = b * a$.

If $*$ is a binary operation on S and there is an element $e \in S$ such that for every element $x \in S$, $e * x = x = x * e$, then we say that e is **the identity element** of S under the operation $*$.

The identity element of a binary operation $*$ on S is unique.

Let $*$ be a binary operation on S with identity e. Then for all $x \in S$ if there exists an element $y \in S$ such that $x * y = e = y * x$ then we call y the inverse of x, and we write $y = x^{-1}$.

For a binary operation $*$ in S with identity e, if the inverse exists it is unique, i.e. each x element of S has a unique inverse.

Let $*$ be an invertible associative binary operation on a non-empty set S with identity e. The operation is said to satisfy

i the **left cancelation law**, i.e. $a * b = a * c \Rightarrow b = c$

ii the **right cancelation law**, i.e. $a * b = c * b \Rightarrow a = c$

3

The ‘Universal Theory of Everything’ in Mathematics

CHAPTER OBJECTIVES:

8.7 The definition of a group $\{G, *\}$; the operation table of a group is a Latin square, but the converse is false; Abelian groups.

8.8 Examples of groups: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{C}$ under addition; integers under addition modulo *n*; non-zero integers under multiplication modulo *p*, where *p* is prime; symmetries of plane figures, including equilateral triangles and rectangles; invertible functions under composition of functions.

8.9 The order of a group; the order of a group element; cyclic groups; generators; proof that all cyclic groups are Abelian.

8.11 Subgroups; proper subgroups; use and proof of subgroup tests.

Before you start

You should know how to:

1 Given that $f(x) = \frac{1}{2}x + 1$ and $g(x) = \mathrm{e}^x$,

a Find the inverses of functions, e.g. find $f^{-1}(x)$ and $g^{-1}(x)$. Exchanging x and $f(x)$, solving for x, and then using inverse notation, we obtain $f^{-1}(x) = 2(x - 1)$; $g^{-1}(x) = \ln x$

b Find the composition of functions, e.g. find $(f^{-1} \circ g^{-1})(x)$. Substituting $g^{-1}(x)$ for the variable in $f^{-1}(x)$ we obtain $(f^{-1} \circ g^{-1})(x) = 2(\ln x - 1)$

c Recognize that function composition is not commutative, e.g. find $(g^{-1} \circ f^{-1})(x)$. Substituting f^{-1} for the variable in g^{-1} we obtain $(g^{-1} \circ f^{-1})(x) = \ln[2(x - 1)]$ Clearly, by considering the formulas, function composition is not commutative.

Skills check:

1 Given that f and g are functions on $\mathbb{R}^+$ such that $f(x) = \ln(x + 1)$ and $g(x) = x^2$, find the following:

a $(f \circ g)(x)$

b $(f \circ g)^{-1}(x)$

c $(g \circ f)(x)$

d $(f^{-1} \circ g^{-1})(x)$

2 Check whether the properties of closure, commutativity, associativity, identity and inverse hold for a set under a given binary operation, e.g. $\{\mathbb{R}, *\}$, $a * b = 2ab$. Determine if any element(s) would have to be removed from $\mathbb{R}$ in order for the properties of identity and inverse to hold under $*$.

Closure, i.e. for all $a, b \in \mathbb{R}$, $a * b \in \mathbb{R}$.
Since $a * b = 2ab$, $2ab \in \mathbb{R}$, $\{\mathbb{R}, *\}$ is closed.

Commutativity, i.e. for all a, $b \in \mathbb{R}$, $a * b = b * a$. Since $a * b = 2ab = 2ba = b * a$, $\{\mathbb{R}, *\}$ is commutative.

Associativity, i.e. for all $a, b, c \in \mathbb{R}$, $a * (b * c) = (a * b) * c$. Since $a * (b * c) = a * (2bc) = 2a(2bc) = 4abc$ and $(a * b) * c = (2ab) * c = 4abc$, $\{\mathbb{R}, *\}$ is associative.

Identity, i.e. for all $a \in \mathbb{R}$ there exists an $e \in \mathbb{R}$ such that $a * e = a = e * a$.

We need to find an $m \in \mathbb{R}$ such that $a * m = a = m * a$. (Note that since we are not sure that the set has an identity under the binary operation, we do not yet use the symbol e for identity.)

For the right hand identity, $a * m = a \Rightarrow 2am = a$, $2am = a \Rightarrow m = \frac{a}{2a} = \frac{1}{2}$, $a \neq 0$. For the left hand identity, $m * a = a \Rightarrow m = \frac{1}{2}$, $a \neq 0$. Hence, $e = \frac{1}{2}$.

Strictly speaking, since $\{\mathbb{R}, *\}$ is commutative, it is enough to look for either the right identity or left identity, since they will be equal.

Inverse, i.e. for all $a \in \mathbb{R}$ there exists an $a^{-1} \in \mathbb{R}$ such that $a * a^{-1} = e = a^{-1} * a$. We need to find an $n \in \mathbb{R}$ such that $a * n = e = n * a$.

(Note again, that since we do not know if each element has an inverse, we do not yet use the notation for inverse, a^{-1}.) Since $a * n = 2an = \frac{1}{2}$, $n = \frac{1}{4a}$, $a \neq 0$. And since $(\mathbb{R}, *)$ is commutative, we need only find either the right or left inverse. For $\mathbb{R}$ to have an identity and inverse under $*$, 0 would have to be excluded. Hence, all the properties hold for $\{\mathbb{R}\backslash\{0\}, *\}$.

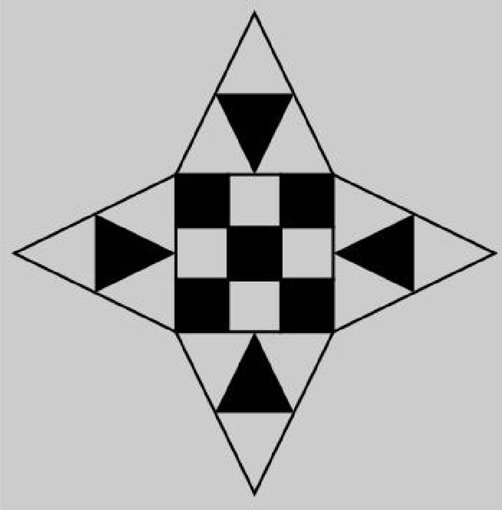
2 Check whether the properties of closure, commutativity, associativity, identity and inverse hold for the following sets under the given binary operations.

a $(\mathbb{Z}^+, \odot)$, $a \odot b = a^b$

b $(\mathbb{R}^+, *)$, $a * b = 2^{ab}$

c $(\mathbb{Q}, \otimes)$, $a \otimes b = ab + 1$

The geometric nature of Islamic art incorporates complex symmetries that have been mathematically analyzed and explored. Perhaps the most famous of such art forms lies within the Alhambra, a fortress constructed in Andalusia, Spain, in the 9th century during the last Islamic sultanate on the Iberian Peninsula. Some of the geometric murals in the Alhambra are examples of symmetry groups, which you will learn about in this chapter, and have some of the properties that you have been working with on the left hand side in the given example.



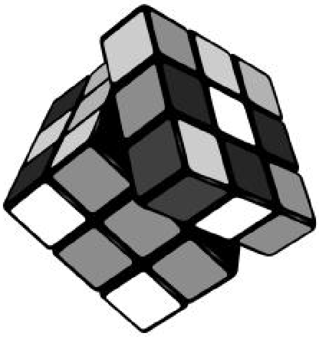
Group Theory

The search in Physics for a theory that fully explains and connects all physical aspects of the universe results from two major scientific paradigms in the last century: General Relativity and Quantum Mechanics. General theorems providing a mathematical basis for such a ‘universal theory of everything’ have been attempted, and, at the time of writing, a recent work entitled “Generalized Mathematical Proof of Einstein’s Theory Using a New Group Theory” was reviewed by both the American Mathematical Society and the European Mathematical Society.

Indeed, increasingly it seems as if Group Theory is the ‘unifying theory of everything’ in mathematics, i.e. a branch of mathematics that can connect all other branches by finding similarities in their inherent structures. In essence, Group Theory measures symmetry, the *“one idea by which man through the ages has tried to comprehend and create order, beauty, and perfection*” – Hermann Weyl.

In 1824, the Norwegian Mathematician Niels Henrik Abel published his ‘impossibility theorem’, in which he proved there is no general solution, or formula, for finding the solutions of polynomial equations of degree 5 (quintics) or higher. At about the same time, a brilliant French teenager, Evariste Galois, explained *why* this is the case. He not only resolved one of the great challenges of his day, but more importantly, he discovered a compelling connection between symmetry, permutation groups (which you will learn about in Chapter 4), and the solvability of polynomial equations.

Although Galois and Abel laid the foundations of the mathematics of Group Theory, it is a 20th century female mathematician, Emily Noether, who is credited with the title of 'father' of Abstract Algebra, mainly through changing the 19th century emphasis of its use from solving polynomial equations into creating an abstract axiomatic system.



Today, Group Theory is used in many different areas of study, such as elementary Particle Physics, Music Theory, Crystallography, Chemistry, Campanology (the study of bells and bell-ringing), and perhaps its most popular usage in terms of the masses: solving Rubik's Cube!

3.1 Groups

A group consists of a set and a binary operation on that set.

The set with a binary operation has the four properties of closure, associativity, existence of an identity element, and existence of inverses.

Definition

The set G with a binary operation $*$ is called a **group** if the following four axioms (properties) hold:

1 Closure: for all $a, b \in G$, $a * b \in G$

2 Associativity: for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$

3 Identity: for all $a \in G$, there exists an element $e \in G$ such that $a * e = a = e * a$

4 Inverse: for each $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$

The group G with binary operation $*$ is denoted by $\{G, *\}$.

Note that the commutative property is **not** a required group axiom. For this reason it is important that both the left and right identity and inverse properties be confirmed. For example, the set $\mathbb{Z}$ under the binary operation of subtraction has a unique right identity 0, i.e. $a - 0 = a$ for all $a \in \mathbb{Z}$. However, $0 - a = -a$, hence it has no left identity. Therefore $\{\mathbb{Z}, -\}$ is not a group.

It is not necessary to check for both left and right identities if the binary operation is commutative.

If in addition to the four properties above, a set G with binary operation $*$ is also commutative, then it is said to be an **Abelian group**.

Definition

A group $\{G, *\}$ is an **Abelian group** if G is commutative under $*$, i.e. for all $a, b \in G$, $a * b = b * a$.

It is important to note that the identity element is unique, as are the inverses, i.e. a group contains only one identity element, and each element contains a unique inverse. In Chapter 2 you proved these results for binary operations on a set S using the left and right cancellation laws.

Groups may be finite or infinite, i.e. consist of finite or infinite sets. Set A is finite, i.e. its cardinality is $n \in N$, if there is a bijection from set $\{0, 1, 2, \ldots, n\}$ to A. A set is infinite if it is not finite. If a set G is finite, then the group is also finite, otherwise it is an infinite group.

Infinite groups

You have already been working with many examples of infinite groups, e.g. the sets $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{C}$ under the binary operation of addition. Since the binary operation of addition is commutative, these four sets under addition are furthermore Abelian groups.

Example 1

Show that the following infinite sets are groups under the given binary operation. Determine if any are Abelian groups.

a $\{\mathbb{R}^+, \times\}$

b $\{\mathbb{Q} \setminus \{0\}, \times\}$

c The set of all real-valued functions with domain $\mathbb{R}$ under addition.

a Closure: for all $a, b \in \mathbb{R}^+$, $ab \in \mathbb{R}^+$ Associativity: for all $a, b, c \in \mathbb{R}^+$, $a(bc) = (ab)c$ Identity: for all $a \in \mathbb{R}^+$, $a \times 1 = a = 1 \times a$ Inverse: for all $a \in \mathbb{R}^+$, $\frac{1}{a} \in \mathbb{R}^+$ and $a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$ $\{\mathbb{R}^+, \times\}$ is a group since all group properties hold.	*Show that all four of the group properties hold.*
Commutativity: for all $a, b \in \mathbb{R}^+$, $ab = ba$, hence $\{\mathbb{R}^+, \times\}$ is an Abelian group.	*Determine if the commutative property holds.*
b Closure: for all $a, b \in \mathbb{Q} \setminus \{0\}$, $ab \in \mathbb{Q} \setminus \{0\}$ Associativity: for all $a, b, c \in \mathbb{Q} \setminus \{0\}$, $a(bc) = (ab)c$ Identity: for all $a \in \mathbb{Q} \setminus \{0\}$, $a \times 1 = a = 1 \times a$, $1 \in \mathbb{Q} \setminus \{0\}$ Inverse: for all $a \in \mathbb{Q} \setminus \{0\}$, $\frac{1}{a} \in \mathbb{Q} \setminus \{0\}$ and $a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$ $\{\mathbb{Q} \setminus \{0\}, \times\}$ is a group since all group properties hold.	*Show that all four of the group properties hold.*
Commutativity: for all $a, b \in \mathbb{Q} \setminus \{0\}$, $ab = ba$, hence $\{\mathbb{Q} \setminus \{0\}, \times\}$, is an Abelian group.	*Determine if the commutative property holds.*

c Closure: for all real-valued functions f and g, $f + g$ is a real-valued function. Associativity: for all real-valued functions f, g and h, $f + (g + h) = (f + g) + h$. Identity: for all real-valued functions f, $g(x) = 0$ is a real valued function for all real values of x, and $f + g = f = g + f$. Inverse: for all real-valued functions f, there exists a real valued function $-f$ such that $f + (-f) = g = (-f) + f$, where $g(x) = 0$, for all x. The set of all real-valued functions under addition is a group, since all group properties hold.	*Show that all four of the group properties hold.*
Commutativity: for all real-valued functions f and g, $f + g = g + f$, hence the set of all real-valued functions under addition is an Abelian group.	*Determine if the commutative property holds.*

We now consider other infinite sets under a binary operation and determine if each is a group. For example, the set $\mathbb{Z}^+$ under addition is not a group, since there is no identity for addition in the set $\mathbb{Z}^+$. Also, the set of all non-negative integers under addition is not a group, because although it contains the identity element 0, there are no inverses for the non-zero elements of the set. (It is sufficient to find just one element in the set for which an inverse does not exist in order to show that the set under the binary operation is not a group.)

Example 2

Determine if the following sets are groups under the given binary operation.

a $\mathbb{Z}^+$ under multiplication

b $\mathbb{N}$ under the binary operation $*$ defined as $a * b = \|a - b\|$

c $\mathbb{Q}^+$ under the binary operation # defined as $a \# b = \frac{ab}{2}$, $a, b \in \mathbb{Q}^+$

a Since the identity is 1, there is no inverse for 2. Indeed, other than 1, no other elements of the given set have an inverse.	*Identify a property of groups that is not satisfied.*
b If $a = 1$, $b = 2$, and $c = 3$, then $a * (b * c) = 1 * \|2 - 3\| = \|1 - \|-1\|\| = 0$ $(a * b) * c = \|1 - 2\| * 3 = \|\|-1\| - 3\| = 2$ Associativity does not hold, so $(\mathbb{N}, *)$ is not a group.	*Identify a property of groups that is not satisfied.*

c Closure: $a \# b = \dfrac{ab}{2} \in \mathbb{Q}^+$, so closure holds.

Go through all the group axioms to see if they hold.

Associativity:

$$a \# (b \# c) = a \# \left(\frac{bc}{2}\right) = \frac{a\frac{bc}{2}}{2} = \frac{abc}{4}$$

$$(a \# b) \# c = \frac{ab}{2} \# c = \frac{\frac{ab}{2}c}{2} = \frac{abc}{4}$$

Hence associativity holds.

Identity: find $b \in \mathbb{Q}^+$ such that:

$a \# b = a \Rightarrow \dfrac{ab}{2} = a \Rightarrow b = 2$, and

$b \# a = a \Rightarrow \dfrac{ba}{2} = a \Rightarrow b = 2$

Hence, the identity $e = 2$; $2 \in \mathbb{Q}^+$.

Inverse: find $c \in \mathbb{Q}^+$ such that

$a \# c = 2 \Rightarrow \dfrac{ac}{2} = 2 \Rightarrow c = \dfrac{4}{a}$, and

$c \# a = 2 \Rightarrow \dfrac{ca}{2} = 2 \Rightarrow c = \dfrac{4}{a}$

Hence, $a^{-1} = \dfrac{4}{a}$; $a^{-1} \in \mathbb{Q}^+$.

Since all the group axioms hold, $\{\mathbb{Q}^+, \#\}$ is a group.

Write your conclusion.

Investigation

Consider the different number sets and their subsets, e.g. $\mathbb{Z}$, $\mathbb{Z}^+$, and $\mathbb{C}$ etc., the arithmetic operations +, ×, and the inverse operations − and ÷. Select a set and determine the binary operations under which it forms a group.

The following table headings might help organize your work.

Number Set	Operation	Group (Yes, No)	Reason

From the examples and the investigation, you have seen that in order to show a given set with a binary operation is *not* a group, it is sufficient to show that any one of the group properties does not hold.

In part **c** of Example 2 you may have noticed that it is important to ascertain the following when checking to see if the properties hold:

- The identity element must be in the given set, and must commute with every element in the set.
- The inverse for each element must be in the given set, and must commute with the original element.

Example 3

Show that the set of bijections forms a group under function composition.	
Closure: if *f* and *g* are bijections such that $f: A \to B,\ g: B \to C$ then $g \circ f: A \to C$. Hence, the composition of two bijections is a bijection and closure holds.	*Confirm the group properties. This was proven in Chapter 2, theorem 5c.*
Associativity: if *f*, *g* and *h* are bijections, then for all *x*, $(h \circ g) \circ f = (h \circ g)\big(f(x)\big)$ $= h\big(g(f(x))\big)$ $= h\big((g \circ f)(x)\big)$ $= h \circ (g \circ f)$ Hence, the composition of bijections is also associative.	*The proof that function composition is associative is done in Chapter 2, theorem 4.*
Identity: the function $e: x \mapsto x$ is a bijection. For all functions *f*, $e \circ f = f = f \circ e$. Hence, *e* is the identity.	
Inverse: every bijection *f* has an inverse f^{-1} that is also a bijection such that $f \circ f^{-1} = e = f^{-1} \circ f$ Hence, the set of bijections forms a group under function composition.	*This was proven in Chapter 2, theorem 3b.* *State your conclusion.*

You have already seen that function composition is not usually commutative, hence the group in Example 3 is not Abelian.

Exercise 3A

1 Show that the set $S = \{2^n | n \in \mathbb{Z}\}$ under multiplication forms a group.

2 Show that under addition, the following sets of functions f: $\mathbb{R}$ form a group:

a all continuous functions

b all differentiable functions.

3 Determine if the following sets under the given binary operation form a group:

a $\mathbb{R}^+$ under the operation # defined as $a \# b = \sqrt{ab}$

b $\mathbb{R}\backslash\{0\}$ under the operation ∘ defined as $a \circ b = |a|b$

c $\{3^n | n \in \mathbb{N}\}$ under multiplication

d $\{a + bi | a, b \in \mathbb{R}, |a + bi| = 1\}$ under multiplication.

4 **a** Show that the set $S = \mathbb{R}\backslash \{-1\}$ under $*$ defined as $a * b = ab + a + b$ forms a group.

b Determine if $\{S, *\}$ is an Abelian group.

c Find the solution of the equation $2 * x = 7$ in S.

d Explain why $\{\mathbb{R}, *\}$ does not form a group.

5 Let $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ and $S = \mathbb{R} \times \mathbb{R}^*$, i.e. S is the set of all ordered pairs (a, b) such that a and b are real numbers, and b is non-zero. Define $\oplus$ such that $(a_1, b_1) \oplus (a_2, b_2) = (a_1+b_1a_2, b_1b_2)$.

a Show that $\{S, \oplus\}$ is a group.

b Calculate the following:

i $(3, -2) \oplus (1, -1)$

ii $(1, 2) \oplus (-0.125, 1.4)$

c Determine if $\{S, \oplus\}$ is Abelian.

6 Show that $S = \{nm \mid n \in \mathbb{Z}, m \in \mathbb{Z}\}$ forms a group under addition.

7 Show that the set of all real-valued functions of the form $f(x) = ax + b$, $a \neq 0$, whose domain is $\mathbb{R}$ form a group under the binary operation composition of functions. Does it form an Abelian group?

Finite groups

So far all our examples have been of infinite groups, i.e. groups where the set G has an infinite number of elements. We will now consider groups defined on finite sets.

Since a group must contain an identity, it must contain at least one element. The only possible binary operation $*$ on $\{e\}$ must necessarily be defined as $e * e = e$. The identity element is its own inverse, and the properties of closure and associativity obviously hold. We say that the order of $\{\{e\}, *\}$ is 1, i.e. the number of elements in the group is 1.

Definition

The **order** of a group $\{G, *\}$ is the number of elements in the group. If a group has an infinite number of elements, it is said to have infinite order, i.e. $|G| = \infty$.

We will now create a finite group of order 2. Since one of the elements must be the identity, we define the set S as $\{e, a\}$, $e \neq a$, and the binary operation $*$. We now set up an operation table for these two elements. Checking the group properties, we see from the table below that closure holds, since there are no extraneous elements. We have said that e is the identity element, and checking, we see that $e * e = e$ and $a * e = e * a = a$. If e is the identity, three out of our four group axioms are satisfied.

The one that remains to consider is $a * a$. For the closure property to hold, the result can only be e or a. The result cannot be a since then axiom 4 would not be valid, i.e. a would not have an inverse in the set S. Hence, in order for $\{S, *\}$ to satisfy all the group properties, we can fill out the table only in the following way.

*	**e**	**a**
e	*e*	*a*
a	*a*	*e*

Note that we can exchange the rows and columns, and obtain

*	**a**	**e**
a	*e*	*a*
e	*a*	*e*

which is actually the same as the first table. By convention, however, we put the identity element first.

Checking for the associative property can be a tedious process for larger sets, but we will find ways to get around this later on. For this set of order 2, 2^3 or 8 distinct cases would have to be checked, and is left for the student as an exercise.

Let us do the same with a set of three elements, $S = \{e, a, b\}$, under the binary operation $*$. Since e is the identity, the 1st row and column mirrors the initial order of the elements.

*	**e**	**a**	**b**
e	*e*	*a*	*b*
a	*a*		
b	*b*		

For the 2nd row, 2nd column entry, we can choose either e or b. If we choose e, we would have to enter b in the 2nd row, 3rd column.

*	**e**	**a**	**b**
e	*e*	*a*	*b*
a	*a*	*e*	*b*
b	*b*		

This would mean, however, that we have two left identities for b, namely e and a, since $e * b = b$ and $a * b = b$. Hence, we have no choice but to put b in the 2nd row, 2nd column, and complete the table as below. You should now justify the completion of the table using the group axioms.

*	**e**	**a**	**b**
e	*e*	*a*	*b*
a	*a*	*b*	*e*
b	*b*	*e*	*a*

To confirm the associative property, you would have to show that it holds in 3^3, or 27, distinct cases. To spare you the task of going through this tedious process, we can confirm for you here that indeed the associative property holds.

With the previous examples of finite sets of orders 2 and 3 as background, we will be able to list some necessary conditions that an operation table must satisfy in order to give a group structure on a set.

- In the row and column containing the identity element e, the rows and columns are mirrored in the same order as they originally appear, i.e. the condition $e * x = x = x * e$ means that the row and column representing the operations with e must contain exactly the elements appearing in the same order as across the top of the table and down the left side of the table.
- Since every element has a unique inverse, the identity element e can appear only once in each row and column.
- The equations $a * x = b$ and $y * a = b$ must have unique solutions x and y. (This property will be proved later.) This means that each element of the group must appear in each row and column **only once**.

An operation table that has the above properties is called a Latin Square.

Definition

A **Latin Square** is a square array of n rows and n columns such that each element or symbol occurs only once in each row and each column.

Latin squares first arose in the 18th century with card games, such as the problem of arranging the kings, queens, jacks and aces into a 4 by 4 array such that each row and column contains one card from each of the 4 suits, and one card from each of the 4 ranks previously mentioned. In 1779, Euler posed the problem that he claimed was impossible to solve: of arranging 36 officers from 6 ranks and 6 regiments into a 6 by 6 square so that each row and each column contains one officer from each rank and one from each regiment. Recently, the development of Latin squares has gained a major impetus in designing statistical experiments and also in finite geometries.

A♥	?	Q♠	K♦
J♠	?	?	Q♥
?	?	K♥	J♣
?	Q♣	J♦	?

We have shown above that if the elements of a set under a given binary operation form a group, we can place the elements in a Latin square. Conversely, if elements of a set under a given binary operation are placed in a Latin square, the set under the binary operation will form a group provided that the group properties hold. It is therefore not enough to assume that the set under the binary operation is a group because it can be placed in a Latin square.

Although the IB HL syllabus uses *Cayley table* and *operation table* interchangeably, historically a Latin square that forms a group structure is called a Cayley table, after the 19th century mathematician Arthur Cayley. He was instrumental in founding the British school of pure mathematics and was also responsible for obtaining admission for women into Cambridge University. He was one of the first to realize that many seemingly different areas of mathematics can be brought together under Group Theory. His *n*-dimensional geometry has been applied to both relativity theory and quantum mechanics.

Example 4

Construct a Cayley table for the set $S = \{1, -1, i, -i\}$ under multiplication, and show that $\{S, \times\}$ is a group.

×	**1**	**−1**	***i***	***−i***
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
−i	$-i$	i	1	−1

Construct an operation table, writing the identity element as the first element.

$\{S, \times\}$ forms a group if the following properties hold:

Confirm the group properties.

Closure: for all $a, b \in S$, $a \times b \in S$. From the operation table it is evident that the set is closed under ×.

Associativity: for all $a, b, c \in S$, $a \times (b \times c) = (a \times b) \times c$ Multiplication of complex numbers is associative.

You may assume multiplication of complex numbers is associative.

Identity: for all $a \in S$, $1 \times a = a = a \times 1$, $1 \in S$.

State the identity.

Inverse: for all $a \in S$ there exists $a^{-1} \in S$ such that $a \times a^{-1} = 1 = a^{-1} \times a$.

a	1	−1	i	$-i$
a^{-1}	1	−1	$-i$	i

It is not enough to simply state that inverses exist. You must also identify the inverse of each element.

From the table we see that 1 and −1 are self-inverses and i and $-i$ are mutual inverses. Hence $\{S, \times\}$ is a group.

State your conclusion.

Is the above group Abelian? We know that the set of complex numbers under multiplication is commutative, therefore the commutative property will hold for S, since $S \subseteq \mathbb{C}$. A visual method for determining if it is Abelian is to consider the symmetry about the main diagonal of its Cayley table, i.e. the diagonal from the upper left hand corner to the lower right hand corner.

Since there is symmetry about the main diagonal of the Cayley table, the group is Abelian.

×	**1**	**−1**	***i***	***−i***
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
−i	$-i$	i	1	−1

Groups of integers modulo *n*

You have worked with integers modulo n, written (mod n), in Chapter 1. Two integers, a and b, are said to be congruent (mod n) if a and b have the same remainder on division by n. In other words, $a \equiv b(\bmod n) \Leftrightarrow a - b = kn, k \in \mathbb{Z}$.

Notation for Modular arithmetic:

- $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, n \in \mathbb{N}, n \geq 2$
- $+_n$ denotes addition (mod n), and $a +_n b$ is the remainder when $a + b$ is divided by n, i.e. $a +_n b = a + b(\bmod n)$
- $\times_n$ denotes multiplication (mod n), and $a \times_n b$ is the remainder when $a \times b$ is divided by n, i.e. $a \times_n b = ab(\bmod n)$

? Modular arithmetic is used in modern day banking. Banks require an IBAN (International Bank Account Number) identification for transferring funds between bank accounts. IBAN makes use of modulo 97 to trap user input errors in bank account numbers.

Example 5

a Construct a Cayley table for $\{\mathbb{Z}_4, +_4\}$ and confirm that it forms a group.
b Construct an operation table for $\mathbb{Z}_4 \setminus \{0\}$ under $\times_4$ and show that it does not form a group.
c Determine whether or not $\{\mathbb{Z}_4, \times_4\}$ is a group.

a Closure: for all $a, b \in \mathbb{Z}_4$, $a +_4 b \in \mathbb{Z}_4$
Closure is evident from the table.

Construct the Cayley table.

$+_4$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Confirm the group properties.

Associativity: for all $a, b, c \in \mathbb{Z}_4$,
$a +_4 (b +_4 c) = (a +_4 b) +_4 c$

Addition (mod n) is associative.

You may assume addition (mod n) is associative.

Identity: for all $a \in \mathbb{Z}_4$,
$0 +_4 a = a = a +_4 0, 0 \in \mathbb{Z}_4$

State the identity.

Inverse: for all $a \in \mathbb{Z}_4$ there exists $a^{-1} \in \mathbb{Z}_4$ such that $a +_4 a^{-1} = 0 = a^{-1} +_4 a$

Identify the inverses of the elements.

a	0	1	2	3
a^{-1}	0	3	2	1

Hence, $\{\mathbb{Z}_4, +_4\}$ forms a group.

State your conclusion.

b The operation table for $\mathbb{Z}_4 \setminus \{0\}$ under the binary operation $\times_4$ is:

Construct the operation table.

$\times_4$	**1**	**2**	**3**
1	1	2	3
2	2	0	2
3	3	2	1

We see from the table that closure does not hold, since 0 appears in the table, and $0 \notin \mathbb{Z}_4 \setminus \{0\}$.

Hence, $\{\mathbb{Z}_4 \setminus \{0\}, +_4\}$ does not form a group.

Identify a group axiom that does not hold. (It is sufficient to find just one axiom that does not hold.)
State your conclusion.

c The operation table for $\{\mathbb{Z}_4, \times_4\}$ is:

Construct the operation table.

$\times_4$	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Method 1

The operation table is not a Latin Square, i.e. the elements 0 and 2 appear more than once in certain rows and columns.

Check if the operation table is a Latin Square.

Method 2

The identity element for all elements is 1, but 0 and 2 have no inverses.

Find one example of a group property that does not hold.

Hence $\{\mathbb{Z}_4, \times_4\}$ does not form a group.

Example 6

The Cayley table for a set of 5 elements under the operation $*$ is given here.

$*$	$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{s}$	$\boldsymbol{t}$
$\boldsymbol{p}$	s	r	t	p	q
$\boldsymbol{q}$	t	s	p	q	r
$\boldsymbol{r}$	q	t	s	r	p
$\boldsymbol{s}$	p	q	r	s	t
$\boldsymbol{t}$	r	p	q	t	s

a State with reason why the Cayley table is a Latin Square.

b Determine whether or not each of the group properties hold.

c Solve the equation $(p*x)*x=x*p$.

a The Cayley table is a Latin Square because each element appears only once in each row and column.

Use the definition of Latin Square.

b Closure is evident from the table. The right and left identity for each element is s. Each element is a self-inverse. The property of associativity does not hold, since $(p*q)*t=r*t=p$ and $p*(q*t)=p*r=t$ and $t\neq p$.

Go through all the group properties to determine if they hold.

c Solutions are: q, r, s and t.

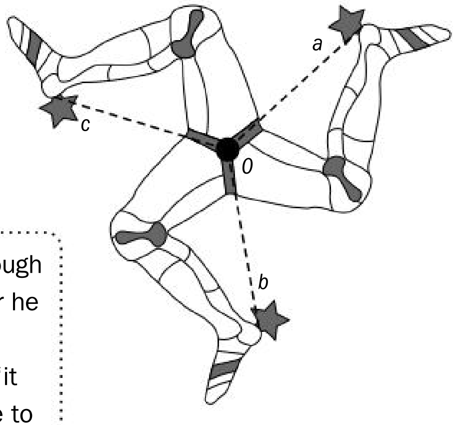
In this example it is best to substitute the elements for x as the operation is not associative.

The example above shows a Latin Square that is not a group table.

Symmetry groups

We will now consider groups of plane figures under the composition of certain plane transformations that preserve symmetrical properties.

Consider the symmetry in the Isle of Man motif here.



The coat of arms of the Isle of Man is the three-legged motif. Although Alexander III introduced it to Scotland in the mid 13th century after he gained control of the Manx territory, its origins go back to ancient times. The motif carries the latin words "Quocunque Jeceris Stabit", meaning "it will stand which ever way you throw it". This is thought to be a reference to the independent and resilient spirit of the Manx people.

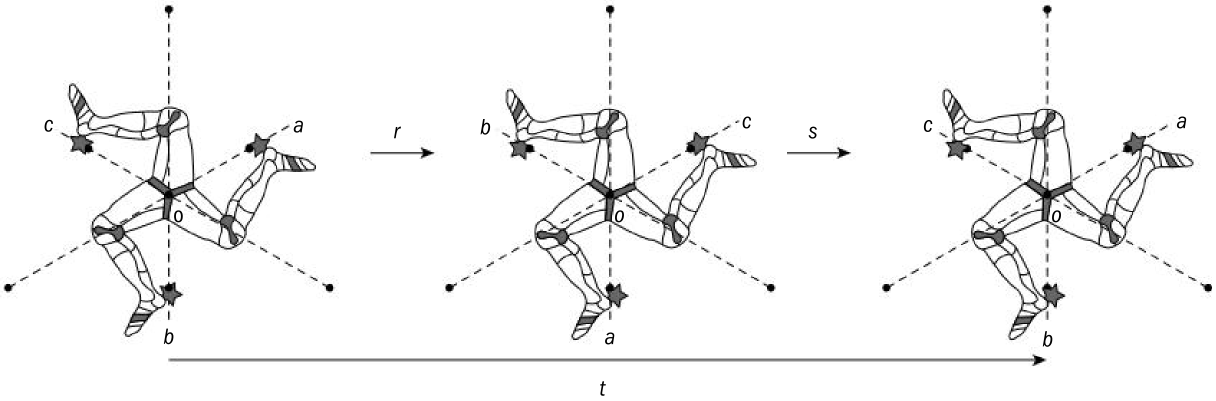
This figure has three rotation symmetries about the center O of $120°$, $240°$ and $360°$ (or $0°$). We can label these transformations as follows:

r is a clockwise rotation of $120°$ about O

s is a clockwise rotation of $240°$ about O

t is a clockwise rotation of $360°$ about O

Since symmetries are transformations, they can be combined, i.e. given two transformations, we can perform one followed by the other. For example, on the original figure we can perform the transformation *r* (rotation of 120 degrees through *O* clockwise) and follow this with the transformation *s* (rotate through 240° through *O* clockwise). The result is illustrated as follows:



Looking at the combined transformations, the result is to leave the original figure unchanged. This same result can be obtained by rotating the original diagram 360°, or transformation *t*. Hence, "transformation *r* followed by transformation *s*" is the same as "transformation *t*", and is written in symbols as $s \circ r = t$. This is read as "transformation *s* following transformation *r*". In other words, similar to function composition, $s \circ r = t$ is called the composition of *r* with *s*, i.e. we *first* apply *r*, and then apply *s*. Likewise, as with function compositions, $s \circ r = t$ is performed from ***right to left***.

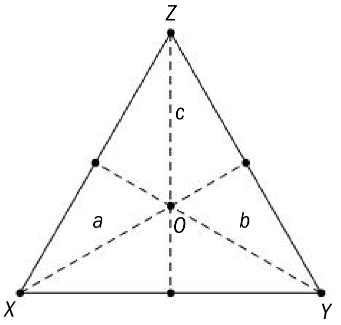
We will now determine if our set of rotations forms a group under composition of symmetry transformations by creating its Cayley table. We will place *t* first, since it is the identity transformation. It is easy for you to confirm the results on the right.

○	***t***	***r***	***s***
t	*t*	*r*	*s*
r	*r*	*s*	*t*
s	*s*	*t*	*r*

Notice that this table is a Latin Square, hence closure holds. The identity is *t*, which is its own inverse, and *r* and *s* are mutual inverses. Just as with function composition, symmetry transformation is associative.

Let us now consider the symmetries of the equilateral triangle *XYZ*.

There are three reflective symmetries about the medians of the triangle. (A median connects a vertex of a triangle to the midpoint of the side opposite the vertex.) We can label the transformations as follows:



A: reflection in median *a*

B: reflection in median *b*

C: reflection in median *c*

There are three rotation symmetries about O. We can label these:

I: rotation about the center 360° (or 0°) clockwise (or anti-clockwise).

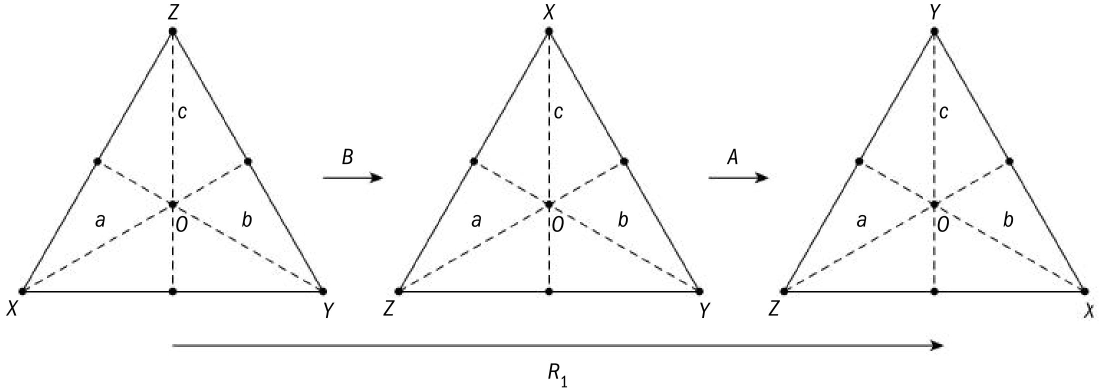
R_1: rotation about the center 120° anti-clockwise (which is the same as "rotation about the center 240° clockwise").

R_2: rotation about the center 120° clockwise (which is the same as rotation about the center 240° anti-clockwise).

It might be helpful to make a cardboard copy of the triangle in order to see the results of the various transformations.

In the three diagrams below, we see transformation B followed by transformation A, and this is the same as the single transformation R_1.

Note that the median lines are fixed in space and do not rotate with the triangles.



Hence, $AB = R_1$, or B followed by A results in R_1.

We will now construct the Cayley table for the symmetries of the equilateral triangle, and it is left to you to confirm the results in the table.

○	$\boldsymbol{I}$	$\boldsymbol{R_1}$	$\boldsymbol{R_2}$	$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{C}$
$\boldsymbol{I}$	I	R_1	R_2	A	B	C
$\boldsymbol{R_1}$	R_1	R_2	I	C	A	B
$\boldsymbol{R_2}$	R_2	I	R_1	B	C	A
$\boldsymbol{A}$	A	B	C	I	R_1	R_2
$\boldsymbol{B}$	B	C	A	R_2	I	R_1
$\boldsymbol{C}$	C	A	B	R_1	R_2	I

The Cayley table confirms that the set $\{I, R_1, R_2, A, B, C\}$ forms a group under composition of transformations. The property of closure is evident. I is the identity. I, A, B and C are all self-inverses and R_1 and R_2 are mutual inverses. Composition of transformations is associative.

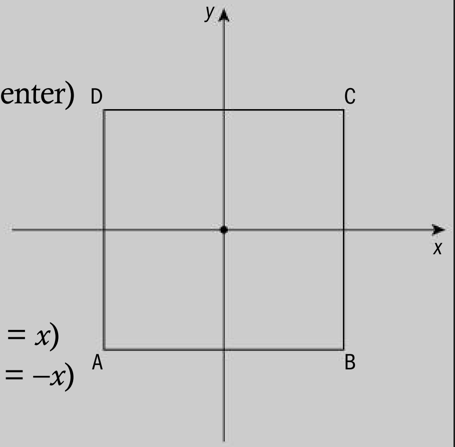
Since the table is not symmetrical about the main diagonal, this group is not Abelian.

The set of six symmetries of the equilateral triangle with the binary operation of composition of transformations is called the *symmetry group of equilateral triangles*. All the symmetries of geometrical figures are elements of a larger set of transformations called **isometries**, i.e. a transformation of the points in 2D or 3D space such that distances between points remain unchanged. Hence, under an isometry, a geometrical figure retains its shape and size, but changes its position in space. There are four types of plane isometry: rotation, reflection, translation, and glide-reflection, i.e. reflection together with a translation in the direction of the line of reflection. It can be shown that the set of all plane isometries forms a group under the different transformations.

Example 7

a Construct a Cayley table for the group of symmetries of a square $\{S, \circ\}$ using the following notation:

I: identity (rotation of 360° in either direction about the center)
R_1: rotation of 90° anti-clockwise about the center
R_2: rotation of 180° anti-clockwise about the center
R_3: rotation of 270° anti-clockwise about the center
X: reflection in the x-axis
Y: reflection in the y-axis
A: reflection in the diagonal AC (reflection in the line $y = x$)
B: reflection in the diagonal BD (reflection in the line $y = -x$)



b State whether or not the group is Abelian.

a

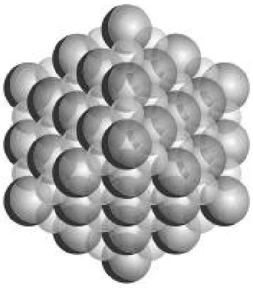
$\circ$	I	R_1	R_2	R_3	X	Y	A	B
I	I	R_1	R_2	R_3	X	Y	A	B
R_1	R_1	R_2	R_3	I	A	B	Y	X
R_2	R_2	R_3	I	R_1	Y	X	B	A
R_3	R_3	I	R_1	R_2	B	A	X	Y
X	X	B	Y	A	I	R_2	R_3	R_1
Y	Y	A	X	B	R_2	I	R_1	R_3
A	A	X	B	Y	R_1	R_3	I	R_2
B	B	Y	A	X	R_3	R_1	R_2	I

Enter the results of the binary operation under the different transformations into the table.

b Since the table is not symmetric about the main diagonal, the group is not Abelian.

Since we are told that this is a group, we need only consider the commutative property to determine if it is Abelian.

? Symmetry groups are used throughout the study of chemistry. The symmetry of a molecule provides information on the energy levels of its orbital and transitions that can occur between energy levels. These can all be found without rigorous calculations, which makes group theory so very powerful in the study of the physical aspects of molecules.



Exercise 3B

1 **a** Copy and complete the given table so that the set $\{e, x, y, z\}$ forms a group under $*$.

$*$	e	x	y	z
e	e	x	y	z
x	x			e
y	y		e	
z	z	e		

b Use the table to simplify the following:

i $y * (z * x)$ **ii** $(x * y) * (y * z)$

2 $S = \{a, b, c, d, e\}$ under the binary operation $*$ is defined in the table below.

$*$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	e	a	d
c	c	a	d	e	b
d	d	e	a	b	c
e	e	d	b	c	a

a Simplify:

i $a*(b*c)$ **ii** $(a*b)*c$ **iii** $b*(d*c)$ **iv** $(b*d)*c$.

b Determine if $\{S, *\}$ has an identity element, and name it if it does.

c Determine whether each element has an inverse, and name its inverse.

d Give two reasons why $\{S, *\}$ does not form a group.

3 Show that the set $S=\{f, g, h\}$ such that $f(x) = x$, $g(x) = 1 - \frac{1}{x}$, and $h(x) = \frac{1}{1-x}$ forms a group under function composition. Determine if the group is Abelian.

4 Construct Cayley tables for $\{\mathbb{Z}_5, +_5\}$ and $\{\mathbb{Z}_5 \backslash \{0\}, \times_5\}$, and confirm that both form a group. Use the tables to solve the following equations in $\mathbb{Z}_5$:

a $x + 4 = 3$ **b** $2x = 3$ **c** $4x + 1 = 3$

d $3(x + 1) = 1$ **e** $4x + 1 = 2x$

5 Construct an operation table for $S = \{2, 4, 6, 8\}$ under $\times_{10}$ and determine if it forms an Abelian group.

6 A set of six complex numbers forms a group under multiplication. If one of the complex numbers is $\frac{1}{2}(1 + i\sqrt{3})$, find the other five numbers.

7 Construct Cayley tables for the symmetries of the following figures, and show that each one forms a group. (You must first decide on all the symmetries that the figure contains.)

a An isosceles triangle
b A rectangle
c A cuboid

8 Express the cube roots of unity in the form $a + bi$, and show that they form a group under multiplication.

9 Write out the operation table for $\mathbb{Z}_2 \times \mathbb{Z}_2$ and determine if it forms a group under $+_2$.
($\mathbb{Z}_2 = \{0, 1\}$, hence $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$).

10 Show that if $n = pq$, where p, q are both integers greater than 1, then $(\mathbb{Z}_n, \times_n)$ does not form a group.

3.2 Properties and theorems of groups and subgroups

In the first part of this chapter, you have been working with both finite and infinite groups, and using some group properties intuitively.
We will now write these group properties, or theorems, and their proofs.
First we will prove the right and left cancellation laws for groups.

Right and left cancellation laws for groups

Given a group $\{G, *\}$ and $a, b, c \in G$

i the right cancellation law holds, i.e. $a * c = b * c \Rightarrow a = b$ and
ii the left cancellation law holds, i.e. $c * a = c * b \Rightarrow a = b$.

Proof:

i $a * c = b * c \Rightarrow (a * c) * c^{-1} = (b * c) * c^{-1}$ since $c^{-1} \in G$.
$\Rightarrow a * (c * c^{-1}) = b * (c * c^{-1})$ by the associative property.
$\Rightarrow a * e = b * e$ by the property of inverse, and
$a * e = b * e \Rightarrow a = b$ by the identity property. Q.E.D.

The proof of **ii** is left for you to complete.

Theorem 1

A group $\{G, *\}$ has the following properties.

a The identity element for a group is unique.

b For all $a \in G$, the inverse of a, a^{-1}, is unique.

c For any $a, b \in G$, the equations $a * x = b$ and $y * a = b, x, y \in G$, have unique solutions in G. (For finite groups, this means that each element would appear only once in every row and column of its operation table.)

Proofs:

A common strategy to prove uniqueness is to assume that uniqueness does not hold, i.e. there are two distinct elements, and then show that these two elements are indeed equal.

a Suppose there are two identity elements e_1 and e_2. Then, for any $a \in G$, $a * e_1 = a = e_1 * a$ and $a * e_2 = a = e_2 * a$. Therefore, taking each corresponding part of both expressions separately, $a * e_1 = a * e_2 \Rightarrow e_1 = e_2$ by the left cancellation law, and, $e_1 * a = e_2 * a \Rightarrow e_1 = e_2$ by the right cancellation law. Hence, uniqueness of the identity holds.

b Suppose that $a \in G$ has two inverses, a_1^{-1} and a_2^{-1}. It follows then that $a * a_1^{-1} = e = a_1^{-1} * a$ and $a * a_2^{-1} = e = a_2^{-1} * a$. Taking each corresponding part of both expressions separately, $a * a_1^{-1} = a * a_2^{-1} \Rightarrow a_1^{-1} = a_2^{-1}$ by the left cancellation law, and $a_1^{-1} * a = a_2^{-1} * a \Rightarrow a_1^{-1} = a_2^{-1}$ by the right cancellation law. Hence, uniqueness of the inverse of an element holds.

c We first need to show the existence of at least one solution for the equations $a * x = b$ and $y * a = b$.

Solving for x: $a * x = b \Rightarrow a^{-1} * (a * x) = a^{-1} * b$, since $a^{-1} \in G$.

$\Rightarrow (a^{-1} * a) * x = a^{-1} * b$ by the associative property.

$\Rightarrow e * x = a^{-1} * b$ by the property of inverse, and

$\Rightarrow x = a^{-1} * b$ by the property of identity. Hence, we obtain $x = a^{-1} * b$.

Finding the solution for y is left for you to do.

Now, substituting the solution we found for x,

$a * (a^{-1} * b) = (a * a^{-1}) * b$	by the associative property,
$= e * b$	by the inverse property,
$= b$	by the identity property.

Checking the solution of the 2nd equation is left for you to do.

To show uniqueness of these solutions, we again assume that there exist two solutions, i.e. $a * x_1 = b$ and $a * x_2 = b$. Therefore $a * x_1 = a * x_2$ by substitution, and by the left cancellation law, we conclude that $x_1 = x_2$. Similarly, the uniqueness of y is similarly proved.

Some properties of groups

a For any $a, b \in G,$

i $a * b = e \Rightarrow a = b^{-1}$

ii $a * b = e \Rightarrow b = a^{-1}$

iii $a * b = e \Rightarrow b * a = e$

b For any $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$

c For any $a \in G$, $(a^{-1})^{-1} = a$

a **i** $a * b = e \Rightarrow (a * b) * b^{-1} = e * b^{-1}$ since $b^{-1} \in G$

$\Rightarrow a * (b * b^{-1}) = b^{-1}$ by the associative and identity properties

$\Rightarrow a * e = b^{-1}$ by the inverse property

$\Rightarrow a = b^{-1}$ by the identity property

ii and **iii** are left as exercises for you to complete.

b The inverse of $a * b$ is $(a * b)^{-1}$. If $b^{-1} * a^{-1}$ is the inverse of $a * b$, then it follows that $(a * b) * (b^{-1} * a^{-1})$ must equal the identity e, and this is what we need to confirm. $(b^{-1} * a^{-1}) * (a * b)$ must also equal e. (This latter part is left for you to do.).

$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$ by the associative property

$= a * e * a^{-1}$ by the inverse property

$= a * a^{-1}$ by the identity property

$= e$ by the inverse property

The latter part is left for you do to.

Hence, $b^{-1} * a^{-1}$ is the inverse of $a * b$ by Theorem 1 which we have proven above, i.e. the uniqueness of the inverse.

c The inverse of a^{-1} is $(a^{-1})^{-1}$. If a is the inverse of a^{-1} then it follows that $a^{-1} * a = e = a * a^{-1}$ which is true by the inverse property of group G. Hence by the uniqueness of inverse property, the result follows.

Alternatively, since $a^{-1} * a = e$, using property **a** with $a^{-1} = b$, $(a^{-1})^{-1} = b^{-1} = a$.

Example 8

Given the group $\{G, *\}$ prove that if $a * a = e$ for all $a \in G$, then $\{G, *\}$ is Abelian.

To show that $\{G, *\}$ is Abelian, we need to show that $a * b = b * a$ for all $a, b \in G$. For all $a, b \in G$, $(a * b) * (a * b) = e$, by the given. $a * (b * a) * b = e$ by the associative property. $a * a * (b * a) * b = a * e$ $e * (b * a) * b = a$ by the given and identity property. $(b * a) * b * b = a * b$ by the identity property. $(b * a) * e = a * b$ by the given. $b * a = a * b$ by the identity property.	*Use group properties and axioms to arrive at your results.*

Exercise 3C

1 $\{G, *\}$ contains exactly four elements: e, a, b, and c. State with reasons why $a * b$ cannot equal e, a or b, and hence must equal c.

2 Prove that if $\{G, *\}$ is a group and $a \in G$, then $(a^2)^{-1} = (a^{-1})^2$.

3 $\{G, \#\}$ is a group such that $x \# x \# x \# x = e$, or $x^4 = e$, $y^2 = e$, and $x \# y = y \# x^3$.

a Show that

i $y \# x = x^3 \# y$

ii $y \# (x^2 \# y) = x^2$

b Simplify $(x \# y) \# (x^2 \# y)$.

4 $\{G, \circ\}$ is an Abelian group and $a^n = a \circ a \circ a \circ \ldots \circ a$ for n factors of a, where $a \in G$ and $n \in \mathbb{Z}^+$. Prove by mathematical induction that $(a \circ b)^n = a^n \circ b^n$ for all $a \in G$.

5 Show that in any group $\{G, *\}$, if $(a * b)^2 = a^2 * b^2$ then $a * b = b * a$.

6 A set S is defined as the set of all elements of a group $\{G, \circ\}$ that commute with every element of G, i.e. $a \in S \Leftrightarrow a \circ x = x \circ a$ for every element $x \in G$. Prove that $\{S, \circ\}$ is also a group.

Subgroups

In question 6 of Exercise 3C you proved that a subset S of a set G under the same binary operation as G was also a group. When a subset of a group forms a group in its own right under the same binary operation, then we say that the subset is a subgroup of the given group.

Definition

If a non-empty subset H of a set G is also a group under $*$, then $\{H, *\}$ is a **subgroup** of $\{G, *\}$.

An example of an infinite subgroup of $\{\mathbb{R}, +\}$ is $\{\mathbb{Q}, +\}$. However, although $\mathbb{Q}^+ \subset \mathbb{R}$, $\{\mathbb{Q}^+, +\}$ is not a subgroup of $\{\mathbb{R}, +\}$. For finite sets, consider Example 7, the table for the symmetries of a square, S. If we consider a subset T of the table with the elements $T = \{I, R_1, R_2, R_3\}$ we can determine if this subset T of S under the defined transformations is a subgroup of $\{S, \circ\}$.

$\circ$	$\boldsymbol{I}$	$\boldsymbol{R_1}$	$\boldsymbol{R_2}$	$\boldsymbol{R_3}$
$\boldsymbol{I}$	I	R_1	R_2	R_3
$\boldsymbol{R_1}$	R_1	R_2	R_3	I
$\boldsymbol{R_2}$	R_2	R_3	I	R_1
$\boldsymbol{R_3}$	R_3	I	R_1	R_2

We can see from the table that $\{T, \circ\}$ is closed. In addition, T contains I, the identity element of S. Each element in T has an inverse in T. We know that $\{S, \circ\}$ is associative, hence the operation will be associative with the elements of the subset T. So we can conclude that $\{T, \circ\}$forms a subgroup of $\{S, \circ\}$ under $\circ$.

Notice also that the order of the subgroup is a factor of the order of the group. When looking for possible subgroups of a given group, this fact can minimize the amount of work in our search. In the next chapter we will prove this famous and important result, i.e. the order of a subgroup divides the order of the group.

Therefore, in order for a set to form a subgroup of a given group under a given binary operation, it must also fulfill the group axioms. Any subset of the group under the given binary operation is associative, so this property does not need to be shown.

Theorem 2: Subgroup Theorem

A subset H of a group $\{G, *\}$ is a subgroup $\{H, *\}$ if and only if:

1 H is closed under the binary operation $*$, i.e.
$a, b \in H \Rightarrow a * b \in H$

2 The identity e of $\{G, *\}$ is in H.

3 For all $a \in H$, $a^{-1} \in H$.

Proof:

$\Rightarrow$: Since $\{H, *\}$ is a subgroup of $\{G, *\}$, then all the group properties must hold.

$\Leftarrow$: If $H \subseteq G$ such that **1**, **2** and **3** hold, then we need only show the property of associativity. Since all elements in H are also in G, and for all elements in G, $*$ is associative then $\{H, *\}$ is also associative.

A corollary of the above theorem is that every group $\{G, *\}$ has at least two subgroups: the group itself and the group consisting only of the identity.

Definitions

In many textbooks, the subgroup $\{\{e\},*\}$ is a proper subgroup. For the IB syllabus however, we consider it an improper subgroup.

If $\{G, *\}$ is a group, then the subgroup consisting of G itself and the subgroup consisting of only the identity are the **improper subgroups** of G. All other subgroups are **proper subgroups**. The subgroup $\{\{e\}, *\}$ is also referred to as the **trivial subgroup** of G.

Example 9

Show that the set $S = \{1, 5, 7, 11\}$ forms an Abelian group under $\times_{12}$, and list all of its non-trivial subgroups.

$\times_{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Construct a Cayley table.

To show that $\{S, \times_{12}\}$ forms a group, the following properties must hold:
Closure: It is evident from the table that for all $a, b \in S$, $a \times_{12} b \in S$.
Identity: It is evident from the table that 1 is the identity, since for all $a \in S$, $a \times_{12} 1 = a = 1 \times_{12} a$.
Inverse: For all $a \in S$ there exists $a^{-1} \in S$ such that $a \times_{12} a^{-1} = 1 = a^{-1} \times_{12} a$.

Confirm all the group properties.

a	1	5	7	11
a^{-1}	1	5	7	11

Each element is its own inverse.
Associativity: Multiplication mod(n) is associative.
The above confirms that $\{S, \times_{12}\}$ is a group.

It is also an Abelian group, since for all $a, b \in S$, $a \times_{12} b = b \times_{12} a$. This is true since the Cayley table is symmetric about its main diagonal.

Determine if there is symmetry about the main diagonal of the Cayley table.

In addition to the set itself, the sets of the non-trivial subgroups under the given operation are: $\{1, 5\}$, $\{1, 7\}$, $\{1, 11\}$.

Since the order of a subgroup must divide the order of a group, we are looking only for subgroups of order 1, 2 and 4.

Example 10

Let $\{H, *\}$ and $\{K, *\}$ be subgroups of $\{G, *\}$.
Prove that $\{H \cap K, *\}$ is a subgroup of $\{G, *\}$.

$H \cap K$ is **i** non-empty and **ii** a subset of G. **i** Since H and K are subgroups, then $e_G \in H$ and $e_G \in K$, hence $e_G \in H \cap K$. $H \cap K$ is non-empty. **ii** Let $x \in H \cap K$. Then $x \in H$ and $x \in K$. Since both H and K are subsets of G, $x \in G$, thus $H \cap K \subseteq G$.	*First show that the conditions of the definition of subgroup are satisfied, that $H \cap K$ is a non-empty subset of G.*
For $\{H \cap K, *\}$ to be a subgroup of $\{G, *\}$ it must satisfy the group properties: Closure, i.e. for all $a, b \in H \cap K$, $a * b \in H \cap K$. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since both $\{H, *\}$ and $\{K, *\}$ are groups, $a * b \in H$ and $a * b \in K$, thus $a * b \in H \cap K$. Identity: We have already proved in **i** that since H and K are subgroups, $e_G \in H$ and $e_G \in K$, hence $e_G \in H \cap K$. Inverse: For $a \in H \cap K$, $a \in H$ and $a \in K$. Hence $a^{-1} \in H$ and $a^{-1} \in K$, since both $\{H, *\}$ and $\{K, *\}$ are subgroups. Hence, $a^{-1} \in H \cap K$. By the Subgroup Theorem, therefore, $\{H \cap K, *\}$ is a subgroup of $\{G, *\}$.	*Show that $\{H \cap K, *\}$ satisfies the properties of the Subgroup Theorem.*

We will now prove a theorem with subgroups that might be helpful in showing that finite or infinite subsets of a group form a subgroup under the given binary operation.

Theorem 3

Let $\{G, *\}$ be a finite or infinite group and H a non-empty subset of G. Then H is a **subgroup** of G if $a * b^{-1} \in H$ for $a, b \in H$.

Proof:

We are given that $a, b \in H \Rightarrow a * b^{-1} \in H$.

Identity: Letting $b = a \Rightarrow a * a^{-1} \in H$, hence $e \in H$.

Inverse: Letting $a = e$ and $b = a$, then $e, a \in H \Rightarrow e * a^{-1} \in H$ from the given. Since $e * a^{-1} = a^{-1}$, $a^{-1} \in H$. In the same way, $b^{-1} \in H$. Hence, for $a, b \in H$, $a^{-1}, b^{-1} \in H$.

Closure: From the above, we know that if a and b are in H then a and b^{-1} are in H too. Using the given, therefore, $a * (b^{-1})^{-1} \in H$, hence $a * b \in H$.

The following is an example where you might use this theorem instead of the Subgroup Theorem.

Example 11

Prove: Given $\{H, +\}$ where $H = \left\{4x + 7y \middle| x, y \in \mathbb{Z}\right\}$, $\{H, +\}$ is a subgroup of $\{\mathbb{Z}, +\}$.

$x, y \in \mathbb{Z} \Rightarrow 4x + 7y \in \mathbb{Z}$, hence H is a non-empty subset of $\mathbb{Z}$.	*First show that the condition of the definition of subgroup is satisfied, i.e. H is a non-empty subset of* $\mathbb{Z}$.
Let $a, b \in H$, $a = 4x_1 + 7y_1$, $b = 4x_2 + 7y_2$.	
Since $e = 0\,x + 0\,y = 0$, for $x \in \mathbb{Z}$ we have $x^{-1} = -x$.	*To define the inverse of an element in a group, you must first find the identity.*
Hence $a + b^{-1} = (4x_1 + 7y_1) - (4x_2 + 7y_2)$ $= 4(x_1 - x_2) + 7(y_1 - y_2) \in H$.	*Use Theorem 3 and show that* $a + b^{-1} \in \mathbb{Z}$.
Hence H is a subgroup of $\{\mathbb{Z}, +\}$.	*Write your conclusion.*

Before we examine sufficient conditions for proving that a set H is a subgroup of G under the same binary operation, we need to define what is meant by the order of an element of a group.

If $a \in G$ under the binary operation $*$, then we can use the binary operation on a itself, i.e. $a * a$. We can do this as many times as we need, e.g. $\overbrace{a * a * \ldots * a}^{n \text{ times}} = a^n$. We can now formulate the following definition and theorem.

Definition

Let $a \in G$ where $\{G, *\}$ is a group. Then a is said to have **finite order** if $a^n = e$ for some $n \in \mathbb{Z}^+$. The **order** of a is the least such n. If no such n exists, the element a has **infinite order**.

Theorem 4

Let a be an element of a finite group $\{G, *\}$. Then there exists a smallest positive integer n such that $a^n = e$, and n is the order of a.

Proof:

The set of all possible powers of a is an infinite set. Since G is finite, however, the set of possible powers of a cannot all be different.
Hence, if r and s are two positive integers with $r < s$ such that $a^r = a^s = e$, then, (for convenience sake we will omit $*$)

$a^r = a^s \Rightarrow a^s a^{-r} = a^r a^{-r} = e$. Hence, there is at least one $n = s - r$, such that $a^n = e$.
We have proven the existence of n, and you may want to prove its uniqueness as an exercise.

Theorem 5

If H is a non-empty subset of a **finite** group $\{G, *\}$ then $\{H, *\}$ is a subgroup if and only if, for all $a, b \in H$, $a * b \in H$. In other words, H need only be closed.

Proof:

Identity: $a * b \in H \Rightarrow a^2 \in H$ for $b = a$. Now, $b = a^2 \Rightarrow a^3 \in H$.
Continuing in this way, let the order of a be n, hence $a^n = e$, and $e \in H$.

Inverse: Consider a^{n-1}. Since $a^{n-1}a = a^n = e = aa^{n-1}$, then a^{n-1} is the inverse of a, and $a^{n-1} \in H, a^{-1} \in H$.

The condition of closure is given in the theorem, hence $\{H, *\}$ is a subgroup by the Subgroup Theorem.

This is a very useful theorem, since when you are asked to show that a subset of a **finite** group is a subgroup, you need only show the property of closure! This is particularly useful when you have a Cayley table to work from.

Exercise 3D

1 List the proper subgroups of the given groups.

a The set containing the sets Ø, $A = \{a\}$, $B = \{b\}$, and $C = \{a, b\}$ under the operation symmetric difference, Δ.

b The set of functions under function composition, where $p(x) = x$, $q(x) = 1 - \dfrac{1}{2x}$, $r(x) = \dfrac{1-x}{1-2x}$, and $s(x) = \dfrac{1}{2-2x}$.

c The symmetry group of the rectangle.

d The set $\{2, 4, 8, 10, 14, 16\}$ under $\times_{18}$

e $\{\mathbb{Z}_6, +_6\}$

2 The set $S = \{1, 2, 4, 7, 8, 11, 13, 14\}$ forms a group under the operation $\times_{15}$.

a Write down the inverses and orders of each element.

b Given that the set $\{1, 2, a, b\}$ is a subgroup of S, find a and b.

c Find one of the subgroups of S that also has four elements and includes 4 but not 2.

3 A group G under the binary operation $*$ has distinct elements $\{e, a, b, c, \ldots\}$, where e is the identity element.

a If $a * b = e$ and $b * b = a$, prove the set $\{e, a, b\}$ forms a subgroup of G under $*$.

b If $a * a = b$, $b * b = c$, $c * c = a$, then prove the set $\{e, a, b, c\}$ does not form a subgroup of G under $*$.

4 Let F be the group of all real-valued functions with domain $\mathbb{R}$ under addition of functions. Prove that the subset of F consisting of those functions in F that are differentiable forms a subgroup.

5 A group G that contains more than ten elements contains an element q of order 10. Prove that $\{q, q^2, q^3, \ldots, q^{10}\}$ is a subgroup of G.

6 Let $\{G, *\}$ be an Abelian group. Prove that if H is the set of all elements x in G satisfying the equation $x^2 = e$, then H is a subgroup.

7 Let $\{G, *\}$ be a group, and a is a fixed element in G. Prove that if H is the subset of G whose elements commute with a, i.e. $H = \left\{ x \in G \,\middle|\, xa = ax \right\}$, then H is a subgroup of $\{G, *\}$.

3.3 Cyclic groups

In Theorem 4 we saw that if a is an element of a finite group G then the powers of a cannot all be different. Consider the subgroup of the symmetries of a square group consisting of the rotations symmetries only, and its Cayley table.

I: identity (rotation of 0° or 360° in either direction about the center).

R_1: rotation through 90° anti-clockwise

R_2: rotation through 180° anti-clockwise

R_3: rotation through 270° anti-clockwise

$\circ$	$\boldsymbol{I}$	$\boldsymbol{R_1}$	$\boldsymbol{R_2}$	$\boldsymbol{R_3}$
$\boldsymbol{I}$	I	R_1	R_2	R_3
$\boldsymbol{R_1}$	R_1	R_2	R_3	I
$\boldsymbol{R_2}$	R_2	R_3	I	R_1
$\boldsymbol{R_3}$	R_3	I	R_1	R_2

We see that $R_1 \circ R_1 = R_1^2 = R_2$; $R_1 \circ R_1 \circ R_1 = R_1^3 = R_3$; $R_1 \circ R_1 \circ R_1 \circ R_1 = R_1^4 = I$.

As we proceed with higher powers, we obtain repetitions of the elements, e.g. $R_1 \circ R_1 \circ R_1 \circ R_1 \circ R_1 = R_1^5 = R_1^4 \circ R_1 = I \circ R_1 = R_1$.

We can therefore rewrite the table using powers of R_1:

$\circ$	$\boldsymbol{I}$	$\boldsymbol{R_1}$	$\boldsymbol{R_1^2}$	$\boldsymbol{R_1^3}$
$\boldsymbol{I}$	I	R_1	R_1^2	R_1^3
$\boldsymbol{R_1}$	R_1	R_1^2	R_1^3	I
$\boldsymbol{R_1^2}$	R_1^2	R_1^3	I	R_1
$\boldsymbol{R_1^3}$	R_1^3	I	R_1	R_1^2

This subgroup is an example of a finite cyclic group, because all of the elements of the group can be written as a power of a single element. We say that the subgroup is generated by the element R_1.

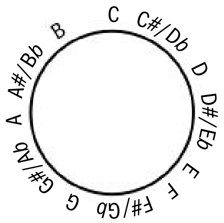
Definitions

A group whose elements can be expressed in the form $\{e, a, a^2, a^3, \ldots., a^{n-1}\}$ is called a **cyclic group** of order n and is denoted by C_n. The element a is said to generate the group and is described as the **generator** of the group. It follows therefore that a group of order n is cyclic if an only if it contains an element of order n.

A cyclic group can be a finite group, as seen above, or an infinite group.

Recently it was discovered that the sequence of pitches which forms a musical melody can be transposed (translation) or inverted (reflection) and can be modeled using a cyclic group of order 12. This allows for the creation of different melodies by assigning functions to the transpositions and inversions.

C	C#	D	E*b*	E	F	F#	G	A*b*	A	B*b*	B
0	1	2	3	4	5	6	7	8	9	10	11



Example 12

a Show that the group $\{\mathbb{Z}_5 \setminus \{0\}, \times_5\}$ forms a cyclic group, and find its generator(s).
b Find all the possible subgroups.

a

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Construct the Cayley Table. Since we are told that it is a group we do not need to test the group properties.

$2^2 = 4$, $2^3 = 3$, $2^4 = 1$ hence the group can be expressed as $\{1, 2, 2^2, 2^3\}$ and is therefore cyclic.

Determine if the powers of an element generate all elements of the group.

$3^2 = 4$; $3^3 = 2$, and the group can be expressed as $\{1, 3, 3^2, 3^3\}$.
2 and 3 are generators.

Determine if any other elements also generate the elements of the group.

b From the table it is evident that $\{1, 4\}$ forms a subgroup since it is closed, 1 is the identity, 4 is a self-inverse, and associativity is implied.

Since the order of a subgroup must divide the order of a group, we look only for subgroups of order 2.
Test the properties for subgroup.

Notice in Example 12 that 3 is the inverse of 2. Since 2 was a generator, its inverse will also be a generator. The following is left as a proof for the student, and is one of the exercises at the end of this section (See Exercise 3E question 2).

Theorem 6

In a finite group $\{G, *\}$, the order of an element a is the same as the order of its inverse a^{-1}. (The proof is left as an exercise for you to complete.)

We will now establish some properties of cyclic groups.

Theorem 7

Every cyclic group is Abelian.

Proof:

Let C_n be a cyclic group and let a be a generator of C_n so that $C_n = \left\{a^n \middle| n \in \mathbb{Z}\right\}$. Let x and y be two elements of C_n. Hence, there exists integers p and q such that $x = a^p$ and $y = a^q$. Then, $xy = a^p a^q = a^{p+q} = a^{q+p} = a^q a^p = yx$.
Hence, C is Abelian.

We now know that if we have a cyclic group it is also Abelian, but the converse is not necessarily true.

Before discussing subgroups of cyclic groups, it is convenient to prove the following theorem.

Theorem 8

Let $\{G, *\}$ be any group and let $a \in G$. Then $\{H, *\}$ where $H = \left\{a^n \middle| n \in \mathbb{Z}\right\}$ is the smallest subgroup of $\{G, *\}$ that contains $\{a\}$, i.e. every subgroup containing $\{a\}$ contains H.

Proof:

Checking the three conditions for subgroup, since $a^r a^s = a^{r+s}$, $r, s \in \mathbb{Z}$, H is closed. Since $a^0 = e$, $0 \in \mathbb{Z}$, $e \in H$, and since for $a^r \in H$, $a^{-r} \in H$, and $a^r a^{-r} = a^{-r} a^r = e$, every element in H has an inverse in H. Since any subgroup of $\{G, *\}$ that contains $\{a\}$ must contain H, H is therefore the smallest subgroup of G containing $\{a\}$.

Definition

The subgroup of $\{G, *\}$, $H = \left\{a^n \middle| n \in Z\right\}$, is the **cyclic subgroup** of $\{G, *\}$ generated by a.

Theorem 9

A subgroup of a cyclic group is cyclic.

Proof:

(This proof is placed here to enhance understanding; it is not required for examination purposes.)

Let C be a cyclic group generated by a and let H be a subgroup of C. If $H = \{e\}$, then it is cyclic. If $H \neq \{e\}$, then $a^n \in H$, $n \in \mathbb{Z}^+$. Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$.

For $c = a^m$ to generate H, we must show that every $b \in H$ is a power of c. Since $b \in H$ and $H \subseteq C$, $b = a^n$ for some n. We can express n as $mq + r$, for $0 \leq r < m$ (Division Algorithm Theorem). Then $a^n = a^{mq+r} = (a^m)^q a^r$, or $a^r = (a^m)^{-q} a^n$.

Since $a^n \in H$, $a^m \in H$ and H is a group, both $(a^m)^{-q}$ and a^n are in H. Hence, $(a^m)^{-q} a^n \in H$, i.e. $a^r \in H$. Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Hence $n = qm$ and $b = a^n = (a^m)^q = c^q$. Hence b is a power of c.

Division Algorithm Theorem: If m is a positive integer and n is any integer then there exist unique integers q and r such that $n = mq + r$ and $0 \leq r < m$.

Example 13

A cyclic group C consists of the following elements: $e, x, x^2, x^3, x^4, x^5, x^6, x^7$.
Determine:

a the elements that are generators of C, and
b the orders of the remaining elements.

a $x^8 = e$, $(x^3)^8 = e$, $(x^5)^8 = e$, and $(x^7)^8 = e$ are the smallest such powers to equal e. Hence these elements are all generators of C.	*Since the order of C is 8, we need to look for elements such that the least power of such an element to equal e is 8, i.e.* $(x^n)^8 = e$, $1 \le n \le 7$. *This occurs when n and 8 are relatively prime.*
b Since $(x^2)^4$, $(x^4)^2$, and $(x^6)^4$ all equal e, the orders of these elements are respectively 4, 2 and 4. Hence, they cannot generate C.	*Since the powers of the elements 2, 4, and 6 are factors of 8 or factors of its multiples, the elements with these powers cannot generate C.*

At the beginning of this section on cyclic groups, we saw that R_1, rotation through 90° anti-clockwise, was a generator of the subgroup of rotation symmetries of the square group. Since the order of an element of a finite group is the same as the order of the cyclic subgroup generated by the element, and the order of a subgroup must divide the order of a group, we can state the following theorem.

Theorem 10: Lagrange's Corollary

The order of an element of a finite group divides the order of the group.

Theorem 10 follows directly from Lagrange's Theorem, which we will study and prove in Chapter 4.

Exercise 3E

1 Show that the group $\{\mathbb{Z}_{10}, +_{10}\}$ is generated by the number 7.

2 Prove by mathematical induction:

a For all $a \in \{G, *\}$, $(a_1 * a_2 * \ldots * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \ldots * a_1^{-1}$, $n \ge 2$.

b For all $a \in \{G, *\}$, $(a^n)^{-1} = (a^{-1})^n$, $n \ge 2$.

c Hence, or otherwise, prove that the order of an element is equal to the order of its inverse.

3 $\mathbb{Z}_n \times \mathbb{Z}_m = \left\{(a, b) \middle| a \in \mathbb{Z}_n, b \in \mathbb{Z}_m\right\}$ forms a group under the binary operation $*$ defined as $(a_1, b_1) * (a_2, b_2) = (a_1 +_n a_2, b_1 +_m b_2)$, where $+_n$ and $+_m$ denote additions of integers modulo n and m, respectively.

- **a** State the order of $(\mathbb{Z}_4 \times \mathbb{Z}_5, *)$, and evaluate $(3, 2) * (1, 4)$.
- **b** Show that $\{\mathbb{Z}_2 \times \mathbb{Z}_3, *)$ is cyclic, and list any generators.
- **c** Determine how many elements of $\{\mathbb{Z}_2 \times \mathbb{Z}_4, *\}$ have order 4.

4 Show that

- **a** the nth roots of unity can be expressed in the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where α is the complex root with the smallest positive principal argument
- **b** the nth roots of unity form a cyclic group under multiplication.

5
- **a** Prove that if a group G has order p, where p is prime, then G is cyclic.
- **b** Prove that if a group G has order pq, $p, q \in$ {Primes}, then every proper subgroup of G is cyclic.
- **c** Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

Review exercise

EXAM-STYLE QUESTIONS

1
- **a** Show that the set of real numbers, excluding a single number, forms a group under the operation $*$ defined as $a * b = a + b - ab$, and determine the single number which must be excluded from $\mathbb{R}$.
- **b** Hence, solve the equation $5 * x = 12$.

2 H is a subgroup of G and R is a relation defined on G such that for all $a, b \in G$, $aRb \Leftrightarrow ab^{-1} \in H$. Show that R is an equivalence relation.

3 Let x, a, b and c be elements of a group with identity element e.

- **a** Solve for x: $axb = c$
- **b** Solve simultaneously for x: $ax^2 = b$ and $x^3 = e$

4 A group G with identity element e contains elements x and y such that $yx = x^2y$ and $y^3 = e$.

Prove:

a $y^2xy^{-2} = x^4$ **b** $x^8 = x$.

5 **a** Given that $f_1(x) = x,\ f_2(x) = 1 - x,\ f_3(x) = \frac{1}{x}$,
obtain expressions for $f_4(x),\ f_5(x)$, and $f_6(x)$ if:

$f_4(x) = (f_2 \circ f_3)(x)$; $f_5(x) = (f_3 \circ f_2)(x)$; $f_6(x) = (f_3 \circ f_4)(x)$.

b Given that $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ forms a group with respect to function composition, construct its Cayley table.

c Determine the order of each element of the group.

d Find a subgroup of G containing only three elements.

6 Let $\{G, *\}$ be a group and a is a fixed element of G. Define a function $f\colon G \to G$ by $f(x) = a * x$, for every $x \in G$. Prove that f is bijective.

7 For the group $\{\mathbb{Z}_{12}, +_{12}\}$:

a Find the order of the elements 4, 5 and 9.

b Show that the group is cyclic, and find all possible generators.

8 Let min (x, y) be the minimum value of two numbers x and y.
The operation # is defined on the set of negative integers by
$x \# y = \min(x, y)$. ($\min(x, x) = x$)

a Show that # is commutative.

b Determine which of the group axioms are satisfied.

9 Let $\{G, *\}$ be a group with subgroups $\{H, *\}$ and $\{K, *\}$. Prove that $\{H \cup K, *\}$ is a subgroup of $\{G, *\}$ if and only if either $H \subseteq K$ or $K \subseteq H$.

10 Find the order of a group generated by two elements a and b if $a^3 = b^2 = (ab)^2 = e$, and find all subgroups of the group.

11 Construct a Latin Square of order 6 which has an identity element and all other elements have order 2, and prove that this Latin Square does not represent a group.

12 Let $\{H, *\}$ be a subgroup of $\{G, *\}$. Let $a \in G$, $a \notin H$, and
$aH = \{ah \mid h \in H\}$.

i Show that $H \cap aH = \varnothing$.

ii Show that $H \cup aH$ is a subgroup of G.

iii Show that the number of elements in $H \cup aH$ is twice the number of elements of H.

Chapter 3 summary

Definitions

A group $\{G, *\}$ is an Abelian group if G is **commutative** under $*$, i.e. for all $a, b \in G$, $a * b = b * a$.

The **order** $|G|$ of a group $\{G, *\}$ is the number of elements in the group. If a group has an infinite number of elements, it is said to have infinite order, i.e. $|G| = \infty$.

A **Latin Square** is a square array of n^2 compartments such that each element or symbol occurs exactly once in each row and column.

Symmetry groups are groups of transformations of plane figures that preserve symmetrical properties.

If a non-empty subset H of a group $\{G, *\}$ is also a group under $*$, then $\{H, *\}$ is a **subgroup** of $\{G, *\}$.

If $\{G, *\}$ is a group, then the subgroup consisting of G itself and the subgroup consisting of only the identity are the **improper subgroups** of G. All other subgroups are **proper subgroups**. The subgroup $\{\{e\}, *\}$ is also referred to as the **trivial subgroup** of G.

Let $a \in G$ where $\{G, *\}$ is a group. Then a is said to have **finite order** if $a^n = e$ for some $n \in \mathbb{Z}^+$. The **order** of a is the least such n. If no such n exists, the element a has **infinite order**.

The set G with a binary operation $*$ is called a **group** if the following four axioms (properties) hold:

1 Closure: For all $a, b \in G$, $a * b \in G$
2 Identity: For all $a \in G$, there exists an element $e \in G$ such that $a * e = a = e * a$
3 Inverse: For each $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$
4 Associativity: For all $a, b, c, \in G$, $a * (b * c) = (a * b) * c$

The group G with binary operation $*$ is denoted by $\{G, *\}$

Integers modulo *n* and modular arithmetic

- $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, n \in \mathbb{N}, n \geq 2$
- $+_n$ denotes addition (mod n), and $a +_n b$ is the remainder when $a + b$ is divided by n, i.e. $a +_n b = a + b(\text{mod } n)$.
- $\times_n$ denotes multiplication (mod n), and $a \times_n b$ is the remainder when $a \times b$ is divided by n, i.e. $a \times_n b = ab(\text{mod } n)$.

Properties and theorems of groups and subgroups

1 **Cancellation laws:** Given a group $\{G, *\}$ and $a, b, c \in G$:

   i the right cancellation law holds, i.e. $a * c = b * c \Rightarrow a = b$ and
   ii the left cancellation law holds, i.e. $c * a = c * b \Rightarrow a = b$.

2 A group $\{G, *\}$ has the following properties:

- The identity element for a group is unique.
- For any $a \in G$, the inverse of a, a^{-1}, is unique.
- For any $a, b \in G$, the equations $a * x = b$ and $y * a = b$, $x, y \in G$, have unique solutions in G. (For finite groups, this means that each element would appear only once in every row and column of its operation table.)
- For any $a, b \in G$:
  - ○ $a * b = e \Rightarrow a = b^{-1}$
  - ○ $a * b = e \Rightarrow b = a^{-1}$
  - ○ $a * b = e \Rightarrow b * a = e$
- For any $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.
- For any $a \in G$, $(a^{-1})^{-1} = a$.

3 **Subgroup Theorem:** A subset H of a group $\{G, *\}$ is a subgroup $\{H, *\}$ if and only if:
   1 H is closed under the binary operation $*$, i.e. $a, b \in H \Rightarrow a * b \in H$.
   2 The identity element e of G is in H.
   3 For all $a \in H$, $a^{-1} \in H$.

Let $\{G, *\}$ be a **finite or infinite group** and H a non-empty subset of G. Then H is a subgroup of G if and only if $a * b^{-1} \in H$ for $a, b \in H$.

Theorem: Let a be an element of a finite group $\{G, *\}$. Then a has finite order.

Theorem: If H is a non-empty subset of a finite group $\{G, *\}$ then $\{H, *\}$ is a subgroup if and only if, for all $a, b \in H$, $a * b \in H$.

A group whose elements can be expressed in the form $\{e, a, a^2, a^3, \ldots, a^{n-1}\}$ is called a **cyclic** group of order n and is denoted by C_n. The element a is a generator of the group. A group of order n is cyclic if an only if it contains an element of order n.

Theorem: In a group $\{G, *\}$ the order of an element a is the same as the order of its inverse a^{-1}.

Theorem: Every cyclic group is Abelian.

Theorem: Let $\{G, *\}$ be any group and let $a \in G$. Then $H = \{a^n \mid n \in Z\}$ is the smallest subgroup of $\{G, *\}$ that contains a, i.e., every subgroup containing a contains H.

The subgroup of $\{G, *\}$ above, $H = \{a^n \mid n \in Z\}$, is the **cyclic subgroup** of $\{G, *\}$ generated by a.

Theorem: A subgroup of a cyclic group is cyclic.

Theorem: (Lagrange's Corollary): The order of an element of a finite group divides the order of the group.

4 The classification of groups

CHAPTER OBJECTIVES:

8.10 Permutations under composition of permutations; cycle notation for permutations; result that every permutation can be written as a composition of disjoint cycles.

8.11 Definition and examples of left and right cosets of a subgroup of a group; Lagrange's theorem; use and proof of the result that the order of a finite group is divisible by the order of any element (Corollary to Lagrange's theorem).

8.12 Definition of group homomorphism; definition of a kernel of a homomorphism; proof that the kernel and range of a homomorphism are subgroups; proof of homomorphism properties for identities and inverses; isomorphism of groups; the order of an element is unchanged by an isomorphism.

Before you start

You should know how to:

1 Find the partition of a set induced by an equivalence relation, e.g. if

$A = \left\{\sqrt{5}, -3, \frac{1}{5}, 2\pi, 6, \sqrt{20}\right\}$

and the equivalence relation R on A is defined by $aRb \Leftrightarrow \frac{a}{b} \in \mathbb{Q}$, find the partition of A induced by R.

The partition of A induced by R is

$\left\{\{\sqrt{5}, \sqrt{20}\}, \left\{-3, \frac{1}{5}, 6\right\}, \{2\pi\}\right\}.$

Skills check:

1 Find the partition of the set induced by the given equivalence relations:

a For $a, b \in \mathbb{Z}$, $aRb \Leftrightarrow 2\,|\,(a^2 + b^2)$, i.e. 2 divides $(a^2 + b^2)$.

b R is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$, such that for all $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$, $(a, b)R(c, d) \Leftrightarrow a = c$. Describe how the equivalence relation R partitions $\mathbb{Z} \times \mathbb{Z}$.

c The equivalence relation R on $S = \{1, 2, 3, \ldots, 10\}$ is defined as $xRy \Leftrightarrow x \equiv y (\text{mod } 4)$. Find the partition of S induced by R.

2 Determine if a function $f: A \to B$ is surjective, injective, or both, e.g. let $A = \mathbb{R}\backslash\{-2\}$, and $f: A \to \mathbb{R}$ such that $f(x) = \frac{3x}{x+2}$.

Determine whether or not f is bijective. For f to be bijective, it must be (i) injective and (ii) surjective.

(i) To show that f is injective,

Method I
We must show that $f(a) = f(b) \Rightarrow a = b$.

Hence,

$$\frac{3a}{a+2} = \frac{3b}{b+2} \Rightarrow 3a(b+2) = 3b(a+2)$$
$$\Rightarrow 6a = 6b$$
$$\Rightarrow a = b$$

or

Method II
We must show that f is either strictly increasing or strictly decreasing on its domain.

$$\frac{d\left(\frac{3x}{x+2}\right)}{dx} = \frac{6}{(x+2)^2} \text{ For all } x \neq -2, \frac{dy}{dx} > 0,$$

therefore f is strictly increasing.

Hence f is injective.

(ii) To show that f is surjective, we must show that for all $b \in \mathbb{R}$ there exists an $a \in A$ such that $f(a) = b$. Hence,

$$\frac{3a}{a+2} = b \Rightarrow 3a = b(a+2)$$
$$\Rightarrow 3a - ba = 2b$$
$$\Rightarrow a(3-b) = 3b$$
$$\Rightarrow a = \frac{3b}{3-b}$$

When $b = 3$ it is not the image of any element in A, so f is not surjective.

Therefore f is not bijective.

2 a Let $A = \{x \mid x \in \mathbb{R}, x \geq 0\}$ and let $f: A \to A$ be defined as $f(x) = \frac{3x^2+5}{5x^2+3}$.

Determine if f is bijective.

b Given that $f: \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(a, b) = (2a + b, a - 2b)$, show that f is bijective, and find its inverse.

Injective and surjective functions can be represented graphically, as shown below.

In Figure 1, since the function is steadily increasing over its entire domain, the function is injective. Also, if you imagine a horizontal line drawn anywhere through the graph, the function will intersect such a line at only one point.

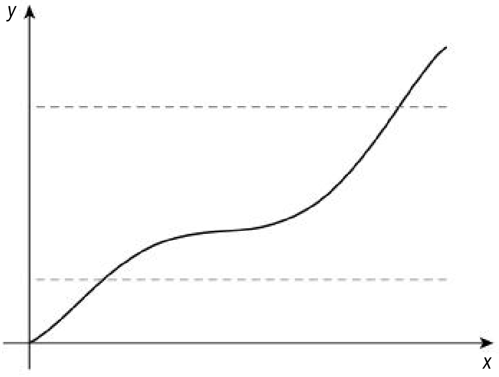


Figure 1

Imagine that the graph in Figure 2 continues to infinity at both ends. Then any horizontal line drawn through the graph will intersect it in at least one point. This function is surjective.

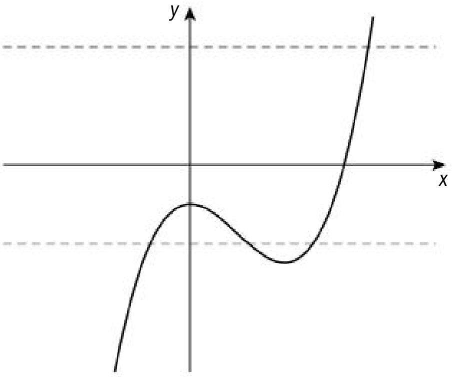


Figure 2

Group structures

The entire theory of groups originally grew out of an understanding of permutations. You are familiar with permutations as arrangements of a given finite set. The search for solutions of polynomial equations led the French mathematician Lagrange and others, in the late 18th century, to think of permutations as bijections from a finite set onto itself. However it was the French mathematician Augustin-Louis Cauchy who developed in detail the basic theorems of permutation theory and introduced the standard notation we still use today.

In addition to permutation groups, we will also focus on isomorphisms and homomorphisms, which are functions between groups that preserve certain group structures. The German mathematician Emmy Noether first treated the ideas on group structures in a paper published in 1927. She is considered one of the most famous mathematicians of our modern era.

4.1 Permutation groups

When you shuffle a deck of 52 playing cards you are essentially rearranging all of the cards, or forming permutations on the set of cards. A permutation is therefore essentially a bijection of a set onto itself.

Definition

A permutation of a non-empty finite set A is a **bijection** from A to A.

If we consider the set of the three natural numbers $A = \{1, 2, 3\}$ and form all of the possible permutations from A onto itself, one possible mapping is $1 \to 1$, $2 \to 2$, $3 \to 3$. We can illustrate this permutation in the following way:

$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. This mapping leaves all elements unchanged.

Another possible mapping is $1 \to 3$, $2 \to 2$, $3 \to 1$ or $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

How many possible mappings are there from A to itself? You should know the answer from your work on permutations in the core book: 3!, or 6.

Let us now complete the other four permutations:

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

We perform operations on permutations in the same way as function composition or transformations on a set of isometries. In other words, if we want the operation $p_3 p_4$, then just as in the set of isometries, this means p_4 followed by p_3.

p_4 maps 1 to 2, and p_3 maps 2 to 3, hence $p_3 p_4$ maps 1 to 3.
p_4 maps 2 to 1, and p_3 maps 1 to 1, hence $p_3 p_4$ maps 2 to 1.
p_4 maps 3 to 3, and p_3 maps 3 to 2, hence $p_3 p_4$ maps 3 to 2.

Therefore, $p_3 p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, which is p_5.

Now consider $p_4 p_3$. This means p_3 followed by p_4.

p_3 maps 1 to 1, and p_4 maps 1 to 2, hence $p_4 p_3$ maps 1 to 2.
p_3 maps 2 to 3, and p_4 maps 3 to 3, hence $p_4 p_3$ maps 2 to 3.
p_3 maps 3 to 2, and p_4 maps 2 to 1, hence $p_4 p_3$ maps 3 to 1.

Therefore, $p_3 p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, which is p_6.

We see already in this case that composition of permutations, just as in function composition, is not commutative, since $p_3 p_4 \neq p_4 p_3$.

We will now determine whether the set of permutations on three elements, $S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, forms a group under composition of permutations. Composition of permutations, just like composition of functions, is associative.

The set would need an identity, and clearly p_1 is the identity.

We now consider the inverses of the elements. Since a permutation is a bijection from a set onto itself, we know that all elements have inverses.

Consider $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Since p_2 maps 1 to 3, p_2^{-1} would map 3 to 1.

In the same way, p_2^{-1} would map 2 to 2, and 1 to 3. Hence, $p_2^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

which means that p_2 is its own inverse. Finding the rest of the inverses is left as an exercise before you see the answers in Example 1.

Example 1

Show that the set S_3 of all permutations of the set {1, 2, 3} forms a group under composition of permutations. The definitions of p_1, p_2, etc. are those used on the previous page.

Work out all the permutations and put the results in a Cayley table.

$\circ$	$\boldsymbol{p_1}$	$\boldsymbol{p_2}$	$\boldsymbol{p_3}$	$\boldsymbol{p_4}$	$\boldsymbol{p_5}$	$\boldsymbol{p_6}$
$\boldsymbol{p_1}$	p_1	p_2	p_3	p_4	p_5	p_6
$\boldsymbol{p_2}$	p_2	p_1	p_5	p_6	p_3	p_4
$\boldsymbol{p_3}$	p_3	p_6	p_1	p_5	p_4	p_2
$\boldsymbol{p_4}$	p_4	p_5	p_6	p_1	p_2	p_3
$\boldsymbol{p_5}$	p_5	p_4	p_2	p_3	p_6	p_1
$\boldsymbol{p_6}$	p_6	p_3	p_4	p_2	p_1	p_5

Ascertain the group properties.

Closure: It is evident that the set under composition of permutations is closed, i.e. for all $p_i, p_j \in S_3$, $p_i p_j \in S_3$.

Identity: p_1 is the identity, since for all $p_i \in S_3$, $p_i p_1 = p_1 p_i = p_i$.

Inverse: For all $p_i \in S_3$ there exists a $p_j \in S_3$ such that $p_i p_j = p_j p_i = p_1$.

p_i	p_1	p_2	p_3	p_4	p_5	p_6
p_i^{-1}	p_1	p_2	p_3	p_4	p_6	p_5

Composition of permutations is associative. Hence, S_3 is a group under composition of permutations.

Composition of functions is associative.

Is a permutation of a set A consisting of four elements also a group? We know from our core work with permutations that this set would consist of 4!, or 24 elements. It would not be practical to set up a Cayley table for S_4, so instead we will prove the following theorem.

Theorem 1

Let A be a non-empty set of n elements, and let S_n be the set of all permutations of A. Then S_n forms a group under composition of permutations, i.e. $\{S_n, \circ\}$forms a group.

Proof:

We shall examine the group properties.

Closure: Similar to function composition, the composition of two permutations yields a permutation, so S_n is closed.

Identity: The identity permutation is $p_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.

The identity permutation is the identity function $f(x) = x$.

Inverse: Since a permutation is a bijection, for any permutation $p \in S_n$ there is an inverse permutation $p^{-1} \in S_n$.

Associativity: Just as function composition, the permutation composition is associative.

Therefore, $\{S_n, \circ\}$forms a group.

Definition

Let A be the finite set $\{1, 2, 3, \dots, n\}$. The group of all permutations of A is called the **symmetric group** on n elements and is denoted by S_n.

Example 2

Given $x \in S_6$, $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$, find

a the inverse

b the order of x.

a $x^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$

Since x maps $1 \to 3$, $2 \to 1$, $3 \to 2$, $4 \to 4$, $5 \to 6$, $6 \to 5$, x^{-1} maps $3 \to 1$, $1 \to 2$, $2 \to 3$, $4 \to 4$, $6 \to 5$, $5 \to 6$

$x^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$;

$x^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}$; $x^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}$;

$x^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$; $x^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$.

Find the first power of x that equals e, i.e., the identity permutation p_1.

Hence the order of x is 6, since $x^6 = p_1$ and $x, x^2, x^3, x^4, x^5 \neq p_1$.

Exercise 4A

1 Show that the subset of permutations of S_4, $\{e, x, y, z\}$ forms a group, where $z = xy$ and

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},\ x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix},\ y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

2 Determine the order of the smallest subgroup of S_5 containing the element $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$.

3 Find a cyclic subgroup of $\{S_3, \circ\}$ of order 3, and state a generator of this subgroup.

4 The following are permutations on the set S_5.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},\ \upsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$$

a Find the permutations:

i $\sigma\tau$ **ii** $\tau\sigma$ **iii** $\sigma^2\tau$ **iv** $\sigma\upsilon^{-1}$ **v** $(\sigma\upsilon)^{-1}$ **vi** $\upsilon^{-1}\tau\upsilon$

b Solve for x in the following equations:

i $\sigma x = \tau$ **ii** $\sigma x\tau = \upsilon.$

Permutations and cycle form

Another way of writing a permutation is in cycle form. Using the elements of S_3, since $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, p_2 can be expressed as a cycle using the notation (13). This means 1 is mapped onto 3 and since 3 is mapped onto 1, the cycle ends. Since 2 is mapped onto 2, we can write this as (2). We can then write the permutation as a product of cycles. In other words, p_2 = (13)(2) or (2)(13). The single element that is in brackets is mapped onto itself, i.e. the element that is invariant under the mapping is put in its own brackets. The cycle notation for the identity element of S_3, p_1, is (1)(2)(3); in other words, each element is mapped onto itself. For simplicity of notation, the invariant element(s) will be omitted. The identity, therefore, would be represented simply as (1), and for p_2 its cycle form is simply (13).

Let's now write the other permutations of S_3 using cycle notation.

$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, or p_3 = (23).

Using cycle notation, (23) means that 1 maps onto itself.

$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, or $p_4 = (12)$.

Again, this means that 3 is invariant and maps onto itself.

$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, or $p_5 = (132)$; $p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, or $p_6 = (123)$.

We will now write the element x from Example 2 using cycle notation.

$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} = (132)(4)(56)$, or $(132)(56)$. Since the cycles are disjoint, we can also write this as $x = (56)(132)$, i.e. whenever the cycles are disjoint, the cycle form is commutative.

We can also write the inverse of x in cycle notation.

$x^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} = (123)(56)$

Again, since the cycles are disjoint, we can also write $x^{-1} = (56)(123)$.

Notice that to find the inverse of an element in cycle notation, we simply reverse the integers in the cycle. For example, inverting the integers in (132) gives us (123), since it is understood that the number at the end of the cycle is the same number as at the beginning of the cycle. Thus (132) is $1 \to 3 \to 2 \to 1$ and its reverse is $1 \to 2 \to 3 \to 1$. The cycle (56), i.e. $5 \to 6 \to 5$, is the same as (65), i.e. $6 \to 5 \to 6$.

Let us now consider a permutation and write the permutation and its inverse in cycle form.

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 6 & 8 & 4 & 10 & 7 & 2 & 9 & 3 \end{pmatrix}$

We see that $1 \to 5 \to 4 \to 8 \to 2 \to 1$, which gives us the cycle (15482). Then starting with the smallest number that we have yet to use, 3, we have $3 \to 6 \to 10 \to 3$, giving us the cycle (3 6 10). (Notice that we leave spaces in this cycle between the numbers to avoid confusion since we have a two-digit number in our cycle.) The only remaining numbers are 7 and 9, which are invariant.

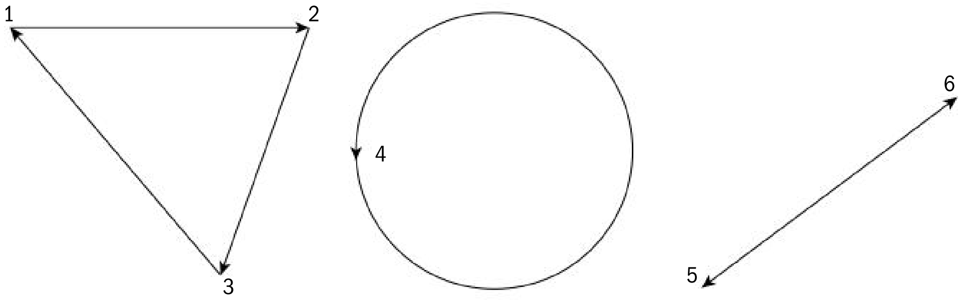
Hence, $\sigma = (15482)(3\ 6\,10)$, or $\sigma = (3\ 6\,10)(15482)$. Using cycle notation, let's now find the inverse of σ. Reversing the numbers in the cycle after the first number we obtain (12845)(3 10 6). In other words, $1 \to 2 \to 8 \to 4 \to 5 \to 1$ and $3 \to 10 \to 6 \to 3$. Since 7 and 9 are not present in our cycles, they are invariant.

Hence, $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 8 & 10 & 5 & 1 & 3 & 7 & 4 & 9 & 6 \end{pmatrix}$

How can we also use cycles to find the order of a permutation? We can define the **length of a cycle** as the number of moves required to come full cycle, i.e. the cycle (123) requires 3 moves to go from 1 back to 1 again. Let's look again at Example 2,

where $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$.

We know that x can be written in cycle form as (132)(56). The length of the cycles are 3 and 2. The diagram below illustrates what this means.



We want to determine the smallest power n such that $x^n = p_1$. Let's label the first cycle of length 3 as a, and label the second cycle of length 2 as b. Every application or permutation of x moves the numbers around in a cycle so that x would require 3 moves in cycle a to go from 1 back to 1. In cycle b, x would require 2 moves to go from 5 to 6 and back again. This means that both 3 and 2 would need to divide n, the total number of applications of x. Since we want both 3 and 2 to divide n, and n must be the lowest such number, we want the lowest common multiple of 3 and 2, which is 6. We have already seen in Example 2 that the order of x is 6.

From all the previous examples, we can summarize our findings into cycle properties.

Properties of cycle form

- Every permutation can be written as a product of disjoint cycles.
- Disjoint cycles are commutative.
- The order of a permutation written as a product of disjoint cycles is the least common multiple of the lengths of the cycles.

The proofs of the above properties are not required for examination purposes, and are not included in this course companion but you may decide to prove them informally.

Example 3

Find the order of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 6 & 8 & 4 & 10 & 7 & 2 & 9 & 3 \end{pmatrix}$.

σ = (15482)(3 6 10)	*Write the permutation in cycle form.*
The length of the cycles are 5 and 3. Since lcm (3, 5) = 15, the order of σ is 15.	*Find the lowest common multiple of the lengths of the cycles.*

Let's now consider permutation composition using cycles. Consider the cycles a = (124) and b = (1256) in S_6. We can write these as permutations.

In cycle a, since 3, 5 and 6 are invariant, $a = (124) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$.

In cycle b, 3 and 4 are invariant, hence $b = (1256) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 4 & 6 & 1 \end{pmatrix}$.

We already know how to find the composition of these two cycles using permutation composition. Let's concentrate now in finding the product through the cycles, i.e. we want $a \circ b$, or (124)(1256) in cycle form.

For convenience, at times we refer to composition as a product, particularly when writing it in cycle form.

As you already know, for permutation composition we move from right to left. The right cycle maps 1 to 2, and then the left cycle maps 2 to 4, so the composition maps 1 to 4. The right cycle then maps 2 to 5 and the left one maps 5 to 5, so 2 is mapped onto 5. The right cycle maps 5 to 6, and the left one maps 6 to 6, so 5 is mapped onto 6. The right cycle maps 6 to 1, and the left cycle maps 1 to 2, so 6 is mapped onto 2.

We can write the permutation $a \circ b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 & 6 & 2 \end{pmatrix}$ or (14)(256).

In cycle notation, $a \circ b$ = (124)(1256) = (14)(256).

Can we arrive at the result in cycle form without writing out the permutation?

We see that in composing (124)(1256), starting on the right cycle, 1 maps onto 2, and 2 maps onto 4 on the left cycle, so 1 maps onto 4, and we'll write this as an unclosed cycle, i.e. with no closing bracket: (14. Then in the right cycle, 4 is mapped onto 4, and on the left cycle 4 is mapped onto 1, so now we can close this cycle (14).

Then, the cycle on the right maps 2 to 5, and 5 is invariant in the first cycle, so 2 maps onto 5. We begin this cycle as (25. Then in the right cycle 5 maps onto 6, and 6 is invariant in the left cycle, so 5 maps onto 6, or (256. Now 6 maps onto 1, and 1 maps onto 2 in the left cycle, hence 6 maps onto 2, and we now have a full cycle (256). Therefore, (124)(1256) = (14)(256).

We will now compute $b \circ a$ or (1256)(124).

Using arrows to indicate a mapping, starting on the right, $1 \to 2$, then on the left $2 \to 5$, hence $1 \to 5$, or (15. Since 5 is invariant in the right cycle, $5 \to 5$, and on the left $5 \to 6$, so $5 \to 6$, or (156. In the right cycle, $6 \to 6$, and on the left $6 \to 1$, hence $6 \to 1$, so we have a complete cycle (156). In the right cycle, $4 \to 1$, and on the left $1 \to 2$, hence $4 \to 2$, or (42. On the right, $4 \to 1$ and on the right $1 \to 2$, hence $4 \to 2$, so we have a complete cycle (42). This means the 3 is invariant, and $b \circ a$ = (156)(42), or (1256)(124) = (156)(42).

We see again that permutation composition is not commutative, since $a \circ b \neq b \circ a$.

Exercise 4B

1 **a** Write each of the following permutations as a product of disjoint cycles.

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 1 & 4 \end{pmatrix},\ y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 6 & 7 & 8 & 5 \end{pmatrix},$$

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 5 & 4 & 7 & 6 \end{pmatrix}$$

b Write the inverses of x, y and z in cycle form.

c Find the orders of x, y and z.

2 Write the following products of cycles in permutation form.

a on S_6: (123)(46)

b on S_7: (12)(345)(67)

c on S_8: (245)(378)

d on S_9: (3457)(689)

3 Given that $\alpha = (136)(24)$ and $\beta = (1452)$, both on S_6, find the following in cycle form:

a α^{-1} **b** $\alpha\beta$ **c** $(\alpha\beta)^{-1}$ **d** $\beta^{-1}\alpha^{-1}$

4 Prove that the order of a cycle is equal to its length.

4.2 Cosets and Lagrange's theorem

We will start this section with an important definition needed to prove the theorem you are already familiar with: Lagrange's theorem.

Definition

Let $\{H, *\}$ be a subgroup of $\{G, *\}$ and let $x \in G$. Then the set of elements $xH = \{xh \mid h \in H\}$ is called a **left coset** of $\{H, *\}$ in G. The set of elements $Hx = \{hx \mid h \in H\}$ is called a **right coset** of $\{H, *\}$ in G.

We will show how this definition works by finding the left and right cosets of the subgroup $\{3\mathbb{Z}, +\}$ of $\{\mathbb{Z}, +\}$.

The left coset of $3\mathbb{Z}$ containing x is $x + 3\mathbb{Z}$.
If $x = 0$, then $0 + 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.

To find another left coset, let's take an element that is not in $3\mathbb{Z}$, for example 1. Then, $1 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.
Another element not in $3\mathbb{Z}$ is 2. Then, $2 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.
Now, consider the coset of k, i.e. $k + 3\mathbb{Z}$. If $k \equiv 0(mod\,3)$, then $k + 3\mathbb{Z} = 3\mathbb{Z}$.
If $k \equiv 1(mod 3)$ then $k + 3\mathbb{Z} = 1 + 3\mathbb{Z}$. If $k \equiv 2(mod 3)$, then $k + 3\mathbb{Z} = 2 + 3\mathbb{Z}$.
It should be clear that there are only these three unique cosets.
Furthermore, these three left cosets partition $\mathbb{Z}$ into left cosets of $3\mathbb{Z}$.

Finding the right cosets in the same manner will yield the exact same results. However, since $\mathbb{Z}$ is Abelian, the left coset $k + 3\mathbb{Z}$ and the right coset $3\mathbb{Z} + k$ are the same, hence the partition of $\mathbb{Z}$ into right cosets is the same as its partition in to left cosets.
Observe that in general, the equivalence relation R for the subgroup $\{n\mathbb{Z}, +\}$ of $\{\mathbb{Z}, +\}$ is the same as the relation of congruence modulo n. This means that the partition of $\mathbb{Z}$ into cosets of $n\mathbb{Z}$ is the partition of $\mathbb{Z}$ into residue classes modulo n. (We do not have to distinguish left and right cosets since addition is commutative.)

Example 4

The group $\{\mathbb{Z}_6, +\}$ is Abelian. Find the partition of $\mathbb{Z}_6$ into cosets of the subgroup $H = \{0, 3\}$ under addition.

One coset is $\{0, 3\}$ itself. $1 + \{0, 3\} = \{1, 4\}$ $2 + \{0, 3\} = \{2, 5\}$	*Find the cosets containing 0, 1, 2, …*
The cosets are $\{0, 3\}, \{1, 4\}, \{2, 5\}$.	*Since these three sets exhaust all of $\mathbb{Z}_6$, they are the only cosets.*

You will have noticed that for a subgroup $\{H, \circ\}$ of an Abelian group $\{G, \circ\}$, the partition of G into left cosets of H and the partition of G into right cosets of H are the same.

Example 5

Let $G = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ under complex number multiplication be the cyclic group consisting of the sixth roots of unity, where $\alpha = e^{\frac{\pi i}{3}}$. Let $H = \{1, \alpha^2, \alpha^4\}$ be a subgroup of $\{G, \times\}$. Find the left cosets of H.

For $x \in G$, $x = 1$, $1H = \{1, \alpha^2, \alpha^4\}$ For $x \in G$, $x = \alpha$, $\alpha H = \{\alpha, \alpha^3, \alpha^5\}$	*Choose an $x \in G$, e.g. $x = 1$ and form the left cosets. Then choose another $x \in G$, e.g. $x = \alpha$ and form the left cosets.*
The only two cosets are: $1H = \{1, \alpha^2, \alpha^4\}$ and $\alpha H = \{\alpha, \alpha^3, \alpha^5\}$	*These two cosets partition the group, so all other cosets would be identical to one of these two.*

Also in Example 5, since every cyclic group is Abelian, the left and right cosets will be the same.

We will now list some properties of cosets which you will undoubtedly have noticed in the previous examples.

Theorem 2: Properties of cosets

For any subgroup $\{H, \circ\}$ of a group $\{G, \circ\}$:

1 G is the union of disjoint cosets of $\{H, \circ\}$, i.e., the group is partitioned by the left (or right) cosets of its subgroup.

2 Every coset (left or right) of a subgroup $\{H, \circ\}$ has the same number of elements as H.

3 Every element of G lies in one of the cosets of H in G.

The proofs of these properties are left as an exercise.

We will now consider an example where the left and right cosets are not the same.

Example 6

Consider the Cayley table for S_3 shown in Example 1, and consider the subgroup $\{H, \circ\}$ such that $H = \{p_1, p_3\}$. Find the partitions of S_3 into left and right cosets of H. Comment on your results.

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix};\ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};\ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix};\ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};\ p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Work out all the possible permutations.

$\circ$	$\boldsymbol{p_1}$	$\boldsymbol{p_2}$	$\boldsymbol{p_3}$	$\boldsymbol{p_4}$	$\boldsymbol{p_5}$	$\boldsymbol{p_6}$
$\boldsymbol{p_1}$	p_1	p_2	p_3	p_4	p_5	p_6
$\boldsymbol{p_2}$	p_2	p_1	p_5	p_6	p_3	p_4
$\boldsymbol{p_3}$	p_3	p_6	p_1	p_5	p_4	p_2
$\boldsymbol{p_4}$	p_4	p_5	p_6	p_1	p_2	p_3
$\boldsymbol{p_5}$	p_5	p_4	p_2	p_3	p_6	p_1
$\boldsymbol{p_6}$	p_6	p_3	p_4	p_2	p_1	p_5

Compose the Cayley table.

The left cosets of H are:

$p_2H = \{p_2p_1, p_2p_3\} = \{p_2, p_5\}$

$p_3H = \{p_3p_1, p_3p_3\} = \{p_3, p_1\} = H$

$p_4H = \{p_4p_1, p_4p_3\} = \{p_4, p_6\}$

$p_5H = \{p_5p_1, p_5p_3\} = \{p_5, p_2\} = p_2H$

$p_6H = \{p_6p_1, p_6p_3\} = \{p_6, p_4\} = p_4H$

The partition of S_3 into left cosets of H is either $[H, p_5H, p_6H]$, $[H, p_2H, p_4H]$, $[H, p_2H, p_6H]$, or $[H, p_4H, p_5H]$.

Find all the left cosets of H.

The right cosets of H are:

$Hp_2 = \{p_1p_2, p_3p_2\} = \{p_2, p_6\}$

$Hp_3 = \{p_1p_3, p_3p_3\} = \{p_3, p_1\}$

$Hp_4 = \{p_1p_4, p_3p_4\} = \{p_4, p_5\}$

$Hp_5 = \{p_1p_5, p_3p_5\} = \{p_5, p_4\}=Hp_4$

$Hp_6 = \{p_1p_6, p_3p_6\} = \{p_6, p_2\} = Hp_2$

The partition of S_3 into right cosets of H is either: $[H, Hp_5, Hp_6]$, $[H, p_2H, p_4H]$, $[H, Hp_2, Hp_5]$, or $[H, Hp_4, Hp_6]$.

Find all the right cosets of H.

The partitions into left and right cosets are not the same, e.g. $p_2H = \{p_2, p_5\}$ and $Hp_2 = \{p_2, p_6\} \neq p_2H$. This makes sense since $\{S_3, \circ\}$ is not Abelian.

You need show only one example where the partitions into left and right cosets are not the same.

Through the use of cosets, we are now in a position to prove Lagrange's theorem, which you have already been using in Chapter 3.

Theorem 3: Lagrange's theorem

If $\{H, \circ\}$ is a subgroup of $\{G, \circ\}$, then the order of the subgroup $\{H, \circ\}$ is a divisor of the order of $\{G, \circ\}$.

Proof:

Let the order of $\{G, \circ\}$ be n and the order of $\{H, \circ\}$ be m, where $m < n$.
Let k be the number of cells, or sets, in the partition of $\{G, \circ\}$ into left cosets of $\{H, \circ\}$.
Hence, $n = km$, since every coset of H must also have m elements.
Therefore m is a divisor of n.

It is quite astonishing that this elegant and useful theorem comes from simply counting cosets, and the number of elements in each coset!
We will now consider two famous corollaries of Lagrange's theorem.

Corollary 1 The order of an element of a finite group divides the order of the group.

Proof:

Since the order of an element is the same as the order of the cyclic subgroup generated by the element, the result follows from Lagrange's theorem.

Corollary 2 Every group of prime order is cyclic.

Proof:

Let $\{G, \circ\}$ be of prime order p. Since $p > 1$ there is some $a \in G$ such that $a \neq e$. Then, the cyclic subgroup of $\{G, \circ\}$ generated by a contains at least two elements, i.e. it has order m such that $m \geq 2$.
Since by Lagrange's theorem, m must divide p, then $m = p$.
Since $\{G, \circ\}$ is generated by a, $\{G, \circ\}$ is cyclic.

In the syllabus, the corollary to Lagrange's theorem is defined as Corollary 1.

Exercise 4C

1 Write out the proofs for the three properties of cosets.

2 Find the left and right cosets of the following subgroups:

a $H = \{4\mathbb{Z}, +\}$ of the group $G = \{\mathbb{Z}, +\}$

b $H = \{4\mathbb{Z}, +\}$ of the group $G = \{2\mathbb{Z}, +\}$

c H which is the set of elements generated by the element 4 in the group $\{\mathbb{Z}_{12}, +_{12}\}$

d Find in cycle form the left and right cosets of the subgroup $\{H, \circ\}$, $H = \{(1), (12)\}$, of the group $G = \{S_3, \circ\}$, i.e. find gH and Hg.

3 $H = \{\mathbb{Z}_2 \times \{0\}, +\}$is a subgroup of the group $\{\mathbb{Z}_2 \times \mathbb{Z}_3, +\}$. Let $(a, b) + (c, d) = (a + c(\text{mod } 2), b + d(\text{mod } 3))$.

a List the sets $H = \mathbb{Z}_2 \times \{0\}$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$.

b Find the left and right cosets of H.

4 Show that the right cosets of the subgroup $\{\mathbb{Z}_{2k}, +_8\}$, $k \in \mathbb{Z}_8$ of the group $\{\mathbb{Z}_8, +_8\}$ partitions the group.

5 Let $\{H, *\}$ be a subgroup of a group $\{G, *\}$. Prove that if $x \in yH$ then $xH = yH$.

6 Let $\{H, *\}$ be a subgroup of $\{G, *\}$ and let $a \in G$. Prove that $aH = H$ if and only if $a \in H$.

4.3 Homomorphisms

In Group Theory, we are interested in the properties induced by the inner structure of groups. We want to make comparisons among the groups, and decide which ones have equivalent structures, regardless of the particular sets and binary operations that define particular groups.

To do this, we define a relationship between two groups $\{G, *\}$ and $\{H, \circ\}$ in terms of a mapping that relates the structures of the groups. The groups may be finite or infinite.

Definition

Let $\{G, *\}$ and $\{H, \circ\}$ be groups. A **homomorphism** is a function $f: G \to H$ such that $f(x * y) = f(x) \circ f(y)$ for all $x, y \in G$.

Essentially this means that the operation $*$ takes place in G while the operation $\circ$ takes place in H. These may or may not be the same binary operations. The function therefore defines a relation between these two binary operations, and hence between the two group structures.

You are already familiar with many homomorphisms because you have actually been using them throughout your mathematics courses, without really referring to them as such. Here are some examples:

- The distributive property of multiplication over addition in the set of real numbers says that for every real number c, $c(x + y) = cx + cy$ for all $x, y \in \mathbb{R}$. In the language of groups we can say that $f_c: \mathbb{R} \to \mathbb{R}$ where $f_c(x) = cx$ is a homomorphism from $\{\mathbb{R},+\}$ to $\{\mathbb{R},+\}$.
- Another property of real numbers states that $|xy| = |x|\,|y|$, for $x, y \in \mathbb{R}$. In the language of groups, the absolute value function $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = |x|$ is a homomorphism from $\{\mathbb{R}\backslash\{0\}, x\}$ to $\{\mathbb{R}\backslash\{0\}, x\}$.
- We know that for all real numbers x and y, $(xy)^2 = x^2y^2$. Again, in the language of groups, we can say that $f: \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$ is a homomorphism from $\{\mathbb{R}\backslash\{0\}, x\}$ to $\{\mathbb{R}\backslash\{0\}, x\}$.
- We know that for all real numbers x and y, $2^{x+y} = 2^x \times 2^y$. Again, in the language of groups, we can say that $f: \mathbb{R} \to \mathbb{R}^+$ such that $f(x) = 2^x$ is a homomorphism between the groups $\{\mathbb{R}, +\}$ and $\{\mathbb{R}^+, \times\}$.

The function definitions in a homomorphism need not be injective or surjective. The third bullet point contains the squaring function, which is neither surjective nor injective. If we change the mapping of the sets in the same example to $f: \mathbb{R}^+ \to \mathbb{R}$, the function is injective but not surjective. If again we change the function to $f: \mathbb{R}^+ \to \mathbb{R}^+$, this function is bijective.

We will now consider homomorphisms among different groups, both finite and infinite. In the following example, we first consider a homomorphism between an infinite group and a finite group.

Example 7

Given are the two groups $\{\mathbb{Z}, +\}$ and $\{S, \times\}$ such that $S = \{1, i, -1, -i\}$.

a Show that the function $f(x) = i^x$ defines a homomorphism between the two groups.

b Determine if the function is injective, surjective, both or neither.

c Describe the mapping of $f: \mathbb{Z} \to S$ as a partition of $\{\mathbb{Z}, +\}$ induced by an equivalence relation, and define the equivalence relation.

a Let $m, n \in \mathbb{Z}$. Then $f(m + n) = i^{m+n} = i^m i^n = f(m)f(n)$, hence f is a homomorphism.

Use the definition of homomorphism.

b $i^{4k}, k \in \mathbb{Z} \to 1$, i.e. $4k = \{\ldots, -8, -4, 0, 4, 8, \ldots\} \to 1$
$i^j, j = \{\ldots, -7, -3, 1, 5, 9, \ldots\} \to i$
$i^r, r = \{\ldots, -6, -2, 2, 6, \ldots\} \to -1$
$i^t, t = \{\ldots, -5, -1, 3, 7, 11, \ldots\} \to -i$
The mapping is surjective since for all $y \in S$ there exists an $x \in Z$ such that $f(x) = y$.

The mapping is not injective since many different integers have the same image, for example, $f(2) = -1 = f(6)$.

Use the function to determine the elements resulting from the mapping.

c $\{\mathbb{Z}, +\}$ has been partitioned into the four cosets $4\mathbb{Z}$, $4\mathbb{Z} + 1$, $4\mathbb{Z} + 2$, and $4\mathbb{Z} + 3$ by the equivalence relation $xRy \Leftrightarrow f(x) = f(y)$.

Describe the mapping and define the equivalence relation.

For any groups $\{G, *\}$ and $\{H, \circ\}$ there is always at least one homomorphism, namely the **trivial homomorphism**. The function $f: G \to H$ defined as $f(x) = e_H$ maps every element x in G onto the identity element in H, e_H. This function is a homomorphism since $f(x * y) = e_H = e_H \circ e_H = f(x) \circ f(y)$, for $x, y \in G$.

We will now define and prove some properties of homomorphisms, which, loosely speaking, means that the homomorphism preserves the identity and inverses.

Theorem 4: Properties of Homomorphisms

Let f be a homorphism from group $\{G, *\}$ to group $\{H, \circ\}$. Let a be an element in G. Then the following properties hold.

1 The homomorphism maps the identity in group G onto the identity in group H, i.e. if e_G and e_H are the identity elements in $\{G, *\}$ and $\{H, \circ\}$ respectively, then $f(e_G) = e_H$.

2 The homomorphism maps the inverse of an element in group G to the inverse of the element's image in group H, i.e. for all $a \in G, f(a^{-1}) = (f(a))^{-1}$.

3 The range of the homomorphism f is a subgroup of $\{H, \circ\}$, i.e. $f(G) = \{f(a) | a \in G\}$ is a subgroup of $\{H, \circ\}$.

4 The homomorphism preserves all powers, i.e. $f(a^n) = (f(a))^n$ for all $a \in G$.

Proofs:

1 Let $f: G \to H$ be a homomorphism from group $\{G, *\}$ to $\{H, \circ\}$. Then, for all a in $G, f(a) = f(a * e_G) = f(a) \circ f(e_G)$ by definition of homomorphism and the identity element e_G. By definition of e_H, $f(a) \circ f(e_G) = f(a) \circ e_H$. Therefore by the left cancellation law, $f(e_G) = e_H$.

2 By definition of inverse and property 1, $f(a * a^{-1}) = f(a^{-1} * a) = f(e_G) = e_H$ for all a in G. By definition of homomorphism, $f(a) \circ f(a^{-1}) = f(a^{-1}) \circ f(a) = e_H$ for every a in G. Therefore, by the group property of uniqueness of inverses, $f(a^{-1}) = (f(a))^{-1}$.

3 In order for $f(G) = \{f(a) | a \in G\}, \{f(G), \circ\}$ to be a subgroup of $\{H, \circ\}$, the following properties must hold:

Closure: This property follows from the definition of homomorphism, and from closure of $\{G, *\}$.

Identity: The range of f contains the identity, i.e. $e_H = f(e_G) \in f(G)$.

Inverse: This follows from property 2 of homomorphisms, and from the inverses in $\{G, *\}$.

So $\{f(G), \circ\}$ is the subgroup of $\{H, \circ\}$.

The proof of property 4 using mathematical induction is left as an exercise.

Property 3 is actually a corollary of part **i** of a more general theorem. The proof of the theorem is left for you to do.

Let $\{G, *\}$ and $\{H, \circ\}$ be groups with subgroups $\{G_0, *\}$ and $\{H_0, \circ\}$ respectively. If $f: G \to H$ is a homomorphism, then

i $f(G_0) = \{f(x) \mid x \in G_0\}$, $\{f(G_0), \circ\}$ is a subgroup of $\{H, \circ\}$, and

ii $f^{-1}(H_0) = \{x \in G \mid f(x) \in H_0\}$, $\{f^{-1}(H_0), *\}$ is a subgroup of $\{G, *\}$

Example 8

Let f be a homomorphism from group $\{G, *\}$ to $\{H, \circ\}$. Furthermore, let f be surjective. Prove that if $\{G, *\}$ is Abelian, then $\{H, \circ\}$ is Abelian.

Let $c, d \in H$.
Since f is surjective, there exist elements $a, b \in G$ such that $f(a) = c$ and $f(b) = d$.

By definition of homomorphism, $f(a * b) = f(a) \circ f(b) = c \circ d$.
Furthermore, since $\{G, *\}$ is Abelian,
$f(a * b) = f(b * a) = f(b) \circ f(a) = d \circ c$.
Hence, $c \circ d = d \circ c$

You need to show that for $c, d \in H$, $c \circ d = d \circ c$.

The kernel of a homomorphism

There is no simple way of showing that a homomorphism between two groups is surjective. There is, however, an important theorem that is useful in showing that it is injective.

Theorem 5

A homomorphism $f: \{G, *\} \to \{H, \circ\}$ is injective if and only if the unique solution to $f(x) = e_H$ is $x = e_G$.

Proof:

$\Rightarrow$: $f(x) = e_H \Leftrightarrow f(x) = f(e_G)$ by Theorem 4 and by the assumption that f is injective, $x = e_G$.

$\Leftarrow$: Let $x = e_G$ be the only solution of $f(x) = e_H$. Suppose that $f(a) = f(b)$ for $a, b \in G$. Then, $f(a) = f(b) \Rightarrow f(a) \circ f(b)^{-1} = e_H \Rightarrow f(a * b^{-1}) = e_H$. Since $a * b^{-1} = e_G$, $a = b$ and f is injective.

An injective homomorphism is called a monomorphism, and a surjective homomorphism is called an epimorphism.

In Example 7 we saw how the homomorphism $f(x) = i^x$ from group $\{\mathbb{Z}, +\}$ to group $\{S, \times\}$, $S = \{1, i, -1, -i\}$, partitioned the set of integers $\mathbb{Z}$ according to the image of each integer in S, i.e.

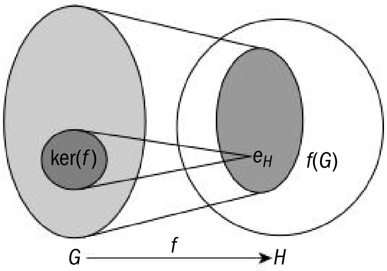
$\{..., -8, -4, 0, 4, 8, ...\} \to 1$
$\{..., -7, -3, 1, 5, 9, ...\} \to i$
$\{..., -6, -2, 2, 6, 10, ...\} \to -1$
$\{..., -5, -1, 3, 7, 11, ...\} \to -i$

The set of elements from $\mathbb{Z}$, $\{\ldots, -8, -4, 0, 4, 8, \ldots\}$that are mapped onto the identity in S, $e = 1$, is called the *kernel* of the homomorphism f.

The following definition therefore shows how the identity appears as the value of a homomorphism.

Definition

Given the group homomorphism $f: \{G, *\} \to \{H, \circ\}$ the **kernel** of the homomorphism f, $\ker(f)$, is defined as the set of all elements of G which are mapped to e_H, i.e. $\ker(f) = \{a \in G | f(a) = e_H\}$.



You saw from the example that the kernel of $f(x) = i^x$ formed a subgroup of $\{\mathbb{Z}, +\}$. We shall now prove this observation.

Theorem 6

The kernel of a homomorphism $f: \{G, *\} \to \{H, \circ\}$ is a subgroup of $\{G, *\}$.

Proof:

We will show that the subgroup properties hold.

Identity: By Theorem 4, $f(e_G) = e_H \Rightarrow e_G \in \ker(f)$.

Closure: Let $a, b \in \ker(f)$ for some $a, b \in G$. Then, by definitions of homomorphism and kernel, $f(a * b) = f(a) \circ f(b) = e_H \circ e_H = e_H$. Hence, $a * b \in \ker(f)$.

Inverse: Let $a \in \ker(f)$ for some $a \in G$. Then by property 2 of homomorphism, $f(a^{-1}) = (f(a))^{-1} = e_H^{-1} = e_H$. Hence, $a^{-1} \in \ker(f)$.

Hence $\ker(f)$ is a subgroup of $\{G, *\}$, since associative property holds for all the elements of G.

As an exercise, you may want to work out the same proof using a different subgroup theorem, e.g. show that if a,b are elements of $\ker(f)$, then $a * b^{-1}$ is an element of $\ker(f)$.

It is interesting to note that the kernel can be useful in solving equations. For example, consider the solutions for the equation $z^3 = 8i$. We can change this to an example with homomorphisms. Let us consider $f: \{\mathbb{C}\backslash\{0\}, \times\} \to \{\mathbb{C}\backslash\{0\}, \times\}$ such that $f(z) = z^3$ for $z \in \mathbb{C}\backslash\{0\}$. We can easily show that f is a homomorphism, since $f(z_1 z_2) = (z_1 z_2)^3 = z_1^3 z_2^3 = f(z_1) f(z_2)$. Using De Moivre's theorem, we can find one solution to the equation $z^3 = 8i$, $z_1 = 2cis\left(\frac{\pi}{6}\right)$.

The elements of the kernel of the homomorphism are the solutions to the equation $z^3 = 1$, since $\ker(f) = 1, f(z) = z^3$. Therefore $\ker(f) = K = \left\{1, cis\left(\frac{2\pi}{3}\right), cis\left(\frac{4\pi}{3}\right)\right\}$.

Hence, the solutions to our original equation are elements of the coset $z_1K = \left\{2cis\left(\frac{\pi}{6}\right), 2cis\left(\frac{5\pi}{6}\right), 2cis\left(\frac{3\pi}{2}\right)\right\}$.

Exercise 4D

1 **a** Show that $f:\{\mathbb{R}\backslash\{0\}, \times\} \to \{\mathbb{R}\backslash\{0\}, \times\}$ is a homomorphism, and determine the kernel, when:

i $f(x) = |x|$ **ii** $f(x) = \frac{1}{x}$

b Show that $f:\{\mathbb{R}, +\} \to \{\mathbb{Z}, +\}$ is not a homomorphism when:

i $f(x) =$ the largest integer $\leq x$ **ii** $f(x) = x + 1$

2 Let $\{\mathbb{R}, +\}$ and $\{C, +\}$ be groups such that C is the set of continuous functions with domain [0, 1]. Show that $f: C \to \mathbb{R}, f(c) = \int_0^1 c(x)dx$ for $c \in C$, is a homomorphism.

3 Given two groups $\{\mathbb{Z}, +\}$ and $\{\mathbb{Z}_2, +_2\}$, show that $f:\mathbb{Z} \to \mathbb{Z}_2$ is a homomorphism if for $x \in \mathbb{Z}$, $f(x) = \begin{cases} 0, & x \in \text{even numbers} \\ 1, & x \in \text{odd numbers} \end{cases}$

4 Prove part 4 of Theorem 4 by mathematical induction.

5 Prove that the composition of homomorphisms is a homomorphism, i.e. if $f:G \to H$ and $g:H \to K$, then $(g \circ f)$: $G \to K$ is a homomorphism.

6 Let f:$\{G, *\} \to \{H, \circ\}$ be a homomorphism. Prove the inverse image of a subgroup of $\{H, \circ\}$ is a subgroup of $\{G, *\}$.

7 Let $f:G \to H$ define a group homomorphism. Let $K = \ker(f)$. Prove $f^{-1}(f(a)) = \{x \in G \mid f(x) = f(a)\}$ is the left coset aK of K and is also the right coset Ka of K, i.e. the two partitions of G into left and right cosets of K are the same. (Hint: Use the double inclusion method for proving two sets are equal.)

4.4 Isomorphisms

In Chapter 3 we saw that there was only one way to construct a Cayley table for a group of order 2 and a group of order 3. In other words, interchanging a row or a column did not change any of the results of the operation. For example, the Cayley table for a group of order 3 is shown next, and beside it is the same table where the columns for elements e and b have been interchanged.

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$
$\boldsymbol{e}$	e	a	b
$\boldsymbol{a}$	a	b	e
$\boldsymbol{b}$	b	e	a

$*$	$\boldsymbol{b}$	$\boldsymbol{a}$	$\boldsymbol{e}$
$\boldsymbol{e}$	b	a	e
$\boldsymbol{a}$	e	b	a
$\boldsymbol{b}$	a	e	b

A quick check of the results of the operations on all elements in the 2nd table will show that the results are the same as those in the 1st table. Therefore we say that the two tables are structurally equivalent.

We now consider the question "How many *different* groups of order 4 are there?" Consider two Cayley tables that you have already seen of two cyclic groups of order 4: $S = \{1, i, -1, -i\}$ under multiplication, and $\{\mathbb{Z}_4, +_4\}$.

$\times$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	-1

$+_4$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$
$\mathbf{0}$	0	1	2	3
$\mathbf{1}$	1	2	3	0
$\mathbf{2}$	2	3	0	1
$\mathbf{3}$	3	0	1	2

Notice the following:

- The orders of the groups are the same.
- The identity is in the first row and column of each table.
- If we consider a function f which maps the elements of the first group to the elements of the second group as follows, $1 \to 0$, $i \to 1$, $-1 \to 2$, $-i \to 3$, we obtain the 2nd table.
- The function f maps the results of the binary operation on the elements of the first table onto the corresponding results of the binary operation in the 2nd table.

To expand upon this last bullet point, let us consider $f(-1\times i)$.
We see that $f(-1 \times i) = f(-i) = 3$, i.e. $f: -i \to 3$.

Furthermore, $f(-1) + f(i) = 2 + 1 = 3$, hence $f(-1 \times i) = f(-1) + f(i)$.
If you test all the other pairs of elements you will see that $f(a \times b) = f(a) + f(b)$, for $a, b \in S$ and $f(a), f(b) \in \mathbb{Z}_4$.

Additionally we can consider the order of the elements in the tables. These tables show the orders of the elements in both groups:

$\{S, \times\}$

element	1	i	-1	$-i$
order	1	4	2	4

$\{\mathbb{Z}_4, +_4\}$

element	0	1	2	3
order	1	4	2	4

As you can see, each of these groups has an identity, one element of order 2, and two generators, i.e. two elements of order 4.
The function f maps $1 \to 0$, $i \to 1$, $-1 \to 2$, $-i \to 3$, i.e. f maps elements whose orders are equal onto each other.

We could reconstruct both tables using one of the generators, e.g. i in the first group and 1 in the second group.

In the first group $e = 1 = i^4$, and the in second group $e = 0 = 1^4$, i.e. $1^4 = 1 + 1 + 1 + 1 = 4(\text{mod}\,4) = 0$.

$\times$	e	i	i^2	i^3
e	e	i	i^2	i^3
i	i	i^2	i^3	e
i^2	i^2	i^3	e	i
i^3	i^3	e	i	i^2

$+_4$	e	1	1^2	1^3
e	e	1	1^2	1^3
1	1	1^2	1^3	e
1^2	1^2	1^3	e	1
1^3	1^3	e	1	1^2

Then, both tables can essentially be expressed by the same table using a generator a, and are structurally equivalent to this table.

$\times$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

We could also have achieved the same effect by mapping the generators differently, e.g. $f: -i \mapsto 1$ and $f: i \mapsto 3$. The identities are still corresponding elements, as well as the only element of order 2 in both groups.
The mapping of these elements remains the same, i.e. $f: 1 \mapsto 0$ and $f: -1 \mapsto 2$.
We leave it to you to construct the Cayley tables using this new mapping, i.e. the row and column of the elements i and $-i$ would need to be interchanged. You will notice again that the new Cayley table is structurally equivalent to the first one we constructed. We conclude that all cyclic groups of order 4 are structurally identical.

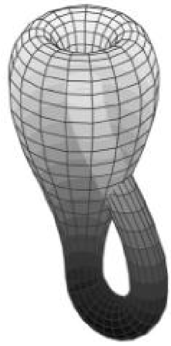
Is there a group of order 4 that is not cyclic, i.e. that is not structurally equivalent to the cyclic group of order 4? Consider the Abelian group in Example 9 from Chapter 3:
$\{S, \times_{12}\}$, $S = \{1, 5, 7, 11\}$. Here is the Cayley table:

$\times_{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

The identity is 1, and the order of the elements 5, 7 and 11 is 2. This group is clearly not cyclic, although it is Abelian. Therefore this group of order 4 is not structurally equivalent to our two cyclic groups of order 4. In group theory this group is called the Klein four-group, or K_V, where the subscript V stands for the German word for four – vier. Its definition is $K_V = \{a,b \mid a^2 = b^2 = (ab)^2 = e\}$. It is the smallest non-cyclic group. Another example of the K_V group is from Chapter 3, Exercise 3B, question 7(b), the symmetries of a rectangle.

This group is structurally equivalent to $\{S, \times_{12}\}$. There are only **two** groups of order 4, the cyclic group and the Klein four-group. All groups of order 4 will be structurally equivalent to one of these two groups, i.e. the cyclic group of order 4 or the K_V group.

? The Klein 4-group is the subgroup V (Vierergruppe) of the permutation group S_4. The group consists of the following 4 permutations written in cycle notation: the identity permutation (1), (12)(34), (13)(24) and (14)(23). The group is named after the German mathematician Felix Klein, who was an early pioneer in Group Theory applied to Geometry. He also devised the famous topological figure, the Klein bottle, an 'impossible' figure with no inside.



We will now define what we mean by 'structurally equivalent'.

Definition

An **isomorphism** is a bijective homomorphism, i.e. given groups $\{G, *\}$ and $\{H, \circ\}$, $f: G \to H$ is an isomorphism if and only if

i f is bijective, and

ii f is a homomorphishm, i.e. for all $a, b \in G$, $f(a * b) = f(a) \circ f(b)$.

In other words, to show that two groups are isomorphic, you must show that the homomorphism is both injective and surjective. The bijection guarantees that the sets have the same size, or cardinality, and the homomorphism guarantees that the groups have the same structure.

As you have already seen, to show that two finite sets are isomorphic we need only show that their Cayley tables are structurally equivalent, i.e. their tables can be shown to be structurally the same by rearranging or swapping columns or rows.

We will next show a worked-out example for finite sets.

Example 9

a Determine if any of the following three groups are isomorphic by constructing their Cayley tables.

- $\{\mathbb{Z}_{6,}\ +_6\}$
- Symmetries of an equilateral triangle as defined in Chapter 3, on page 101, i.e. $S = \{I, R_1, R_2, A, B, C\}$
- $\{\mathbb{Z}_7 \backslash \{0\}, \times_7\}$

b Reconstruct the Cayley table(s) to show the equivalent structure of the isomorphic groups.

a Creating the Cayley tables for each group:

$+_6$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\circ$	$\boldsymbol{I}$	$\boldsymbol{R_1}$	$\boldsymbol{R_2}$	$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{C}$
$\boldsymbol{I}$	I	R_1	R_2	A	B	C
$\boldsymbol{R_1}$	R_1	R_2	I	C	A	B
$\boldsymbol{R_2}$	R_2	I	R_1	B	C	A
$\boldsymbol{A}$	A	B	C	I	R_1	R_2
$\boldsymbol{B}$	B	C	A	R_2	I	R_1
$\boldsymbol{C}$	C	A	B	R_1	R_2	I

$\times_7$	**1**	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

All three groups have the same order. Since $\{S, \circ\}$ is not Abelian, and the other two groups are, the only possibility for an isomorphism is between $\{\mathbb{Z}_6, +_6\}$ and $\{\mathbb{Z}_7\backslash\{0\}, \times_7\}$.

Notice the structures of the Cayley table, e.g. Abelian.

The orders of the elements in each table are:

$a \in \mathbb{Z}_6$	0	1	2	3	4	5
order	1	6	3	2	3	6
$b \in \mathbb{Z}_7$	1	2	3	4	5	6
order	1	3	6	3	6	2

Determine the orders of the elements in both groups.

The groups are cyclic. The identities are corresponding elements, hence 0 ↔ 1. The only elements of order 2 are also corresponding elements, so 3 ↔ 6.
Mapping the generators 1 ↔ 3 and 5 ↔ 5 leaves two possible mappings for the remaining elements: 2 ↔ 2 and 4 ↔ 4, or 2 ↔ 4 and 4 ↔ 2.
Mapping the generators 1 ↔ 5 and 5 ↔ 3 again leaves the two possible mappings of 2 ↔ 2 and 4 ↔ 4, or 2 ↔ 4 and 4 ↔ 2.

Map elements of similar orders.

b Using the first mapping, we can leave $+_6$ as is, and reconstruct the $\times_7$ table.

Rearrange one of the tables so that the corresponding elements are in the same positions.

$\times_7$	**1**	**3**	**2**	**6**	**4**	**5**
1	1	3	2	6	4	5
3	3	2	6	4	5	1
2	2	6	4	5	1	3
6	6	4	5	1	3	2
4	4	5	1	3	2	6
5	5	1	3	2	6	4

How many groups of order 6 are there? You have worked with the cyclic group of order 6 above. In Chapter 3 you worked with the symmetries of the equilateral triangle, and saw that it formed a non-Abelian group of order 6. From a previous theorem we know that if a group is cyclic, it must be Abelian, or if a group is not Abelian, it cannot be cyclic. Again as with order 4, there are two distinct groups of order 6.

We can classify finite groups by isomorphism classes, i.e. the number of distinct groups of a particular order.

- All groups of prime order are cyclic, hence there is only one class of groups whose order is a given prime number.
- There are two distinct groups or classes of order 4 and order 6: one cyclic group and one non-cyclic group.
- There are five distinct groups of order 8, three of which are cyclic.
- There are two distinct groups of order 9, and both are cyclic.
- There are two distinct groups of order 10, one cyclic and one non-cyclic.

Although none of the above results are needed for examination purposes, you might want to research this further and investigate how many classes of groups there are of a given order greater than 11.

We shall now illustrate an example showing an isomorphism between infinite sets.

Example 10

Show that the mapping $f : x \to 2^x$ from the set of integers $\mathbb{Z}$ to the set $S = \left\{\cdots \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\right\}$ is an isomorphism between the groups $\{\mathbb{Z}, +\}$ and $\{S, \times\}$.

Since $f(x + y) = 2^{x+y} = 2^x \times 2^y = f(x) \times f(y)$, f defines a homomorphism between the two groups.

Show that f is a homomorphism, i.e. determine if f maps the sum of two elements in $\mathbb{Z}$ to the product of two elements in S.

Show that f is bijective, i.e. injective and surjective.

Method I
f is injective if $f(a) = f(b) \Rightarrow a = b$.
$2^a = 2^b \Rightarrow a = b$, hence f is injective.

Method II
To show f is injective, we can make use of Theorem 5, showing that the unique solution of $f(x) = e_s$ is $e_{\mathbb{Z}}$. Assume that the solution is not unique, i.e. $x \neq y$ such that $f(x) = e_s$ and $f(y) = e_s$.

Hence, $2^x = 2^y \Rightarrow x = y$, which is a contradiction. Therefore the solution is unique, and is $e_{\mathbb{Z}} = 0$.

f is surjective if for every $b \in S$ there exists an $a \in \mathbb{Z}$ such that $f(a) = b$. If $2^a = b \Rightarrow a = \frac{\log b}{\log 2} = \log_2 b \in \mathbb{Z}$.

Hence f is bijective.

Therefore f is an isomorphism.

We see therefore from Example 10 that to show $f:\{G, *\} \to \{H, \circ\}$ is an isomorphism, we need to show that:

- f is a homomorphism
- $\ker(f) = e_G$, i.e. f is injective.
- f is surjective.

Since an isomorphism is a homomorphism, all the properties of a homomorphism will apply. In addition to these, there is another important property specific to isomorphisms which you will already have observed in the examples so far.

Theorem 7

If $f: \{G, *\} \to \{H, \circ\}$ is an isomorphism, the order of $a \in G$ is equal to the order of $f(a) \in H$ for every $a \in G$.

Proof:

Let n be the order of a. Therefore by definition, n is the smallest positive integer such that $a^n = e$. Then:

$$(f(a))^n = f(a) \circ f(a) \circ \ldots \circ f(a)$$

$$= f(\underbrace{a * a * \ldots * a}_{n\,times}) \text{ by definition of isomorphism,}$$

$$= f(a^n)$$

$$= f(e_G)\text{, since the order of } a \text{ is } n$$

$$= e_H$$

We now must show that n is the least positive integer such that $(f(a))^n = e_H$. Let the order of $f(a)$ be m, $m < n$. Then, by definition, $(f(a))^m = e_H$.

Hence, e_H is the image of both a^n and a^m. Since $a^m = a^n = e_G$, and n is the smallest such integer, then this is a contradiction with the assumption that $m < n$. Hence $n \leq m$ and the order of $a \in G$ is the same as the order of $f(a) \in H$.

This property is very useful for showing that two groups are not isomorphic, i.e. if the orders of the elements of the groups do not match, then the groups are not isomorphic. The following example illustrates how to use this property.

Example 11

Determine whether or not $\{\mathbb{R}, +\}$ and $\{\mathbb{C} \setminus \{0\}, \times\}$ are isomorphic.	
The only element in $\mathbb{R}$ with finite order is the identity, 0, whose order is 1. In $\mathbb{C} \setminus \{0\}$, the identity 1 has order 1, and the element -1 has order 2, i.e. there are at least two elements with finite order. Hence, the groups are not isomorphic.	*Determine if all elements in both groups have the same orders.*

Is the converse of this theorem true, i.e. if the orders of the elements of two groups are the same, are the groups isomorphic? This is not true, and the smallest group with this property has order 16, i.e. there exist two groups of order 16 whose elements have the same orders but which are not isomorphic. You may want to research this very important result further.

Exercise 4E

1 Determine which of the following groups of order 6 are isomorphic.

a The symmetry group of the equilateral triangle

b The set $\{1, 2, 4, 5, 7, 8\}$ under $\times_9$

c The set $\{2, 4, 6, 8, 10, 12\}$ under $\times_{14}$

d The permutation group with the following elements:

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix};\ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix};\ p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix};\ p_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix};\ p_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

2 Prove that the mapping $f : \mathbb{R}^+ \to \mathbb{R}, f(x) = \ln x$, is an isomorphism between the groups $\{\mathbb{R}^+, \times\}$ and $\{\mathbb{R}, +\}$.

3 Prove that the mapping $f : x \mapsto x^{-1}$ is an isomorphism of a group $\{G, *\}$ onto itself if and only if $\{G, *\}$ is Abelian.

4 Let $\{H, \circ\}$ be a subgroup of $\{G, *\}$, and let $M = \{x^{-1}hx \mid h \in H\}$ be a subset of G for some given element $x \in G$.

a Prove that M is closed under the operation $*$ of the group G and that each element of M has an inverse under $*$ in M.
Hence, deduce that M is a subgroup.

b Show that M is isomorphic to H.

5 Let (ab) denote a cycle defined by the permutation $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$

a Consider the permutations on the set $\{1, 2, 3, 4\}$. Let $p_1 = (1)$, $p_2 = (12)(34)$, $p_3 = (13)(24)$ and $p_4 = (14)(23)$ be four of these permutations. Write out the Cayley table for the set $P = \{p_1, p_2, p_3, p_4\}$ under composition of permutations.

b Prove that $\{P, \circ\}$ is an Abelian group.

c Determine whether or not $\{P, \circ\}$ is isomorphic to $\{\mathbb{Z}_4, +_4\}$.

6 Given that two groups $\{G, *\}$ and $\{H, \circ\}$ are isomorphic, prove that $\{G, *\}$ is Abelian if and only if $\{H, \circ\}$ is Abelian.

Review exercise

EXAM-STYLE QUESTIONS

1. **a** Let G be a group of order 6 such that it contains no elements of order 6. State Lagrange's theorem and hence prove by contradiction that at least one of the elements will have order 3.

b Let G be of order n, and g be an element of G that has order k. Write down a cyclic subgroup of order k and use Lagrange's theorem to show that $g^n = e$.

2 **a** Let $\{\mathbb{Z}_n, +_n\}$ be the cyclic group of integers under $+_n$. Write down the elements of this group, and identify a generator for the group.

b Let $\{\mathbb{C}_n, \times\}$ be the group whose elements are the nth roots of unity under multiplication. Write down the elements of this group, and show that the group is cyclic. Write down a generator of the group.

c Show that $f:\{\mathbb{Z}_n, +_n\} \to \{\mathbb{C}_n, \times\},\ f(x) = \mathrm{e}^{\frac{2ix\pi}{n}},\ x \in \mathbb{Z}_n$ is an isomorphism.

3 Let G be a set of isomorphic groups, i.e. $G_1 \equiv G_2$ (G_1 is isomorphic to G_2) for all $G_1, G_2 \in G$. If $f: G_1 \to G_2$, show that the relation on G defined by $\equiv$ is an equivalence relation.

4 Prove that the mapping $f: x \mapsto x^2$ is an isomorphism of a group $\{G, *\}$ if and only if $\{G, *\}$ is Abelian.

5 Prove that if $f:\{G, *\} \to \{G, *\}$ is a homomorphism with kernel K then $f(x) = f(y)$ if and only if $y = xk$ for some $k \in K$.

6 Let G be the group of permutations S_3 and H is a subgroup of G such that $H = \{(1), (12)\}$. Find the left and right cosets of H in G.

7 Let G be a group. Prove that the relation on G defined as $xRy \Leftrightarrow x = y$ or $x = y^{-1}$ is an equivalence relation, and write down the equivalence classes.

8 Prove that the groups $\{\mathbb{R}, +\}$ and $\{\mathbb{R}^+, \times\}$ are isomorphic.

9 **a** Show that $\{S, \times\}$, $S = \{2^a 3^b \mid a, b = \mathbb{Z}\}$, $a, b \in \mathbb{Z}$ forms a group.

b Show that $\{S, \times\}$ is isomorphic to the group $\{\mathbb{C}, +\}$, $\mathbb{C} = \{a + bi \mid a, b \in \mathrm{Z}, i = \sqrt{-1}\}$.

10 Express $p = (13256)(23)(46512)$ as a product of disjoint cycles.

11 Explain why $f: \mathbb{Z}_{12} \to \mathbb{Z}_{10}$, $f(x) = 3x \pmod{10}$ is not a homomorphism.

12 Given the permutation group S_3, find a subgroup $\{H, \circ\}$ and an element of g such that $gH \neq Hg$.

13 Let $G = \{\mathbb{R} \backslash \{0\}, \times\}$.

a Show that $f: x \mapsto x^n$ is a homomorphism for all $n \in \mathbb{Z}^+$.

b Determine $\ker(f_n)$.

c Determine n so that the mapping is an isomorphism.

14 Let S be the set of polynomials in x with real coefficients under addition. Define the mapping $f: p(x) \mapsto P(x) = \int p(x)\,dx$ such that $P(0) = 0$.

Show that f is a homomorphism, and determine its kernel.

Chapter 4 summary

A permutation of a non-empty finite set A is a **bijection** from A to A.

Theorem 1: Let A be a non-empty set of n elements, and let S_n be the set of all permutations of A. Then S_n forms a group under composition of permutations.

Let A be the finite set $\{1, 2, 3, \ldots, n\}$. The group of all permutations of A is the **symmetric group** on n elements and is denoted by S_n.

Permutations and cycle form

- Every permutation can be written as a product of disjoint cycles.
- Disjoint cycles are commutative.
- The order of a permutation written as a product of disjoint cycles is the least common multiple of the lengths of the cycles.

Let $\{H, *\}$ be a subgroup of $\{G, *\}$ and let $x \in G$. Then the set of elements $xH = \{xh \mid h \in H\}$ is called a **left coset** of $\{H, *\}$ in G. The set of elements $Hx = \{hx \mid h \in H\}$ is called a **right coset** of $\{H, *\}$ in G.

Properties of cosets: For any subgroup $\{H, \circ\}$ of a group $\{G, \circ\}$:

1. G is the union of disjoint cosets of $\{H, \circ\}$.
2. Every coset (left or right) of a subgroup $\{H, \circ\}$ has the same number of elements as H.
3. The group is partitioned by the left (or right) cosets of its subgroup.
4. Every element of G lies in one of the cosets of H in G.

Lagrange's theorem: If $\{H, \circ\}$ is a subgroup of $\{G, \circ\}$, then the order of the subgroup $\{H, \circ\}$ is a divisor of the order of $\{G, \circ\}$.

Corollaries to Lagrange's theorem:

1. The order of an element of a finite group divides the order of the group.
2. Every group of prime order is cyclic.

Let $\{G, *\}$ and $\{H, \circ\}$ be groups. A **homomorphism** is a function $f: G \to H$ such that $f(x * y) = f(x) \circ f(y)$ for all $x, y \in G$.

Properties of homomorphisms: Let f be a homomorphism from group $\{G, *\}$ to group $\{H, \circ\}$. Let a be an element in G. Then the following properties hold.

1. The homomorphism maps the identity in group G onto the identity in group H, i.e. if e_G and e_H are the identity elements in $\{G, *\}$ and $\{H, \circ\}$ respectively, then $f(e_G) = e_H$.
2. The homomorphism maps the inverse of an element in group G to the inverse of the element's image in group H, i.e. for all $a \in G, f(a^{-1}) = (f(a))^{-1}$.
3. The range of the homomorphism f is a subgroup of $\{H, \circ\}$, i.e. for $f(G) = \{f(a) \mid a \in G\}$, $\{f(a), \circ\}$ is a subgroup of $\{H, \circ\}$.
4. The homomorphism preserves all powers, i.e. $f(a^n) = (f(a))^n$ for all $a \in G$.

Theorem: A homomorphism $f:\{G, *\} \rightarrow \{H, \circ\}$ is injective if and only if the unique solution to $f(x) = e_H$ is $x = e_G$.

Given the group homomorphism $f:\{G, *\} \rightarrow \{H, \circ\}$ the **kernel** of f, ker(f), is defined as the set of all elements of G which are mapped to e_H , i.e. $\ker(f) = \{a \in G \mid f(a) = e_H\}$

Theorem: The kernel of a homomorphism $f:\{G, *\} \rightarrow \{H, \circ\}$ is a subgroup of G.

Given the groups $\{G, *\}$ and $\{H, \circ\}$, $f: G \rightarrow H$ is an **isomorphism** if and only if

i f is bijective, and
ii f is a homomorphism, i.e. for all $a, b \in G, f(a * b) = f(a) \circ f(b)$.

Theorem: If $f:\{G, *\} \rightarrow \{H, \circ\}$ is an isomorphism, the order of $a \in G$ is equal to the order of $f(a) \in H$.

Answers

Chapter 1

Skills check

1 **a** 24

Exercise 1A

1 **a** $A \setminus B = \{b, c, d\}$

b $B \setminus A = \{i, o, u\}$

c $A \, \Delta \, B = \{b, c, d, i, o, u\}$

d $(A \cap B) \setminus (A \cap C) = \{a, e\}$

e $A \cap (B \cup C) = \{a, b, c, d, e\}$

Exercise 1B

1 Many examples possible, such as:
$P = \{\{\text{red cards}\}, \{\text{black cards}\}\}$
$P = \{\{\text{number cards}\}, \{\text{picture cards}\}\}$

2 **a** P is a partition.

b Q is not a partition.

c B is not a partition since 2 is an element of both sets.

3 **a** Partition **b** Partition **c** Partition

4 Many examples possible such as

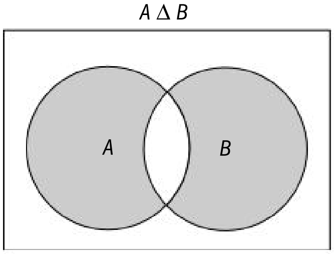
a $\{\{x \in \mathbb{N}, x \le 10\}, \{x \in \mathbb{R} \mid x \notin \{0, 1, 2, 3, \ldots, 10\}\}\}$
or $\{\{\pi, e\}, \{x \in \mathbb{R} \mid x \ne \pi, x \ne e\}\}$

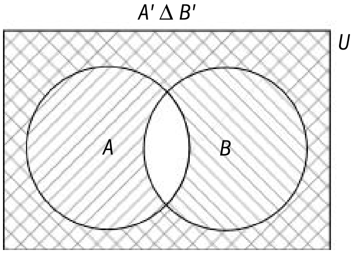
b $\{\{x \mid x \in \mathbb{Z}\}, \{x \mid x \in \mathbb{R}, x \notin \mathbb{Z}\}\}$
or $\{\{\text{primes}\}, \{x \mid x \in \mathbb{R}, x \text{ is not a prime number}\}\}$

c $\{\ldots, [-3, -2[, [-2, -1[, [-1, 0[, [0, 1[, [1, 2[, [2, 3[, \ldots\}$

Exercise 1C

6 **a**





Exercise 1D

1 $A \times B = \{(1, p), (1, q), (2, p), (2, q), (3, p), (3, q)\}$
$B \times A = \{(p, 1), (p, 2), (p, 3), (q, 1), (q, 2), (q, 3)\}$
The two products are not equal since the Cartesian product is made up of ordered pairs and hence $(1, q) \ne (q, 1)$ etc…

2 **a** Tabulate the Cartesian product $A \times B$

$A \times B$	1	2	3	4	5	6
1	**(1, 1)**	**(1, 2)**	**(1, 3)**	**(1, 4)**	(1, 5)	(1, 6)
2	**(2, 1)**	**(2, 2)**	**(2, 3)**	**(2, 4)**	(2, 5)	(2, 6)
3	**(3, 1)**	**(3, 2)**	**(3, 3)**	**(3, 4)**	(3, 5)	(3, 6)
4	**(4, 1)**	**(4, 2)**	**(4, 3)**	**(4, 4)**	(4, 5)	(4, 6)

The ordered pairs in bold represent $A \times A \subset A \times B$

b **i** $R = \{(1, 1), (1, 2), (1, 4), (1, 6), (2, 1), (2, 3), (2, 5), (3, 2), (3, 4), (4, 1), (4, 3)\}$

ii $R = \{(1, 1), (2, 4)\}$

iii $R = \{(1, 3), (1, 4), (1, 6), (2, 4), (2, 5), (3, 5), (3, 6), (4, 6)\}$

iv $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (4, 1), (4, 2)\}$

3 $A \times B = \{(a, p), (a, q), (b, p), (b, q)\}$
$n(A \times B) = 4 \Rightarrow n(P(A \times B)) = 2^4 = 16$

4 **a** $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$
$A \times C = \{(a, 3), (a, 4), (b, 3), (b, 4)\}$
$(A \times B) \cap (A \times C) = \{(a, 3), (b, 3)\}$

b $B \cap C = \{3\}$
$\Rightarrow A \times (B \cap C) = \{(a, 3), (b, 3)\}$

c $(A \times B) \cap (A \times C) = A \times (B \cap C)$

5 $A \times C = \{(a, c) \mid a \in A, c \in C\}$
$B \times C = \{(b, c) \mid b \in B, c \in C\}$
Since $A \subset B$ it follows that $a \in A \Rightarrow a \in B$
$\Rightarrow (a, c) \in B \times C$ for all $a \in A, c \in C$.
Therefore $A \times C \subset B \times C$.

6 List the Cartesian product $S \times S$

$S \times S$	0	2	4	6	8
0	**(0, 0)**	**(0, 2)**	**(0, 4)**	**(0, 6)**	**(0, 8)**
2	(2, 0)	**(2, 2)**	**(2, 4)**	**(2, 6)**	**(2, 8)**
4	(4, 0)	(4, 2)	**(4, 4)**	**(4, 6)**	**(4, 8)**
6	(6, 0)	(6, 2)	(6, 4)	**(6, 6)**	**(6, 8)**
8	(8, 0)	(8, 2)	(8, 4)	(8, 6)	**(8, 8)**

The elements of R are the ordered pairs in bold.

10 $R = \{(2, 1), (4, 2), (8, 3), (16, 4), (32, 5), (64, 6), (128, 7), (256, 8), (512, 9), (1024, 10)\}$

$xR^{-1}y \Rightarrow y = \log_2 x = \frac{\ln x}{\ln 2}$

$n(R^{-1}) = 10$

Exercise 1E

1 Since R is reflexive, symmetric and transitive it follows that it is an equivalence relation.

2 Since R is reflexive, symmetric and transitive it follows that it is an equivalence relation.

3 Since R is not transitive it follows that it is not an equivalence relation.

4 Since R is not reflexive and not transitive it follows that it is not an equivalence relation.

5 Since R is reflexive, symmetric and transitive it follows that it is an equivalence relation.

9 One example from not reflexive or not symmetric is enough to show that R is not an equivalence relation.

10 Since R is reflexive, symmetric and transitive it follows that it is an equivalence relation

Exercise 1F

1 a The equivalence classes induced by R:

[set] = {set, car, sea, sun}
[bike] = {bike, wave}
[table] = {table, chair}
[tennis] = {tennis, stairs}

b The equivalence classes induced by R:

[set] = {set, stairs, sea, sun}
[table] = {table, tennis}
[chair] = {chair, car}
[bike] = {bike}
[wave] = {wave}

2 a R partitions the set of line segments into sets of segments of equal length.

b R partitions the set of all polygons into sets of polygons with same number of sides, i.e. {triangles}, {quadrilaterals}, etc…

3 R partitions the set of parabolas into sets containing parabolas with vertex tangent to the line $y = c$.

4 The relation partitions $\mathbb{R} \times \mathbb{R}$ into concentric circles with centre at the origin.

5 Equivalence classes:

$[1] = \{x \mid x + 2 = 3k,\ k \in \mathbb{Z}^+\} = \{1, 4, 7, 10, \ldots\}$

$[2] = \{x \mid x + 4 = 3k,\ k \in \mathbb{Z}^+,\ k \geq 2\} = \{2, 5, 8, \ldots\}$

$[3] = \{x \mid x + 6 = 3k,\ k \in \mathbb{Z}^+,\ k \geq 3\} = \{3, 6, 9, \ldots\}$

6 Equivalence classes

$[1] = \{x \mid x^2 - 1 = 3k,\ k \in \mathbb{Z}^+\} = \{1, 2, 4, 5, 7, 8, 10, 11 \ldots\}$

$[3] = \{x \mid x^2 - 3 = 3k,\ k \in \mathbb{Z}^+\} = \{3, 6, 9, 12, 15 \ldots.\}$

7 R partitions the Cartesian plane into lines parallel to the y-axis.

8 $[(1, 2)] = \{(x, y) \mid 2x = y\} = \{(1, 2), (2, 4), (3, 6), (4, 8) \ldots\}$

$[(a, b)] = \{(x, y) \mid bx = ay\} = \{(x, \frac{b}{a}x)\}$, which represents sets of straight lines passing through the origin.

9 $[(1, 1)] = \{(x, y) \mid xy = 1\} = \{(x, \frac{1}{x}) \mid x \in \mathbb{R} \setminus \{0\}\}$

$[(a, b)] = \{(x, y) \mid xy = ab\} = \{(x, \frac{ab}{x}) \mid x \in \mathbb{R} \setminus \{0\}\}$, which represents a set of rectangular hyperbolas with the x and y axes as asymptotes.

10 b $[0] = \{x \mid x - 0 \in \mathbb{Z}\} = \mathbb{Z}$

c $\left[\frac{3}{4}\right] = \left\{x \mid x - \frac{3}{4} = n,\ n \in \mathbb{Z}\right\}$

$= \left\{\ldots, \frac{-9}{4}, \frac{-5}{4}, \frac{-1}{4}, \frac{3}{4}, \frac{7}{4}, \frac{11}{4}, \ldots\right\}$

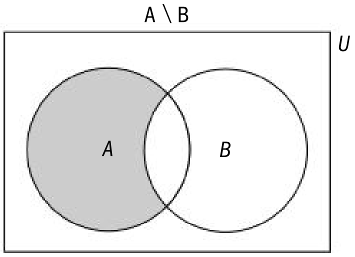
d $\left[\frac{a}{b}\right] = \left\{x \mid x - \frac{a}{b} = n,\ n \in \mathbb{Z}\right\}$

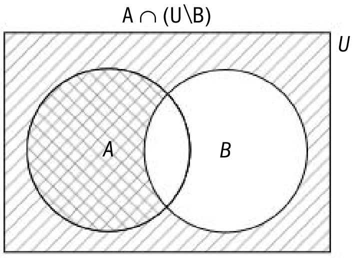
$= \left\{x \mid x = \frac{nb + a}{b},\ n \in \mathbb{Z}\right\}$

R partitions $\mathbb{Q}$ into fractions with denominator b and numerator an infinite arithmetic progression depending on a and with common difference b.

Review Exercise

1 i





In the lower of the two diagrams above, the area shaded in both directions represents $A \cap (U \setminus B)$.

ii Similarly, Venn diagrams demonstrating two expressions that are each the symmetric difference of A and B.

2 Venn Diagrams suitably drawn to show

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

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

3 b The relation R partitions the Argand diagram into lines passing through the origin, since for every each particular angle, θ, all the complex numbers having θ as an argument lie on a straight line passing through the origin and make an angle θ with the positive real axis.

4 a $A = \{2, 3, 5, 7, 11, 13, 17, 19\}$
$B = \{1, 2, 3\}$
C = $\{0, 1, 2, 3\}$
$D = \{-2, 0, 2\}$
$E = \{-1, 0, 1, 2, 3\}$

b i True because $n(A) = 8$, $n(D) = 3$, $n(E) = 5$

ii False because $D \cap A' = \{-2, 0\}$
$\Rightarrow n(D \cap A') = 2$

iii True as evident from list above.

iv True $D \setminus B = \{-2, 0\}$ and neither of these elements are in A

v False $C \,\Delta\, E = (C \cup E) \setminus (C \cap E) = \{-1\}$

5 a i R is not reflexive

ii R is symmetric

iii R is not transitive.

b R is not an equivalence relation because it is not reflexive and it is also not transitive.

6 a Since R is reflexive, symmetric and transitive it is an equivalence relation.

b i $C_0 = [0] = \{x \mid x^3 \equiv 0 (\text{mod } 5)\} = \{5, 10, 15, 20 \ldots\}$

ii $C_1 = [1] = \{x \mid x^3 \equiv 1 (\text{mod } 5\} = \{x \mid x^3 = 5k + 1\}$
$= \{6, 11, 16, 21, 26, 31, \ldots\}$

7 a ii $[z^2 - 3z + 4]$ consists of all polynomials of the form $z^2 - 3z + c$

b ii $[z^2 - 3z + 4]$ consists of all polynomials of the form $z^2 + bz + 4$

8 b $[2] = \{2, 4, 6, \ldots\}$
$[1] = \{1, 3, 5, 7 \ldots\}$

c $5^{355} \equiv 5 (\text{mod } 8)$

9 b First consider the equivalence class $[(a, 0)]$ where a is a constant

$[(a, 0)] = \{(x, y) \mid x = a, y - 0 = 5k\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$

$[(a, 1)] = \{(x, y) \mid x = a, y - 1 = 5k\} = \{\ldots, -14, -9, -4, 1, 6, 11, \ldots\}$

$[(a, 2)] = \{(x, y) \mid x = a, y - 2 = 5k\} = \{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}$

$[(a, 3)] = \{(x, y) \mid x = a, y - 3 = 5k\} = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}$

$[(a, 4)] = \{(x, y) \mid x = a, y - 4 = 5k\} = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}$

10 S is not transitive.

11 b $\overrightarrow{AB}\ R\ \overrightarrow{CD}$ if and only if $\overrightarrow{AB}$ and $\overrightarrow{CD}$ are parallel line segments of the same length and oriented in the same direction. Thus an equivalence consists of all translations of a given directed line segment.

Chapter 2

Skills Check

1 a $0 < t < 3$ **b** $t > 3$

2 a $f^{-1}(x) = \dfrac{(3 - 2x)}{(x - 1)}$ where $x \neq 1$ **b** $f^{-1}(x) = \dfrac{\ln x}{\ln 2}$

c $f^{-1}(x) = \ln\left(\frac{1}{2}\left(x + \sqrt{x^2 + 8}\right)\right)$

Exercise 2A

2 a Not a function **b** Not a function
c Not a function

3 a Is a function **b** Not a function
c Not a function

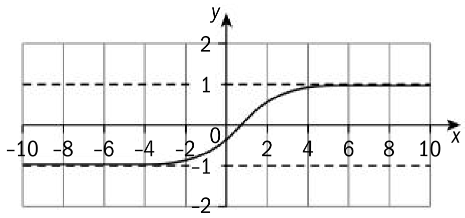
5 a not surjective **b** injective

6 i injective, not surjective
ii injective, not surjective
iii injective and surjective

8 i surjective, not injective
ii surjective, not injective
iii not surjective, not injective

9 a Range $-1 < f(x) < 1$

b



10 a f is not surjective **b** f is injective
c g is surjective **d** g is injective

Exercise 2B

1 $g \circ f(a,b) = b$

3 a i $f \circ g(x) = x^2$ **ii** $g \circ f(x) = 2x$

b $f \circ g$ is not injective and not surjective $g \circ f$ is injective and surjective

4 a $f^{-1}(n, 1) = n + 1$

c $f \circ g(n, m) = (n + m - 1, 1)$, $g \circ f(n) = n$

5 a not injective and not surjective therefore not bijective.

b $f \circ f(x, y) = (xy(x + y), x + xy + y)$

6 b $f \circ g(x) = \dfrac{1}{1-x}$ $g \circ f(x) = \dfrac{x-1}{x}$

d f and g are both self inverses

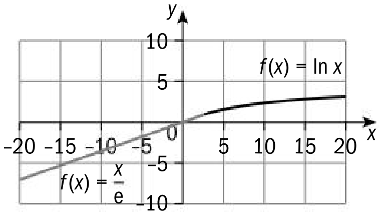
e $f \circ g$ and $g \circ f$ are inverses of each other

7 b $f^{-1}(x, y) = \left(\sqrt[3]{\dfrac{y}{x}}, x\sqrt[3]{\dfrac{y}{x}}\right)$

8 a $f'(x) = 8e^{2x} > 0$ for all $x \in [1, \infty[$

b $f^{-1}(x) = \ln\left(\sqrt{\dfrac{x+3}{4}}\right)$

9 a



b The function is steadily increasing over the whole range and so it is a bijection.

c $f^{-1}(x) = \begin{cases} ex & x \le 1 \\ e^x & x > 1 \end{cases}$

10 a i $\mathbb{Z}$ **ii** $\{0\}$

b -1

c $k = 1 \Rightarrow$ solutions $(1, 0)$ and $(-1, 0)$

$k = 2 \Rightarrow$ no solutions

11 a $16 - n \pmod 8 = -n \pmod 8$

b $\left|\dfrac{n}{2} - 8\right|$ if n is even

$|n - 7|$ if n is odd

c $8 - \dfrac{n}{2}$ if n is even

$17 - n$ if n is odd

d $-\dfrac{n}{2} \pmod 8$ if n is even

$1 - n \pmod 8$ if n is odd

e $|-n \pmod 8 - 8|$

f $\left|\dfrac{n}{2}\right|$ if n is even

$|9 - n|$ if n is odd

12 a $e^{(\ln(2x-1))^2}$ **b** $\ln(2e^{x^2} - 1)$

c $2 \ln (2x - 1)$ **d** $e^{4(\ln(2x-1))^2}$

e $2e^{(\ln(2x-1))2}$

Exercise 2C

1 a $(f \circ g)(x) = x - 2, (g \circ f)(x) = x + \dfrac{2}{3}$, *no*

b $(f \circ g)(x) = x, (g \circ f)(x) = x$, *yes*

c $(f \circ g)(x) = x, (g \circ f)(x) = x$, *yes*

2 a $f^{-1}(x) = e^x$

b $f^{-1}(x) = \begin{cases} x & \text{if } x \text{ is rational} \\ -x & \text{if } x \text{ is irrational} \end{cases}$

3 a i $(f \circ g)^{-1}(x) = \arccos(\ln x)$

ii $(g^{-1} \circ f^{-1})(x) = \arccos(\ln x)$

Exercise 2D

1 a Binary operation – not closed

b Binary operation – closed

c Binary operation – closed

d Binary operation – closed

2 S is not closed under addition or multiplication or division

3 i A is closed under addition and multiplication

ii B is not closed under addition but closed under multiplication

4

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Closed

$\circ$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Closed

5 X is closed under addition

X is closed under subtraction

X is closed under composition

6

$\times$	-1	1	i	$-i$
-1	1	-1	$-i$	i
1	-1	1	i	$-i$
i	$-i$	i	-1	1
$-i$	i	$-i$	1	-1

7 $\mathbb{Z}^+$ is closed under $*$

8

$*$	1	2	3
1	1	1	1
2	3	4	5
3	5	7	9

Not closed

$\circ$	1	2	3
1	1	1	2
2	1	1	2
3	2	2	4

Not closed

9 Not closed under addition
Closed under multiplication

10 a $S \times S = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

b

*	1	2
1	3	6
2	6	12

Not closed

c

∘	(1, 1)	(1, 2)	(2, 1)	(2, 2)
(1, 1)	(3, 3)	(3, 6)	(6, 3)	(6, 6)
(1, 2)	(3, 6)	(3, 12)	(6, 6)	(6, 12)
(2, 1)	(6, 3)	(6, 6)	(12, 3)	(12, 6)
(2, 2)	(6, 6)	(6, 12)	(12, 6)	(12, 12)

Exercise 2E

1 a not commutative not associative
b commutative not associative
c not commutative not associative

3

∘	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

From Cayley table we can see that S is closed because every element in Cayley table is in S. Composition of functions is commutative because the main diagonal of the Cayley table is a line of symmetry.

4 a not commutative **b** not associative.

Exercise 2F

1	commutative	associative	$e = 0$
2	commutative	associative	$e = (1, 1)$
3	commutative	associative	$e = (0, 0)$
4	not commutative	associative	$e = (1, 0)$
5	commutative	associative	no identity

Exercise 2G

1 b Identity = −1
c Inverse $a^{-1} = -a - 2$

2 c Identity = 1
d Inverse $(a + bi)^{-1} = \dfrac{a - bi}{a^2 + b^2}$

3

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The main diagonal is a line of symmetry, so the operation is commutative.

Identity $e = 0$
Inverse of 0 is 0
Inverse of 1 is 3
Inverse of 2 is 2
Inverse of 3 is 1

4 a

	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

Identity $e = 6$
Inverse of 6 is 6
Inverse of 2 is 8
Inverse of 4 is 4
Inverse of 8 is 2

b Identity $e = 2$
Inverse $a^{-1} = \dfrac{4}{a}$

c There is no identity.

6 b $-a$

Review Exercise

3 Bijection

$$f^{-1}(x, y) = \left(\frac{x}{\sqrt{(1 - y^2)}}, \arcsin y\right)$$

4 Identity $e = (1, 0)$

6 a Not injective and not surjective.
b The function f becomes invertible when the domain is restricted to $[0, \pi)$ and the co-domain to $[\frac{1}{2}, \frac{19}{6}]$.

$$f^{-1}(x) = \arccos\left(\frac{\ln(x - \frac{1}{6})}{\ln 3}\right)$$

7 a i commutative
ii associative
b Identity $e = 0$

8 a Range $\left[1 + \frac{1}{e^2}, 1 + e^2\right]$

b i Not injective since $f(x) = f(x + 2n\pi)$, $n \in \mathbb{Z}$.
ii Not surjective since the range of $f(x) \neq \mathbb{R}$ e.g. there is no $x \in \mathbb{R}$ such that $f(x) = 10$.

c i $k = \pi$, $A = \left[1 + \frac{1}{e^2}, 1 + e^2\right]$

ii $g^{-1}(x) = \arccos\left(\ln\sqrt{x - 1}\right)$

iii $x \in \left[1 + \frac{1}{\mathrm{e}^2}, 1 + \mathrm{e}^2\right]$

Chapter 3

Skills check

1 **a** $f(g(x)) = \ln(x^2+1)$ **b** $|f(g(x))|^{-1} = \sqrt{e^x - 1}$

c $g(f(x)) = [\ln(x+1)]^2$ **d** $f^{-1}(g^{-1}(x)) = e^{\sqrt{x}} - 1$

2 **a** The binary operation on the given set is closed. No other properties hold.

b The binary operation on the given set is closed and commutative.

c The binary operation on the given set is closed and commutative.

Exercise 3A

3 **a** not a group
b not a group
c is a group
d is a group

4 **c** $\frac{5}{3}$

5 **b** **i** (1, 2) **ii** (0.75, 2.8)
c not Abelian

Exercise 3B

1 **a**

$*$	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

b **i** y **ii** e

2 **a** **i** e **ii** e

iii b **iv** c

b The identity element is a.

c right inverses

x	a	b	c	d	e
x^{-1}	a	d	b	c	e

left inverses

x	a	b	c	d	e
x^{-1}	a	c	d	b	e

d Left and right inverses are not equal; $*$ is not associative.

4 $\{\mathbb{Z}_5, +_5\}$:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\{\mathbb{Z}_5 \setminus \{0\}, \times_5\}$:

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

a $x = 4$ **b** $x = 4$ **c** $x = 3$
d $x = 1$ **e** $x = 2$

5

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

It does form an Abelian group.

6 ± 1; $\pm\frac{1}{2}(1 + i\sqrt{3})$; $\pm\frac{1}{2}(1 - i\sqrt{3})$

7 **a** R = reflection in the median
$I = R^2$

$\circ$	I	R
I	I	R
R	R	I

b Symmetries of the Rectangle
I: Identity Transformation
X: Reflection in the x-axis
Y: Reflection in the y-axis
H: Rotation of 180 degrees about its center.

$\circ$	I	X	Y	H
I	I	X	Y	H
X	X	I	H	Y
Y	Y	H	I	X
H	H	Y	X	I

c Symmetries of a cuboid
I: Identity transformation
X: Reflection in the y-z plane
Y: reflection in the x-z plane
Z: reflection in the x-y plane
H_1: rotation of 180 degrees about x-axis
H_2: rotation of 180 degrees about y-axis
H_3: rotation of 180 degrees about z-axis
C: central inversion

$\circ$	I	X	Y	Z	H_1	H_2	H_3	C
I	I	X	Y	Z	H_1	H_2	H_3	C
X	X	I	H_3	H_2	C	Z	Y	H_1
Y	Y	H_3	I	H_1	Z	C	X	H_2
Z	Z	H_2	H_1	I	Y	X	C	H_3
H_1	H_1	C	Z	Y	I	H_3	H_2	X
H_2	H_2	Z	C	X	H_3	I	H_1	Y
H_3	H_3	Y	X	C	H_2	H_1	I	Z
C	C	H_1	H_2	H_3	X	Y	Z	I

9

$+_2$	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

$\{\mathbb{Z}_2 \times \mathbb{Z}_2, +_2\}$ does form a group.

Exercise 3C

3 b x^3

Exercise 3D

1 a $\{\varnothing, A\}$; $\{\varnothing, B\}$; $\{\varnothing, C\}$

b $\{p, r\}$

c Symmetries of the Rectangle
I: identity Transformation
X: Reflection in the x-axis
Y: Reflection in the y-axis
H: Rotation of 180 degrees about its center.

$\circ$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	H	Y
Y	Y	H	I	X
Z	H	Y	X	I

Subgroups: $\{I, X\}$; $\{I, Y\}$; $\{I, H\}$

d $\{8, 10\}$; $\{4, 10, 16\}$

e $\{0, 3\}$; $\{0, 2, 4\}$

2 a

a	1	2	4	7	8	11	13	14
a^{-1}	1	8	4	13	2	11	7	14
order	1	4	2	4	4	2	4	2

b $a = 4$; $b = 8$

c $\{1, 4, 7, 13\}$ or $\{1, 4, 11, 14\}$

Exercise 3E

4 a 20; (0, 1) **b** (1, 1); (1, 2)

c 4 elements have order 4: (0, 1); (0, 3); (1, 1); (1, 3)

Review exercise

1 a 1 **b** $x = -\frac{7}{4}$

3 a $x = a^{-1}cb^{-1}$ **b** $x = b^{-1}a$

5 a $f_4(x) = 1 - \frac{1}{x}$; $f_5(x) = \frac{-1}{x-1}$; $f_6(x) = \frac{x}{x-1}$

b Let $f_1 = 1$; $f_2 = 2$; etc.

$\circ$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	5	1	6	2	4
4	4	6	2	5	1	3
5	5	3	6	1	4	2
6	6	4	5	2	3	1

c

f	1	2	3	4	5	6
order	1	2	2	3	3	2

d $\{f_1, f_4, f_5\}$

7 a order = 3; order = 12; order = 4

b 1, 5, 7 and 11

8 b The operation # is closed, associative and has an identity $e = -1$. Not all elements have inverses.

10 Order of the group is 6.
Subgroups: $\{e\}$, $\{e, a, a^2\}$; $\{e, b\}$; $\{e, ab\}$; $\{e, a^2b\}$; $\{e, a, a^2, b, ab, a^2b\}$

11 Many answers possible, such as:

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	c	d	f	b
b	b	c	e	f	a	d
c	c	d	f	e	b	a
d	d	f	a	b	e	c
f	f	b	d	a	c	e

The Latin Square is not associative.

Chapter 4

Skills check

1 **a** R partitions $\mathbb{Z}$ into two sets: even integers and odd integers.

b Each ordered pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ belongs to an equivalence class consisting of all ordered pairs with integer coordinates lying on a vertical line passing through (a, b).

c The partition of S induced by R is $\{\{1, 5, 9\}, \{2, 6, 10\}, \{3, 7\}, \{4, 8\}\}$

3 **a** not bijective

b $f^{-1}(a,b)=\left(\dfrac{2a+b}{5},\dfrac{a-2b}{5}\right)$

Exercise 4A

2 3

3 $\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$

Both $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ and $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ are generators.

4 **a** **i** $\sigma\tau=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$

ii $\tau\sigma=\begin{pmatrix}1&2&3&4&5\\1&4&5&2&3\end{pmatrix}$

iii $\sigma^2\tau=\begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}$

iv $\sigma\upsilon^{-1}=\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}$

v $(\sigma\upsilon)^{-1}=\begin{pmatrix}1&2&3&4&5\\4&1&3&2&5\end{pmatrix}$

vi $\upsilon^{-1}\sigma\upsilon=\begin{pmatrix}1&2&3&4&5\\5&4&2&1&3\end{pmatrix}$

b **i** $x=\begin{pmatrix}1&2&3&4&5\\5&2&3&1&4\end{pmatrix}$

ii $x=\begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix}$

Exercise 4B

1 **a** $x = (1645)(23)$; $y = (13)(24)(5678)$; $z = (23)(45)(67)$

b $x^{-1} = (1546)(23)$; $y^{-1} = (13)(24)(5876)$; $z^{-1} = (23)(45)(67)$

c order = 4; order = 4; order = 2

2 **a** $\begin{pmatrix}1&2&3&4&5&6\\2&3&1&6&5&4\end{pmatrix}$

b $\begin{pmatrix}1&2&3&4&5&6&7\\2&1&4&5&3&7&6\end{pmatrix}$

c $\begin{pmatrix}1&2&3&4&5&6&7&8\\1&4&7&5&2&6&8&3\end{pmatrix}$

d $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&2&4&5&7&8&3&9&6\end{pmatrix}$

3 **a** (163)(24)

b (1236)(45)

c (1632)(45)

d (1632)(45)

Exercise 4C

2 **a** Left cosets: $4\mathbb{Z}$; $1 + 4\mathbb{Z}$; $2 + 4\mathbb{Z}$; $3 + 4\mathbb{Z}$
Right cosets are the same as the left cosets.

b Left cosets: $4\mathbb{Z}$; $2 + 4\mathbb{Z}$
Right cosets are the same as the left cosets.

c $H = \{0, 4, 8\}$
Left cosets: H; $1 + H = \{1, 5, 9\}$; $2 + H = \{2, 6, 10\}$; $3 + H = \{3, 7, 11\}$
Right cosets are the same as left cosets.

d

$x \in G$	Left coset xH	Right coset Hx
(1)	{(1), (12)}	{(1), (12)}
(13)	{(13), (123)}	{(13), (132)}
(23)	{(23), (132)}	{(23), (123)}

3 **a** $H = \{(0, 0), (1, 0)\}$; $\mathbb{Z}_2$ x $\mathbb{Z}_3 = \{(0, 0), (1, 0), (0, 1), (1, 1), (0, 2), (1, 2)\}$

b Left cosets: $H = \{(0, 0), (1, 0)\}$;
$(0, 1) + H = \{(0, 1), (1, 1)\}$;
$(0, 2) + H = \{(0,2), (1,2)\}$.
Right cosets are the same as the left cosets.
Left and right cosets are equal: $\mathbb{Z}_2 \times \{0\}$; $\mathbb{Z}_2 \times \{1\}$; $\mathbb{Z}_2 \times \{2\}$

Exercise 4D

1 **a** **i** $\{-1,1\}$ **ii** $\{1\}$

Exercise 4E

1 a and d; b and c

5 **a** Let $p_1 = 1$; $p_2 = 2$; $p_3 = 3$; $p_4 = 4$

∘	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

c The groups are not isomorphic.

Review exercise

2 **a** $\{0, 1, 2, \ldots, n-1\}$; 1 is a generator.

b $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$; ω is a generator.

6 right cosets: $\{e, (12)\}$; $\{(13), (132)\}$; $\{(23), (123)\}$
left cosets: $\{e, (12)\}$; $\{(13), (123)\}$; $\{(23), (132)\}$

7 $[x] = \{x, x^{-1}\}$

10 (124)(35)

12 $H = \{(1), (12)\}$ and $g(13)$, for example.

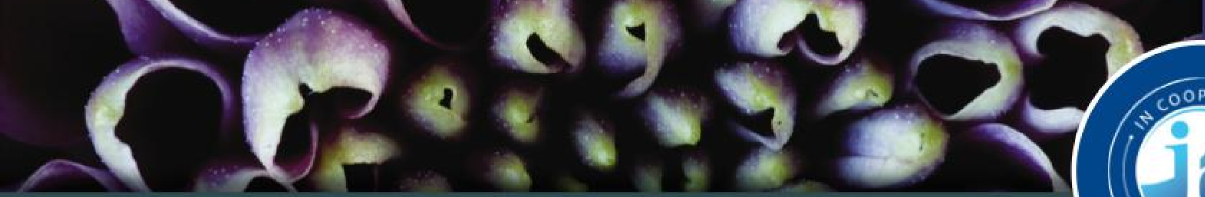
13 **b** $\ker(f_n) = \begin{cases} \{1\} \text{ if } n \text{ is odd} \\ \{1, -1\} \text{ if } n \text{ is even} \end{cases}$

c f_n is an isomorphism when n is odd.

14 ker(f) only contains the zero polynomial.

Index

Page numbers in *italics* refer to review exercises.



MATHEMATICS HIGHER LEVEL: SETS, RELATIONS AND GROUPS

The **most comprehensive and accurate** coverage of the Sets, Relations and Groups Option for HL, with unrivalled support straight from the IB. Offering a rigorous approach and supported by a **full set of worked solutions online**, this book will **fully challenge** learners to drive top achievement.

Oxford course books are the only DP resources developed with the IB. This means that they are:

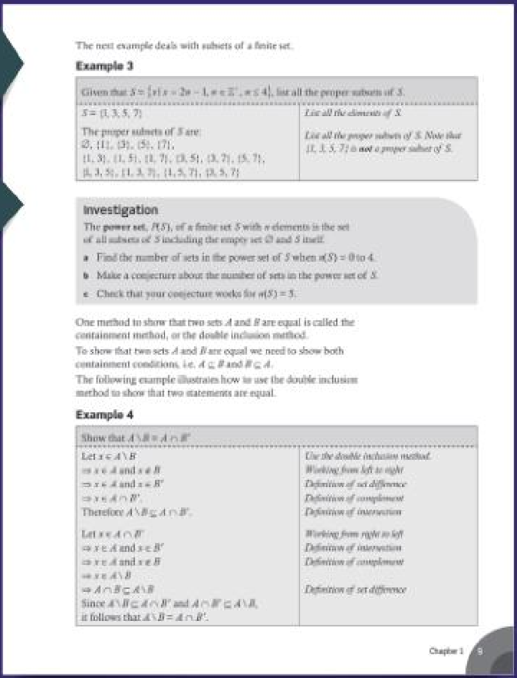
- The **most accurate** match to IB specifications
- Written by expert and experienced IB examiners and teachers
- Packed with accurate **assessment support, directly from the IB**
- Truly aligned with the IB philosophy

Authors
Josip Harcet
Lorraine Heinrichs
Palmira Mariz Seiler
Marlene Torres-Skoumal

Free support material online at
www.oxfordsecondary.co.uk/ibmathhl

Extensive **challenge material** thoroughly **stretches learners**, supporting the highest levels of comprehension

Examples and investigations help to put complex theory into practice



The next example deals with subsets of a finite set.

Example 3

Given that $S = \{x \mid x = 2n - 1, n \in \mathbb{Z}^+, n \le 4\}$, list all the proper subsets of S.	
$S = \{1, 3, 5, 7\}$	*List all the elements of S.*
The proper subsets of S are: $\varnothing$, $\{1\}$, $\{3\}$, $\{5\}$, $\{7\}$, $\{1, 3\}$, $\{1, 5\}$, $\{1, 7\}$, $\{3, 5\}$, $\{3, 7\}$, $\{5, 7\}$, $\{1, 3, 5\}$, $\{1, 3, 7\}$, $\{1, 5, 7\}$, $\{3, 5, 7\}$	*List all the proper subsets of S. Note that {1, 3, 5, 7} is **not** a proper subset of S.*

Investigation

The **power set**, $P(S)$, of a finite set S with n elements is the set of all subsets of S including the empty set $\varnothing$ and S itself.

a Find the number of sets in the power set of S when $n(S) = 0$ to 4.

b Make a conjecture about the number of sets in the power set of S.

c Check that your conjecture works for $n(S) = 5$.

One method to show that two sets A and B are equal is called the containment method, or the double inclusion method.

To show that two sets A and B are equal we need to show both containment conditions, i.e. $A \subseteq B$ and $B \subseteq A$.

The following example illustrates how to use the double inclusion method to show that two statements are equal.

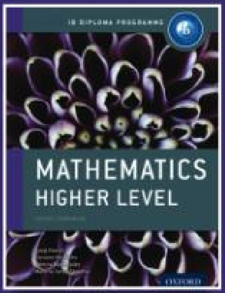
Example 4

Show that $A \setminus B = A \cap B'$	
Let $x \in A \setminus B$	*Use the double inclusion method.*
$\Rightarrow x \in A$ and $x \notin B$	*Working from left to right*
$\Rightarrow x \in A$ and $x \in B'$	*Definition of set difference*
$\Rightarrow x \in A \cap B'$.	*Definition of complement*
Therefore $A \setminus B \subseteq A \cap B'$.	*Definition of intersection*
Let $x \in A \cap B'$	*Working from right to left*
$\Rightarrow x \in A$ and $x \in B'$	*Definition of intersection*
$\Rightarrow x \in A$ and $x \notin B$	*Definition of complement*
$\Rightarrow x \in A \setminus B$	
$\Rightarrow A \cap B \subseteq A \setminus B$	*Definition of set difference*
Since $A \setminus B \subseteq A \cap B'$ and $A \cap B' \subseteq A \setminus B$, it follows that $A \setminus B = A \cap B'$.	

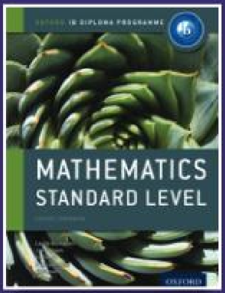
Chapter 1 9

Also available

978 0 19 839012 1



978 0 19 839011 4



OXFORD
UNIVERSITY PRESS

How to get in contact:
web www.oxfordsecondary.co.uk/ib
email schools.enquiries.uk@oup.com
tel +44 (0)1536 452620
fax +44 (0)1865 313472

ISBN 978-0-19-830486-9

9 780198 304869