Groups

2

Objectives

After completing this chapter you should be able to:

- know and be able to use the axioms for a group → pages 00–00
- be able to use Cayley tables and describe properties of cyclic groups → pages 000–00
- be able to identify the order of an element and that of a group → pages 000–000
- be able to identify subgroups of a group → pages 00–00
- be able to use Lagrange's theorem → pages 00–00
- Be able to recognise and describe isomorphism between two groups → pages 00–00

Analysis of the symmetry groups of molecules has led to the discovery of new molecular structures such as carbon nanotubes, the strongest and stiffest material known to man.

Prior knowledge check

1 The functions f and g are defined as

$$\mathrm{f}(x) = x^2 + 1, x \in \mathbb{R}$$

$$\mathrm{g}(x) = |x - 3|, x \in \mathbb{R}$$

Find: **a** fg(2) **b** gf(2)

← Pure Year 2, Chapter 2

2 Find $n \in \{0, 1, 2, 3, 4, 5, 6\}$ such that:

a $12 \equiv n \pmod 7$ **b** $3^3 \equiv n \pmod 7$

c $2n \equiv 1 \pmod 7$ **d** $6^{99} \equiv n \pmod 7$

← Section 1.3

3 $\mathbf{M} = \begin{pmatrix} 4 & 1 \\ -1 & 3 \end{pmatrix}$ and $\mathbf{N} = \begin{pmatrix} 5 & 0 \\ 2 & 1 \end{pmatrix}$. Find:

a $\mathbf{MN}$ **b** $\det \mathbf{N}$ **c** $\mathbf{N}^{-1}$

← Core Pure Book 1, Chapter 6

4 Write down the 2 × 2 matrix corresponding to:

a a reflection in the x-axis

b a rotation through 90° anticlockwise about the origin. ← Core Pure Book 1, Chapter 7

2.1 The axioms for a group

You have encountered sets of numbers previously in your course, but a set can be any collection of distinct objects.

- **A binary operation on a set is a calculation that combines two elements of the set to produce another element of the set.**

Some binary operations occur naturally in mathematics. For example, the operation of addition (+) on the set of integers, $\mathbb{Z}$, is a binary operation, as it combines two integers to produce a third integer.

Similarly, matrix multiplication is a binary operation on the set of 2 × 2 matrices with real elements.

Notation $S = \{a, b, c, \ldots\}$ means that the set S contains the elements, $a, b, c, \ldots$ You can write $a \in S$ to show that a, for example, is a member of S.

Watch out The **order** in which the elements of the set are combined in a binary operation is important. For example, subtraction (–) forms a binary operation on the set of real numbers, but in general $a - b \neq b - a$.

Example 1

$S = \{x + y\sqrt{3} : x, y \in \mathbb{Z}\}$

Show that addition is a binary operation on S.

Let $s_1 = a + b\sqrt{3}$, $s_2 = c + d\sqrt{3}$ where $a, b, c, d \in \mathbb{Z}$.

Define two elements of the set.

$s_1 + s_2 = a + b\sqrt{3} + c + d\sqrt{3} = (a + c) + (b + d)\sqrt{3}$

Add the elements.

As $a, b, c, d \in \mathbb{Z}$, $a + c \in \mathbb{Z}$ and $b + d \in \mathbb{Z}$.

Use properties of integers to show that the sum is also a member of S.

So $s_1 + s_2 \in S$, and therefore addition is a binary operation on S.

Notation You can say that the set S is **closed** under addition.

Example 2

Show that the set of natural numbers, $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$, is not closed under subtraction.

For example, $4, 5 \in \mathbb{N}$, but $4 - 5 = -1 \notin \mathbb{N}$

You only need to find one counter-example to show that $\mathbb{N}$ is **not** closed under subtraction.

For the set of integers, $\mathbb{Z}$, and the binary operation of addition, the number 0 has the property that for any integer $a \in \mathbb{Z}$, $a + 0 = a$. You say that 0 is an **identity element** of $\mathbb{Z}$ under addition.

- **An identity element of a set S under a binary operation $*$ is an element $e \in S$ such that, for any element $a \in S$, $a * e = e * a = a$.**

Notation Binary operations do not always have to correspond to familiar operations such as +, −, × or ÷. You sometimes use the symbols $*$ or $\circ$ to denote an unfamiliar or general binary operation.

An identity element depends on both the set and the binary operation, and does not necessarily exist. For example, the set of natural numbers ℕ does not contain 0, so does not have an identity element under addition. However, the number $1 \in \mathbb{N}$ satisfies $a \times 1 = 1 \times a = a$, so ℕ does have an identity element under multiplication.

Example 3

Prove that an identity element of a set S under a binary operation must be unique.

Let $*$ denote the binary operation on S.

Assume that there are two distinct identity elements, $e, f \in S$

Use proof by contradiction. ← Pure Year 2, Section 1.1

$e * f = f$

e is an identity element and $f \in S$ so $e * f = f$.

$e * f = e$

Similarly, because f is an identity element, $e * f = e$.

So $e = f$, which contradicts the fact that e and f are distinct.

So it is impossible for a set to contain two distinct identity elements, and the identity element is unique.

The set of integers ℤ under the binary operation of addition has identity element 0. The integers 4 and −4, for example, are such that $-4 + 4 = 4 + (-4) = 0$. You say that 4 and −4 are **inverse** elements of each other.

- **Let S be a set and $*$ be a binary operation on S. If an identity element e exists, and there exist elements $a, b \in S$ such that $a * b = b * a = e$, then a is the inverse of b and b is the inverse of a.**

Notation You can write $b = a^{-1}$ and $a = b^{-1}$.

Example 4

The binary operation $*$ on the set of real numbers is defined as $a * b = a + b + ab$.

a Find a real number e that satisfies the property $a * e = a$.

The real number m has inverse m^{-1} that satisfies the property $m * m^{-1} = e$.

b Express m^{-1} in terms of m.

a $a * e = a$

Set up and solve an equation.

$\Rightarrow a + e + ae = a$

$\Rightarrow e + ae = 0$

$\Rightarrow e(1 + a) = 0$

$\Rightarrow e = 0$

0 is the identity element for this binary operation on ℝ.

b $m * m^{-1} = 0$

$\Rightarrow m + m^{-1} + mm^{-1} = 0$

$\Rightarrow m + (1 + m)m^{-1} = 0$

So $m^{-1} = -\dfrac{m}{m+1}$, $m \neq -1$

The real number −1 has no inverse under this binary operation.

Consider three elements of $\mathbb{Z}$ under the binary operation of addition. For example, $6, 3, 99 \in \mathbb{Z}$:

$$6 + (3 + 99) = 6 + 102 = 108$$
$$(6 + 3) + 99 = 9 + 99 = 108$$

So $6 + (3 + 99) = (6 + 3) + 99$. This is an example of the **associative** property of addition.

- **A binary operation $*$ on a set S is associative if, for any $a, b, c \in S$,**

  $$a * (b * c) = (a * b) * c$$

Example 5

A binary operation on $\mathbb{R}$ is defined by $a \circ b = ab + 1$.

Show that $\circ$ is not associative.

Consider the elements $2, 3, 4 \in \mathbb{R}$.

$$2 \circ (3 \circ 4) = 2 \circ (3 \times 4 + 1)$$
$$= 2 \circ 13$$
$$= 2 \times 13 + 1 = 27$$
$$(2 \circ 3) \circ 4 = (2 \times 3 + 1) \circ 4$$
$$= 7 \circ 4$$
$$= 7 \times 4 + 1 = 29$$

So $2 \circ (3 \circ 4) \neq (2 \circ 3) \circ 4$, so the operation $\circ$ is not associative.

Problem-solving

In order for the operation $\circ$ to be associative, it must satisfy $a \circ (b \circ c) = (a \circ b) \circ c$ for **any** $a, b, c \in \mathbb{R}$. If you can find three real numbers which do not satisfy this condition, then you have shown that $\circ$ is not associative.

Write a conclusion.

You can use the properties of binary operations to define a **group**.

- **If G is a set and $*$ is a binary operation defined on G, then $(G, *)$ is a group if the following four axioms hold:**
  - **Closure: for all $a, b \in G$, $a * b \in G$**
  - **Identity: there exists an identity element $e \in G$, such that for all $a \in G$, $a * e = e * a = a$**
  - **Inverses: for each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$**
  - **Associativity: for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$**

Watch out A group is a set **together with** a binary operation that satisfies these four axioms. A set on its own is not a group.

Example 6

Show that:

a the set of integers forms a group under addition

b the set of integers does not form a group under multiplication.

a **Closure:** The sum of two integers is an integer, so the set is closed under addition.

Identity: For all $n \in \mathbb{Z}$, $n + 0 = n = 0 + n$. $0 \in \mathbb{Z}$ so there is an identity element.

Inverses: For all $n \in \mathbb{Z}$, $n + (-n) = (-n) + n = 0$. $-n \in \mathbb{Z}$ so $-n$ is the inverse of n.

Associativity: $a + (b + c) = a + b + c = (a + b) + c$ for all $a, b, c \in \mathbb{Z}$.

Hence the set of integers forms a group under addition.

b For all $n \in \mathbb{Z}$, $n \times 1 = 1 \times n = n$.

So the identity element is 1.

0 is an integer, but there is not an integer n such that $0 \times n = 1$.

The inverse axiom fails, so the set of integers does not form a group under multiplication.

Notation You can write this group as $(\mathbb{Z}, +)$.

List each axiom and explain why it holds for integers under addition.

Watch out Check that inverse elements are members of the set. If the question was about 'positive integers', then the negative of each integer would not be a member of the set.

It is possible to prove associativity more formally. In your exam, you will be told if you can assume that the associativity axiom holds. → **Exercise 2A, Challenge**

Problem-solving

You only need to show that one of the four axioms fails. For the inverse axiom to hold, **every** element in the set must have an inverse. You could also say that there is no integer n such that $2 \times n = 1$.

Example 7

The operation $*$ is defined by $a * b = a + b - 1$, where a and b are real numbers.

Determine whether the set of real numbers under the operation $*$ forms a group.

Closure: The real numbers are closed under addition and subtraction, so $a + b - 1$ is a real number.

Identity: $a * 1 = a + 1 - 1 = a$

$1 * a = 1 + a - 1 = a$

1 is a real number.

So the identity element is 1.

Inverses: $a * (2 - a) = a + (2 - a) - 1 = 1$

$(2 - a) * a = (2 - a) + a - 1 = 1$

If a is a real number , then $2 - a$ is a real number.

The inverse of each element a is $2 - a$.

Associativity:

$$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1$$
$$= a + b + c - 2$$
$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1$$
$$= a + b + c - 2$$

Therefore $*$ is associative.

Hence the set of real numbers form a group under $*$.

Watch out You must check that that the identity works when applied in either direction, so that $a * e = e * a = a$

Remember to show inverses in both directions.

Show that the associativity axiom holds.

All four group axioms hold, so $(\mathbb{R}, *)$ is a group.

Example 8

Prove that, for all elements a, b in a group $(G, *)$, there exists a unique element c such that $a * c = b$.

Existence: Let $c = a^{-1} * b$

$a^{-1} \in G$ (by inverse axiom) and $a^{-1} * b \in G$ (by closure axiom)

Then $a * c = a * (a^{-1} * b) = (a * a^{-1}) * b$ (by associativity axiom)

$$= e * b = b$$

Uniqueness: Assume there is a distinct element $d \in G$ which also satisfies $a * d = b$.

Then $d = e * d = (a^{-1} * a) * d = a^{-1} * (a * d)$ (by associativity axiom)

$$= a^{-1} * b$$
$$= a^{-1} * (a * c)$$
$$= (a^{-1} * a) * c$$
$$= e * c = c$$

So $d = c$, which is a contradiction, so c must be unique.

Start by proving that such an element exists, and then prove that it must be unique.

$b = a * c$

Notation Similarly, there is a unique element $f \in G$ which satisfies $f * a = b$. These two properties are called the **latin square** property, and are important when constructing Cayley tables. → **Section 2.2**

Exercise 2A

1 $S = \{x + y\sqrt{3} : x, y \in \mathbb{Z}\}$

Determine whether each of the following is a binary operation on S.

a subtraction **b** multiplication

c division

Hint You need to determine whether S is closed under each operation.

2 Determine whether each set is closed under the operation $*$.

a positive integers, $x * y = \dfrac{x!y!}{xy}$ **b** real numbers, $x * y = \sqrt{x + y}$

c odd numbers, $x * y = x^2 y$ **d** complex numbers, $x * y = |x| + |y|$

3 For the set $\mathbb{C}$ of complex numbers under the binary operation of multiplication,

a state the identity element

b find the inverse of $1 + \mathrm{i}$, giving your answer in the form $a + \mathrm{i}b$.

4 For the set of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $a \in \mathbb{R}$, $a \neq 0$, under matrix multiplication,

a state the identity element **b** find the inverse of $\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$

5 Determine whether each of the following operations is associative over the real numbers.

a $x * y = xy^2$ **b** $x * y = 3^{xy}$

c $x * y = |x| + |y|$ **d** $x * y = xy + x + y$

6 Determine whether each of the following pairs of sets and operations form a group. You may assume that the real numbers are associative over addition and multiplication.

Hint **Positive** means that 0 is excluded.

a positive real numbers, × **b** integers, ÷

c odd integers, + **d** even integers, ×

e real numbers, − **f** positive rational numbers, ÷

P **7** The operation $*$ on the set of rational numbers, $\mathbb{Q}$, is defined by $a * b = \dfrac{ab}{a+b}$

a Prove that $\mathbb{Q}$ is closed under $*$.

b Show that this binary operation does not have an identity element.

E/P **8** The operation $*$ on the set of positive integers $\mathbb{Z}^+$ is defined by $a * b = a + b - 2$.

a Determine whether or not $*$ is:

i closed **ii** associative. **(3 marks)**

b **i** Find the identity element for $*$.

ii Hence show that $\mathbb{Z}^+$ does not form a group under $*$. **(4 marks)**

Problem-solving Find an element of $\mathbb{Z}^+$ that does not have an inverse.

E/P **9** The operation $*$ is defined by $a * b = ab + a$, where a and b are real numbers. Show that $\mathbb{R}$ does not form a group under *. **(4 marks)**

E/P **10** Show that the set of integer-valued 2 × 2 matrices forms a group under addition. You may assume that addition of integers is associative. **(5 marks)**

E/P **11** Show that the set of 2 × 2 diagonal matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \neq 0$, forms a group under matrix multiplication. **(4 marks)**

E/P **12** Let M be the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$, and $a \neq 0$ and $c \neq 0$.

Prove that M is a group under matrix multiplication. **(6 marks)**

E/P **13** Show that the set of functions of the form $f(x) = ax + b$, where $a, b \in \mathbb{R}$ and $a \neq 0$, forms a group under function composition. **(6 marks)**

E/P **14** Prove that for any element a in a group, the inverse of a is unique. **(2 marks)**

P **15** Prove that for all elements a, b in a group $(G, *)$,

a $(a^{-1})^{-1} = a$ **b** $(a * b)^{-1} = b^{-1} * a^{-1}$

E/P **16** A set G forms a group under the operation of multiplication. For $a, b \in G$, prove that $a^2b^2 = (ab)^2 \Rightarrow ab = ba$ **(3 marks)**

Problem-solving Multiply by a^{-1} on the left and b^{-1} on the right.

E/P **17** A group $(G, \circ)$ contains elements a and b such that a and b are self-inverse.
Given that $a \circ b = b \circ a$, prove that $a \circ b$ is also self-inverse. **(4 marks)**

Problem-solving An element of a group x is **self-inverse** if $x = x^{-1}$.

Challenge

The set $\mathbb{N}^0$ is the natural numbers including 0. The **Peano axioms** for defining this set are:

1 $0 \in \mathbb{N}^0$

2 For any $a \in \mathbb{N}^0$ there exists a **successor** $\text{S}(a) \in \mathbb{N}^0$.

3 0 is not the successor of any number.

4 For $m, n \in \mathbb{N}^0$, $m = n \Leftrightarrow \text{S}(m) = \text{S}(n)$

5 If a set N contains 0, and $a \in N \Rightarrow \text{S}(a) \in N$, then $N = \mathbb{N}^0$.

a Prove that $\mathbb{N}^0$ must contain an infinite number of elements.

You can define **addition** (+) on the set $\mathbb{N}^0$ as follows.

For any $a, b \in \mathbb{N}^0$,

6 $a + 0 = a$

7 $a + \text{S}(b) = \text{S}(a + b)$

b Using this definition of addition, prove by induction that, for any $a, b, c \in \mathbb{N}^0$, $(a + b) + c = a + (b + c)$

Problem-solving

The Peano axioms are a formal way of defining natural numbers:

$1 = \text{S}(0)$

$2 = \text{S}(1) = \text{S}(\text{S}(0))$

$3 = \text{S}(2) = \text{S}(\text{S}(\text{S}(0)))$

and so on.

2.2 Cayley tables and finite groups

In the previous section, all the groups you considered contained an infinite number of elements. A **finite group** contains only a finite number of elements in its underlying set.

You can represent a finite group in a **Cayley table**.

- **A Cayley table fully describes the structure of a finite group by showing all possible products of elements of the group.**

Here is part of a Cayley table for a group with underlying set $\{a, b, c, \ldots\}$ and operation $*$.

$*$	a	b	c	…
a		↓		
b		↓		
c	→	d		
⋮				

All the elements of the underlying set are written as row and column headings (in the same order).

The element corresponding to $c * b$ is at the intersection of the row containing c with the column containing b. In this case, $c * b = d$.

Watch out The row heading is always the first element in the operation, and the column heading is the second element in the operation.

Example 9

The set $\{1, -1, \mathrm{i}, -\mathrm{i}\}$, where $\mathrm{i}^2 = -1$, forms a group under multiplication.

a Draw a Cayley table for this group.

b Write down:

i the identity element **ii** the inverse of i **iii** the inverse of -1

a

×	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

b i 1 is the identity

ii −i

iii −1

$-1 \times (-\mathrm{i}) = \mathrm{i}$, so the entry at this position is i.

Problem-solving

The entries in the Cayley table are all members of the underlying set $\{1, -1, \mathrm{i}, -\mathrm{i}\}$. This shows that the set is closed under multiplication.

The entries in the row corresponding to 1 are the same as the corresponding column headings, and similarly for the column corresponding to 1. This shows that $1 \times a = a \times 1 = a$ for all elements a, so 1 is the identity.

Look for the identity in the row corresponding to i, then read off the corresponding column heading.

The properties of groups give rise to corresponding properties of Cayley tables:

- **When a group's elements are displayed in a Cayley table, then:**
  - **all entries must be members of the group**
  - **every entry appears exactly once in every row and every column**
  - **the identity element must appear in every row and column**
  - **the identity elements are symmetric across the leading diagonal**

This is a consequence of the latin square property of groups. ← **Example 8**

Because every element has an inverse.

Because $a^{-1} * a = a * a^{-1}$ for every element in a group.

Modular arithmetic groups

You can use modular arithmetic to define finite groups on sets of integers. You will need to use the operations of **multiplication modulo *n*** and **addition modulo *n***.

- **The operation $\times_n$ of multiplication modulo *n* is defined on integers *a* and *b* as the remainder when *ab* is divided by *n*.**
- **The operation $+_n$ of addition modulo *n* is defined on integers *a* and *b* as the remainder when $a + b$ is divided by *n*.**

Notation You can use $\equiv_n$ to show multiplication or addition modulo n. For example,
$4 \times 3 \equiv_{10} 2$, because $4 \times 3 \equiv 2 \pmod{10}$
$6 + 5 \equiv_7 4$, because $6 + 5 \equiv 4 \pmod 7$
← **Section 1.3**

The Cayley tables below show the set {0, 1, 2, 3, 4} under the actions of addition and multiplication modulo 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

$\times_5$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2 × 4 = 8 and 8 ≡ 3 (mod 5)

Example 10

The set $S = \{0, 1, 2, 3, 4\}$. Use the Cayley tables above to determine whether S forms a group under:

a addition modulo 5 **b** multiplication modulo 5

a **Closure:** All elements are members of S, so the set is closed under addition modulo 5.

Identity: The identity element is 0.

Inverses: Since 0 appears in every row and every column, then every element has an inverse.

For example, the inverse of 2 is 3.

Associativity: Addition on the integers is associative, so addition modulo 5 is associative.

Hence $(S, +_5)$ is a group.

b The identity element is 1.

1 does not appear in the 0 row, or the 0 column. $(S, \times_5)$ is not a group since 0 does not have an inverse.

Problem-solving

You can see from the Cayley table that the set {1, 2, 3, 4} **does** form a group under multiplication modulo 5.

Example 11

$S = \{1, 3, 7, 9\}$. Determine whether each of the following are groups. You may assume that the associative law holds in each case.

a $(S, \times_{10})$ **b** $(S, \times_{12})$

a Construct a Cayley table

$\times_{10}$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Closure: From the table, the set is closed under multiplication modulo 10.

Identity: The identity element is 1 since $1 \times a = a \times 1 = a$ for all $a \in S$.

Inverses: 1 and 9 are self-inverse, and 7 is the inverse of 3 and vice versa.

Associativity: Assumed

Hence $(S, \times_{10})$ is a group.

b $1 \times 3 \equiv_{12} 3$

$3 \times 3 \equiv_{12} 9$

$7 \times 3 \equiv_{12} 9$

$9 \times 3 \equiv_{12} 3$

So 3 has no inverse, so S is not a group under $\times_{12}$.

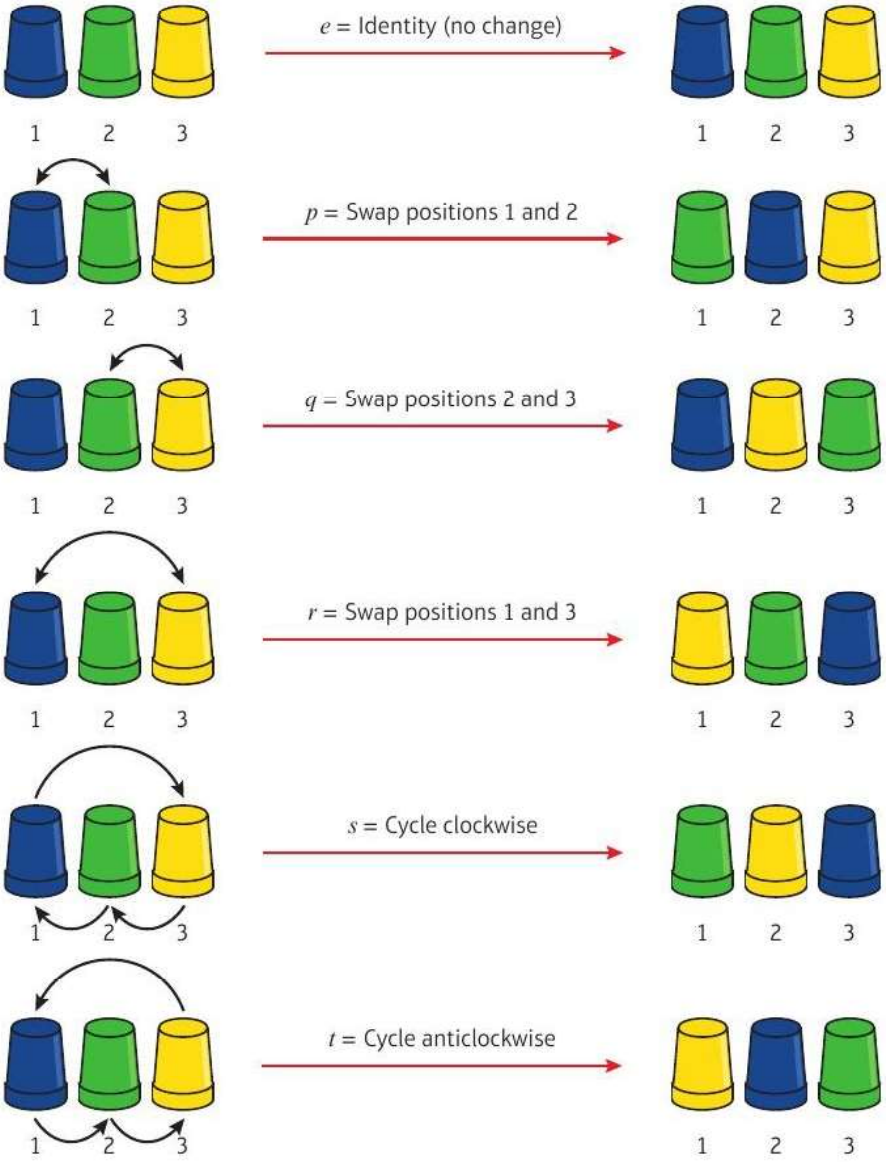
For a small set you can write down all the inverses.

Problem-solving

An element of a set (other than 1) that is a divisor of n cannot have an inverse under multiplication modulo n. Work out $a \times 3 \pmod{12}$ for every element $a \in S$ to show that no inverse exists.

Groups of permutations

Operations on sets do not need to correspond to familiar arithmetic operations. For example, consider an arrangement of 3 cups. The order in which the cups are arranged can be altered in 6 different ways. Each of these ways is called a **permutation**:

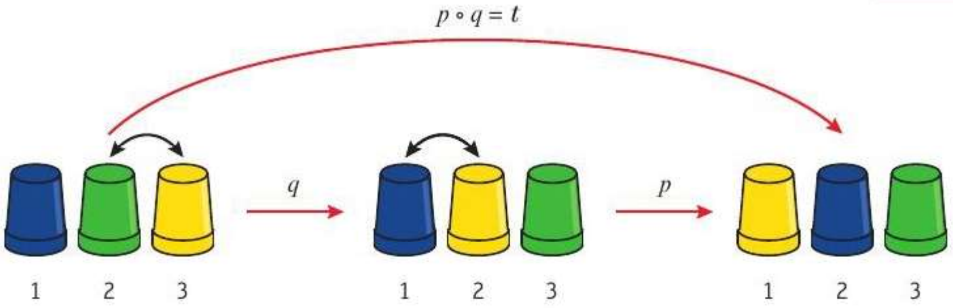

e = Identity (no change)
p = Swap positions 1 and 2
q = Swap positions 2 and 3
r = Swap positions 1 and 3
s = Cycle clockwise
t = Cycle anticlockwise
1 2 3

Note The cups move, but the positions (numbered 1, 2 and 3) stay the same. An **identity** permutation (one which does not move any cups) is also included.

You can define a set S of these 6 permutations, and you can define an operation $\circ$ on this set as the **composition** of two permutations. For example, the composition $p \circ q$ would mean 'swap positions 2 and 3 and then swap positions 1 and 2'.

The diagram below shows that this has the same effect as the single permutation t:

Notation Unless you are told otherwise in a question, permutations are composed in the same way as functions, so that $p \circ q$ means do q first and then p.



Example 12

For the set of permutations of 3 cups, $\{e, p, q, r, s, t\}$ as defined above, find:

a $q \circ p$ **b** $r \circ r$

a $BGY \xrightarrow{p} GBY \xrightarrow{q} GYB$

So $q \circ p = s$

b $BGY \xrightarrow{r} YGB \xrightarrow{r} BGY$

So $r \circ r = e$

Note that $q \circ p \neq p \circ q$

$r \circ r$ is the identity permutation, e, so r is self-inverse.
The construction of the complete Cayley table for this group is left as an exercise. → **Exercise 2B Q12**

This group of all 6 possible permutations of 3 objects, together with the operation of composition, is called the **symmetric group** on 3 elements.

- **The symmetric group on n elements is defined as the group of all possible permutations that can be performed on n objects, together with the operation of composition.**

Notation This group is often denoted as S_n.

You can use **two-row notation** to write permutations more quickly. Here are the permutations in the example above written using two-row notation.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad q = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

The use of two-row notation for permutations makes it easy to find compositions and inverses.

Consider the following two permutations on 5 objects.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

In the **composition** $\alpha \circ \beta$, the element in position 1 moves to position 5 (under β), then to position 3 (under α). So in $\alpha \circ \beta$ the element in position 1 moves to position 3:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \downarrow \\ 5 & 1 & 2 & 4 & \boxed{3} \end{pmatrix} \circ \begin{pmatrix} \boxed{1} & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} \boxed{1} & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ \boxed{3} & 4 & 1 & 2 & 5 \end{pmatrix}$$

Similarly,

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

The identity permutation on 5 objects is $e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$, so to find the **inverse** of a permutation read from the bottom row to the top row rather than from top to bottom. For example, if 1 appears below 2 in a permutation α then 2 must appear below 1 in α^{-1}.

If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$, then $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$

Example 13

Show that the permutations

$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ $\quad p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ $\quad q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $\quad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

form a group under composition. You may assume the associativity axiom is satisfied.

$\times_{10}$	e	p	q	r
e	e	p	q	r
p	p	e	ⓡ	q
q	q	r	e	p
r	r	q	p	e

$$p \circ q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = r$$

Closure: The elements of the table are all members of the set and hence it is closed.

Identity: e is the identity element.

Inverses: The identity transformation e is included in every row and column, so every element has an inverse.

$e \circ e = e$, $p \circ p = e$, $q \circ q = e$ and $r \circ r = e$.

Associativity: Associativity is assumed in the composition of transformations.

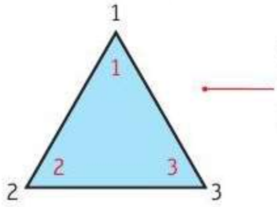
Hence the set is a group under composition.

Notation

This group is called the **Klein four-group**, K_4.

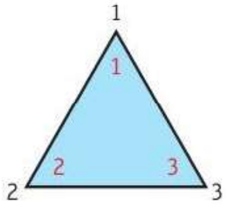
Groups of symmetries

You can construct finite groups by considering the symmetries of shapes. Consider the different ways in which an equilateral triangle can be rigidly transformed onto itself.

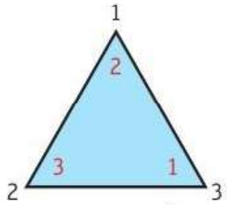


Start by labelling the positions (outside the triangle) and the vertices (inside the triangle). The positions will stay the same, but the vertices will move as the triangle is transformed.

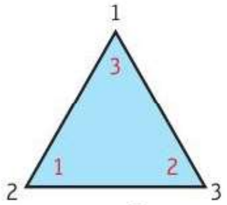
There are three rotational symmetries:



0



Clockwise $\frac{2\pi}{3}$

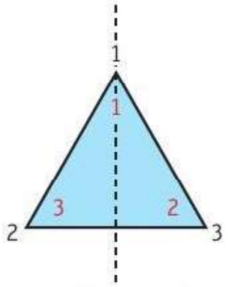


Anticlockwise $\frac{2\pi}{3}$ (or clockwise $\frac{4\pi}{3}$)

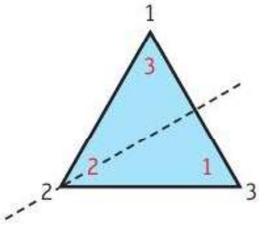
$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad R = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad S = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Using two-line notation where the second row shows the image of each vertex after the transformation.

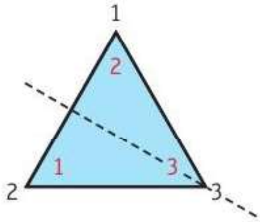
There are three reflections through the three medians:



$L = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$



$M = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$



$N = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Example 14

Show that $G = \{I, R, S, L, M, N\}$ forms a group under composition of transformations. You may assume that the associative law holds.

$\circ$	I	R	S	L	M	N
I	I	R	S	L	M	N
R	R	S	I	N	L	M
S	S	I	R	M	N	L
L	L	M	N	I	R	S
M	M	N	L	S	I	R
N	N	L	M	R	N	I

Closure: The elements of the table are all members of the set, so the set is closed.

For example, $R \circ L = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = N$

Notation The element S is sometimes called R^2 because $S = R \circ R$

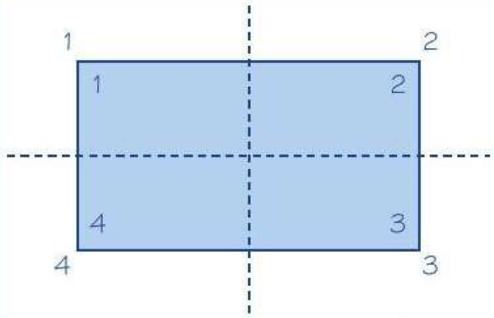
Identity: I is the identity element.
Inverses: The identity transformation I is included in every row and column, so every element has an inverse.
Associativity: Associativity is assumed in the composition of transformations.
So the set of symmetries of the equilateral triangle forms a group under composition.

Use the Cayley table to show that the four group axioms hold.

Notation The group of symmetries of an **n-sided regular** polyhedron is sometimes called a **dihedral group**, and is denoted as D_{2n} (as it contains $2n$ elements).

Example 15

Show that the symmetries of a rectangle form a group under composition of transformations. You may assume that the associativity axiom holds.



Problem-solving Label the positions of the vertices, and the vertices themselves, with integers. You could use a piece of cardboard to help you visualize the possible transformations. Make sure you label both sides of the cardboard.

Identity transformation: $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Rotation π about the centre: $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

Reflection about horizontal axis of symmetry:

$q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Use two-line notation to define the image of each transformation.

Reflection about vertical axis of symmetry:

$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

From the working shown in Example 13, these permutations form a group under composition.

These are the same permutations shown in Example 13. This group is also the **Klein four-group**. It is not a dihedral group because the rectangle is not a regular polygon.
→ Section 2.4

Cyclic Groups

Some of the groups you have already considered have the property that all of the elements of the group can be obtained by repeatedly applying the group operation to a particular single group element.

■ **A cyclic group is a group is a group in which every element can be written in the form a^k, where a is the group generator and k is a positive integer.**

Notation a^k means applying the group operation k times. For example, $a^3 = a \circ a \circ a$.

- $(\mathbb{Z}, +)$ is cyclic, as applying repeated addition to 1 generates every element of the group.
- $\{0, 1, 2, 3, \ldots, n-1\}$ is a cyclic group under addition modulo n.
  1 and $n - 1$ are both generators of this group.

Notation This group is sometimes denoted as $\mathbb{Z}_n$.

Example 16

The set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is a group under addition modulo 8. Show that 3 is a generator of this group and write each element in terms of this generator.

$3 \equiv_8 3$
$3^2 \equiv_8 6$
$3^3 \equiv_8 1$
$3^4 \equiv_8 4$
$3^5 \equiv_8 7$
$3^6 \equiv_8 2$
$3^7 \equiv_8 5$
$3^8 \equiv_8 0$

All the elements of S can be written in the form 3^k for some p1ositive integer k, so 3 generates the group.

Watch out In this notation, 3^2 means 'apply the group operation twice', so $3^2 = 3 + 3 \equiv_8 6$.

This group also has generators 1, 7 and 5.

Example 17

The set $\{1, 3, 5, 7\}$ forms a group under multiplication modulo 8.
Show that this group is not cyclic.

1 can only generate 1.
$3^2 \equiv_8 1$, $3^3 \equiv_8 3$, …
so 3 can only generate 1 and 3.
$5^2 \equiv_8 1$, $5^3 \equiv_8 5$, …
so 5 can only generate 1 and 5.
$7^2 \equiv_8 1$, $7^3 \equiv_8 7$, …
so 7 can only generate 1 and 7.

There is no element that can generate every element of the group, so the group is not cyclic.

Under multiplication, 1 is the identity.

Check each element to see whether it can generate the group. If the pattern repeats without having generated every element then you know that element cannot be a generator.

Links This is another example of the **Klein four-group**. This is the smallest non-cyclic group.
→ Section 2.4

Exercise 2B

1 The set $S = \{1, -1\}$ forms a group under multiplication. Construct a Cayley table for $(S, \times)$.

2 Construct a Cayley table for each set under the given operation. Determine, with reasons, whether the set and operation form a group.

a $\{-1, 0, 1\}$ with addition

b $\{1, 5, 7, 11\}$ with multiplication modulo 12

E **3** The set $G = \{1, 2, 3, 4, 5, 6\}$ forms a group under multiplication modulo 7. Complete the following Cayley table for this group.

$\times_7$	**1**	**2**	**3**	**4**	**5**	**6**
1				4		
2						
3			2			
4						
5		3				
6						1

(3 marks)

E **4** The set $S = \{1, 2, 4, 8\}$ is a group under multiplication modulo 15.

a ii Construct a Cayley table for $(S, \times_{15})$

ii Show that S forms a group under multiplication modulo 15. You may assume that the associative axiom is satisfied. **(6 marks)**

b Show that S does not form a group under multiplication modulo 12. **(3 marks)**

E **5** The set $G = \{a, 2, 4, 6\}$ forms a group under the operation of addition modulo 8.

a Write down the value of a. **(1 mark)**

b Complete the following Cayley table for $(G, +_8)$.

$+_8$		**2**	**4**	**6**
2		4		
4				2
6				

(3 marks)

c Find an element which generates $(G, +_8)$ and write each element in terms of this generator. **(2 marks)**

E/P **6** The operation $\circ$ is defined on the set $S = \{0, 1, 2, 3\}$ by $a \circ b = ab + a + b \pmod 5$

a Complete the following Cayley table for $(S, \circ)$.

$\circ$	**0**	**1**	**2**	**3**
0				
1				
2				1
3	3			

(3 marks)

Hint $a \circ b$ is equal to the remainder when $ab + a + b$ is divided by 5.

b Show that S is a group. You may assume that the associative law is satisfied. **(3 marks)**

P **7** Consider a set $A = \{a, b\}$. Let $M = \{q, r, s, t\}$ be the set containing mappings on the elements of A defined by:

$$q(a) = a,\ q(b) = a;\ r(a) = a,\ r(b) = b;\ s(a) = b,\ s(b) = a;\ t(a) = b,\ t(b) = b$$

a Construct a Cayley table for composition of mappings, $\circ$, as an operation on M.

b Write down the identity element for $\circ$.

c State, with reasons, whether $(M, \circ)$ forms a group.

Hint So the element $q \in M$ maps both a and b onto a.

P **8** The operation $*$ is defined on the set $A = \{10, 20, 30, 40, 50\}$ by the Cayley table below.

*	**10**	**20**	**30**	**40**	**50**
10	10	10	20	30	40
20	10	20	10	20	30
30	20	10	30	10	20
40	30	20	10	40	10
50	40	30	20	10	50

Determine whether each of the following statements is true or false, giving reasons for your answers.

a A is closed under the operation $*$.

b There is an identity element.

c $*$ is associative.

d $(S, *)$ is a group.

E/P **9** The binary operation $*$ is defined on the set $G = \{0, 1, 2, 3\}$ by

$$a * b = a + 2b + ab \text{ (mod 4)}$$

a Construct a Cayley table for $(G, *)$. **(3 marks)**

b Determine whether $*$ is associative, justifying your answer. **(3 marks)**

c Find all solutions to the equation $x * 1 = 2 * x$, for $x \in G$ **(3 marks)**

E/P **10** A student writes the following:

> S = {1, 9, 16, 22, 53, 74, 79, 81} forms a group under multiplication modulo 91.

a Show that the student is not correct. **(2 marks)**

b Write down one additional element the student can include in S to make the statement correct. **(1 mark)**

E/P **11** Let S be the set of non-negative integers less than n.
Given that S contains an element $a \neq 1$ such that $a \mid n$, prove that S does not form a group under multiplication modulo n. **(4 marks)**

P **12** The group S_3 consists of the set of all possible permutations of 3 objects, together with composition. The underlying set has 6 elements:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad q = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

a Construct a Cayley table for S_3.

b Verify that S_3 satisfies the closure, identity and inverse axioms.

Hint These are the possible permutations of 3 cups given on page 12.

13 Consider the permutations $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

Compute each of the following, where $\circ$ is the composition of permutations. Give your answers in two-row notation.

a $b \circ a$ **b** $a \circ b$ **c** a^{-1} **d** b^{-1}

e $b^{-1} \circ a^{-1}$ **f** $a^{-1} \circ b^{-1}$ **g** $(b \circ a)^{-1}$ **h** $(a \circ b)^{-1}$

E/P **14** Consider the set $M = \{1, 3, 9, 11\}$ under multiplication modulo 16. For the purposes of this question, denote this multiplication by ×.

a Show that $3 \times (9 \times 11) = (3 \times 9) \times 11$. **(2 marks)**

b Show that $(M, \times)$ is a group. **(5 marks)**

c Show that this group is cyclic, and write down all possible generators of this group. **(3 marks)**

15 Show that the following groups are cyclic and find their generators.

a $\{1, 3, 7, 9\}$ under multiplication modulo 10

b $\{4, 8, 12, 16\}$ under multiplication modulo 20

c $\{1, 2, 4, 5, 7, 8\}$ under multiplication modulo 9

P **16** Explain why 6 cannot generate a group under multiplication modulo 8.

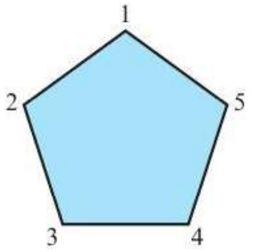
E/P **17** A group $(G, \times_{21})$ is generated by the number 5.

Find the members of G, and write each one in terms of the generator. **(3 marks)**

E/P **18 a** Show that $\omega = \frac{\sqrt{2}}{2}(1 + \mathrm{i})$ generates a group under the operation of complex multiplication. **(5 marks)**

b Write down the other generators of this group. **(2 marks)**

E/P **19** The vertices of a pentagon are labelled as follows:



The permutations $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$ correspond to clockwise rotations of 0°, 72° and 144°.

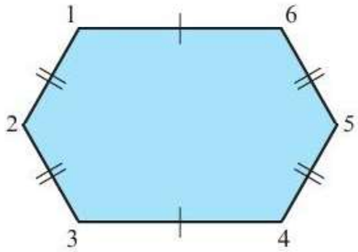
a Write the permutations p_4 and p_5 that correspond to clockwise rotations of 216° and 288° respectively. **(2 marks)**

b Complete a Cayley table for $P = \{p_1, p_2, p_3, p_4, p_5\}$ under composition. **(4 marks)**

c Prove that the set of rotational symmetries of a pentagon form a group under composition. **(5 marks)**

d Show that this group is cyclic, and that it is generated by p_2. **(3 marks)**

E/P **20** The vertices of a hexagon are labelled as follows:



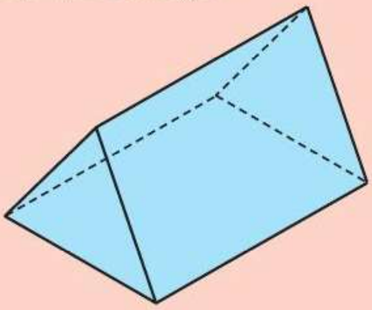
a Write down four permutations h_1, h_2, h_3, h_4 that correspond to the four symmetries of the hexagon. **(4 marks)**

b Show that the set of symmetries $H = \{h_1, h_2, h_3, h_4\}$ form a group under composition. **(6 marks)**

c Explain why H is not a cyclic group. **(2 marks)**

Challenge

The solid shown is a right triangular prism whose cross-section is an equilateral triangle.



Construct a Cayley table for the group of symmetries of this solid.

Hint Your group should contain 12 elements.

2.3 Order and subgroups

You can use **order** to describe the size of a finite group.

- **If a finite group G has n distinct elements, then the order of G is n.**

Notation The order of G is written as $|G|$. Groups with an infinite number of elements, such as $(\mathbb{Z}, +)$ are said to have infinite order.

You can also consider the order of individual elements within a group. In Example 17, you looked at the group {1, 3, 5, 7} under multiplication modulo 8. This group has identity 1, and $3^2 = 1$, $5^2 = 1$ and $7^2 = 1$.

You say that the elements 3, 5 and 7 all have **order 2**.

- **The order of an element a in a group $(G, *)$ with identity e is the smallest positive integer k such that $a^k = e$.**
- **If $(G, *)$ is finite with $a \in G$, then $|a|$ divides $|G|$.**
- **$(G, *)$ is cyclic if and only if there exists an element a such that $|a| = |G|$. This element will be a generator of the group.**

Notation The order of the element a is written as $|a|$.
An element has **finite order** if $a^m = e$ for some $m \in \mathbb{Z}^+$.
An element has **infinite order** if $a^m \neq e$ for every $m \in \mathbb{Z}^+$.

Example 18

Let $(G, \circ)$ be a finite group. Prove that every element in G must have finite order.

$|G| = n$

G is a finite group, so it must have a finite number of elements.

Let a be any element in G, and consider a, a^2, a^3, … , a^{n+1}

Since G is closed, these values are $n + 1$ elements of a group with n distinct elements.

So at least two of them must be equal, say $a^j = a^k$, with $j > k$

Then $a^j a^{-k} = a^k a^{-k}$

$\Rightarrow \quad a^{j-k} = e$

So $|a| \leqslant j - k$, and must be finite, as required.

Notation a^{-k} means $\underbrace{a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}}_{k \text{ times}}$

Example 19

For each of the following groups, write down the order of the group, and the order of each element in the group.

a {1, −1, i, −i} under complex multiplication

b {1, 3, 7, 9} under multiplication modulo 10

a The group contains 4 elements so it has order 4.

$|1| = 1$

$|-1| = 2$

$|\mathrm{i}| = 4$

$|-\mathrm{i}| = 4$

b The group contains 4 elements so it has order 4.

$|1| = 1$, $|3| = 4$, $|7| = 4$ and $|9| = 2$

The identity element always has order 1.

$(-1)^2 = 1$
Any element of a group with order 2 is self-inverse.

$\mathrm{i}^2 = -1$, $\mathrm{i}^3 = -\mathrm{i}$, $\mathrm{i}^4 = 1$
This is a cyclic group with order 4, and both i and $-\mathrm{i}$ generate the group, so they both have order 4.

$3^4 = 81 \equiv_{10} 1$, $7^4 = 2401 \equiv_{10} 1$ and $9^2 = 81 \equiv_{10} 1$

Example 20

G has elements $\{e, p, p^2, p^3, q, pq, p^2q, p^3q\}$ under multiplication, where e is the identity.

You can assume the associativity axiom is satisfied.

A partially completed Cayley table is shown below.

×	e	p	p^2	p^3	q	pq	p^2q	p^3q
e	e	p	p^2	p^3	q	pq	p^2q	p^3q
p	p	p^2	p^3	e	pq	p^2q	p^3q	q
p^2	p^2	p^3	e	p	p^2q	p^3q	q	pq
p^3	p^3	e	p	p^2	p^3q			
q	q	p^3q	p^2q	pq	e			
pq	pq	q	p^3q	p^2q	p			
p^2q	p^2q	pq	q	p^3q	p^2			
p^3q	p^3q	p^2q	pq	q	p^3			

a State the order of the group.

b State the order of p and q.

c Complete a Cayley table and verify that G forms a group.

d Find the order of pq, p^2q and p^3q.

Watch out You cannot assume that $pq = qp$.

a The group has 8 elements, so $|G| = 8$.

b p has order 4.

q has order 2.

From the table, $p \times p^3 = e$, so $p^4 = e$.

From the table, $q \times q = e$ so $q^2 = e$.

c

$\times$	e	p	p^2	p^3	q	pq	p^2q	p^3q
e	e	p	p^2	p^3	q	pq	p^2q	p^3q
p	p	p^2	p^3	e	pq	p^2q	p^3q	q
p^2	p^2	p^3	e	p	p^2q	p^3q	q	pq
p^3	p^3	e	p	p^2	p^3q	q	pq	p^2q
q	q	p^3q	p^2q	pq	e	p^3	p^2	p
pq	pq	q	p^3q	p^2q	p	e	p^3	p^2
p^2q	p^2q	pq	q	p^3q	p^2	p	e	p^3
p^3q	p^3q	p^2q	pq	q	p^3	p^2	p	e

Closure: Each element that appears in the table is a member of G, so G is closed.

Identity: e is the identity.

Inverses: e appears in every row and column, so every element has an inverse.

Associativity: Associativity is assumed.

Hence, G is a group under multiplication.

d $(pq)^2 = (pq^2)^2 = (pq^3)^2 = e$

So pq, p^2q and p^3q are of order 2.

Problem-solving

Use the associative law, the orders of p and q and the existing entries in the Cayley table to write each product as an element of the set.

For example,

$p^3 \times pq = p^4q = q$

$q \times pq = qp \times q = p^3q \times q = p^3q^2 = p^3$

$pq \times p^3q = p(qp^3)q = p(pq)q = p^2$

$p^2q \times p^2q = p^2(qp^2)q = p^4q^2 = e$

$p^3q \times p^2q = p^3(qp^2)q = p^5q^2 = p$

Use the Cayley table to show that the four group axioms hold.

Example 21

The set $\{0, 1, 2, 3, 4\}$ forms a group under addition modulo 5.

Explain why no element of this group, other than the identity, can be self-inverse.

The order of the group is 5.

Any self-inverse element, other than the identity, must have order 2.

But the order of an element must divide the order of the group. Since 2 does not divide 5, there can be no such self-inverse element in the group.

0 is the identity element. If the element a was self-inverse you would have $a + a \equiv_5 0$.

Note The identity element of any group is always self-inverse, since $e \circ e = e$.

Any group with odd order cannot contain a self-inverse element, other than the identity.

- **Let a be an element in a group $(G, *)$, then:**
  - **if a has a finite order n, then $a^m = e$ if and only if $n|m$**
  - **if a has infinite order, then $x \neq y \Rightarrow a^x \neq a^y$**
  - **if $a^x = a^y$ with $x \neq y$, then a must have finite order.**

Subgroups

If some subset of the underlying set of a group satisfies the group axioms under the **same operation**, then it is called a **subgroup**. For example, consider the set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of non-negative integers less than 8, which forms a group under addition modulo 8.

The **subset** of S given by $T = \{0, 2, 4, 6\}$ also forms a group under addition modulo 8.

Since T is a subset of S, and because each set forms a group **under the same operation**, you say that $(T, +_8)$ is a subgroup of $(S, +_8)$.

- **If a non-empty subset H of a group G is itself a group under the binary operation of G, we call H a subgroup of G.**
  - **If $H \subset G$, then H is a proper subgroup of G.**
  - **If $H \subseteq G$, then H is a subgroup of G.**

Every group has at least two subgroups, $(\{e\}, *)$ and $(G, *)$ itself. $(\{e\}, *)$ is called the **trivial subgroup**, and any other subgroups are called **non-trivial subgroups**.

Notation $B \subseteq A$ means that the set B is **contained in** the set A. B is a **subset** of A. $B \subset A$ means that B is contained in, **but not equal to**, A. B is a **proper subset** of A. This notation can be applied either to sets or to groups.

Note $H \subset G \Rightarrow |H| < |G|$
$H \subseteq G \Rightarrow |H| \leqslant |G|$

Example 22

a Show that the set $S = \{5^n : n \in \mathbb{Z}\}$ forms a group under multiplication.

b Determine, with reasons, whether each of the following subsets of S forms a subgroup of $(S, \times)$.

i $T = \{5^{2n} : n \in \mathbb{Z}\}$ **ii** $U = \{5^n : n \in \mathbb{Z}^+\}$

a **Closure:** $5^a \times 5^b = 5^{a+b}$.
For any $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$, so $5^{a+b} \in S$.
Identity: $5^0 \in S$, and $5^0 \times 5^n = 5^n \times 5^0 = 5^n$ for all $n \in \mathbb{Z}$, so 5^0 is the identity element.

$5^0 = 1$

Inverses: $5^{-a} \times 5^a = 5^a \times 5^{-a} = 5^0$.
For any $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$, so $5^{-a} \in S$
Associativity:
$5^a \times (5^b \times 5^c) = 5^a \times 5^{b+c} = 5^{a+b+c}$
$(5^a \times 5^b) \times 5^c = 5^{a+b} \times 5^c = 5^{a+b+c}$
So $5^a \times (5^b \times 5^c) = (5^a \times 5^b) \times 5^c$ for all $a, b, c \in \mathbb{Z}$, so associativity holds.
Hence $(S, \times)$ forms a group.

b **i** $5^{2a} \times 5^{2b} = 5^{2(a+b)}$ so T is closed.
$5^0 = 5^{2(0)}$ so identity element exists.
$5^{-2a} = 5^{2(-a)}$ so inverses exist in T.
Associativity holds in S so must hold in T.
So $(T, \times)$ is a subgroup of $(S, \times)$.

ii The element 5^0 is not a member of U, so U has no identity element.
U does not form a subgroup of $(S, \times)$.

Problem-solving

Associativity asserts a relationship between 3 fixed elements in a set. If T is a subset of S, then any 3 elements of T must also be elements of S. So if associativity holds in S, then it must also hold in T.

You can use the following rule to find subgroups of **finite groups** quickly.

- **Let G be a group and H a finite non-empty subset of G. Then, H is a subgroup of G if H is closed under the operation of G.**

Watch out Part **b ii** in Example 22 illustrates that this result does not necessarily hold for infinite subsets.

Example 23

The set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ forms a group under addition modulo 8.

Find two nontrivial proper subgroups of $(S, +_8)$.

+	0	2	4	6	1	3	5	7
0	0	2	4	6	1	3	5	7
2	2	4	6	0	3	5	7	1
4	4	6	0	2	5	7	1	3
6	6	0	2	4	7	1	3	5
1	1	3	5	7	2	4	6	0
3	3	5	7	1	4	6	0	2
5	5	7	1	3	6	0	2	4
7	7	1	3	5	0	2	4	6

There are two possible subgroups:
$A = \{0, 2, 4, 6\}$ and $B = \{0, 4\}$.

Delete rows and columns from the Cayley table. If you can leave a Cayley table which is **closed** (i.e. the entries in your remaining rows and columns are only those elements in the corresponding row and column headings) then it will represent a subgroup.

Problem-solving

Any subgroup must contain the identity element.

Note B is also a subgroup of A.

In the previous example, you can see that the subgroup {0, 2, 4, 6} is generated by the element 2, and the subgroup {0, 4} is generated by the element 4. This illustrates one method that can be used to find subgroups.

- **If G is a finite group, then any element $a \in G$ generates a subgroup of G, written $\langle a \rangle$.**

Watch out The converse of this result is not true: not every subgroup of G can be generated by an element of G. Only **cyclic** subgroups are generated in this way.

You can also use **Lagrange's theorem** to make deductions about subgroups.

- **Lagrange's theorem states:**

  If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Note You can quote this theorem by name in your examination. You do not need to be able to prove it.

Example 24

The set $G = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ forms a group under multiplication modulo 21.

a Find the elements in the subgroup of $(G, \times_{21})$ generated by the element 5, and state its order.

b Explain why $(G, \times_{21})$ has no subgroup of order 5.

a $5^2 \equiv_{21} 4$

$5^3 \equiv_{21} 20$

$5^4 \equiv_{21} 16$

$5^5 \equiv_{21} 17$

$5^6 \equiv_{21} 1$

So the subgroup $\langle 5 \rangle \subset (G, \times_{21})$ consists of the set $\{1, 4, 5, 16, 17, 20\}$.

The order of $\langle 5 \rangle$ is 6.

b The order of the group is 12, and 5 does not divide 12, so by Lagrange's theorem there can be no subgroup of order 5.

$5 \times 5 = 25 \equiv 4 \pmod{21}$

$5^4 = 5^3 \times 5 = 100 \equiv 16 \pmod{21}$

You can write the subgroup as the set of elements $\{1, 4, 5, 16, 17, 20\}$ or in terms of its generator, as $\langle 5 \rangle$.

There are 6 elements in the underlying set.

Exercise 2C

1 The set $\{1, 2, 4, 5, 7, 8\}$ forms a group under multiplication modulo 9. Find:

a the order of the group

b the order of each element in the group

2 The Cayley table for the Klein four-group is given below

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

a Write down the order of each element.

b Hence state, with a reason, whether the group is cyclic.

E **3** The set $\{0, 1, 2, 3, 4, 5\}$ forms a group under addition modulo 6. Find:

a the order of the group **(1 mark)**

b the order of each element in the group **(3 marks)**

c a subgroup of order 3. **(1 mark)**

E/P **4** The operation ∘ is defined on the set H, where $H = \{0, 1, 2, 4, 5, 6\}$ by $x \circ y = x + y + 2xy \pmod 7$

a **i** Complete the Cayley table shown to the right.

ii Show that $(H, \circ)$ is a group. You may assume that the associative axiom is satisfied. **(6 marks)**

b Find:

i an element that generates $(H, \circ)$

ii a subgroup of order 3

iii a subgroup of order 2 **(5 marks)**

∘	**0**	**1**	**2**	**4**	**5**	**6**
0		1				
1		4				
2						
4					0	2
5						
6					1	

E/P **5** The set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ forms a group under multiplication modulo 11.

a State the order of $(U, \times_{11})$, and hence write down the possible orders of its proper subgroups. **(2 marks)**

b Show that U is cyclic and write down its generators. **(5 marks)**

c Find all the proper subgroups of $(U, \times_{11})$ **(4 marks)**

P **6** The integers together with addition form the group $(\mathbb{Z}, +)$. State, with reasons, which of the following sets form subgroups of $(\mathbb{Z}, +)$ under the operation of addition.

a $\mathbb{Z}^+$ **b** $\{2k : k \in \mathbb{Z}\}$ **c** $\mathbb{R}$ **d** $\{-1, 1\}$

E/P **7** The set $S = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under multiplication modulo 20.

a Explain why S cannot have a subgroup of order 3. **(1 mark)**

b Find the order of each element of S. **(3 marks)**

c Find three different subgroups of S, each of order 4. **(4 marks)**

Watch out One of the three subgroups cannot be generated by a single element of S.

P **8** The Cayley table shows the action of a binary operation $*$ on the set $S = \{a, b, c, d e, f, g\}$.

a Show that the set $G = \{a, b, c\}$ forms a group under $*$. You may assume that the associative law is satisfied.

b S contains 7 elements, and the order of g is 3. What can you deduce about S from this information? Give a reason for your answer.

$*$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$	$\boldsymbol{f}$	$\boldsymbol{g}$
$\boldsymbol{a}$	a	b	c	d	e	f	g
$\boldsymbol{b}$	b	c	a	e	f	g	d
$\boldsymbol{c}$	c	a	b	f	g	d	e
$\boldsymbol{d}$	d	e	f	g	a	b	c
$\boldsymbol{e}$	e	f	g	a	d	c	b
$\boldsymbol{f}$	f	g	d	b	c	e	a
$\boldsymbol{g}$	g	d	e	c	b	a	f

E/P **9** The set $\mathbb{C}_{\neq 0}$ of non-zero complex numbers forms a group under complex multiplication. Show that the set $S = \{z \in \mathbb{C}_{\neq 0} : |z| = 1\}$ of points formed by the unit circle in the complex plane is a subgroup of $\mathbb{C}_{\neq 0}$. **(5 marks)**

Watch out $\mathbb{C}_{\neq 0}$ is not finite so you must show that S is closed, and that it contains inverses and an identity element. You can assume associativity as you are told that $\mathbb{C}_{\neq 0}$ is a group.

E/P **10** A finite group contains distinct elements x and y. Given that $x^5 = y^2$ and $|x| = 10$, find:

a $|x^2|$ **(1 mark)**

b $|y^2|$ **(1 mark)**

c $|y|$ **(1 mark)**

d $|y^3|$ **(1 mark)**

P **11** Let G be a group with $|G| = p$, where p is a prime number. Explain why:

a G must be cyclic

b every element of G except the identity must generate G.

P **12** Let G be a finite group, and x be an element of the group of order 4. State, with reasons, whether each of the following statements is true or false.

a x is the identity element

b x is self-inverse

c x^2 is self-inverse

d x^3 is self-inverse

e $|G| = 4k$, $k \in \mathbb{Z}^+$

f x generates a subgroup of order 4

g G cannot be a cyclic group

h $x^8 = e$

i $x = x^5$

j x^3 has order 4

k x^2 has order 4

E/P **13** A group H has order 8.

a State the possible orders of subgroups of H. **(2 marks)**

Given that H is the group formed by the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$ under addition modulo 8,

b find subgroups of each of the orders given in your answer to part **a**. **(4 marks)**

P **14** Prove that if G is a group with $|G| = p^2$, where p is a prime number, then G must have a subgroup of order p.

P **15** $\mathbb{Q}^{\times}$ is the group formed by the set of non-zero rational numbers under multiplication. State, with reasons, which of the following sets form subgroups of $\mathbb{Q}^{\times}$.

a $\mathbb{Z}_{\neq 0}$ (the non-zero integers)

b $\{x : x \in \mathbb{Q}, x > 0\}$

c $\{-1, 1\}$

d $\mathbb{R}_{\neq 0}$ (the non-zero real numbers)

e $\{3^k : k \in \mathbb{Z}\}$

f $\{1\}$

g $\{x : x \in \mathbb{Q}, x < 0\}$

h $\{x : x \in \mathbb{Q}, x < 0\} \cup \{1\}$

E/P **16** The set of real-valued non-singular matrices forms a group under matrix multiplication.

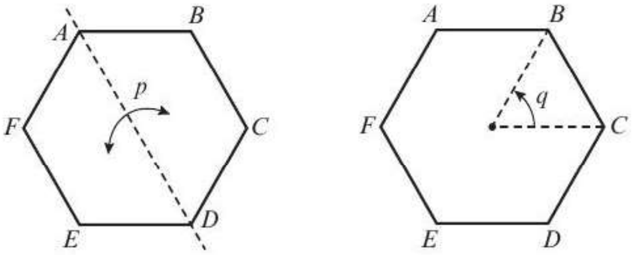
Show that the matrix $\begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$ generates a finite subgroup of this group, and state the order of this group. **(4 marks)**

E/P **17** S_4 is the group of all possible permutations of 4 elements under the operation of composition.

a Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ generates a subgroup of S_4 of order 3. **(3 marks)**

b Find a subgroup of S_4 of order 2. **(2 marks)**

P **18** The rigid symmetries of a regular hexagon $ABCDEF$ form a group under the operation of composition. This group contains the element p representing a reflection in the line through A and D, and the element q representing a rotation through 60° anticlockwise about the centre of the hexagon.



a Write down the order of p and the order of q.

b Construct a Cayley table for the subgroup generated by p

c Describe the effect of the transformation q^2, and write down the elements of the subgroup generated by q^2 in terms of q.

Challenge

1 Let G be a group and H be a finite non-empty subset of G. Given that H is closed under the group operation of G, prove that H is a subgroup of G.

2 Consider a group $(G, \circ)$ with an identity element e.

a Given that $x \in G$ has order n, state the order of x^{-1}. Justify your answer.

b For $x, y, z \in (G, \circ)$, prove that $y = z^{-1}xz \Rightarrow y^n = z^{-1}x^nz$ for $n \in \mathbb{Z}^+$.

Hint Look at Example 18 for a clue about how to begin.

Hint In part **b**, use mathematical induction.

2.4 Isomorphism

Sometimes groups defined differently can behave in the same way. If two groups contain exactly the same number of elements, and if those elements combine under the group operation in exactly the same way, then the two groups are **isomorphic**. Consider the following two groups:

- $i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ under composition of permutations
- {0, 1, 2} under addition modulo 3

The Cayley tables for these two groups are:

$\circ$	$\boldsymbol{i}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$
$\boldsymbol{i}$	i	α	β
$\boldsymbol{\alpha}$	α	β	i
$\boldsymbol{\beta}$	β	i	α

+	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

You can show that the elements of the two groups behave the same under the group operation by setting up a **one-to-one function** that maps elements of one group onto elements of the other:

$$f(i) = 0,\ f(\alpha) = 1 \text{ and } f(\beta) = 2$$

You can see from the Cayley tables that this function preserves group operations. For example,

$$\alpha \circ \beta = i \text{ and } 1 + 2 = 0$$

So $f(\alpha) + f(\beta) = f(\alpha \circ \beta)$

Because $f(i) = 0$

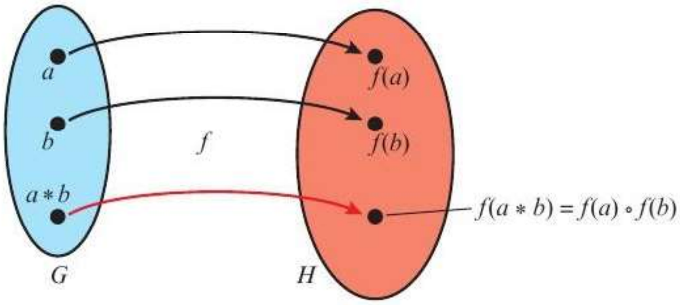
This technique allows you to formally define group isomorphism:

- **Two groups $(G, *)$ and $(H, \circ)$ are isomorphic if there exists a mapping f: $G \to H$ such that:**
  - **f maps all of the elements of G onto all of the elements of H**
  - **f is one-to-one**
  - **f preserves structure: $f(a * b) = f(a) \circ f(b)$**

Note If two groups are isomorphic then they are considered to be **exactly the same** for the purposes of group theory.

Notation If $(G, \circ)$ and $(H, *)$ are isomorphic you write $G \cong H$. The function f is called an **isomorphism** from G to H. Its inverse f^{-1} would be an isomorphism from H to G.

Because the group operation is preserved, it makes no difference whether you apply the function before or after combining elements:



Example 25

Let $(G, *)$ and $(H, \circ)$ be isomorphic groups with identity elements e_G and e_H respectively, and let f: $G \to H$ be an isomorphism from G to H.

Prove that $f(e_G) = e_H$.

$f(e_G * e_G) = f(e_G) \circ f(e_G)$

By the definition of an isomorphism

$\Rightarrow f(e_G) = f(e_G) \circ f(e_G)$

$e_G * e_G = e_G$

$\Rightarrow f(e_G) \circ e_H = f(e_G) \circ f(e_G)$

$f(e_G) \in H$

$\Rightarrow (f(e_G))^{-1} \circ f(e_G) \circ e_H = (f(e_G))^{-1} \circ f(e_G) \circ f(e_G)$

$\Rightarrow e_H = f(e_G)$

Cancel by left-multiplying by the inverse of $f(e_G)$.

A

- **If $(G, *)$ and $(H, \circ)$ are isomorphic groups with identity elements e_G and e_H respectively, and f: $G \rightarrow H$ is an isomorphism from G to H then, for all $a \in G$ and $n \in \mathbb{Z}$,**
  - **$\mathrm{f}(e_G) = e_H$**
  - **$\mathrm{f}(a^{-1}) = (\mathrm{f}(a))^{-1}$**
  - **$\mathrm{f}(a^n) = (\mathrm{f}(a))^n$**

Note Group isomorphisms preserve **identities**, **inverses**, and the **order** of elements.

→ Exercise 2D, Q2

- **Group isomorphisms also preserve order and subgroups:**
  - **$|G| = |H|$**
  - **If G has k elements of order n, then H has k elements of order n.**
  - **If G has k subgroups of order n, then H has k subgroups of order n.**
  - **If J is a subgroup of G, then H has a subgroup isomorphic to J.**

Problem-solving

If G has an element of order $|G|$ then H has an element of order $|H|$. In other words, if G is cyclic, then H is cyclic.

Example 26

The Cayley tables for two isomorphic groups G and H are shown to the right.

a State the identity element of each group.

b Describe an isomorphism from G onto H.

$(G, *)$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

$(H, \circ)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

a In group G, b is the identity.
In group H, 1 is the identity.

The row corresponding to the identity matches the top row.

b $\mathrm{f}(b) = 1$
$\mathrm{f}(a) = 3$
$\mathrm{f}(c) = 7$
$\mathrm{f}(d) = 5$

You know that the identity element in G must map to the identity element in H, so $\mathrm{f}(b) = 1$. Try other mappings until you find one that preserves the structure of the Cayley table.

Example 27

G and H are cyclic groups with $|G| = |H|$. Prove that $G \cong H$.

G and H are both cyclic, so they both contain generators, g and h respectively.
Define a mapping f: $G \rightarrow H$ as $\mathrm{f}(g^r) = h^r$ for $r \in \mathbb{Z}$.

You can use the generators of each group to define an isomorphism between the two groups. Once you have defined the mapping, you need to show that it is an isomorphism.

f maps all elements of G to all elements of H
g is a generator of G so $\{g^r : r \in \mathbb{Z}\}$ is exactly the elements of G.
h is a generator of H so $\{h^r : r \in \mathbb{Z}\}$ is exactly the elements of H.

A

f is one-to-one

If $h^j = h^k$ then $j \equiv k \pmod{n} \Rightarrow g^j = g^k$

So $f(g^j) = f(g^k) \Rightarrow g^j = g^k$

If you need to show that a mapping is one-to-one, it is sufficient to show that $f(a) = f(b) \Rightarrow a = b$.

f preserves structure

$f(g^j \circ g^k) = f(g^{j+k}) = h^{j+k} = h^j \circ h^k = f(g^j) \circ f(g^k)$

So f is an isomorphism from G onto H.

Problem-solving

The result proved in Example 27 means that there is only one cyclic group of any given order. If you need to specify an isomorphism between cyclic groups you should find generators for each group and map corresponding powers of each generator onto each other:

$$\begin{array}{l} \{e, g, \; g^2, \; g^3, \ldots, g^{n-1}\} \\ \;\downarrow\;\downarrow\;\;\;\downarrow\;\;\;\;\downarrow\;\;\;\;\;\;\;\;\;\;\;\downarrow \\ \{e, h, \; h^2, \; h^3, \ldots, h^{n-1}\} \end{array}$$

In Example 26, the elements in G were written in the Cayley table in a different order to the elements in H. This can make it hard to spot group isomorphisms from Cayley tables, especially with larger groups.

You can find isomorphisms between finite groups by classifying **all possible groups** of a given order, and considering their properties. In your examination you will only need to consider isomorphisms of finite groups of order 8 or less.

Notation Some of these groups have special names, which can be useful to learn. ← **Section 2.2**

Order	Name	Examples	Properties
1	$\mathbb{Z}_1$	Trivial group	Only group of order 1
2	$\mathbb{Z}_2$	{0, 1} under $+_2$	Only group of order 2
3	$\mathbb{Z}_3$	{0, 1, 2} under $+_3$	Only group of order 3
4	$\mathbb{Z}_4$	{0, 1, 2, 3} under $+_4$	Cyclic group of order 4
	Klein four-group (K_4)	Symmetry group of a rectangle	Only non-cyclic group of order 4 Every element (except the identity) has order 2.
5	$\mathbb{Z}_5$	{0, 1, 2, 3, 4} under $+_5$	Cyclic group of order 5
6	$\mathbb{Z}_6$	{0, 1, 2, 3, 4, 5} under $+_6$	Cyclic group of order 6
	S_3, D_6	Set of all possible permutations of 3 elements, symmetry group of an equilateral triangle.	No element of order 6
7	$\mathbb{Z}_7$	{0, 1, 2, 3, 4, 5, 6} under $+_7$	Cyclic group of order 7
8	$\mathbb{Z}_8$	{0, 1, 2, 3, 4, 5, 6, 7} under $+_8$	Cyclic group of order 8
	D_8	Symmetry group of a square	No element of order 8 Exactly 2 elements of order 4
	$\mathbb{Z}_4 \times \mathbb{Z}_2$		No element of order 8 Exactly 4 elements of order 4
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$		No element of order 8 Every element (except the identity) has order 2.
	Quaternion group		No element of order 8 Exactly 6 elements of order 4

A From the table above, there are two different groups of order 4, two different groups of order 6, and five different groups of order 8. In each case, the orders of the elements of each group are different.

- **Groups of order 8 or less can be classified entirely by the orders of their elements.**

Note The names of the groups of order 8 are given here for completeness. You do not need to know these names for your exam.

Note For groups of order 16 or greater, it is possible to find non-isomorphic groups which have exactly the same numbers of elements of each order.

Example 28

The group G consists of the elements $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$, $\begin{pmatrix}0 & -1\\-1 & 0\end{pmatrix}$, $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ and $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ under the operation of matrix multiplication.

The set $H = \{1, 3, 5, 7, 9, 11, 13, 15\}$ forms a group under multiplication modulo 16.

a Show that H contains a subgroup that is isomorphic to G.

b Determine whether H is isomorphic to the symmetry group of a square, giving reasons for your answer.

a Orders of elements in G

$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ is the identity element so has order 1.

$\begin{pmatrix}0 & -1\\-1 & 0\end{pmatrix}^2 = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}^2 = \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}^2 = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$

So $\begin{pmatrix}0 & -1\\-1 & 0\end{pmatrix}$, $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ and $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ each have order 2.

So G is the Klein four-group.

G has no element of order 4, so it is not cyclic. The only non-cyclic group of order 4 is the Klein four-group.

Orders of elements in H

1 is the identity so has order 1.

$3^2 \equiv_{16} 5^2 \equiv_{16} 11^2 \equiv_{16} 13^2 \equiv_{16} 9$ so none of these elements have order 2.

However, $3^4 \equiv_{16} 5^4 \equiv_{16} 11^4 \equiv_{16} 13^4 \equiv_{16} 1$

So 3, 5, 11, 13 all have order 4.

$7^2 \equiv_{16} 9^2 \equiv_{16} 15^2 \equiv_{16} 1$

So 7, 9 and 15 all have order 2.

If H has a subgroup isomorphic to G then it must be $K = \{1, 7, 9, 15\}$.

The order of an element in a subgroup must be the same as its order in the group. Since the Klein four-group does not contain an element of order 4, none of the elements of order 4 could be contained in a subgroup isomorphic to it.

Check that $K = \{1, 7, 9, 15\}$ is a subgroup of H:

$7 \times 9 \equiv_{16} 9 \times 7 \equiv_{16} 15$

$7 \times 15 \equiv_{16} 15 \times 7 \equiv_{16} 9$

$9 \times 15 \equiv_{16} 15 \times 9 \equiv_{16} 7$

$7^2 \equiv_{16} 9^2 \equiv_{16} 15^2 \equiv_{16} 1$

H is a finite group so if K is a subset of H which is closed under the group operation, then K is a subgroup of H.

K is closed under multiplication modulo 16, so it is a subgroup of H.

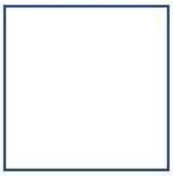
K is also the Klein four-group, so $K \cong G$ and K is a subgroup of H as required.

K is a group of order 4 under $\times_{16}$, and has three elements of order 2, so it is the Klein four-group.

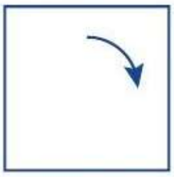
Problem-solving

You will be able to solve many problems about group isomorphisms by finding the orders of the elements in each group.

b The symmetry group of a square, D_8, consists of the following elements:

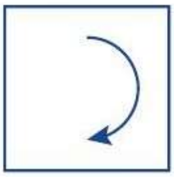


Identity (order 1)

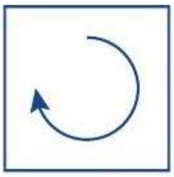


Rotation 90° (order 4)

Write out the elements of the group, and state the order of each element.

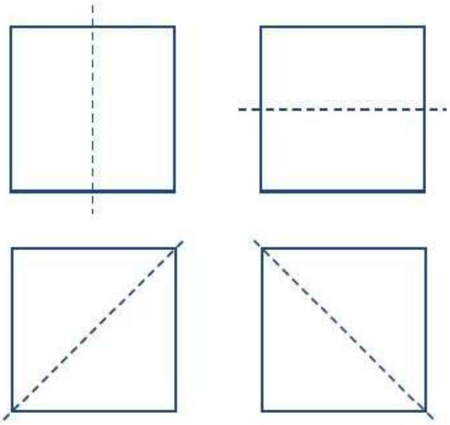


Rotation 180° (order 2)



Rotation 270° (order 4)

A clockwise rotation of 270° is the same as an anticlockwise rotation of 90°. You would need to perform this operation 4 times to get back to the original square (the identity).



Four different reflections (each of order 2)

So D_8 contains exactly 2 elements of order 4.

H contains 4 elements of order 4, so H is not isomorphic to D_8.

Isomorphic groups must contain exactly the same number of elements of each order.

Watch out Make sure you show your working by stating the order of each element, and write a clear conclusion based on your working.

Exercise 2D

1 $(G, *)$ and $(H, \circ)$ are isomorphic groups, and f: $G \rightarrow H$ is an isomorphism from G to H. Prove that, for all $a \in G$ and $n \in \mathbb{Z}^+$,

a $f(a^{-1}) = (f(a))^{-1}$

b $f(a^n) = (f(a))^n$

Problem-solving Use mathematical induction for part **b**.

2 The set $G = \{1, -1, i, -i\}$ forms a group under complex multiplication. The set $H = \{0, 1, 2, 3\}$ forms a group under addition modulo 4.

a Draw Cayley tables for each group. **(4 marks)**

b By defining an isomorphism, show that $G \cong H$. **(4 marks)**

3 The set $G = \{1, 3, 5, 7\}$.

a Show that $(G, \times_8)$ is a group. **(5 marks)**

b Find all solutions in G to the equation $7 \circ x \circ 3 = y$. Express your answers in the form (x, y). **(3 marks)**

The set $H = \{1, 3, 5, 7, 9\}$.

c Show that H does not form a group under multiplication modulo 10. **(3 marks)**

d Create another set, K, by removing one element from H so that $(K, \times_{10})$ is a group. **(1 mark)**

e Determine, with reasons, whether $(G, \times_8)$ and $(K, \times_{10})$ are isomorphic. **(2 marks)**

4 Consider a group G, of order 4, which has 4 distinct elements e, a, b and c, where e is the identity.

a Explain why ab cannot equal a or b. **(3 marks)**

b Given that c is self-inverse, construct two possible Cayley tables for G. Your Cayley tables should show two groups which are **not** isomorphic. **(4 marks)**

The set $H = \{1, -1, \text{i}, -\text{i}\}$ forms a group under complex multiplication.

c Determine which one of the groups defined in your answer to part **b** is isomorphic to H, and specify an isomorphism between $\{a, b, c, e\}$ and $\{1, -1, \text{i}, -\text{i}\}$. **(6 marks)**

5 The set $G = \{1, 7, 11, 13, 17, 19, 23, 29\}$ forms a group under multiplication modulo 30.

a Find the order of each element of $(G, \times_{30})$. **(3 marks)**

b Find three distinct subgroups of $(G, \times_{30})$, each of order 4. Describe each of these subgroups. **(4 marks)**

Problem-solving

To **describe** a group of order 4 you should state whether it is the **cyclic group** or the **Klein four-group**. Alternatively, you should fully specify the orders of each of its elements.

The group D_8 is the symmetry group of a square.

c By considering the elements of D_8 corresponding to reflections, or otherwise, show that G is not isomorphic to D_8. **(4 mark)**

6 The group $G = \{1, 2, 3, 4, 5, 6\}$ forms a group under multiplication modulo 7.

a Find the order of each element of $(G, \times_7)$. **(4 marks)**

b List all the proper subgroups of $(G, \times_7)$ and describe each group. **(3 marks)**

The group $H = \{1, 5, 7, 11, 13, 17\}$ forms a group under multiplication modulo 18.

c Specify an isomorphism between G and H. **(4 marks)**

7 a Given that G is a group of order p, where p is a prime number, explain G must be isomorphic to the cyclic group of order p. **(3 marks)**

The set $G = \{1, 7, 16, 20, 23, 24, 25\}$ forms a group under multiplication modulo 29.

The set $H = \left\{\text{e}^{\frac{2k\pi i}{7}} : k \in \{0,1,2,3,4,5,6\}\right\}$ forms a group under complex multiplication.

b Specify an isomorphism between G and H. **(3 marks)**

8 The elements of G are the complex numbers $e^{\frac{k\pi i}{4}}$, where $k = 0, 1, 2, 3, 4, 5, 6, 7$.
G forms a group under complex multiplication.
The set $H = \{1, 7, 9, 11, 17, 19, 25, 27\}$ forms a group under multiplication modulo 32.
Specify an isomorphism between $(G, \times)$ and $(H, \times_{32})$. **(4 marks)**

9 The set $G = \left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}-1 & -2\\1 & 1\end{pmatrix}, \begin{pmatrix}1 & 2\\-1 & -1\end{pmatrix}\right\}$ forms a group under matrix multiplication.
The set $H = \{1, 5, 7, 11\}$ forms a group under the operation of multiplication modulo 12.
Determine whether G and H are isomorphic, showing your working clearly. **(5 marks)**

10 The set G consists of eight 2×2 matrices:

$$G = \left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}, \begin{pmatrix}0 & \mathrm{i}\\\mathrm{i} & 0\end{pmatrix}, \begin{pmatrix}-\mathrm{i} & 0\\0 & \mathrm{i}\end{pmatrix}, \begin{pmatrix}0 & -\mathrm{i}\\-\mathrm{i} & 0\end{pmatrix}, \begin{pmatrix}\mathrm{i} & 0\\0 & -\mathrm{i}\end{pmatrix}\right\}$$

G forms a group under matrix multiplication.

a Find the order of each element in this group. **(4 marks)**

b Explain why this group cannot have a subgroup isomorphic to the Klein four-group. **(3 marks)**

The set $H = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under multiplication modulo 20.

c Determine whether G is isomorphic to H, showing your working clearly. **(3 marks)**

Challenge

The set $S = \left\{\begin{pmatrix}a & b\\c & d\end{pmatrix} : a, b, c, d \in \{0, 1\}, ad - bc \neq 0\right\}$ consists of all non-singular 2×2 matrices with elements 0 or 1.

a **i** List all the elements of S.

The operation $\times_2$ is defined as matrix multiplication modulo 2. Matrices are multiplied in the normal way, and each element is replaced with its least residue modulo 2.

ii Show that S forms a group under $\times_2$. You may assume that the associative law is satisfied.

iii Describe one other group which is isomorphic to this group.

The set $T = \left\{\begin{pmatrix}a & b\\c & d\end{pmatrix} : a, b, c, d \in \{0, 1, 2\}, ad - bc \not\equiv 0 \text{ (mod3)}\right\}$ forms a group under matrix multiplication modulo 3.

b **i** Find the order of this group.

ii Find the inverse of the element $\begin{pmatrix}1 & 2\\1 & 1\end{pmatrix}$.

Mixed exercise 2

E/P **1** A group G, under the operation of multiplication, contains distinct elements a, b and e, where e is the identity element.

a Show that $ab^2 \neq a^2b$. **(1 mark)**

b Given that $ab^2 = ba$, prove that $ab \neq ba$. **(3 marks)**

E **2** The set $G = \{1, 3, 5, 9, 11, 13\}$ forms a group under multiplication modulo 14. Copy and complete the following Cayley table for this group.

$\times_{14}$	**1**	**3**	**5**	**9**	**11**	**13**
1			5			
3		9				
5						
9				11		
11		5				
13						1

(3 marks)

E/P **3** The set $S = \{1, 3, 5, 7, 9, 11, 13, 15\}$ forms a group under the operation of multiplication modulo 16.

a List the order of each element in $(S, \times_{16})$. **(2 marks)**

b State, with a reason, whether this group is cyclic. **(2 marks)**

c Explain why $(S, \times_{16})$ can have no subgroup of order 3. **(1 mark)**

d Find a cyclic subgroup of $(S, \times_{16})$ and state a generator of this subgroup. **(3 marks)**

E/P **4 a** Describe the linear transformation represented by the matrix

$$M = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix}$$

(2 marks)

A group $(G, \circ)$ is generated by M, where $\circ$ represents matrix multiplication.

b Write down $|G|$, and write the elements of G in terms of M. **(4 marks)**

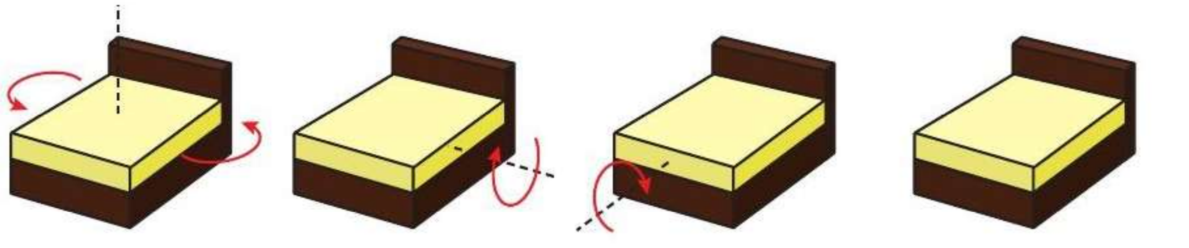
c Write in the form $\begin{pmatrix} a & b \\ \mathrm{c} & \mathrm{d} \end{pmatrix}$

i M^{-1}

ii two further generators of G. **(2 marks)**

d Find a subgroup of $(G, \circ)$ of order 4, giving each element in terms of M. **(2 marks)**

E/P **5** A mattress manufacturer suggests that customers 'flip' their mattress regularly so that it wears out evenly. The following instructions are provided:



Option *A*
Rotate 180°

Option *B*
Flip around short axis

Option *C*
Flip around long axis

Option *D*
No change (not recommended)

The operation ∘ is defined on $\{A, B, C, D\}$ as 'followed by', so that, for example, $C \circ A$ means 'flip around long axis then rotate 180°'.

a Complete the Cayley table for these four options, under the operation of combination of transformations, ∘. **(3 marks)**

b Assuming associativity, show that these four options form a group under ∘. **(3 marks)**

c State, with a reason, whether this group is cyclic. **(2 marks)**

		Second option			
	∘	***A***	***B***	***C***	***D***
First option	***A***				
	B				
	C				
	D				

E/P **6** The operation ∘ is defined on the set
$G = \{0, 1, 2, 3, 4, 5, 6, 7\}$
by
$x \circ y = x + y - 2xy \pmod 8$

a **i** Copy and complete the Cayley table shown.

ii Show that $(G, \circ)$ is a group. You may assume that the associative axiom is satisfied. **(6 marks)**

b Find:

i an element $a \in G$, other than the identity such that $a = a^{-1}$

ii a subgroup of G of order 4. **(5 marks)**

c Show that $(G, \circ)$ is not cyclic. **(3 marks)**

∘	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0		1	2					
1		0						
2								
3							5	0
4								
5						0	7	
6		3						
7		2	5					

E/P **7** **a** Explain why the set of real-valued 2 × 2 matrices do not form a group under matrix multiplication. **(1 mark)**

b Show that the set of non-singular real-valued 2 × 2 matrices form a group under matrix multiplication. You should state the identity element, and give the inverse of the general 2 × 2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. You may assume that the associative axiom is satisfied. **(5 marks)**

E/P **8** The binary operator multiplication modulo 18, denoted by $\circ$, is defined on the set

$G = \{2, 4, 8, 10, 14, 16\}$

a **i** Copy and complete the Cayley table below.

$\circ$	**2**	**4**	**8**	**10**	**14**	**16**
2		8		2		
4	8	16	14	4	2	10
8		14		8		
10	2	4	8	10	14	16
14		2		14		
16		10		16		

ii Show that $(G, \circ)$ is a group. You may assume that the associative axiom is satisfied. **(6 marks)**

b Show that the element 4 has order 3. **(2 marks)**

c Find an element which generates $(G, \circ)$, and write each element in terms of this generator. **(3 marks)**

d Set H is defined by $\{x^2 : x \in G\}$. Show that $(H, \circ)$ is a subgroup of $(G, \circ)$. **(2 marks)**

E/P **9** **a** Show that the set $S = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6 is a group. **(5 marks)**

b Show that the group is cyclic and write down its generators. **(3 marks)**

c Explain why $(S, +_6)$ cannot contain a subgroup of order 4. **(1 mark)**

d Find the subgroup of $(S, +_6)$ that contains exactly three elements. **(1 mark)**

E/P **10** Consider the set S of matrices of the form $\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, where $x, y \in \mathbb{R}$.

a Show that S forms a group under matrix multiplication. You may assume that the associative law is satisfied. **(5 marks)**

The set R consists of matrices of the form $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ where $x \in \mathbb{R}$, $x \neq 0$.

b Show that R is a subgroup of S. **(5 marks)**

The set T consists of matrices of the form $\begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix}$ where $y \in \mathbb{R}$, $y \neq 0$.

c Show that T is not a subgroup of S. **(2 marks)**

A E/P **11** The set $G = \{1, 5, 7, 11, 13, 17, 19, 23\}$ forms a group under multiplication modulo 24.

a Find the order of each element in this group. **(4 marks)**

b Explain clearly why this group cannot contain a cyclic subgroup of order 4. **(2 marks)**

The elements of H are the complex numbers $e^{\frac{k\pi i}{4}}$, where $k = 0, 1, 2, 3, 4, 5, 6, 7, 8$. H forms a group under complex multiplication.

c Determine, with reasons, whether $G \cong H$. **(3 marks)**

A E/P **12** Groups A, B and C are defined as follows.

A: the set of numbers $\{1, 3, 7, 9\}$ under multiplication modulo 10

B: the set of numbers $\{1, 2, 4, 8\}$ under multiplication modulo 15

C: the set of matrices $\left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}0 & -1\\-1 & 0\end{pmatrix}\right\}$ under matrix multiplication

a Write down the identity element for each of groups A, B and C. **(2 marks)**

b Determine in each case whether the groups

i A and B **ii** B and C **iii** A and C

are isomorphic. In each case give reasons for your answers. **(5 marks)**

E/P **13** The elements of a group G are the matrices

$$\begin{pmatrix}\cos\frac{k\pi}{3} & \sin\frac{k\pi}{3}\\ -\sin\frac{k\pi}{3} & \cos\frac{k\pi}{3}\end{pmatrix}$$

where $k = 1, 2, 3, 4, 5, 6$.

a State the order of the group and the order of each of its elements. **(4 marks)**

b Determine, with reasons, whether this group is isomorphic to the group of permutations of three elements, S_3. **(2 marks)**

Challenge

The set S_4 consists of all possible permutations of four objects under composition of permutations.

a Find $|S_4|$.

b Find subgroups $G \subseteq S_4$ with each of the following properties. In each case, list the elements of the subgroup in the form

$$\begin{pmatrix}a_1 & a_2 & a_3 & a_4\\ b_1 & b_2 & b_3 & b_4\end{pmatrix}$$

where $a_i, b_i \in \{1, 2, 3, 4\}$.

i G is a cyclic group of order 4

ii G is a cyclic group of order 3

iii $|G| = 6$

A **c** Find a subgroup of S_4 that is isomorphic to:

i the Klein four-group

ii the symmetry group of a square, D_8.

d Explain why S_4 has no subgroups that are isomorphic to:

i the cyclic group of order 6

ii the group $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15.

Summary of key points

1 A **binary operation** on a set is a calculation that combines two elements of the set to produce another element of the set.

2 An **identity element** of a set S under a binary operation $*$ is an element $e \in S$ such that, for any element $a \in S$, $a * e = e * a = a$.

3 Let S be a set and $*$ be a binary operation on S. If an identity element e exists, and there exist elements $a, b \in S$ such that $a * b = b * a = e$, then a is the **inverse** of b and b is the inverse of a.

4 A binary operation $*$ on a set S is **associative** if, for any $a, b, c \in S$, $a * (b * c) = (a * b) * c$

5 If G is a set and $*$ is a binary operation defined on G, then $(G, *)$ is a **group** if the following four axioms hold:
- **Closure**: for all $a, b \in G$, $a * b \in G$
- **Identity**: there exists an identity element $e \in G$, such that for all $a \in G$, $a * e = e * a = a$
- **Inverses**: for each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$
- **Associativity**: for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$

6 A **Cayley table** fully describes the structure of a finite group by showing all possible products of elements of the group. When a group's elements are displayed in a Cayley table, then:
- all entries must be members of the group
- every entry appears exactly once in every row and every column
- the identity element must appear in every row and column.
- the identity elements are symmetric across the leading diagonal

7
- The operation $\times_n$ of **multiplication modulo *n*** is defined on integers a and b as the remainder when ab is divided by n.
- The operation $+_n$ of **addition modulo *n*** is defined on integers a and b as the remainder when $a + b$ is divided by n.

8 The **symmetric group on *n* elements** is defined as the group of all possible permutations that can be performed on n objects, together with the operation of composition.

9 A **cyclic group** is a group in which every element can be written in the form a^k, where a is the **group generator** and k is a positive integer.

10 If a finite group G has n distinct elements, then the **order** of G is n.

11
- The **order of an element** a in a group $(G, *)$ with identity e is the smallest positive integer k such that $a^k = e$.
- If $(G, *)$ is finite with $a \in G$, then $|a|$ divides $|G|$
- $(G, *)$ is cyclic if and only if there exists an element a such that $|a| = |G|$. This element will be a generator of the group.

12 Let a be an element in a group $(G, *)$, then:
- if a has a finite order n, then $a^m = e$ if and only if $n|m$
- if a has infinite order, then $x \neq y \Rightarrow a^x \neq a^y$
- if $a^x = a^y$ with $x \neq y$, then a must have finite order.

13 If a nonempty subset H of a group G is itself a group under the binary operation of G, we call H a **subgroup** of G.

- If $H \subset G$, then H is a proper subgroup of G.
- If $H \subseteq G$, then H is a subgroup of G.

14 Let G be a group and H a finite non-empty subset of G. Then, H is a subgroup of G if H is closed under the operation of G.

15 If G is a finite group, then any element $a \in G$ generates a subgroup of G, written $\langle a \rangle$.

16 **Lagrange's theorem:** If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

17 Two groups $(G, *)$ and $(H, \circ)$ are **isomorphic** if there exists a mapping f: $G \rightarrow H$ such that:

- f maps all of the elements of G onto all of the elements of H
- f is one-to-one
- f preserves structure: $\mathrm{f}(a * b) = \mathrm{f}(a) \circ \mathrm{f}(b)$

18 If $(G, *)$ and $(H, \circ)$ are isomorphic groups with identity elements e_G and e_H respectively, and f: $G \longrightarrow H$ is an isomorphism from G to H then, for all $a \in G$ and $n \in \mathbb{Z}$,

- $\mathrm{f}(e_G) = e_H$
- $\mathrm{f}(a^{-1}) = (\mathrm{f}(a))^{-1}$
- $\mathrm{f}(a^n) = (\mathrm{f}(a))^n$

19 Group isomorphisms also preserve order and subgroups:

- $|G| = |H|$
- If G has k elements of order n, then H has k elements of order n.
- If G has k subgroups of order n, then H has k subgroups of order n.
- If J is a subgroup of G, then H has a subgroup isomorphic to J.

20 Groups of order 8 or less can be classified entirely by the orders of their elements.