

2A The Axioms for a Group

Binary operation:

A set S is closed under a binary operation $*$ if:

1. $S = \{x + y\sqrt{3} : x, y \in \mathbb{Z}\}$. Show that addition is a binary operation on S .
2. Show that the set of natural numbers, $\mathbb{N} = \{1, 2, 3, 4, \dots\}$, is not closed under subtraction.

Identity element of a set S under a binary operation $*$:

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

Inverse elements (a and b are inverses of each other if...):

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 binary operation $*$ on a set S is associative if:

5. A binary operation on $\mathbb{R}$ is defined by $a \circ b = ab + 1$. Show that $\circ$ is not associative.

If G is a set and $*$ is a binary operation defined on G , then $(G, *)$ is a group if these four axioms hold:

- Closure:
- Identity:
- Inverses:
- Associativity:

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.

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.

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

The latin square property:

2B Cayley Tables and Finite Groups

Finite group:

Cayley table:

Which element comes first in a Cayley table?

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

a) Draw a Cayley table for this group.

$\times$	1	-1	i	-i
1				
-1				
i				
-i				

b) Write down: i) the identity element ii) the inverse of i iii) the inverse of -1

When a group's elements are displayed in a Cayley table, then:

-
-
-
-

Multiplication modulo n , $\times_n$:

Addition modulo n , $+_n$:

The Cayley tables below show the set $\{0, 1, 2, 3, 4\}$ under 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. 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

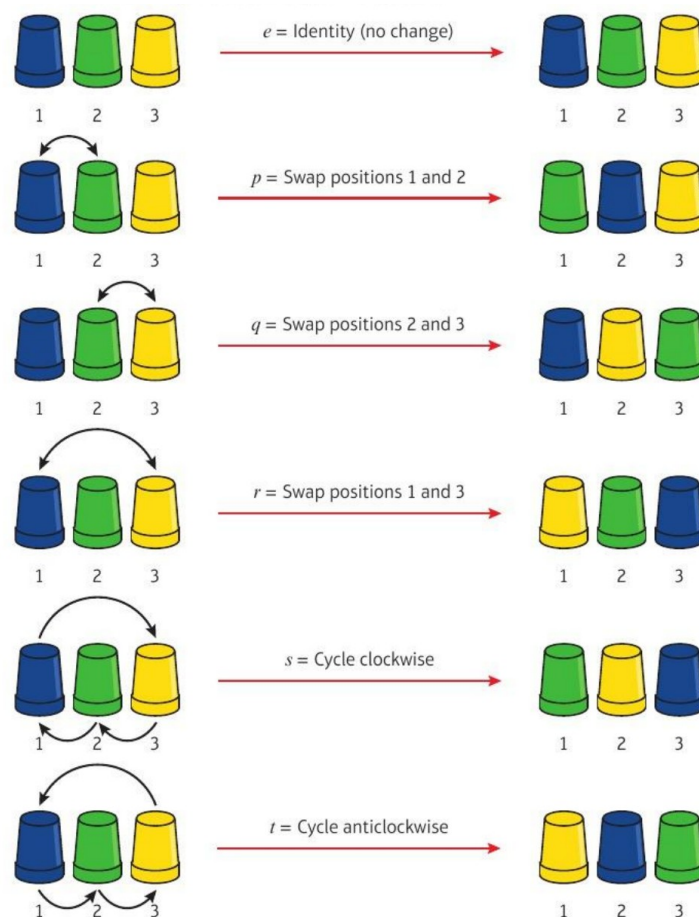
3. $S = \{1, 3, 7, 9\}$. Determine whether each of the following are groups. You may assume that the associative law holds in each case.

a) $(S, \times_{10})$

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

b) $(S, \times_{12})$

Permutation:



Composition: $p \circ q$ means

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

a) $q \circ p$

b) $r \circ r$

The symmetric group on n elements, S_n :

Two-row notation. The six permutations of 3 cups are:

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

Composition and inverses in two-row notation. Find $\alpha \circ \beta$, $\beta \circ \alpha$ and α^{-1} for:

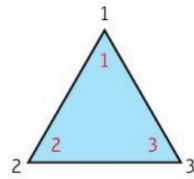
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

5. Show that the permutations below form a group under composition. You may assume the associativity axiom is satisfied.

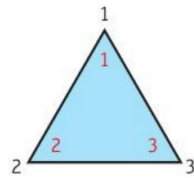
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

◦	e	p	q	r
e				
p				
q				
r				

Groups of symmetries. The symmetries of an equilateral triangle are:

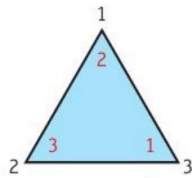


There are three rotational symmetries:



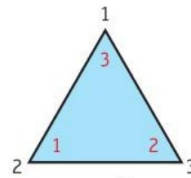
0

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



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

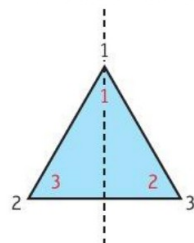
$$R = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



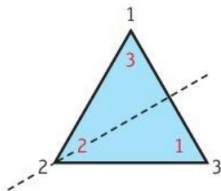
Anticlockwise $\frac{2\pi}{3}$ (or clockwise $\frac{4\pi}{3}$)

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

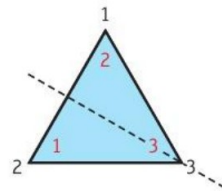
There are three reflections through the three medians:



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



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



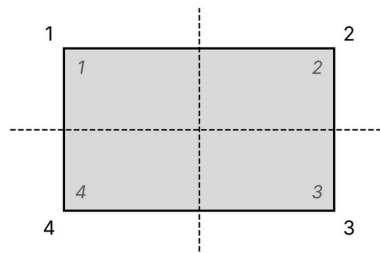
$$N = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

6. 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						
R						
S						
L						
M						
N						

Dihedral group D_{2n} :

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



Cyclic group:

Generator:

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

2C Order and Subgroups

The order of a finite group G , $|G|$:

The order of an element a , $|a|$:

If $(G, *)$ is finite with $a \in G$, then:

$(G, *)$ is cyclic if and only if:

1. Let $(G, \circ)$ be a finite group. Prove that every element in G must have finite order.
2. 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

3. 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.

x	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			

- State the order of the group.
 - State the order of p and q .
 - Complete the Cayley table and verify that G forms a group.
 - Find the order of pq , p^2q and p^3q .
4. 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.

Let a be an element in a group $(G, *)$. Then:

- if a has finite order n , then $a^n = e$ if and only if
- if a has infinite order, then
- if $a^x = a^y$ with $x \neq y$, then

Subgroup:

Proper subgroup:

Trivial subgroup:

5.

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) $U = \{5^n : n \in \mathbb{Z}^+\}$

Let G be a group and H a finite non-empty subset of G . Then H is a subgroup of G if:

6. The set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ forms a group under addition modulo 8. Find two nontrivial proper subgroups of $(S, +_8)$.

$+_8$	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

If G is a finite group, then any element $a \in G$ generates:

Lagrange's theorem:

7. 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.

2D Isomorphism

Isomorphic groups:

Compare these two groups: the permutations below under composition, and $\{0, 1, 2\}$ under addition modulo 3.

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\circ$	i	α	β
i	i	α	β
α	α	β	i
β	β	i	α

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

One-to-one function that maps one group onto the other:

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

-
-
-

Notation:

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

If $f: G \rightarrow H$ is an isomorphism then, for all $a \in G$ and $n \in \mathbb{Z}$:

Group isomorphisms also preserve order and subgroups:

2. The Cayley tables for two isomorphic groups G and H are shown below.

$(G, *)$	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) State the identity element of each group.

b) Describe an isomorphism from G onto H .

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

Groups of order 8 or less (only these are needed in the exam):

Order	Name	Properties
1	$\mathbb{Z}_1$	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4$	
4	Klein four-group, K_4	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	
6	S_3, D_6	
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8$	
8	D_8	
8	$\mathbb{Z}_4 \times \mathbb{Z}_2$	
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	
8	Quaternion group	

Groups of order 8 or less can be classified entirely by:

4. The group G consists of the elements below under the operation of matrix multiplication.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

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.

