Groups Cheat Sheet

Edexcel FP2

In simple terms, a group is a set equipped with an operation that combines two elements in the group to form another element, also in the group. This operation is also associative and there exists an identity and inverse element. The main application of groups is for modelling the symmetry of objects, and so group theory can be applied to many areas of geometry and physics.

The group axioms

Recalling set theory from GCSE Maths, a set is a collection of distinct objects. Writing $a \in S$ shows that the element a is a member of the set S.

- A binary operation on a set is a calculation that combines two elements of the set to output another element of the same set. For example, the addition operation in the set of integers is a binary operation. It's important to note that, unlike addition or multiplication of integers, the order the elements are combined often matters.
- An identity element of a set S under a binary operation $*$ is an element $e \in S$ such that for any $a \in S$, $a * e = e * a = a$. For example, the identity element of the set of the integers with the binary operation of addition is 1. The identity element of a set S under a binary operation must be unique, which can be proven by contradiction
- An inverse element for any element $a \in S$ under a binary operation $*$ is an element $b \in S$ such that $a * b = b * a = e$, where $e \in S$ is the identity element.
- A binary operation $*$ on a set S is associative if, for any $a, b, c \in S$, $a * (b * c) = (a * b) * c$

Example 1: The binary operation $*$ on the set of real numbers is defined as $a * b = a - b + ab$.
Find the identity element. The real number m has inverse m^{-1} that satisfies the property $m * m^{-1} = e$, express m^{-1} in terms of m.

Set up an equation using the definition of the identity element.	$a * e = a$ $a - e + ae = a$
Solve the equation.	$-e + ae = 0$ $e(a-1) = 0$ $e = 0$ So, for this binary operation, $e = 0$ is the identity element
Set up an equation for m using the identity element we have found.	$m * m^{-1} = 0$ $m - m^{-1} + mm^{-1} = 0$
Solve the equation.	$m + m^{-1}(m-1) = 0$ $m^{-1} = \frac{-m}{(m-1)}, m \neq 1$

The properties of binary operations can be used 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:
  - The set is closed: For all $a, b \in G, a * b \in G$
  - There exists an identity element in the group: There exists $e \in G$, such that for all $a \in G$, $a * e = e * a = a$
  - For each element $a \in G$, thee exists an inverse $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$
  - Associativity: for all $a, b, c \in G, a * (b * c) = (a * b) * c$

The group is the set together with a binary operation that satisfies these axioms- the set on its own is **not** a group

Cayley tables and finite groups

All of the groups we've considered up until this point have an infinite number of elements. A finite group, as the name suggests, contains only a finite number of elements in its underlying set. Finite groups can be represented in a Cayley table, which shows all possible elements of the group.

Example 2: Form the Cayley table for the set {0,1,2,3} with the binary operation of addition modulo 4. Find the identity element and the inverse of 3

<table>
<tr><td>At the intersection of each number, compute the two numbers added together modulo 4. Each entry should be a member of the underlying set.</td><td>
<table>
<tr><td>+</td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>0</td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>1</td><td>1</td><td>2</td><td>3</td><td>0</td></tr>
<tr><td>2</td><td>2</td><td>3</td><td>0</td><td>1</td></tr>
<tr><td>3</td><td>3</td><td>0</td><td>1</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>By definition, the identity element is the element e such that $e * a = a$.</td><td>The identity element is 0</td></tr>
<tr><td>The inverse of 3 is the element that when added modulo 4, gives the identity element.</td><td>$3 + 1 = 0 \ (\text{mod } 4)$
So, the inverse of 3 is 1.</td></tr>
</table>

Cayley tables have the following properties:

- All entries must be members of the group
- Every entry appears exactly once in each row and each column, including the identity element
- The identity elements are symmetric across the leading diagonal

Cayley tables can also be used to prove that a group satisfies the group axioms:

- The table must contain the identity element, thus the identity element exists
- As the identity element is included in every row and column, every element has an inverse

The binary operations are not necessarily familiar arithmetic operations, the operation can also define different permutations of objects. Take 3 counters of different colours in the order Red, Green, Blue in positions 1,2,3. We can define 6 operations for the 6 permutations (n objects in a row have n! permutations), with each operation forming a different permutation from the identity, or the original set up of the counters. A set S of the 6 permutations can be defined, along with an operation $*$, which can be defined as the composition of the different operations. As our set is of the 6 different permutations (you can check that there are 6 permutations by calculating 3!). Normally, the composition of permutations works in the same way as functions, so $r * s$ means do s then r.

This group is known as the symmetric group on 3 elements, denoted S_3.

- The symmetric group on n elements, denoted S_n, is defined as the group of all possible permutations on n objects (i.e n! Permutations in total). Two-row notation can be used to write permutations more easily, for example, the operation that we will denote p that takes the counters from order RGB to BGR, in other words swapping positions 1 and 3 can be written as:

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

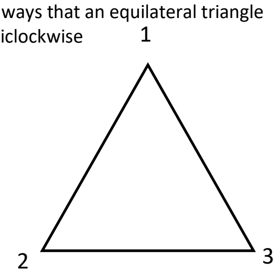
  Two-row notation can be used to show permutations for larger objects, find compositions and find inverses.

Example 3: Given the permutations on 4 objects $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, find the composition $\alpha * \beta$ and the inverse of α

Write out the composition $\alpha * \beta$ without simplifying.	$\alpha * \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$
As stated previously, compositions work from the inside out- β is applied before α. Looking at the element in position 1, when β is applied, it stays in position 1. When α is applied to the element in position 1, it goes to position 3, so the end result is moving the element from position 1 to position 3. Looking at the element in position 2, when β is applied, it moves to position 3. We then apply α and the element from position 3 goes to position 4. The end result of the composition moves the element that was in position 2 into position 4. Continuing the same logic for positions 3 and 4, the two-row notation for the total composition can be written as followed.	$\alpha * \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$
To find the inverse, we must find the permutation that maps the objects back to their original places. For α, the object in position 1 is mapped to position 3, so for α^{-1}, position 3 must be mapped back to position 1.	$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

Groups of symmetries

Finite groups can be constructed by considering the symmetries of shapes- consider the ways that an equilateral triangle can be mapped onto itself, with the vertex at the top being position 1, then labelling anticlockwise



There are 3 rotational symmetries:

- Rotating clockwise $\frac{2\pi}{3}$, denoted $R = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
- Rotating clockwise $\frac{4\pi}{3}$, denoted $S = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- Rotating clockwise 2π. This is the same as not rotating and is the identity, Denoted $I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

There are also 3 reflections:

- Reflection in the line of symmetry passing through position 1, Denoted $L = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
- Reflection in the line of symmetry passing through position 2, denoted $M = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
- Reflection in the line of symmetry passing through position 3, denoted $N = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

The group of symmetries of an n-sided regular polygon is called a dihedral group and is denoted D_{2n}- the group contains $2n$ elements and the process shown above for the equilateral triangle can be extended for any regular polygon

Cyclic groups

A cyclic group is a group in which every element can be found by repeatedly applying the group operation with a particular element, called the group generator. If we denote the group generator as a, every element can be written in the form a^k, where k is a positive integer. For example, the group of positive integers with the operation addition is cyclic, as repeated addition to generates every element of the group.

Example 4: $\{0,1,2,3,4,5\}$ forms a group under addition modulo 6, show that 5 is a generator of the group and thus that the group is cyclic

Write out the elements of the group in terms of 5^k, remember that 5^k means apply the group operation k times, so it is equivalent to $5 + 5 + \cdots + 5$ k times – **not** 5 raised to the power k.	$5 = 5(\text{ mod } 6)$ $5^2 = 4(\text{mod } 6)$ $5^3 = 3(\text{mod } 6)$ $5^4 = 2(\text{mod } 6)$ $5^5 = 1(\text{mod } 6)$ $5^6 = 0(\text{mod } 6)$
Explain why the group is cyclic, it is important to note that there can be more than one generator of a group.	The group is cyclic because each element can be generated from one element of the group

Order and subgroups

Order can be applied to both groups and elements

- The order of a finite group G, denoted $|G|$, is the number of distinct elements
- The order of a finite order element a in a group $(G,*)$ with identity e is the smallest positive integer k such that $a^k = e$. An element has infinite order if $a^m \neq e$ for every positive integer m.

For an element a a group $(G,*)$, if a has finite order n, then $a^m = e$ if and only if $n|m$. If a has infinite order, then $x \neq y \not\Longrightarrow a^x \neq a^y$. If $a^x = a^y$ with $x \neq y$, then a must have finite order

If a subset of the underlying set of a group also satisfies the group axioms with the same operation, then it is denoted a subgroup

- For 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 two subgroups, itself and $(\{e\},*)$, which is called the trivial subgroup.
If H is a finite, non-empty subset of a group G and H is closed under the operation of G, then H is a subgroup.

- If G is a finite group, then any element $a \in G$ generates a subgroup of G, denoted $\langle a \rangle$
- **Lagrange's theorem** states that if H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Isomorphisms (A-level only)

Groups with completely definitions can sometimes behave similarly. If two groups have the same order, and the elements combine using the group operation in exactly the same way, then the two groups are isomorphic. To show this, a one-to-one mapping function can be set up between the two groups

- Two groups $(G,*)$ and $(H,\circ)$ are isomorphic, denoted $G \cong H$ if there exists a mapping $f: G \to H$ such that:
  - f maps all of the elements of G on to all of the elements of H
  - f is on-to-one
  - f preserves the structure: $f(a * b) = f(a) \circ f(b)$ [note the different operations on either side]
- Group isomorphisms preserve identities, inverses, the order of elements, the order of groups and preserves subgroups.

Exercise 5: The set $G = \{1, -1, i, -i\}$ forms a group under complex multiplication and the set $H = \{0, 1, 2, 3\}$ forms a group under addition modulo 4. Define an isomorphism and show that $G \cong H$

<table>
<tr><td rowspan="2">It will be helpful to draw Cayley tables for each group in order to see how the elements interact.</td><td>
<table>
<tr><td>x</td><td>1</td><td>-1</td><td>i</td><td>-i</td></tr>
<tr><td>1</td><td>1</td><td>-1</td><td>i</td><td>-i</td></tr>
<tr><td>-1</td><td>-1</td><td>1</td><td>-i</td><td>i</td></tr>
<tr><td>i</td><td>i</td><td>-i</td><td>-1</td><td>1</td></tr>
<tr><td>-i</td><td>-i</td><td>i</td><td>1</td><td>-1</td></tr>
</table>
</td></tr>
<tr><td>
<table>
<tr><td>+</td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>0</td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>1</td><td>1</td><td>2</td><td>3</td><td>0</td></tr>
<tr><td>2</td><td>2</td><td>3</td><td>0</td><td>1</td></tr>
<tr><td>3</td><td>3</td><td>0</td><td>1</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>Map the identity elements.</td><td>It is clear to see that in G, 1 is the identity element, and in H, 0 is the identity element, so these can be mapped to each other</td></tr>
<tr><td>For the other elements, it is useful to consider the order.</td><td>In G:
-1 has order 2, as $-1 \times -1 = 1$
i has order 4, as $i \times i \times i \times i = 1$
$-i$ has order 4
In H:
1 has order 4 as $1 + 1 + 1 + 1 = 0$
2 has order 2 as $2 + 2 = 0$
3 has order 4 as $3 + 3 + 3 + 3 = 0$</td></tr>
<tr><td colspan="2">As we can map elements of the same order to elements of the same order one to one, then the structure of the group is preserved and $G \cong H$.</td></tr>
</table>