

# INTRODUCTION TO GROUPS

- A set of elements  $S = \{a, b, c, \dots\}$  forms a *group* under the *binary operation*  $\circ$  if the following properties are satisfied.

*Closure:*

For any elements  $a$  and  $b$  in  $S$ ,  $a \circ b \in S$ .

*Associativity:*

For any elements  $a, b$  and  $c$  in  $S$ ,  $a \circ (b \circ c) = (a \circ b) \circ c$ .

*Identity:*

For each  $a \in S$ , there is a unique element  $e \in S$  such that  $a \circ e = e \circ a = a$ .

*Inverse:*

For each  $a \in S$ , there is a unique element  $a^{-1} \in S$  such that  $a \circ a^{-1} = a^{-1} \circ a = e$ .

- If there is no confusion:
  - the operation symbol can be omitted ie. write  $ab$  instead of  $a \circ b$
  - $a \circ b$  can be referred to as a product.
- A group can be *finite* or *infinite*. The number of elements in a finite group is the *order* of the group.
- A group is *commutative* or *Abelian* if for any elements  $a$  and  $b$  in  $S$ ,  $a \circ b = b \circ a$ .

☺ Show that each of the following does not form a group ie. find a counter example:

$\{1, 2, 3, 4, 5\}$  under multiplication mod 6

$\{2, 4, 6, 8\}$  under addition mod 10

$\{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$  under multiplication

$\{0, 2, 4, 6\}$  under the operation defined by  $a \circ b = |a - b|$

the set of positive rational numbers under the operation defined by  $a \circ b = a^b$

☺ Show that each of the following forms an Abelian group:

the integers  $Z$  under addition

the set of non-zero rational numbers under multiplication

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$  under addition mod 12

$\{a + b\sqrt{2} : a \in Z \text{ and } b \in Z\}$  under addition

$\{2^n : n \in Z\}$  under multiplication

the real numbers  $R$  under the operation  $a \circ b = a + b - 5$

set of all real numbers excluding 1 under the operation  $a \circ b = a + b - ab$

- For a finite set of elements, a *Cayley table* can be used to represent the results of a binary operation. The  $c$  in the first row and second column corresponds to  $a * b = c$ .

		second element			
		*	$a$	$b$	$c$
first element	$a$	$b$	$c$	$a$	$a$
	$b$	$c$	$a$	$b$	$b$
	$c$	$a$	$b$	$c$	$c$
	$c$	$a$	$b$	$c$	$c$

If an element is repeated in row or in a column, then the Cayley table cannot represent a group. The operation in the above table is commutative. All groups with 4 or fewer elements are commutative.

- ☺ Show that the above table represents a group. To demonstrate that the associative property holds, it is necessary to investigate 27 different possibilities.
- ☺ Which of the following are groups? A Cayley table can be completed in the case of a finite set.
  - $\{-1, 1\}$  under addition
  - $\{-1, 1\}$  under multiplication
  - $\{-1, 0, 1\}$  under addition
  - $\{-1, 0, 1\}$  under multiplication
  - $\{1, 2, 4, 5, 7, 8\}$  under multiplication mod 9
  - $\{1, 2, 4\}$  under multiplication mod 7
  - $\{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$  under addition
  - the set of integers under subtraction
  - the set of real numbers under the operation defined by  $a \circ b = a + b - 3$
  - the set of integers under the operation defined by  $a \circ b = a + 2b$
  - the set of positive rational numbers under the operation defined by  $a \circ b = \frac{a}{b}$

- ☺ Which of the following sets of integers form a group under multiplication mod 11:  $\{1, 3, 4, 5, 9\}$   $\{1, 3, 5, 7, 8\}$   $\{1, 8\}$   $\{1, 10\}$   $\{1, 3, 10\}$  ?

- ☺ Find a finite set of integers which form a group under multiplication mod 12.

- ☺ For what values of  $p$  does the set of integers  $\{1, 2, 3, \dots, p-1\}$  form a group under multiplication mod  $p$  ?

- Consider the *cartesian plane*. A *transformation* is a function which maps each point onto some point in the plane. For example, the transformation  $T(x, y) = (x, -y)$  maps  $(5, 8)$  onto the point  $(5, -8)$ :  $T$  is the reflection in the  $x$ -axis.

To define  $T_2 \circ T_1$ , we use the idea of *composition* of transformations ie.  $T_2 \circ T_1$  means the single transformation which is equivalent to first performing transformation  $T_1$  and then performing the transformation  $T_2$ .

The composition of transformations is not necessarily commutative. Consider  $T_1$  as the reflection in the  $y$ -axis and  $T_2$  as the rotation of  $180^\circ$  about the origin: what do  $T_2 \circ T_1$  and  $T_1 \circ T_2$  represent?

The composition of transformations is however associative. A proof is as follows:

suppose the transformations  $T_1$ ,  $T_2$  and  $T_3$  map the points

$$T_1: A \rightarrow B, T_2: B \rightarrow C, T_3: C \rightarrow D$$

then  $T_2 \circ T_1: A \rightarrow C$  and  $T_3 \circ T_2: B \rightarrow D$

from which it can be seen that  $T_3 \circ (T_2 \circ T_1): A \rightarrow D$  and  $(T_3 \circ T_2) \circ T_1: A \rightarrow D$

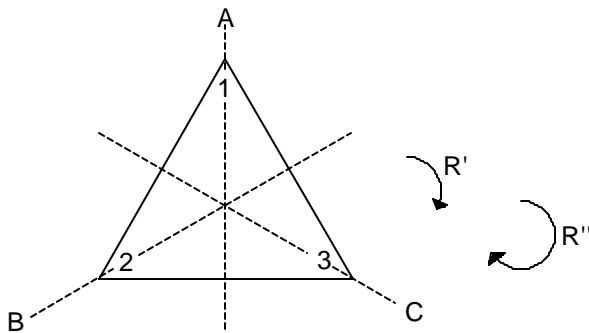
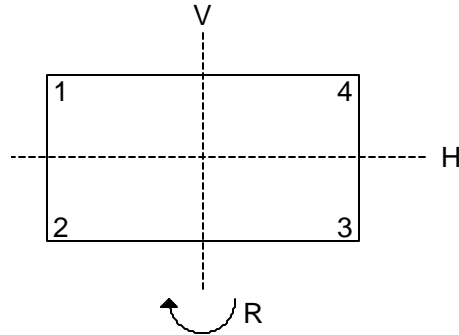
$$\therefore T_3 \circ (T_2 \circ T_1) = (T_3 \circ T_2) \circ T_1$$

A  $1 : 1$  transformation is called a *non singular* transformation. Each non singular transformation  $T$  has an inverse  $T^{-1}$ . A set of non singular transformations which forms a group is called a *transformation group*.

- A *symmetry* of a shape is a non singular transformation which maps the shape onto itself ie. it leaves the shape looking exactly the same.

The symmetries of a rectangle are:

- I - the identity transformation
- H - reflection in the horizontal axis
- V - reflection in the vertical axis
- R - rotation of  $180^\circ$  about the centre



The symmetries of an equilateral triangle are:

- I - the identity transformation
- A - reflection in the axis A
- B - reflection in the axis B
- C - reflection in the axis C
- R' - rotation of  $120^\circ$  clockwise
- R'' - rotation of  $240^\circ$  clockwise

- ☺ Complete the following Cayley table for the symmetries of a rectangle. Show that the symmetries of a rectangle form a transformation group.

$\circ$	I	H	V	R
I				
H				
V				
R				

- ☺ Complete the following Cayley table for the symmetries of an equilateral triangle. Show that the symmetries of an equilateral triangle form a transformation group.

$\circ$	I	R'	R''	A	B	C
I						
R'						
R''						
A						
B						
C						

- A *subgroup* is a subset of the group which satisfies all the properties for a group.

- ☺ Does  $\{I, R', R''\}$  form a subgroup of the symmetries of an equilateral triangle? Are there any other subgroups?

$\circ$	I	R'	R''
I			
R'			
R''			

- *Lagrange's Theorem* states that the order of a subgroup of a finite group is a factor of the order of the whole group.

- ☺ Show that Lagrange's Theorem is true for the subgroup  $\{I, R', R''\}$  of the group of symmetries of an equilateral triangle.

- ☺ If the order of a group is a prime number, what can you say about subgroups?

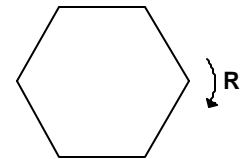
- ☺ Produce a Cayley table for the group which consists of the integers  $\{0, 1, 2\}$  under addition mod 3.

+	0	1	2
0			
1			
2			

Compare the table with that for the subgroup  $\{I, R', R''\}$  of the group of symmetries of an equilateral triangle. What do you notice? This an example of *isomorphism*.

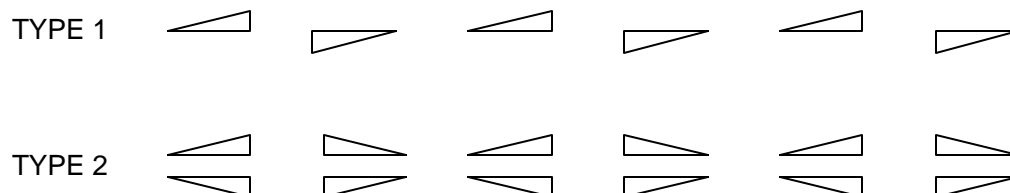
- ☺ The elements of the subgroup  $\{I, R', R''\}$  of the symmetries of an equilateral triangle could be written as  $\{I, R, R^2\}$ . Explain why. Groups of this type are called *cyclic groups*.

- ☺ Produce a Cayley table for the cyclic group of rotational symmetries of a regular hexagon  $\{I, R, R^2, R^3, R^4, R^5\}$  where R is a clockwise rotation of  $60^\circ$ . Describe any subgroups which exist.



- ☺ The set of symmetries of a square form a transformation group of order 8. Determine the elements of the group and complete a Cayley table. Find all the subgroups. Can you match each subgroup with a different type of quadrilateral?

- ☺ Shown below are two types of *strip pattern*. The patterns are infinite ie. they stretch forever in each direction. The track of a tyre is an example of a strip pattern.



Describe the symmetries for each type ie. transformations (identity, reflection, rotation, translation or glide reflection) which map the pattern onto itself? For each type, the symmetries form an infinite transformation group.

- ☺ There are only seven distinct types of infinite strip pattern. Find the other five types. A good reference is *For All Practical Purposes* (p 486 - 493) published by W.H. Freeman. The book also deals with wallpaper patterns of which there are exactly seventeen types where again each type corresponds to a transformation group.