

# Contents

<b>1</b>	<b>Symmetries</b>	<b>1</b>
1.1	Definitions & Notation . . . . .	1
1.1.1	Functions . . . . .	3
1.2	Plane Figures . . . . .	3
1.2.1	The Square . . . . .	4
1.2.2	Representing Symmetries: 2-Line Symbol . . . . .	4
1.3	Cayley Tables . . . . .	5
1.4	The Group Axioms . . . . .	5
1.4.1	Modular Arithmetic . . . . .	6
1.4.2	Checking Group Axioms . . . . .	6
1.4.3	Uniqueness Proofs . . . . .	7
<b>2</b>	<b>Groups &amp; Subgroups</b>	<b>8</b>

## 1 Symmetries

### 1.1 Definitions & Notation

We must start with a load of definitions & notation. This will start to form the basis of group theory. The following are special sets:

- $\mathbb{R}$ : the set of real numbers;
- $\mathbb{R}^*$ : the set of non-zero real numbers;
- $\mathbb{Q}$ : the set of rational numbers, that is, a real number that can be expressed as a fraction;
- $\mathbb{Z}$ : the set of integers, that is,  $\dots - 2, -1, 0, 1, 2, \dots$ ;
- $\mathbb{N}$ : the set of natural numbers  $1, 2, 3, \dots$

To indicate that something is a member of a set (for example, the number 3.142 in  $\mathbb{R}$ ), we write:

$$3.142 \in \mathbb{R}$$

We could write  $x \in \mathbb{R}$  to say that  $x$  is some real variable.

Now, let us write down a set consisting of the first 5 natural numbers:

$$A = \{1, 2, 3, 4, 5\}$$

We could also write this as:

$$A = \{x \in \mathbb{N} : x \leq 5\}$$

Where this is read as: 'let  $x$  be a natural number, such that it is less than or equal to 5'.

Now, suppose we have a set with a single element:  $A = \{2\}$ , say. This is denoted a **singleton**. It is not the same as the number 2. We can also specify a set which is composed of other sets, such as:

$$B = \{\{1, 2\}, \{4, 5, 3\}\}$$

Suppose we have the set:

$$\ell = \{(x, y) \in \mathbb{R}^2 : y = ax + b\}$$

That is, the set of points  $(x, y)$  which satisfy the equation for a straight line. For sets which specify a function, the elements of such a set are the solutions to the function. We can see that we may specify the set of points which lie on the unit circle, or lie within the unit circle, or lie on and within the unit circle:

$$\begin{aligned} C &= \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} \\ C_1 &= \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\} \\ C_2 &= \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\} \end{aligned}$$

Notice that there is a subtle difference between all 3 sets. Similarly, we can obviously write the set of points which lie on a circle, radius  $r$ , centred on  $(a, b)$ , that is  $C = \{(x, y) \in \mathbb{R}^2 : (x-a)^2 + (y-b)^2 = r^2\}$ .

Now, suppose we write 2 apparently different sets:

$$A = \{1, -1\} \quad B = \{x \in \mathbb{R} : x^2 - 1 = 0\}$$

Upon examination, we see that these two sets contain exactly the same elements. That is,  $A = B$ . We may notice that all elements of some set  $C$  are also in  $D$ . Then, we say that  $C \subseteq D$ . For example, this would be the case if:

$$C = \{2, 3, 4\} \quad D = \{9, 8, 5, 2, 6, 3, 4\}$$

We say that  $D$  contains  $C$ . Clearly, we also see that  $C \neq D$ . So, to emphasize that  $D$  contains  $C$ , but is not equal to it, we write  $C \subset D$ . Thus,  $C$  is a proper subset of  $D$ .

The **null set**, or empty set, is one with no elements, and is denoted  $\emptyset$ . A set with  $n$  elements can be written with its elements in  $n!$  different orders. We can also see that a set with  $n$  elements has  $2^n$  subsets.

The **union** of two sets essentially combines the elements of both sets; for example:

$$A = \{2, 5, 1\} \quad B = \{5, 7, 8, 3\} \quad A \cup B = \{2, 1, 5, 7, 8, 3\}$$

The **intersection** of two sets is those elements which are common to both sets, i.e., using the above sets,  $A \cap B = \{5\}$ .

Hence, we see that, for example:

$$\{1, 3, 5\} \cap \{2, 9\} = \emptyset$$

And such sets are known as **disjoint**.

### 1.1.1 Functions

Now, suppose we have some function  $f$  which sends a set of numbers  $A$  to another set  $B$ . Then, we have that the **domain** of  $f$  is  $A$ , and that the **codomain** of  $f$  is  $B$ . We also say that for some element  $x \in A$ , it has a unique image in  $B$ ,  $f(x) \in B$ . In notation:

$$\begin{aligned} f &: A \rightarrow B \\ x &\mapsto f(x) \end{aligned}$$

As an example, consider reducing the plane of numbers  $(x, y)$  to the distance it is away from the origin:

$$\begin{aligned} f &: \mathbb{R}^2 \rightarrow \mathbb{R} \\ (x, y) &\mapsto \sqrt{x^2 + y^2} \end{aligned}$$

Consider also a transformation, such as shifting a set of points  $(x, y)$  to  $(x + 4, y)$ :

$$\begin{aligned} f &: \mathbb{R}^2 \rightarrow \mathbb{R}^2 \\ (x, y) &\mapsto (x + 4, y) \end{aligned}$$

The identity function is one whose codomain is the same as its domain, and the action of the function sends elements in the domain to the same element in the codomain. That is:

$$\begin{aligned} i &: A \rightarrow A \\ x &\mapsto x \end{aligned}$$

We may also form the composite of two functions,  $g \circ f$ ; which means act with  $f$  first, then  $g$ .

## 1.2 Plane Figures

Let us define a plane figure  $F$  as any subset of the plane  $\mathbb{R}^2$ . This can obviously mean any 2D shape, for example an equilateral triangle, square or circle. Let an **isometry** of a plane figure  $F$  be some function  $f$  that preserves distances. That is, the distance between  $f(x)$  and  $f(y)$  is the same as that between  $x$  and  $y$ . Let a **symmetry** of  $F$  be isometry mapping such that it maps onto itself.

So, translation is an isometry, and a rotation about  $2\pi$  for a non-regular triangle is a symmetry. Two symmetries of a figure are equal if they have the same effect on the figure.

Suppose that the set of all symmetries of some plane figure  $F$  are denoted by  $S(F)$ . Let  $f$  and  $g$  be two functions of  $F$ . We also let them be distance preserving. Then, we see that:

$$g \circ f \in S(F)$$

That is, the set is closed under composition of functions. We see that  $S(F)$  is never empty, as it always contains at least the identity symmetry. For some  $f \in S(F)$ , the set contains an identity symmetry  $e$  such that  $f \circ e = e \circ f = f$ .

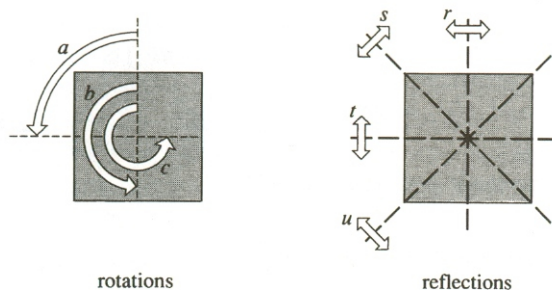


Figure 1: The symmetry transformations on the square. We also have the identity  $e$ , where nothing changes.

### 1.2.1 The Square

Let us consider the set  $S(\square)$ ; the set of symmetries of the square. The elements are defined in Fig (1). So, we have that  $S(\square)$  consists of 3 rotations:  $a$  by  $\frac{\pi}{2}$ ,  $b$  by  $\pi$  and  $c$  by  $\frac{3\pi}{2}$ . We also have 4 reflections:  $r$  in the vertical axis,  $s$  in the upper diagonal axis,  $t$  in the horizontal axis and  $u$  in the lower diagonal. These functions are defined, regardless of any previous symmetry functions that have been applied. Let us consider some composite functions:

Suppose we draw two different dots on opposing corners of the square, so that we can keep track of what is happening, then we can apply two symmetries, and note down what it is equivalent to. We find:

$$a \circ t = u \quad t \circ a = s$$

That is, if we reflect in the horizontal axis ( $t$ ), then rotate by  $\frac{\pi}{2}$  ( $a$ ), it is equivalent to reflecting about the lower diagonal ( $u$ ). We say that two functions acting is a composition, and we see that the order of composition is important, and that composition of symmetries is generally not commutative. We can also see that composing a reflection with itself gives the identity. So, as a few examples:

$$a \circ t = u \quad t \circ a = s \quad r \circ r = e$$

### 1.2.2 Representing Symmetries: 2-Line Symbol

Supposing we label the vertices of the square, starting from the top right, going anti-clockwise, as 1, 2, 3, 4. Then, we may write each symmetry transformation as a set of numbers. Let us do this for the  $a$  symmetry, rotation through  $\frac{\pi}{2}$ . So:

We see that 1 goes to 2, 2 goes to 3, 3 goes to 4, and 4 goes to 1. That is:

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

In general, if  $f$  is some symmetry of a polygonal figure  $F$ , which moves vertices originally at 1, 2, 3, 4, ...,  $n$  to  $f(1), f(2), f(3), \dots, f(n)$ , then:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

Using this notation we can obviously write down compositions, of, say, the symmetries of the square:

$$\begin{aligned} r \circ a &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\ &= u \end{aligned}$$

Doing this, one must be careful to do things in the right order: start from the right.  $1 \rightarrow 2 \rightarrow 3$  etc. The inverse of a symmetry can be found by just turning its two-line symbol upside down, and rearrange its elements into the natural order. So, for example:

$$\begin{aligned} a &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\ \Rightarrow a^{-1} &= \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\ &= c \end{aligned}$$

### 1.3 Cayley Tables

Let us write down in a table, the compositions of the rotational symmetries of the square with each other, as well as the identity symmetry:

$\circ$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$b$	$c$	$e$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$e$	$a$	$b$

Now, one thing to notice is that no reflection composed with another reflection gives anything but a reflection. That is, the group is closed. Also notice, that the group contains the identity element  $e$ . Also, notice that when an element is composed with its inverse,  $e$  appears.

An equivalent table can be constructed for all 8 symmetries of the square, and also for just the reflections.

### 1.4 The Group Axioms

Let  $G$  be a set, and let  $\circ$  be some binary operation on  $G$ . Then,  $(G, \circ)$  is a group if the following 4 axioms hold:

- **Closure:** For all  $g_1, g_2 \in G$ :  
 $g_1 \circ g_2 \in G$ ;

- **Identity:** There exists an identity element  $e \in G$  such that  $\forall g \in G$ :  
 $g \circ e = e \circ g = g$ ;
- **Inverses:** For each  $g \in G$ , there exists an inverse element  $g^{-1} \in G$ , such that:  
 $g \circ g^{-1} = g^{-1} \circ g = e$ ;
- **Associativity:** For all  $g_1, g_2, g_3 \in G$ :  
 $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

An additional property that a group may or may not possess, is that,  $\forall g_1, g_2 \in G$  if  $g_1 \circ g_2 = g_2 \circ g_1$ , then  $G$  is **abelian**. If  $G$  is a finite set with  $n$  distinct elements, then  $(G, \circ)$  is a group of order  $n$ .

### 1.4.1 Modular Arithmetic

We can look at these axioms using another type of example: modular arithmetic. Let us work with the set:

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

Where modular arithmetic takes the remainder after division by the order of the set (4 in this case). Let us construct a Cayley table for the sets (to be confirmed which are groups)  $(\mathbb{Z}_4, +_4)$  and  $(\mathbb{Z}_4, \times_4)$ :

$+_4$	$0$	$1$	$2$	$3$	$\times_4$	$0$	$1$	$2$	$3$
$0$	$0$	$1$	$2$	$3$	$0$	$0$	$0$	$0$	$0$
$1$	$1$	$2$	$3$	$0$	$1$	$0$	$1$	$2$	$3$
$2$	$2$	$3$	$0$	$1$	$2$	$0$	$2$	$0$	$2$
$3$	$3$	$0$	$1$	$2$	$3$	$0$	$3$	$2$	$1$

### 1.4.2 Checking Group Axioms

To show that  $(G, \circ)$  is a group, we need to check if each of the group axioms hold: closure, identity, inverses and associativity. To show that  $(G, \circ)$  is not a group, then we just need to show that one of the axioms fails. We proceed via examples:

**Is  $(\mathbb{Z}, +)$  a Group?** Just to recap:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Closure: For all  $m, n \in \mathbb{Z}$ ,  $m + n \in \mathbb{Z}$ . Hence, the set is closed.

Identity: For all  $n \in \mathbb{Z}$ ,  $n + 0 = 0 + n = n$  and  $0 \in \mathbb{Z}$ . Hence, the set possesses an identity element, which is 0.

Inverses: For each  $n \in \mathbb{Z}$ , if we write  $n + (-n) = (-n) + n = 0$ , and we note that  $-n \in \mathbb{Z}$ , we see that the inverse of  $n$  is  $-n$ . Hence, the set has inverses.

Associativity: Obviously, addition of integers is associative.

Hence,  $(\mathbb{Z}, +)$  is a group.

**Is  $(\mathbb{R}, \times)$  a Group?** Closure:  $\forall x, y \in \mathbb{R}, xy \in \mathbb{R}$ . Hence closed. Identity:  $\forall x \in \mathbb{R}, x \times 1 = 1 \times x = x$ . Hence, the identity element is 1. Inverses:  $\forall x \in \mathbb{R}, x \times \frac{1}{x} = \frac{1}{x} \times x = 1$ ; However, this only holds for  $x \neq 0$ . Hence, we have one element that has no inverse. Therefore, the set is not a group.

**Is  $(\mathbb{Z}_4, \times_4)$  a Group?** We can see from the previously constructed Cayley table that the set is closed, and that the identity element is 1. However, there is not an inverse element for all elements. Therefore, the set is not a group.

We can easily see that a group table is one in which the identity element appears symmetrically, and that each element appears once and only once in each row/column. This is not to say that any table with these properties is a group.

### 1.4.3 Uniqueness Proofs

Here, we prove that the identity and inverse elements are unique.

**Uniqueness of the Identity Element** Now, suppose that a group  $(G, \circ)$  has two identity elements  $e$  and  $e'$ . The identity element property is that

$$\forall g \in G, \quad g \circ e = e \circ g = g. \quad (1.1)$$

We also have, due to our presupposed second identity element:

$$\forall g \in G, \quad g \circ e' = e' \circ g = g. \quad (1.2)$$

Now, in (1.1), let us chose the element  $g = e'$ , as we are allowed to do; this results in us writing:

$$e' \circ e = e \circ e' = e'.$$

In (1.2), let us chose the element  $g = e$ , resulting in:

$$e \circ e' = e' \circ e = e.$$

Upon comparison of the above two equations, we see that:

$$e' \circ e = e' = e' \circ e = e$$

Hence proving that  $e = e'$ . Hence, the identity element is unique.

**Uniqueness of the Inverse Element** Suppose that the group  $(G, \circ)$  has an element  $g$ , and that  $g$  has two inverses  $x, y$ . We also let  $e$  be the identity element in  $G$ . Now, the general property of an inverse element  $g^{-1} \in G$  is that:

$$g \circ g^{-1} = g^{-1} \circ g = e.$$

So, we have that, for our element  $g$ , with two inverses:

$$g \circ x = x \circ g = e \quad (1.3)$$

$$g \circ y = y \circ g = e. \quad (1.4)$$

Now, let us consider (via associativity) the element  $y \circ g \circ x$ . Now, from (1.3), we see that  $g \circ x = e$ . Hence:

$$y \circ g \circ x = y \circ e = y.$$

Now, from (1.4), we see that  $y \circ g = e$ . Hence, we see that:

$$y \circ g \circ x = e \circ x = x.$$

Hence, we see that  $y = x$ . Hence, the inverse of an element is unique.

## 2 Groups & Subgroups

A subgroup of  $(G, \circ)$  is a group  $(H, \circ)$ , where  $H$  is a subset of  $G$ . Notice, the subgroup must have the same binary operation as its parent. So, we have  $H \subseteq G$ .

We say that if  $H$  is a subset of  $G$ , then  $(H, \circ)$  is a subgroup of  $(G, \circ)$  if all the following hold:

- Closure: For all  $h_1, h_2 \in H$ , then  $h_1 \circ h_2 \in H$ ;
- Identity: The identity  $e \in H$ ;
- Inverses: For all  $h \in H$ , there is  $h^{-1} \in H$ .

We see that a group always has at least one subgroup: the trivial subgroup consisting of the identity element  $(\{e\}, \circ)$ . We denote a subgroup other than the whole group a proper subgroup.

As examples, we see that the set of positive integers  $(\mathbb{Z}^+, +)$  is not a subgroup of  $(\mathbb{Z}, +)$ , as it does not contain the identity element 0. We also see that  $(3\mathbb{Z}, +)$  is not a subgroup of  $(4\mathbb{Z}, +)$ , as they do not possess common elements.