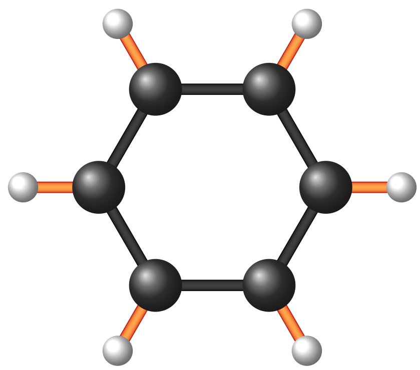
Grade 9/10 Math Circles
March 22, 2023
An Introduction to Group Theory Part 1

What is group theory?

Group theory is an important area in mathematics that studies objects known as *groups*. Groups show up all over mathematics, and even appear in unexpected places. For example, we can solve a Rubik's Cube using group theory! Group theory also has many important applications in physics and chemistry. As an example, consider the following Benzene molecule from chemistry:



In your head, imagine rotating the molecule by multiples of 60 degrees, or reflecting the molecule along axes that go through the center and 2 spheres. Notice that the Benzene molecule appears the same after performing these actions. In other words, the molecule is unchanged. We call such actions *symmetries*. We will see later on that these symmetries actually form a group! Chemists use symmetries of molecules, like the benzene molecule, to try and predict or explain their properties. In this lesson, we define what a group is and look at a special class of groups called *symmetry groups*.

Groups

Briefly put, a *group* is a set together with an operation that follows some specific rules, which are called *group axioms*. Before we define a group, we need to define what a set and a binary operation on a set are.

Definition 1

A **set** is a collection of objects (e.g., numbers, symbols, shapes). We refer to the objects in a set as **elements** of the set.

Notation

Let S be a set.

We write $\boldsymbol{x \in S}$ to mean that x is an element of the set S. The symbol $\in$ is read as "is an element of" or "is in".

We write $\boldsymbol{x \notin S}$ to mean that x is not an element of the set S. The symbol $\notin$ is read as "is not an element of" or "is not in".

Example 1

The collection of all integers is a set which we denote by $\mathbb{Z}$. We write this set as

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

It is true that $5 \in \mathbb{Z}$ as 5 is an integer. However, $1/2 \notin \mathbb{Z}$ as $1/2$ is not an integer.

Example 2

The collection of letters in the english alphabet form a set. We write this set as

$$\mathcal{A} = \{a, b, c, d, ..., w, x, y, z\}.$$

It is true that $h \in \mathcal{A}$ as h is a letter in the alphabet. But $2 \notin \mathcal{A}$ as 2 is a number, not a letter.

Definition 2

For our purposes, an **operation** is a "machine" that takes in one or more inputs, and produces an output.

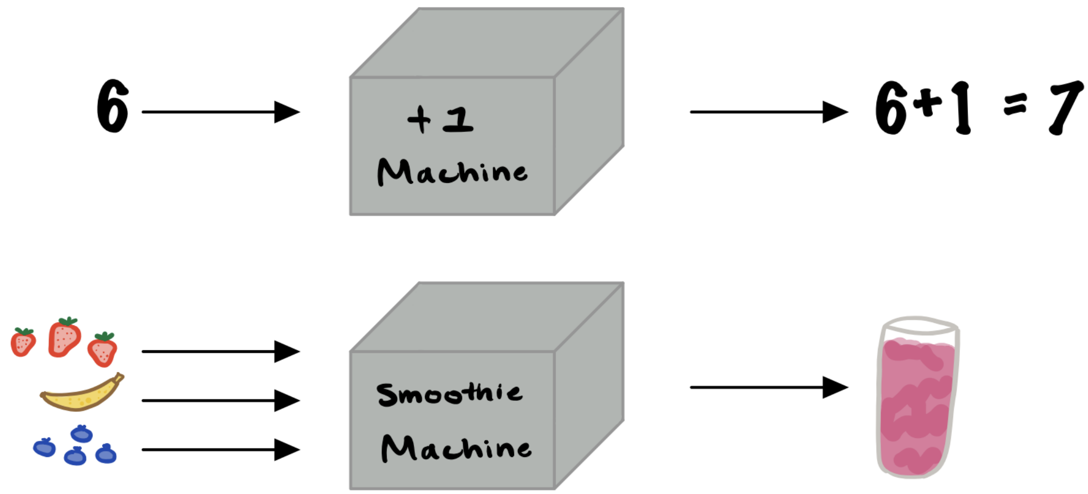


Figure 1: The first machine (operation) takes in a number and adds 1 to that number. The second machine (operation) takes in 3 fruits of your choice and blends them to make a smoothie.

Definition 3

A **binary operation** on a set is an operation that takes in two elements of the set and outputs another element of the set.

Notation

If S is a set and we use $\bullet$ to refer to a binary operation on S, then $a \bullet b$ is the element in S that we get after applying $\bullet$ to the elements $a \in S$ and $b \in S$.

Note: Depending on what S and $\bullet$ are, $a \bullet b$ is not always equal to $b \bullet a$.

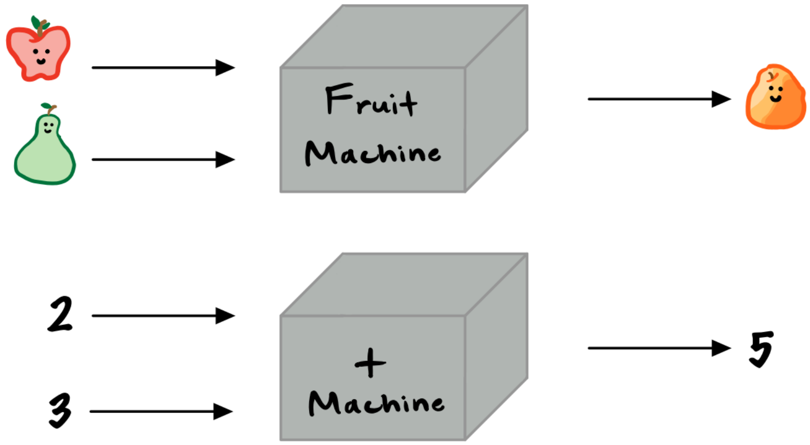


Figure 2: The first machine (binary operation) takes in two fruits and combines them to make a new fruit. In this example, the machine combines an apple and a pear to make a papple. The second machine (binary operation) takes in two numbers and adds them together.

Stop and Think

Binary often refers to 2 things, or a pair of things. And in mathematics, an *operation* roughly means combing a bunch of things in some way to produce something new. So, *binary operation* means combing 2 things to make another thing.

Example 3

Addition is a binary operation on $\mathbb{Z}$ because if we add any two integers together we get another integer. In symbols, if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$. The "machine" here takes in two integers a and b, and outputs the integer $a + b$.

Now that we familiarized ourselves with sets and binary operations, we are ready to define a group.

Definition 4

A **group** is a set G together with a binary operation $\bullet$ on G such that the following rules hold:

1. (Associativity) For every $a, b, c \in G$,
$$(a \bullet b) \bullet c = a \bullet (b \bullet c).$$
2. (Identity element) There exists $\mathrm{id}_G \in G$ such that for all $a \in G$,
$$\mathrm{id}_G \bullet a = a = a \bullet \mathrm{id}_G.$$
3. (Inverse element) For every $a \in G$, there exists $a^{-1} \in G$ such that
$$a \bullet a^{-1} = \mathrm{id}_G = a^{-1} \bullet a.$$

Notation and Terminology

We often write $(G, \bullet)$ for the group G with binary operation $\bullet$. Given a group $(G, \bullet)$, we call G the **underlying set** of the group. Also, we refer to rules 1-3 as the **group axioms**.

Let's go through each group axiom individually! For a concrete example, we will see that the group axioms hold for $\mathbb{Z}$ with the binary operation addition.

Axiom 1 says that the operation is *associative*. Associative means that rearranging the parentheses in an expression will not change the end result. In other words, the order in which we evaluate operations doesn't matter. Addition on the integers is associative. For example

$$5 + (2 + 3) = 10 = (5 + 2) + 3.$$

Axiom 2 says that the underlying set G contains a special element, which we call the identity element. We denote the identity element by id_G. This element is special because if we use the operation on any element in G and the identity, we get that element back. For example, consider addition on $\mathbb{Z}$. We know that

$$0 + a = a = a + 0$$

for any integer a. For instance, $0 + 6 = 6 = 6 + 0$. So $\mathrm{id}_{\mathbb{Z}} = 0$ for $\mathbb{Z}$ with addition. In general, note that the identity element of a group is unique. That is, if $(G, \bullet)$ is a group then id_G is the only element in G that satisfies the property in Axiom 2. Because of this, it's okay to say that id_G is *the* identity element of $(G, \bullet)$.

Axiom 3 says that every element in the underlying set G has an *inverse*. The inverse of an element in G is another element in G, such that when we use the operation on both, we get the identity element id_G. For example, consider $\mathbb{Z}$ with addition. We know that

$$a + (-a) = 0 = (-a) + a$$

for any integer a. For instance, $6 + (-6) = 0 = (-6) + 6$. So, $-a$ is the inverse of a. In general, note that if the inverse of $g \in G$ is $g^{-1} \in G$, then the inverse of g^{-1} is g.

If a set G and binary operation $\bullet$ satisfy these 3 axioms, then $(G, \bullet)$ is a group!

Example 4

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

Solution:

We know from Example 3 that addition is a binary operation on $\mathbb{Z}$. So, we just need to check that the 3 group axioms in Definition 4 hold.

1. We know that it doesn't matter what order we add numbers in. So the first axiom holds.
2. Recall that if we add any integer to zero, we just get the integer back. That is, for any integer $a \in \mathbb{Z}$ we have that $a + 0 = a = 0 + a$. This means that 0 is the identity element. So the second axiom holds.
3. If $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$ and $(-a) + a = a + (-a) = a - a = 0$. This means that $-a$ is the inverse of a. So the third axiom holds.

Exercise 1

Consider the set $\{-1, 1\}$. Convince yourself that multiplication $\times$ is a binary operation on $\{-1, 1\}$. Show that $(\{-1, 1\}, \times)$ is a group.

Exercise 2

In Example 4 we saw that $(\mathbb{Z}, +)$ is a group. Now consider multiplication $\times$ on $\mathbb{Z}$. Convince yourself that $\times$ is a binary operation on $\mathbb{Z}$. Is $(\mathbb{Z}, \times)$ a group?

Exercise 3

Recall that a rational number is of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and b is not zero. Let $\mathbb{Q}$ be the set of all rational numbers. And let $\mathbb{Q}^*$ be the set $\mathbb{Q}$ but with 0 removed. Recall that we multiply two rational numbers by

$$\frac{a}{b} \times \frac{a'}{b'} = \frac{aa'}{bb'}.$$

Convince yourself that multiplication $\times$ is a binary operation on $\mathbb{Q}^*$. Is $(\mathbb{Q}^*, \times)$ a group?

Symmetry groups

At the beginning of the lesson, we said that certain rotations and reflections of the Benzene molecule form a group. In fact, they form a special kind of group called a *symmetry group*. For the reminder of the lesson we are going to explore symmetry groups and see how the rotations and reflections of the Benzene molecule form a group!

Stop and Think

What does the word *symmetry* mean to you? Have you heard it before? If so, where?

If you think back, you may have learnt that the monarch butterfly exhibits what we call symmetry. If you look up the word "symmetry" there are all sorts of definitions, but they all amount to a sense of *balance* and *harmony*. The monarch butterfly exhibits balance in the sense that both of it's wings are the same. Imagine drawing a vertical line between the two wings of the butterfly. You can see that the same image appears on both sides of the line, with the only difference being that each side looks like the opposite side after being flipped over the line. Here we say that this imaginary line is a *line of symmetry*.

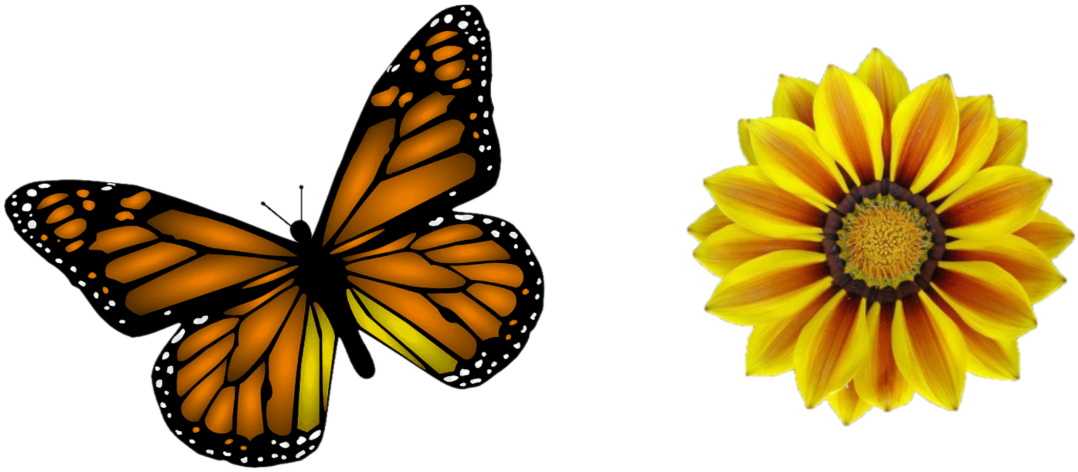


Figure 3: A monarch butterfly[1] and flower[2] that exhibit symmetry.

Stop and Think

Look at the flower in Figure 3. Do you see the symmetry that the flower has? What are the lines of symmetry for this flower?

In mathematics, we like to make our definitions as precise as possible. A "sense of harmony and balance" isn't a very precise definition for symmetry.

Definition 5

In mathematics, a **symmetry of a shape** is an action (e.g., rotation, reflection) such that when applied to the shape you get the shape back.

There are other types of actions in mathematics, but for our purposes, we will only be considering rotations and reflections.

[1]PNGWING. The Monarch Butterfly Insect [Online]. Available from: https://www.pngwing.com/en/free-png-dguvl [Accessed March 19 2023].

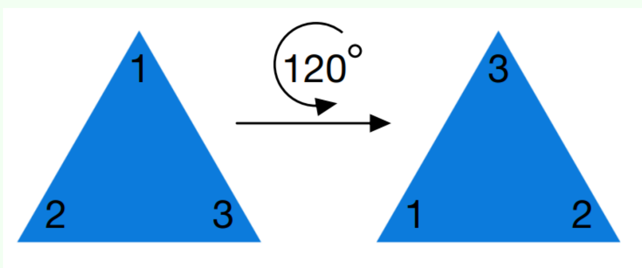
[2]Tes for Teachers. Symmetry Lessons [Online]. Available from: https://www.pinterest.ca/pin/329114685250253709/ [Accessed March 19 2023].

Example 5

Consider the butterfly in Figure 3. Reflection in the line of symmetry discussed earlier is a symmetry of the butterfly because when we reflect the butterfly in this line it is unchanged.

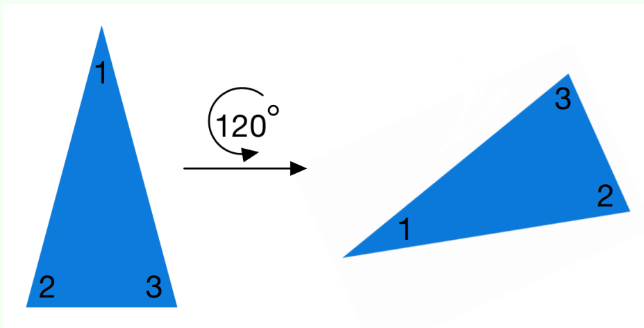
Example 6

Consider the image below. We label the tips of the left triangle with numbers to help us keep track of actions performed on the triangle. In other words, the numbers help us see how actions move the triangle. For example, in this image we see that if we rotate the left triangle counter clockwise by 120 degrees, we end up with the triangle on the right. This action sends tip 1 to where tip 2 was, tip 2 to where tip 3 was, and tip 3 to where tip 1 was. Aside from the labels, the resulting triangle on the right is identical to the original triangle on the left. This means that rotation counter clockwise by 120 degrees is a symmetry of this triangle.



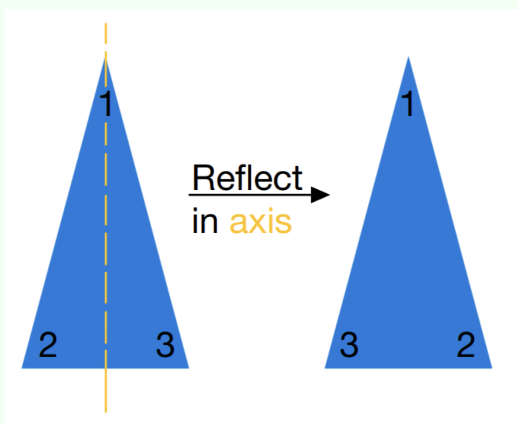
Example 7

Consider the image below. The action here is the same as in Example 6, but on a different triangle. The sides of the triangle in Exercise 6 are all the same length, whereas the sides of the triangle below are not all the same. If we rotate the left triangle counter clockwise by 120 degrees, we end up with the triangle on the right. The resulting triangle on the right does not look like the original triangle on the left. Because of this, rotation counter clockwise by 120 degrees is **not** a symmetry of this triangle.



Example 8

Consider the image below. The action in this example is reflection in the axis (or line) which is depicted as the dotted yellow line. If we reflect in this axis, we see that 1 stays in the same spot and, 2 and 3 swap places. Again, aside from the labelling, the triangle on the right is identical to the one on the left. This means that reflection in this axis is a symmetry of this triangle.



Exercise 4

An equilateral triangle is a triangle whose 3 sides all have the same length. The triangle in Example 6 is an equilateral triangle. Write down all of the symmetries of an equilateral triangle.

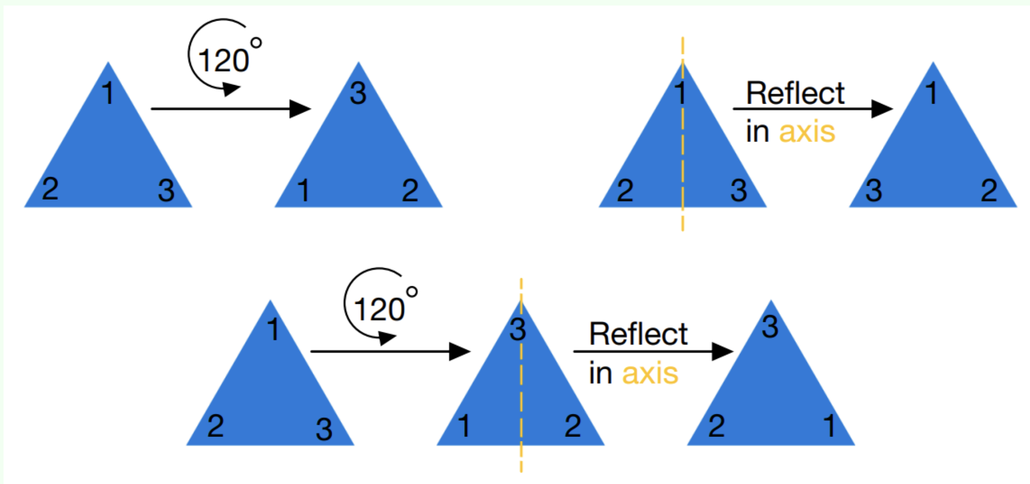
Recall that a group is a set, together with a binary operation, that satisfies the group axioms. Given any shape, we can form a group which we call the *symmetry group* of that shape. The underlying set for the symmetry group of a shape is the set of symmetries of that shape. Next, we define the binary operation for symmetry groups.

Definition 6

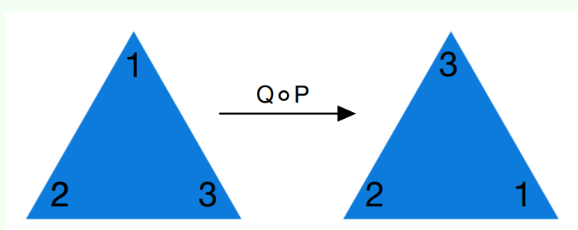
Let P and Q be symmetries of a given shape. The **composition** of Q with P, written $Q \circ P$, is an action that applies P to the shape and then applies Q to this result. The symbol $Q \circ P$ is read as "P followed by Q".

Example 9

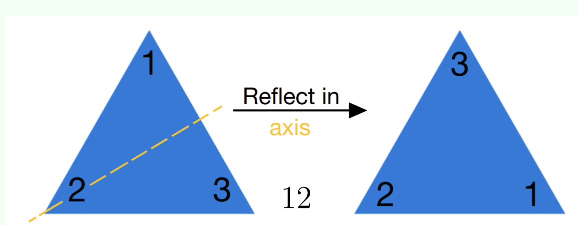
Consider the first image below. The top left symmetry is from Example 6. The top right symmetry is from Example 8, but on an equilateral triangle. The bottom trio of triangles in this image depicts the composition of "reflect in yellow axis" with "rotate counter clockwise by 120 degrees". The composition is computed by first rotating the left most triangle by 120 degrees counter clockwise, and then reflecting this resulting triangle (middle triangle) in the yellow axis.



Let P denote rotation counter clockwise by 120 degrees. Let Q denote reflection in the axis depicted above. Then the above illustrates how to compute the composition $Q \circ P$. This composition can also be depicted with the following photo:



Note that this composition is the same as the following symmetry:



In Example 9, we see that the composition of the two symmetries is itself a symmetry of the triangle. This is true in general. We take it as a fact that if P and Q are symmetries of a shape S, then $Q \circ P$ is a symmetry of S. This means that composition $\circ$ is a binary operation on the set of symmetries of a shape S. Composition is the binary operation that makes the set of symmetries into a group. In other words, the set of symmetries of a shape S, together with composition, form a group.

Definition 7

Let S be a shape and $\mathrm{Sym}(S)$ be the set of symmetries of S. Then $(\mathrm{Sym(S)}, \circ)$ is a group called the **symmetry group of S**.

Exercise 5

Let T be an equilateral triangle. In Exercise 4 you wrote down every element of $\mathrm{Sym}(T)$. Convince yourself that $(\mathrm{Sym}(T), \circ)$ is a group.

$**$ See solutions to Exercise 5 before reading on $**$

The proof for Exercise 5 can be generalized to show that $(\mathrm{Sym}(S), \circ)$ is a group for any shape S. Let's sketch how this works. We need to convince ourselves that the group axioms hold for $\mathrm{Sym}(S)$ with composition, where S is any shape. So, let $P, Q, R \in \mathrm{Sym}(S)$.

Axiom 1: For associativity to hold, we need $(P \circ Q) \circ R$ to be the same symmetry as $P \circ (Q \circ R)$. This axiom is a bit tough to argue rigorously given our current mathematical tools. However, if you know a bit about functions, then by viewing each symmetry as a function, associativity is fairly immediate and you can show that

$$(P \circ Q) \circ R = P \circ Q \circ R = P \circ (Q \circ R).$$

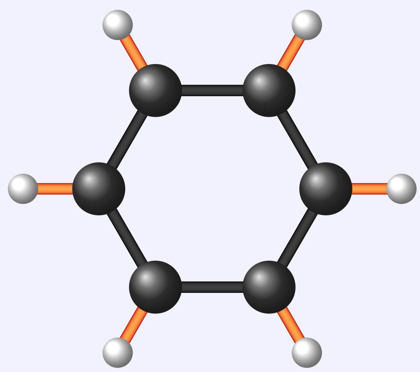
The proof for associativity isn't that enlightening, and it is more valuable to see why it holds for concrete examples, like in Exercise 5. So, if you were able to convince yourself that associativity holds in Exercise 5, that is plenty good enough!

Axiom 2: The action "do nothing" on S is a totally valid symmetry of S. If you apply P to S and then do nothing, it's the same as just applying P to S. Similarly, if you do nothing to S and then apply P, that's the same as just applying P to S. This means that "do nothing" is the identity element for $\mathrm{Sym}(S)$ with composition.

Axiom 3: Lastly, if we apply a symmetry P to S, then we can always undo this action by applying the reverse action. The reverse action of P is itself a symmetry and we denote it by P^{-1}. If we apply P and then undo this action by applying P^{-1}, it is the same as doing nothing. Similarly, if we apply P^{-1} and then P, it is the same as doing nothing. In other words, $P \circ P^{-1}$ and $P^{-1} \circ P$ are the identity element. So, every element of $\text{Sym}(S)$ has an inverse.

Exercise 6

Consider the benzene molecule below and denote it by BM. The benzene molecule is a shape, and so $(\text{Sym}(BM), \circ)$ is a group. Chemists study the symmetries of molecules such as BM and classify molecules according to their symmetry group. The study of such symmetries can be used to predict or explain chemical properties of a molecule.



Write down the symmetry group of the benzene molecule BM. In other words, write down the elements of $\text{Sym}(BM)$.