Grade 9/10 Math Circles

An Introduction to Group Theory Part 1 - Solutions

Exercise Solutions

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 1 Solution

To convince ourselves that multiplication is a binary operation on $\{-1, 1\}$, let's check that the multiplication of any two elements of $\{-1, 1\}$ is again an element of $\{-1, 1\}$. Indeed, this is true since:

$$(-1) \times (-1) = 1, \quad (-1) \times 1 = -1, \quad 1 \times (-1) = -1, \quad 1 \times 1 = 1.$$

To show that $(\{-1, 1\}, \times)$ is a group we need to check that the 3 group axioms hold. Let's go through each axiom:

Axiom 1: It doesn't matter what order we multiply numbers in. So, associativity holds.

Axiom 2: The identity element is 1 because the multiplication of 1 with any number is that number again. In particular,

$$1 \times 1 = 1, \quad 1 \times (-1) = -1 = (-1) \times 1.$$

Axiom 3: The inverse of -1 is -1 since $(-1) \times (-1) = 1$. The inverse of 1 is 1 since $1 \times 1 = 1$. This shows that every element in $\{-1, 1\}$ has an inverse.

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 2 Solution

We know that if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $a \times b = ab \in \mathbb{Z}$. So, multiplication is a binary operation on $\mathbb{Z}$. Although multiplication is a binary operation on $\mathbb{Z}$, $(\mathbb{Z}, \times)$ is **not** a group. To show that $(\mathbb{Z}, \times)$ is not a group, we need to show that at least one of the 3 group axioms does not hold. Axiom 1 is satisfied because it doesn't matter what order we multiply numbers in. And Axiom 2 is satisfied because 1 is the identity element.

We claim that Axiom 3 does not hold. To show that Axiom 3 does not hold, we need to find at least one element of $\mathbb{Z}$ that does not have an inverse. The element $0 \in \mathbb{Z}$ does not have an inverse because 0 times any number is 0, not 1. That is, for any $a \in \mathbb{Z}$,

$$0 \times a = 0 = a \times 0$$

which is not the identity element 1. So, 0 does not have an inverse. This shows that Axiom 3 does not hold and hence $(\mathbb{Z}, \times)$ is not a group. In fact, the only element in $\mathbb{Z}$ that has an inverse is 1. Can you show that any $a \in \mathbb{Z}$ satisfying $a \notin \{0, 1\}$ does not have an inverse?

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?

Exercise 3 Solution

Let $a/b \in \mathbb{Q}^*$ and $a'/b' \in \mathbb{Q}^*$. By definition of $\mathbb{Q}^*$, b and b' are not zero and so bb' is not zero. Thus, the multiplication

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

is in $\mathbb{Q}$ since $aa', bb' \in \mathbb{Z}$ and bb' is not zero. It remains to show that the multiplication of a/b with a'/b' is not zero. Well, since these elements are not zero, a and a' are not zero. Then aa' is not zero, and so aa'/bb' is not zero. So, $aa'/bb' \in \mathbb{Q}^*$. We conclude that multiplication is a binary operation on $\mathbb{Q}^*$. We claim that $(\mathbb{Q}^*, \times)$ is a group. Let's go through each group axiom:

Axiom 1: It doesn't matter what order we multiply numbers in. So, associativity holds.

Axiom 2: The identity element is $1 = 1/1$ because the multiplication of 1 with any number is that number again. In particular, for any $a/b \in \mathbb{Q}^*$, we have that

$$1 \times \frac{a}{b} = \frac{a}{b} = \frac{a}{b} \times 1.$$

Axiom 3: We need to show that every element in $\mathbb{Q}^*$ has an inverse. So, let $a/b \in \mathbb{Q}^*$. Because a and b are not zero, the element b/a is also in $\mathbb{Q}^*$. We compute that

$$\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = 1,$$

and similarly

$$\frac{b}{a} \times \frac{a}{b} = 1.$$

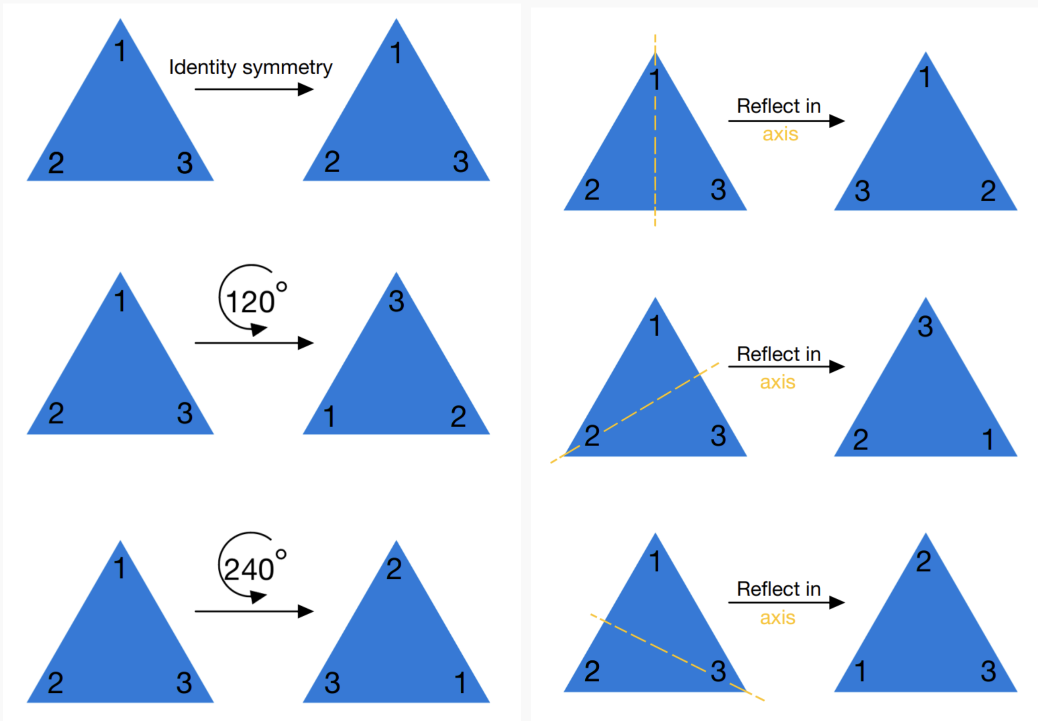
This shows that b/a is the inverse of a/b. So, every element in $\mathbb{Q}^*$ has an inverse.

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

Exercise 4 Solution

The complete list of symmetries of an equilateral triangle are as follows:



In words, these symmetries are:

- The "do nothing symmetry", which is the same as rotation by 360 degrees. This is labelled as the "identity symmetry" because it is the identity element of the group $(\mathrm{Sym}(T), \circ)$, where T is an equilateral triangle (we will see this in Exercise 5).
- Counter clockwise rotation by 120 degrees
- Counter clockwise rotation by 240 degress.
- Reflection in the axis that goes through the center and top tip of the triangle.
- Reflection in the axis that goes through the center and left tip of the triangle.
- Reflection in the axis that goes through the center and right tip of the triangle.

Note that clockwise rotations by multiples of 120 degrees are also symmetries. However, these symmetries are already in the above list. For example, rotation clockwise by 120 degrees is the same as counter clockwise rotation by 240 degrees. If you prefer, you can replace "counter clockwise" with "clockwise" in the above list, it doesn't matter at all. Also note that rotations by $n120$ degrees with $n \geq 4$ are symmetries. Again, they are already in the above list. For example, counter clockwise rotation by 480 degrees is the same as counter clockwise rotation by 120 degrees.

Exercise 5

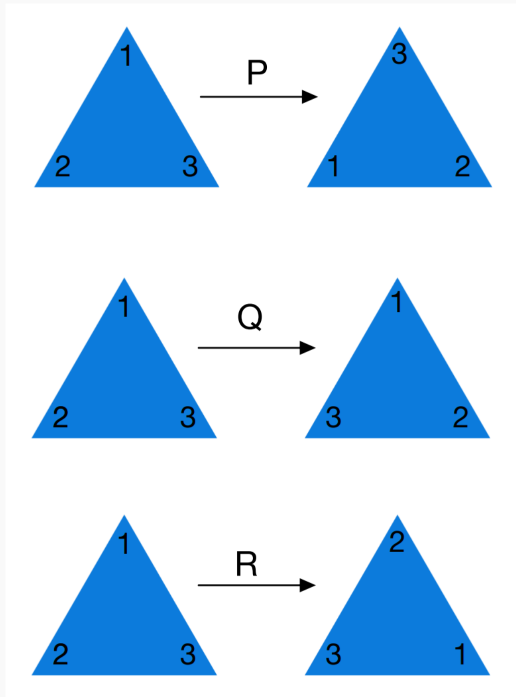
Let T be an equilateral triangle. In Exercise 4 you computed $\text{Sym}(T)$. Convince yourself that $(\text{Sym}(T), \circ)$ is a group.

Exercise 5 Solution

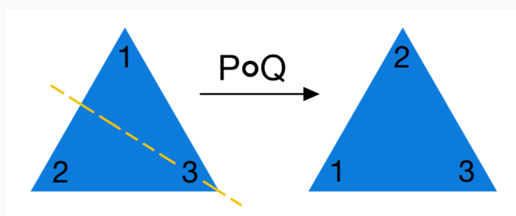
We need to convince ourselves that the 3 group axioms hold for $\text{Sym}(T)$ with composition. Let's go through each axiom:

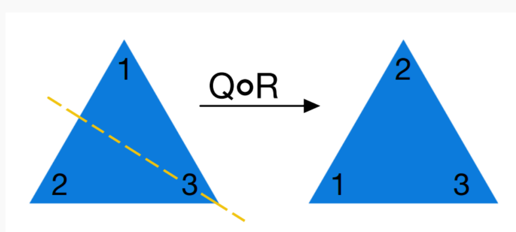
Axiom 1: For all $P, Q, R \in \text{Sym}(T)$, we need $(P \circ Q) \circ R$ to be the same symmetry as $P \circ (Q \circ R)$. Proving this is a bit tough given our current tools, so let's do a concrete example to see why it works.

Let P be counter clockwise rotation by 120 degrees, let Q be reflection in the axis that goes through the center and top tip of the triangle, and let R be counter clockwise rotation by 240 degrees. These symmetries are illustrated as follows:

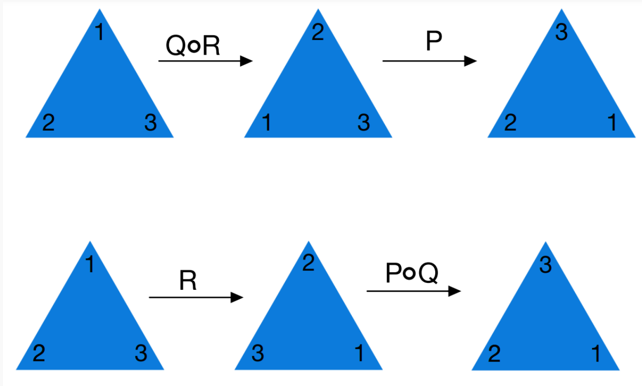


The compositions $P \circ Q$ and $Q \circ R$ are computed to be:

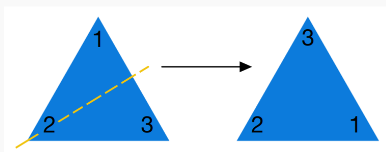




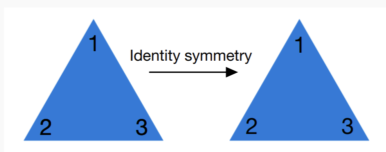
We see that these two compositions are the same symmetry, and they are equal to the symmetry that reflects in the axis going through the center and right tip of the triangle. Using these compositions, we compute $P \circ (Q \circ R)$ and $(P \circ Q) \circ R$:



We see that $P \circ (Q \circ R) = (P \circ Q) \circ R$, as desired. They are equal to the symmetry that reflects in the axis going through the center and left tip of the triangle:

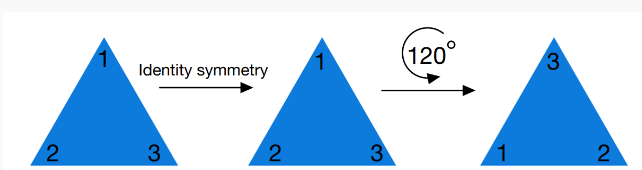


Axiom 2: The identity element in $\mathrm{Sym}(T)$ is the "do nothing" symmetry. Here is an illustration of the identity element:

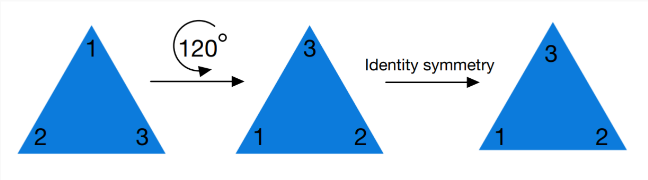


Let P be any symmetry of T. If you do nothing to T and then apply P, it's the same as just applying P to T. Similarly, if you apply P to T and then do nothing, it's the same as just applying P to T. So indeed, this is the identity element $\mathrm{id}_{\mathrm{Sym}(T)}$.

Let's do a concrete example where P is chosen to be counter clockwise rotation by 120 degrees. Here is the composition $P \circ \mathrm{id}_{\mathrm{Sym}(T)}$:



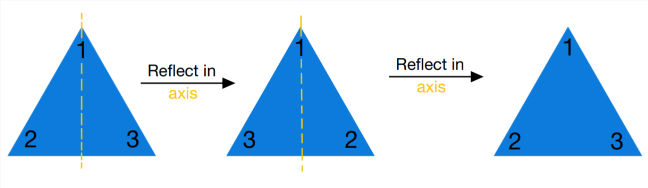
We see that this composition is just P. Here is the composition $\mathrm{id}_{\mathrm{Sym}(T)} \circ P$:



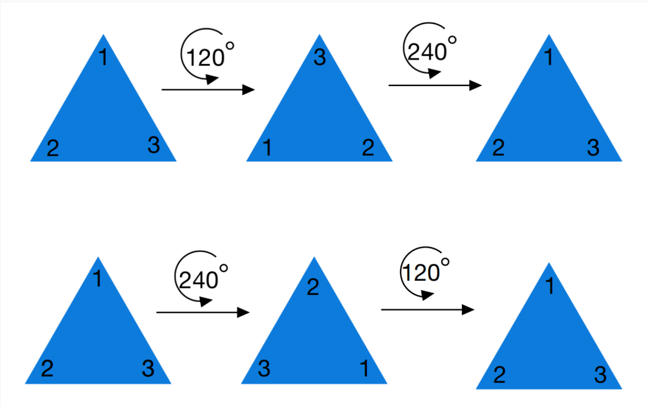
Again, we see that this composition is just P.

Axiom 3: We need to show that every element in $\text{Sym}(T)$ has an inverse. For this, it will be helpful to recall the elements of $\text{Sym}(T)$ from Exercise 4.

First consider the symmetries that are reflections. The inverse of a reflection is itself. In other words, if $R \in \text{Sym}(T)$ is a reflection then the inverse of R is R, that is $R^{-1} = R$. This is because if we reflect in the same axis twice, it's the same as doing nothing. Here is a concrete example:



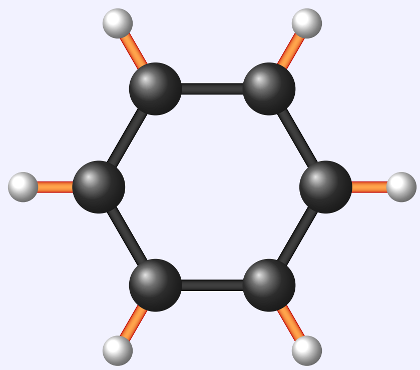
We see that this composition is just $\text{id}_{\text{Sym}(T)}$. Next, consider symmetries that are rotations. If $S \in \text{Sym}(T)$ is a rotation, then by Exercise 4, it's counter clockwise rotation by $n120$ degrees for some $n \in \{0, 1, 2\}$. The inverse of counter clockwise rotation by $n120$ degrees is the symmetry that reverses this rotation, which is clockwise rotation by $n120$ degrees. Note that clockwise rotation by $n120$ degrees is the same symmetry has counter clockwise rotation by $(360 - n120)$ degrees. Here is a concrete example where we take $n = 1$:



We see that these two compositions are just $\text{id}_{\text{Sym}(T)}$.

Exercise 6

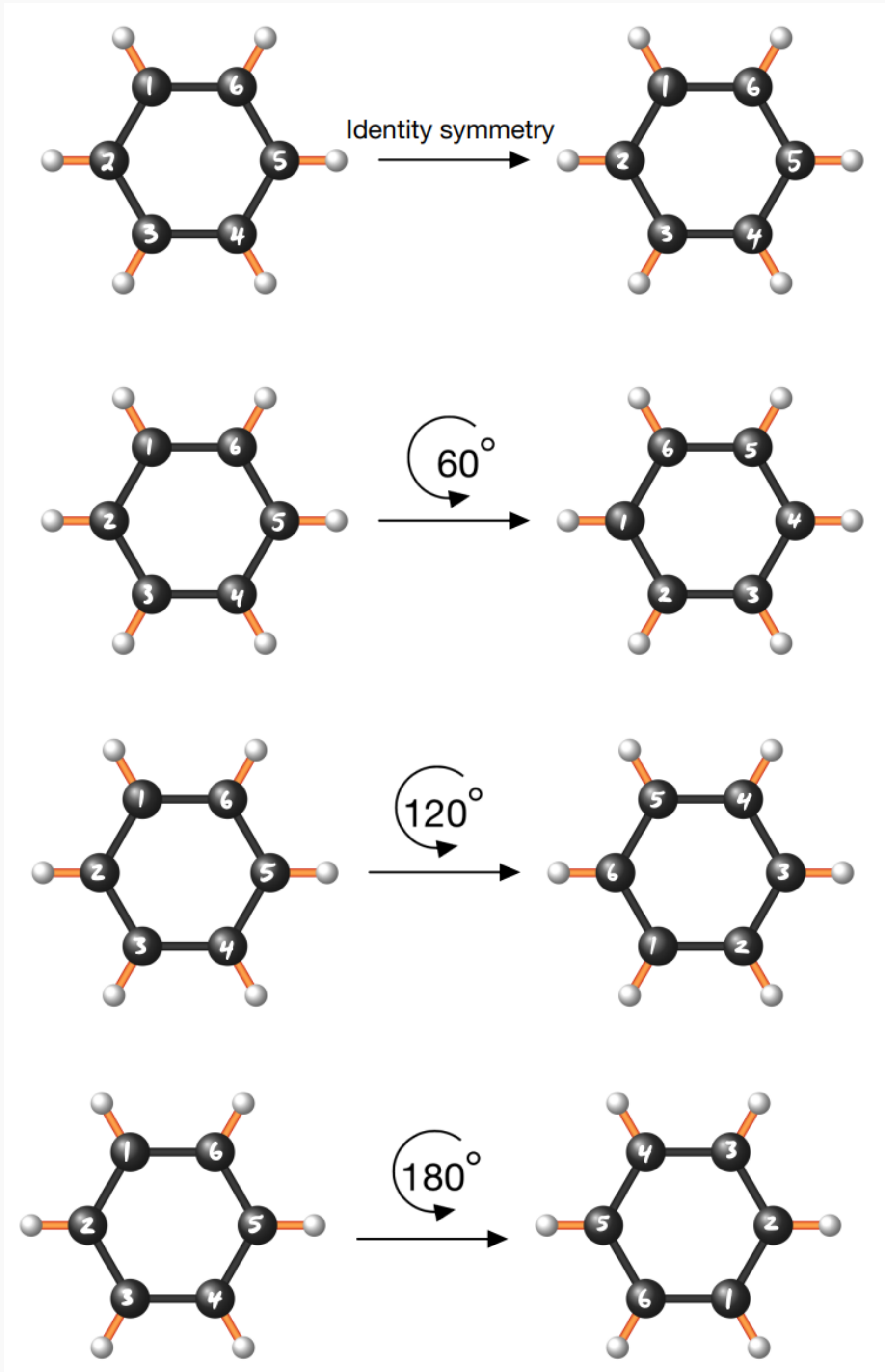
Consider the benzene molecule below and denote it by BM. The benzene molecule is a shape, and so $(\text{Sym}(BM), \circ)$ is a group. Chemists study the symmetries of molecules such as BM, and classify molecules according to their symmetry group. The study of such symmetries can be used to predict or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

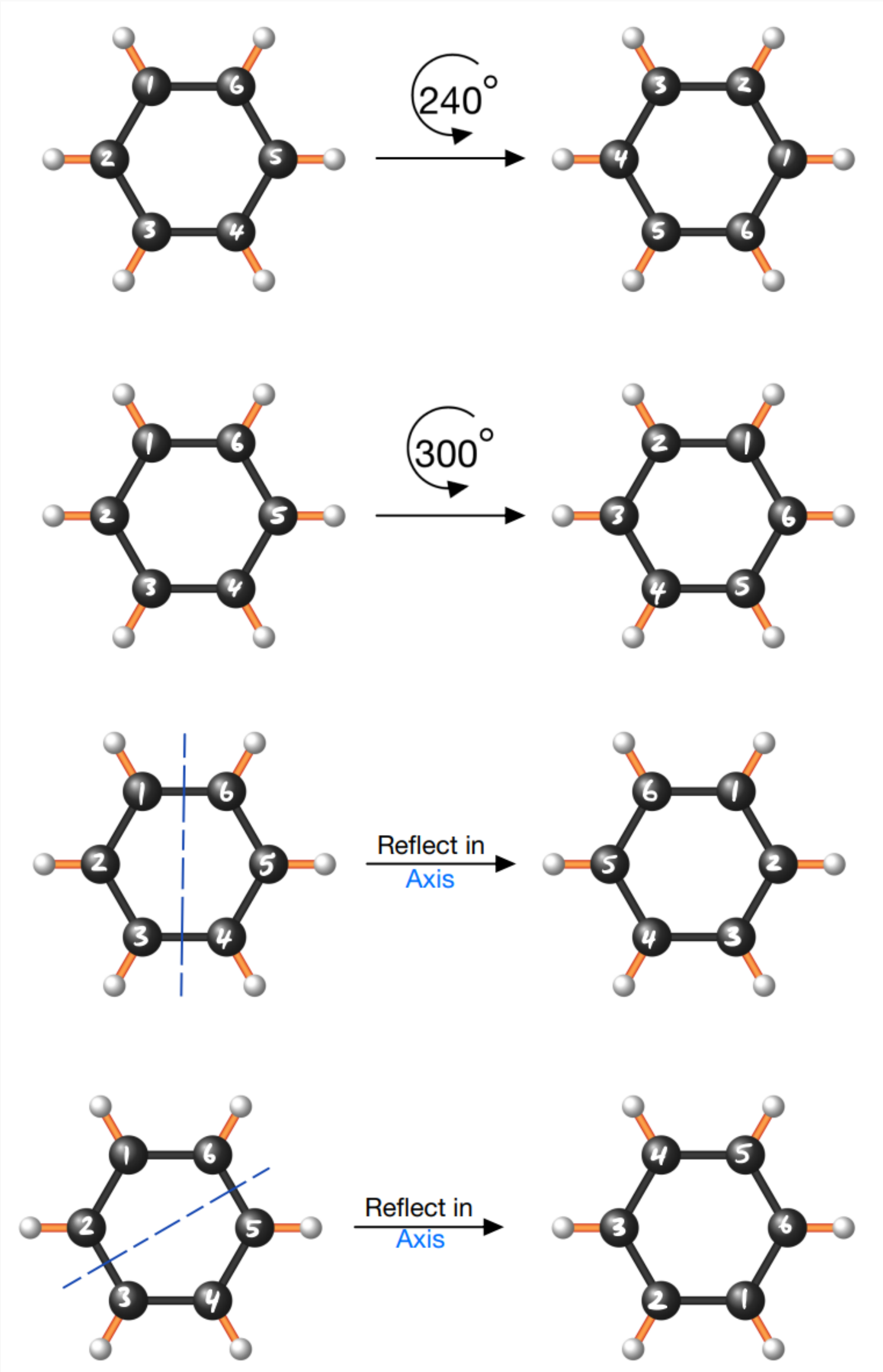


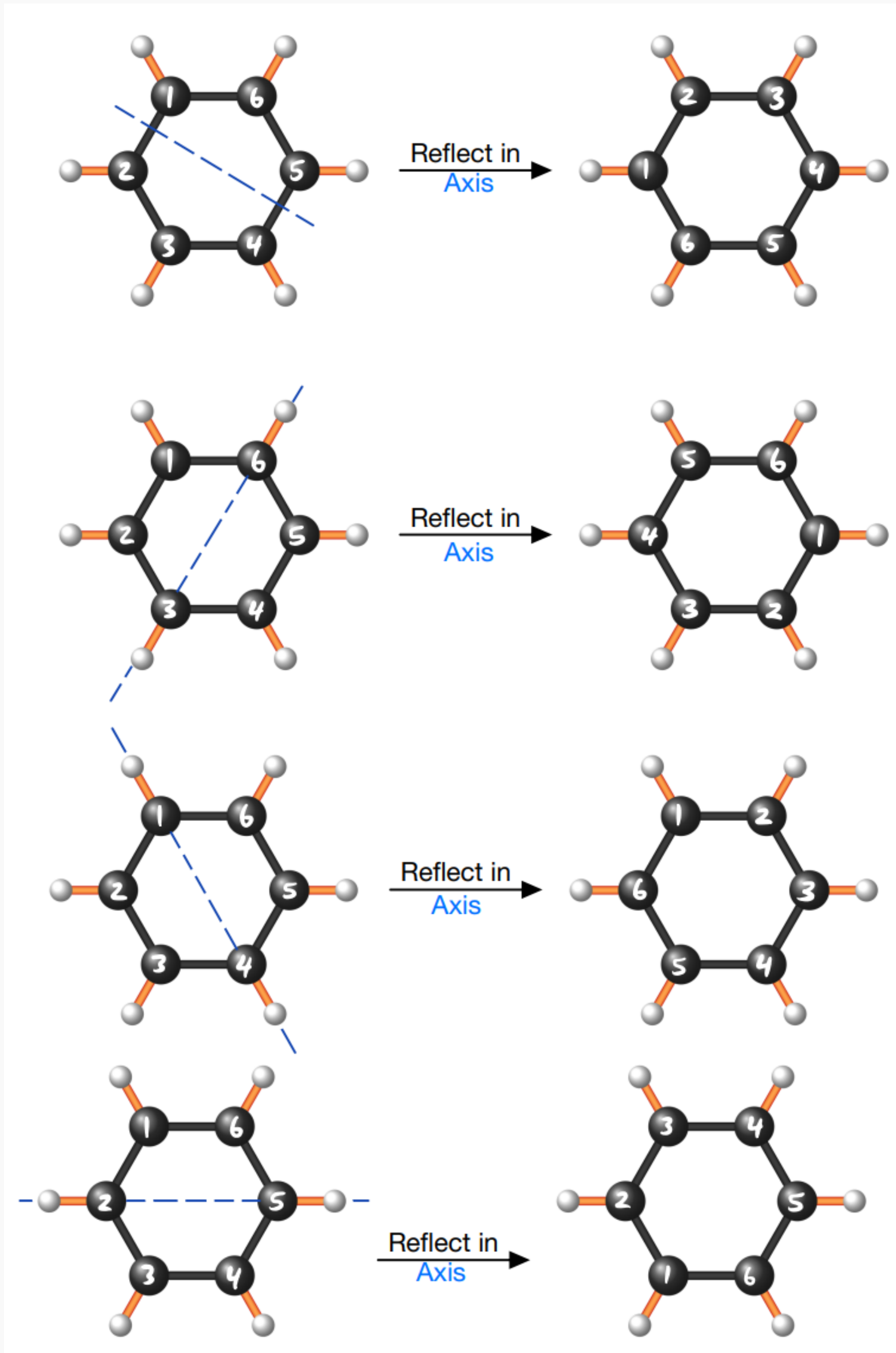
Write down the symmetry group of the benzene molecule BM. In other words, write down the elements of $\text{Sym}(BM)$.

Exercise 6 Solution

The complete list of symmetries of the benzene molecule are as follows:


Identity symmetry
60°
120°
180°


240°
300°
Reflect in
Axis
Reflect in
Axis



There are 6 counter clockwise rotations by multiples of 60 degrees. And there are 6 reflections in the axes shown above.

Problem Set Solutions

1. In Example 4 we saw that $(\mathbb{Z}, +)$ is a group. Now consider subtraction $-$ on $\mathbb{Z}$. Convince yourself that subtraction is a binary operation on $\mathbb{Z}$. Show that subtraction on $\mathbb{Z}$ is not associative and use this to conclude that $(\mathbb{Z}, -)$ is not a group.

Solution: We know that if $a, b \in \mathbb{Z}$, then $a - b \in \mathbb{Z}$. So, subtraction is a binary operation on $\mathbb{Z}$. Next, let's show that subtraction on $\mathbb{Z}$ is not associative. To do this, we need to find integers $a, b, c \in \mathbb{Z}$ such that

$$a - (b - c) \neq (a - b) - c.$$

Here the symbol $\neq$ means "not equal". If $a = 1, b = 2, c = 3$, then

$$a - (b - c) = 1 - (2 - 3) = 1 - (-1) = 1 + 1 = 0$$

and

$$(a - b) - c = (1 - 2) - 3 = (-1) - 3 = -1 - 3 = -4.$$

But $0 \neq -4$, so

$$1 - (2 - 3) \neq (1 - 2) - 3.$$

This shows that subtraction on $\mathbb{Z}$ is not associative, and so Axiom 1 of the group axioms is not satisfied. So $(\mathbb{Z}, -)$ is not a group.

Note: It is true that

$$a - (b - c) \neq (a - b) - c$$

for any $a, b, c \in \mathbb{Z}$ as long as $c \neq 0$. Can you show this?

2. Consider the set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, ...\}$, which is the set containing all non-negative whole numbers. Addition is a binary operation on $\mathbb{N}$. Show that $(\mathbb{N}, +)$ is not a group.

Solution: To show that $(\mathbb{N}, +)$ is not a group, we need to show that at least one of the 3 group axioms does not hold. Axiom 1 holds because it doesn't matter what order we add numbers in. We see that Axiom 2 holds because

$$0 + n = n = n + 0$$

for any $n \in \mathbb{N}$, and so 0 is the identity element for $\mathbb{N}$ with addition.

We claim that Axiom 3 does not hold. To show that Axiom 3 does not hold, we need to find at least one element of $\mathbb{N}$ that does not have an inverse. It turns out that every element of $\mathbb{N}$, aside from 0, does not have an inverse. To see this, let $n \in \mathbb{N}$ and assume that n is not zero. If n had an inverse, say n', then we would have that $n + n' = 0$ and so $n' = -n$. So, if n had an inverse then it would have to be $-n$. However, since n is not zero, we have that $n > 0$. This implies that $-n < 0$, which means that $-n$ is a negative integer, and so $-n \notin \mathbb{N}$. But remember that by definition of inverse, if n had an inverse it would have to be an element of $\mathbb{N}$. So, this shows that n does not have an inverse.

3. Consider the set of even integers

$$2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}.$$

Convince yourself that addition is a binary operation on $2\mathbb{Z}$. Show that $(2\mathbb{Z}, +)$ is a group.

Solution: To convince ourselves that addition is a binary operation on $2\mathbb{Z}$, let's check that the addition of any two elements of $2\mathbb{Z}$ is again an element of $2\mathbb{Z}$. So, let $x, y \in 2\mathbb{Z}$. We know that the addition of two integers is again an integer, so $x+y$ is an integer. It remains to show that $x + y$ is even. Since x and y are even, we can write

$$x = 2k \quad \text{and} \quad y = 2\ell$$

for some $k, \ell \in \mathbb{Z}$. Then

$$x + y = 2k + 2\ell = 2(k + \ell),$$

which shows that $x + y$ is even. We conclude that $x + y \in 2\mathbb{Z}$, and so addition is a binary operation on $2\mathbb{Z}$. To show that $(2\mathbb{Z}, +)$ is a group we need to check that the 3 group axioms hold. Let's go through each axiom:

Axiom 1: It doesn't matter what order we add numbers in. So, associativity holds.

Axiom 2: The identity element is 0 because the addition of 0 with any number is that number again. In particular, for any $x \in 2\mathbb{Z}$,

$$0 + x = x = x + 0.$$

Axiom 3: We need to show that every element of $2\mathbb{Z}$ has an inverse. So, let $x \in 2\mathbb{Z}$. Note that $-x \in 2\mathbb{Z}$ because the negative of an even integer is still an even integer. Then

$$(-x) + x = x + (-x) = x - x = 0.$$

This shows that $-x$ is the inverse of x. So, every element in $2\mathbb{Z}$ has an inverse.

4. Suppose we are given a group $(G, \bullet)$. Axiom 2 of the group axioms says that $(G, \bullet)$ has an identity element, which we denote by $\mathrm{id}_G \in G$. Show that the identity element id_G is unique. In other words, show that there is exactly one element of the group G that satisfies the property: for every $a \in G$, $a \bullet \mathrm{id}_G = a = \mathrm{id}_G \bullet a$.

   Hint: If $e \in G$ satisfies the above property, try to show that $e = \mathrm{id}_G$.

   Solution: Suppose there exists $e \in G$ such that for every $a \in G$,

   $$a \bullet e = a = e \bullet a.$$

   Since this equation holds for every element $a \in G$, it holds for id_G. So

   $$\mathrm{id}_G \bullet e = \mathrm{id}_G. \tag{1}$$

We know id_G satisfies the same property as e. That is, for every $a \in G$,

$$a \bullet \mathrm{id}_G = a = \mathrm{id}_G \bullet a.$$

Since this equation holds for every element $a \in G$, it holds for e. So

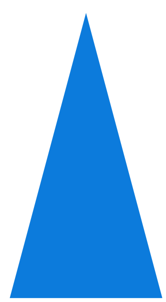
$$e = \mathrm{id}_G \bullet e. \tag{2}$$

Together, Equations (1) and (2) tell us that

$$e = \mathrm{id}_G \bullet e = \mathrm{id}_G.$$

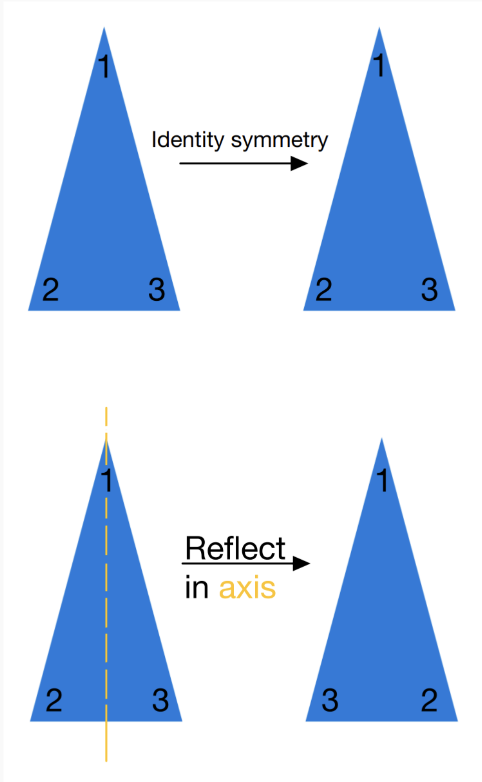
This shows that id_G is the only element of the group that satisfies the above property.

5. Consider the following triangle:



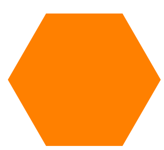
Write down the symmetries of this triangle and compare them with the symmetries of the equilateral triangle found in Exercise 4.

Solution: The complete list of symmetries of the above triangle are as follows:



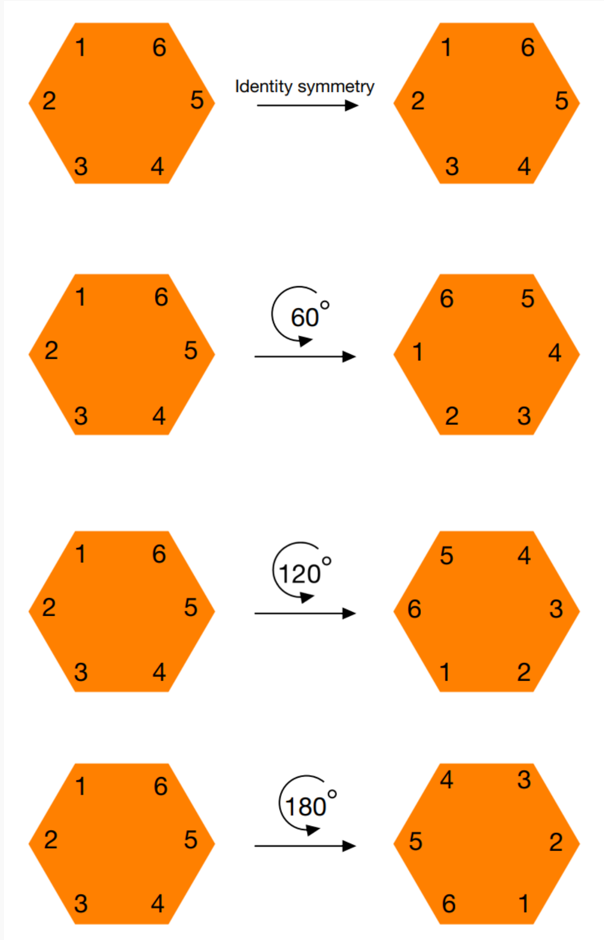
In words, these symmetries are the “do nothing symmetry” (which is the same as rotation by 360 degrees) and reflection in the axis that goes through the center and top tip of the triangle. The symmetries of this triangle are symmetries of the equilateral triangle in Exercise 4. However, the equilateral triangle in Exercise 4 has way more symmetries than this triangle. So, the sets of symmetries are different.

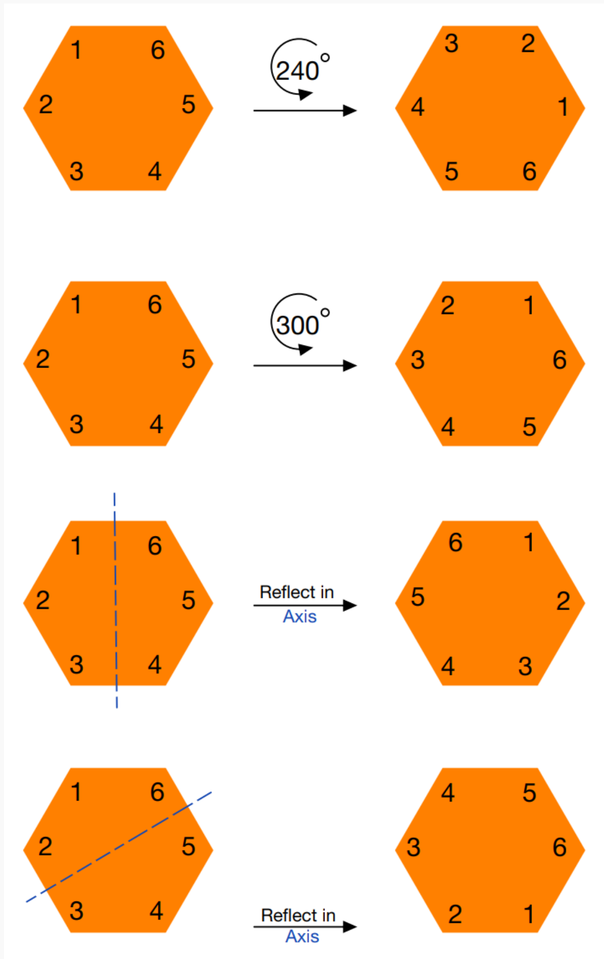
6. Consider the following hexagon:



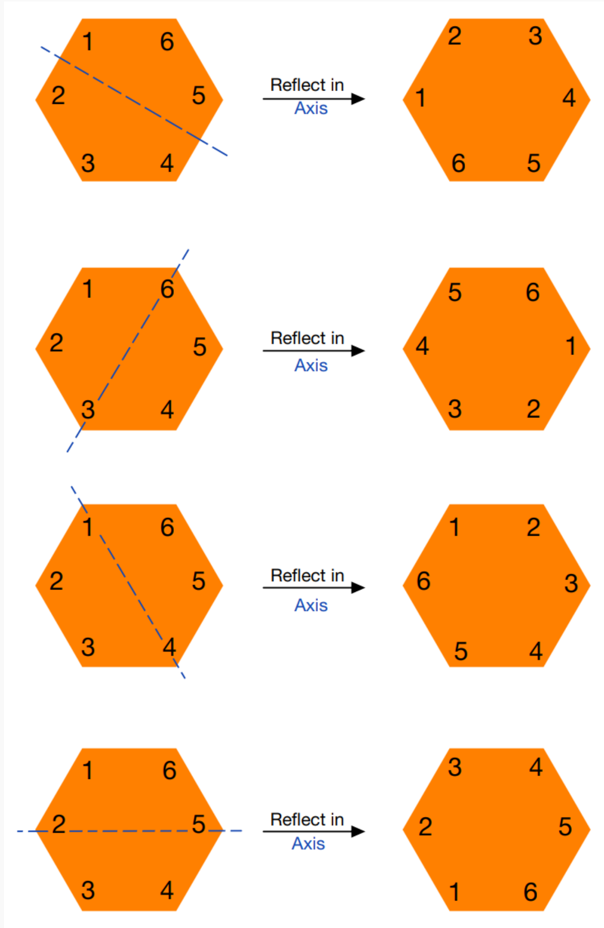
Write down the symmetries of this hexagon. Then compare the symmetries of this hexagon with the symmetries of the benzene molecule, which were found in Exercise 6. Are they the same in some sense? Or are they different?

Solution: The complete list of symmetries of a hexagon are as follows:



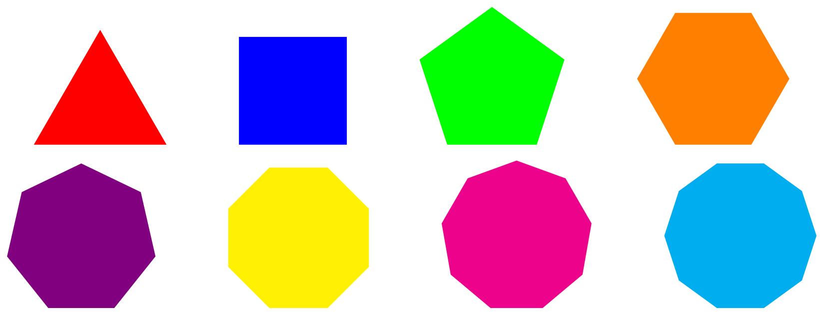


240°
300°
Reflect in
Axis
Reflect in
Axis



There are 6 counter clockwise rotations by multiples of 60 degrees. And there are 6 reflections in the axes shown above. If you compare these 12 symmetries, with the 12 symmetries of the benzene molecule, then we see that they are exactly the same! This is because the benzene molecule has a similar structure to that of the hexagon. You can think of the benzene molecule as a hexagon but with 6 arms sticking out, and these arms do not affect the symmetries.

7. Consider the following shapes:



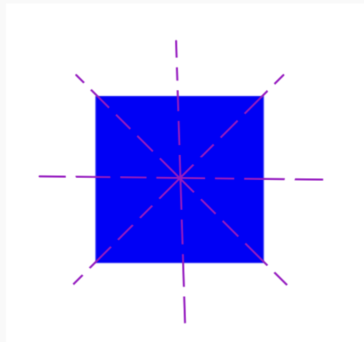
These shapes are examples of regular polygons. A polygon is called regular if all of its sides have the same length and all of its angels are the same. For example, an equilateral triangle is a regular polygon. Write down the symmetry group of an arbitrary regular polygon.
hint: Let P_n be a regular polygon with n sides. The goal is to write down the elements of Sym(P_n). In Exercise 4 you computed Sym(P_3), and in Problem 6 you computed Sym(P_6). If you compute Sym(P_n) for small n, say $n \in \{3, 4, 5, 6\}$, do you see a pattern?

Solution: Let P_n be a regular polygon with n sides. We want to find the elements of $\text{Sym}(P_n)$.

In Exercise 4, we saw that $\text{Sym}(P_3)$ consists of 3 counter clockwise rotations and 3 reflections. The rotations are by multiplies of $120 = 360/3$. And for each tip of the triangle, there is an axis of reflection that goes through the tip and the center of the triangle.

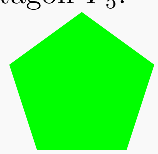
Next, consider the square P_4:

The square has 4 rotations that are symmetries. These are counter clockwise rotations by 0 (or 360), 90, 180, and 270 degrees. There are 4 reflections of the square which are symmetries. These are depicted in the following photo:

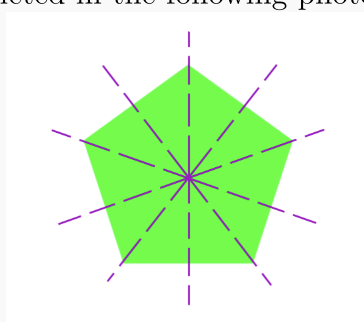


Reflection in each of these 4 axes is a symmetry. To conclude, $\text{Sym}(P_4)$ consists of 4 rotations which are by multiples of $90 = 360/4$ degrees and 4 reflections.

For another example, consider the pentagon P_5:



The pentagon has 5 rotations that are symmetries. These are counter clockwise rotations by 0 (or 360), 72, 144, 216, and 288 degrees. There are 5 reflections of the pentagon which are symmetries. These are depicted in the following photo:



Reflection in each of these 5 axes is a symmetry. To conclude, $\text{Sym}(P_5)$ consists of 5 rotations which are by multiples of $72 = 360/5$ degrees and 5 reflections.

Given these 3 examples, we expect that $\text{Sym}(P_n)$ consists of n counter clockwise rotations by multiples of $360/n$ degrees and n reflections. And indeed, this is true. We do not have the tools to prove this yet, but hopefully the above examples convince you that it is a reasonable expectation.