7 Symmetry and Group Theory

One of the most important and beautiful themes unifying many areas of modern mathematics is the study of symmetry. Many of us have an intuitive idea of symmetry, and we often think about certain shapes or patterns as being more or less symmetric than others. A square is in some sense "more symmetric" than a rectangle, which in turn is "more symmetric" than an arbitrary four-sided shape. Can we make these ideas precise? Group theory is the mathematical study of symmetry, and explores general ways of studying it in many distinct settings. Group theory ties together many of the diverse topics we have already explored – including sets, cardinality, number theory, isomorphism, and modular arithmetic – illustrating the deep unity of contemporary mathematics.

7.1 Shapes and Symmetries

Many people have an intuitive idea of symmetry. The shapes in Figure 38 appear symmetric, some perhaps more so than others. However, despite our general intuitions about symmetry, it may not be clcear how to make this statement precise. Can it make sense to discuss "how much" symmetry a shape has? Is there some way to make precise the idea that the regular pentagon is "more symmetric" than the equilateral triangle, or that the circle is "more symmetric" than any regular polygon? In this section we will explore symmetry and the way in which it arises in various contexts with which we are familiar, especially in the geometry of regular polygons (2D) and regular polyhedra (3D), such as the Platonic solids. The study of symmetry is a recurring theme in many disparate areas of modern mathematics, as well as chemistry, physics, and even economics.

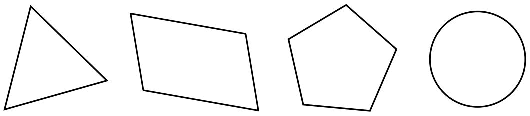
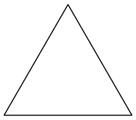


Figure 38: Some symmetric polygons.

To help us explore the idea of symmetry, we begin by considering a single concrete example, the equilateral triangle below. What does it mean for this shape to be symmetric?



Rotation symmetries

An equilateral triangle can be rotated by 120°, 240°, or 360° angles without really changing it. If you were to close your eyes, and a friend rotated the triangle by one of those angles, then after opening your eyes you would not notice that anything had changed. In contrast, if that friend rotated the triangle by 31° or 87°, you would notice that the bottom edge of the triangle is no longer perfectly horizontal.

Many other shapes that are not regular polygons also have rotational symmetries. The shapes illustrated in Figure 39, for example, each have rotational symmetries. The first example can be rotated only 180°, or else 360° or 0°. The third shape can be rotated any integer multiple of 90°. The fourth shape can be rotated any integer multiple of 72°. The fifth shape can be rotated any integer multiple of 60°.

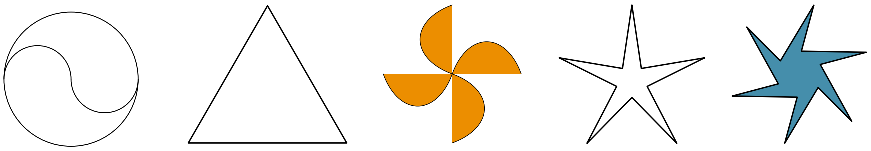


Figure 39: Several shapes with rotational symmetries.

More generally, we say that a shape has **rotational symmetry of order** n if it can be rotated by any multiple of $360°/n$ without changing its appearance. We can imagine constructing other shapes with rotational symmetries of arbitrary order. If the only rotations that leaves a shape unchanged are multiples of 360°, then we say that the shape has only the trivial (order $n = 1$) symmetry.

Mirror reflection symmetries

Another type of symmetry that we can find in two-dimensional geometric shapes is mirror reflection symmetry. More specifically, we can draw a line through some shapes and reflect the shape through this line without changing its appearance. This is called a **mirror reflection symmetry**.

Further consideration of the equilateral triangle (cf. Figure 40) shows that there are actually three distinct mirror lines through which we can reflect the shape without changing its appearance. If we were to reflect the triangle through any other line, the shape as a whole would look different.

Rotational symmetries and mirror reflection symmetries are not exclusive, and the same shape can have symmetries of both kinds. The equilateral triangle clearly has both mirror reflection symmetries and rotational symmetries. Likewise, the fourth shape in Figure 39 has five mirror reflection symmetries, along with many five rotational ones. The shapes in Figure 41, alternatively, have only mirror reflection symmetries but no rotational ones.

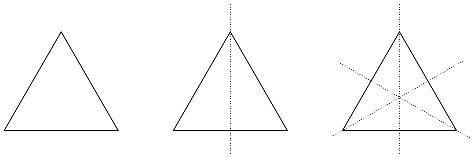


Figure 40: A line can be drawn through a triangle to highlight its symmetry. If the shape is reflected through this line, then we obtain the same equilateral triangle, unmoved.

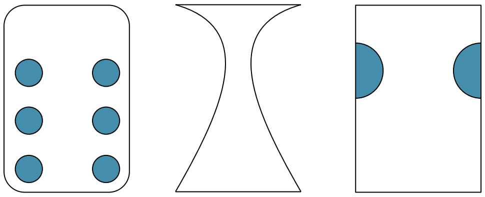


Figure 41: Each of these shapes can be reflected through a vertical line; none of these shapes have any rotational symmetry.

Counting symmetries

One way in which we can quantify the "amount" of symmetry of an object is by counting its number of symmetries. For example, we might count the number of rotational symmetries of an object, along with its mirror reflection symmetries. However, counting the symmetries of a shape can be challenging. It is not immediately clear which symmetries we should count and which, if any, we should not count. To understand why we might not count certain symmetries, consider rotating the equilateral triangle by 120°, 240°, and 360°. Of course the numbers by which we are rotating the triangle are different, and so we might be inclined to count each of them separately. But notice that we can also rotate the triangle by 480°, 600°, and 720°. Should we count those as different symmetries? If we do count them, then what would stop us from counting an infinite number of rotational symmetries for a triangle, or for that matter, any shape?

One way to limit the number of symmetries we count involves coloring, or otherwise labeling, the shape. For example, we can color each edge of the equilateral triangle, as illustrated in Figure 42. Symmetries can then be captured as changes of colors that leave the uncolored shape fixed. Any triangle in either row can be obtained from any other triangle in that row through a rotation; triangles can be obtained from triangles in the other row through reflections.

Using this coloring allows us to count symmetries carefully. If changing the shape in two different ways results in the same coloring, then we should count those two symmetries as the same. For example, rotating the equilateral triangle by 120° or 480° results in the same coloring, so we count those as the same symmetry. Likewise, rotating the triangle by 0° and 360° also result in

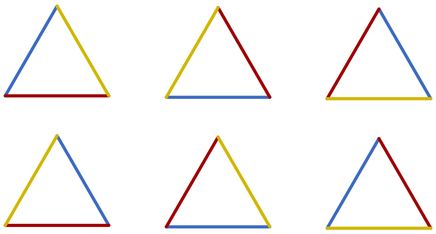


Figure 42: Equilateral triangle with edges colored. Any triangle in either row can be obtained from another triangle in the row through a rotation; triangles can be obtained from triangles in the other row through reflections.

the same coloring, so we count those the same as well. To reduce confusion, we use a number between 0 and 360 (not including 360 itself) to describe the angle of a rotation; thus, we prefer 120° to 480°, despite their equivalence. Likewise, for reasons that will become more clear in the following section, we discussing 0° rotations, or “doing nothing” to 360° rotations, despite their equivalence.

We are therefore left with six symmetries of the triangle – the rotations (0°, 120°, and 240°), and three reflections, one for each of the mirror planes passing through a corner and the center of the triangle. These symmetries can be pictured by how they transform the colored triangle in Figure 42.

Symmetries of the square

A square is in some sense “more symmetric” than a triangle because it has more symmetries. Figure 43 below shows a square with colored edges arranged in different ways. Again you might notice that any two squares in the same row can be obtained from one another through rotations, whereas those in distinct rows can only be obtained from one another through a reflection. Some thought will show that there are no other rotations or mirror reflection symmetries, and so these figures represent all eight symmetries of the square.

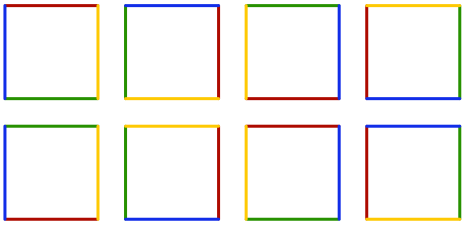


Figure 43: Squares.

Although this section is concerned primarily with rotational and mirror reflection symmetries of single objects in two dimensions, other types of symmetries arise in infinite systems and in higher dimensions. We do not consider those symmetries in this section.

Until now we have considered what symmetries are and briefly discussed how to count them. To say that a particular shape is “more symmetric” than another one can be made precise by considering their total number of symmetries. For example, the three shapes in Figure 44 each have a set of four symmetries. However, notice that the first two shapes have the same set of 4 rotational symmetries (0°, 90°, 180°, and 270°), but no mirror reflection symmetries. In contrast, the third shape has 2 rotational symmetries and 2 mirror reflection symmetries. How can we distinguish between the first and second shapes, on the one hand, and the third shape, on the other? The mathematical development of group theory provides rigorous tools to describe symmetries of shapes. Before consider the actual definition of a *group*, we first consider a more general topic of binary operators.

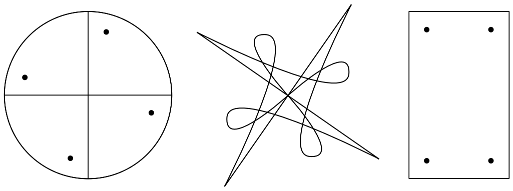


Figure 44: Three shapes, each with 4 symmetries. The first two have 4 rotational symmetries (0°, 90°, 180°, and 270°) and no mirror reflection symmetries. The third has 2 rotational symmetries (0° and 180°), and two mirror reflection symmetries.

7.2 Binary Operators

A precise discussion of symmetry benefits from the development of what mathematicians call a *group*, which is a special kind of set we have not yet explicitly considered. However, before we define a group and explore its properties, we reconsider several familiar sets and some of their most basic features.

Over the last several sections, we have considered many different kinds of sets. We have considered sets of integers (natural numbers, even numbers, odd numbers), sets of rational numbers, sets of vertices, edges, colors, polyhedra and many others. In many of these examples – though certainly not in all of them – we are familiar with rules that tell us how to combine two elements to form another element. For example, if we are dealing with the natural numbers, we might considered the rules of addition, or the rules of multiplication, both of which tell us how to take two elements of $\mathbb{N}$ and combine them to give us a (possibly distinct) third element.

This motivates the following definition.

Definition 26. *Given a set S, a* **binary operator** $\star$ *is a rule that takes two elements $a, b \in S$ and manipulates them to give us a third, not necessarily distinct, element $a \star b$.*

Although the term binary operator might be new to us, we are already familiar with many examples. As hinted to earlier, the rule for adding two numbers to give us a third number is a binary operator on the set of integers, or on the set of rational numbers, or on the set of real numbers. We can specify a set and binary operator on that set by writing down the set and then the operator: $S, \star$. For example, we might specify $\mathbb{Z}, +$ or $\mathbb{N}, /$ to denote the integers and addition on them, or else the natural numbers and division.

Binary operators can be defined on arbitrary sets, not only sets of numbers. For example, we might consider a set C of colors, and define a binary operator $\bowtie$ which tells us how to combine two colors to form another color. If $C = \{$red, yellow, green, blue, purple$\}$, then we can write red $\bowtie$ blue $=$ purple, since we can combine the first two colors to make the third. We might also consider a set of sets, and consider the binary operator $\cup$, the union, which takes any two sets and "combines" them by giving us their union.

Keep in mind that not every set has a natural binary operator. For example, consider the set $F = \{$table, chair, bookshelf, couch, windows, $\ldots\}$ of furniture in your house. While this set appears quite natural, there does not appear to be any natural rule for "combining" its elements.

After understanding what a binary operator is, we next look at several properties that a binary operator might or might not possess.

Closure

Some binary operators are such that when we combine two elements from a set, we always get another element in that set.

Definition 27. *A binary operator $\star$ is* **closed** *on a set S if for every $a, b \in S$, $a \star b$ is also an element of S.*

Many sets with which we are familiar are closed under particular binary operators, while many are not. Let's consider several examples.

Example 1. $\mathbb{N}, +$, the natural numbers under addition. If a and b are both elements of $\mathbb{N}$, then their sum $a + b$ is also an element of $\mathbb{N}$. Therefore, $\mathbb{N}$ is closed under addition.

Example 2. Consider the odd integers under multiplication. If a and b are both odd, then their product $a \times b$ is also odd. Therefore, the set of odd integers is closed under multiplication.

Example 3. The set of odd integers is not closed under addition, since the sum of two odd numbers is not always odd (in fact, it is never odd).

Identity element

For many choices of a set and binary operator, there exists a special element in the set that when "combined" with other elements in the set does not change them. Such an element is called a neutral, or identity, element. When considering addition on the real numbers, for example, the number 0 is unique in that it can be added to any other number and leave that number unchanged.

Definition 28. *For a set S and binary operator $\star$, an* **identity element** *$e \in S$ is one such that for any element $a \in S$, we have $a \star e = e \star a = a$.*

Example 4. Consider addition on the integers. 0 is an identity element, since for all $a \in \mathbb{Z}$ we have $0 + a = a + 0 = a$.

Example 5. Consider multiplication on the natural numbers. 1 is an identity element, since for all $a \in \mathbb{Z}$ we have $1 \times a = a \times 1 = a$.

Example 6. Consider a set whose elements are other sets. The empty set $\emptyset$ is an identity element for the binary operator $\cup$.

Example 7. Consider the even integers. Under addition there is an identity element (which is 0), but under multiplication there is no identity element (since 1 is not an even number). This illustrates the important point that not all sets and binary operators have an identity element.

Example 8. We earlier considered a set of colors, and a rule for combining them. Such a set and binary operator might have no identity element. Or perhaps there is a clear paint so that combining it with any color leaves that color unchanged.

Inverses

We know from elementary school that for every number x, there is another number (which we often write as $-x$) such that when we add it to x, we get the identity element 0. For example, 5 has an "inverse" -5, and adding them together gives us 0. Such inverses exist not only for numbers under addition, but also for many other choices of sets and binary operators. For some choices of sets and binary operators, for every element there is another element so that combining the two elements always gives us the identity element.

Definition 29. *For a set S and binary operator $\star$, an element $a' \in S$ is called the* **inverse** *of a if $a \star a' = a' \star a = e$.*

This idea generalized the concept of a negative in addition, and the concept of reciprocal we find in multiplication to arbitrary sets and binary operators.

Example 9. Consider addition on the integers. For every integer $a \in \mathbb{Z}$ there exists another element a' such that $a + a' = 0$. We often write this inverse as $-a$, so we have $a + -a = -a + a = e = 0$. Sometimes we refer to these as additive inverses.

Example 10. Consider the rational numbers $\mathbb{Q}$ under multiplication. Most elements in $\mathbb{Q}$ have multiplicative inverses. For example, if $a = 3/5$, then there is another element $a' = 5/3 \in \mathbb{Q}$ so that $a \times a' = a' \times a = e = 1$. However, 0 is in $\mathbb{Q}$ but does not have an inverse under multiplication, as there is no rational number q such that $0 \times q = q \times 0 = 1$. This highlights the point that it is possible for some elements to have inverses while others do not.

Example 11. Consider the set $S = \{1, 3, 5, 7\}$ under multiplication modulo 8; in this case 1 is an identity element, since $a \times a = a \times 1 = a$ for any element a. Under multiplication modulo 8, every element in S has an inverse. In fact, each element of S is its own inverse, as $a \times a \equiv 1 \pmod 8$ for all $a \in S$.

Example 12. Consider the set $S = \mathbb{N} \cup \{0\}$ (the set of all non-negative integers) under addition. The number 0 is an identity element, since for all elements $a \in S$ we have $a + 0 = 0 + a = a$. However, no element except for 0 has an inverse.

Combined, the above examples illustrate that sometimes all elements of a set have an inverse, sometimes almost all elements have an inverse, and sometimes almost none of the elements have an inverse.

Associativity

As described above, binary operators take two elements and combine them to produce a third. However, occasionally we will write things such as $5 + 8 + 2$, in which we have a total of three elements that should be combined, and there exists some ambiguity as to which of the following two procedures we should follow:

1. Add 5 and 8 to obtain 13, and then add 13 with 2 to obtain 15, or else

2. Add 8 and 2 to obtain 10, and then add 10 with 5 to obtain 15.

In this particular case, a small miracle occurs, and the two resulting numbers are the same. The two processes are procedurally different, but bottom line they end with the same result. The reader probably knows from elementary school, though, that there is nothing special about the numbers 5, 8, and 2, and in fact the same small miracle would occur with any three numbers. This motivates the definition of a final important property of binary operators.

Definition 30. *A binary operator* $\star$ *on a set* S *is called* **associative** *if for all* $a, b, c \in S$ *we have*

$$a \star (b \star c) = (a \star b) \star c. \tag{83}$$

In elementary school we learned that addition is associative, and so the order in which we add a set of numbers is not important. Likewise, multiplication is also associative, and for any numbers x, y, z we have $x(yz) = (xy)z$. It is for this reason that we can write xyz without bothering to specify whether we intend that x and y be combined first, or whether we intend that y and z be combined first – it doesn't matter.

Although most of us take the associativity of addition and multiplication for granted, we are all familiar with other binary operators which are not associative. For example, if we write $5 - 8 - 2$, the order in which we performing the operations matters, i.e., $(5 - 8) - 2 \neq 5 - (8 - 2)$!

Further complications arise when we mix operators. For example, the expression $5 + 8 \times 2$ can be interpreted in two different ways, making an important difference in the result. Should we add 5 and 8 and then multiply the result by 2 (to obtain 26)? or should we add 5 to the product of 8 and 2 (to obtain 21)? Although there is no "right" answer, certain conventions have evolved, and in general, if parentheses do not indicate otherwise, we first consider multiplications, and only then consider additions. Notice, however, that the famous "order of operations" does not directly address the "correct" interpretation of a statement such as $5/8/2$, which could result in $5/16$ or $5/4$, depending which division we calculate first.

Example 13. Consider the integers under addition. For any integers $a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$.

Example 14. Consider the real numbers under multiplication. For any real numbers $a, b, c \in \mathbb{R}$ we have $a \times (b \times c) = (a \times b) \times c$.

Example 15. Consider positive rational numbers under division. For positive rational numbers a, b, c it is generally the case that $a/(b/c) \neq (a/b)/c$, and so division is not associative. The same is true for subtraction.

Example 16. Consider a set of colors and a binary operator of mixing them. If you take three colors and mix them, the order in which you do will change the intermediate colors observed, but will not change the final color.

Most binary operators we consider will be associative.

Commutativity

Binary operators are rules for taking two elements from a set and combining them to produce something. Addition, subtraction, multiplication, and division are all binary operators with which we are familiar from grade school. For all real numbers a and b, it is always true that $a + b = b + a$ and that $a \times b = b \times a$. Of course we know that this is not the case for subtraction and multiplication, since for almost all a and b, $a - b \neq b - a$ and $\frac{a}{b} \neq \frac{b}{a}$. These motivate the following definition:

Definition 31. *A binary operator $\star$ on a set S is called* **commutative** *if for all $a, b \in S$ we have*

$$a \star b = b \star a. \tag{84}$$

Example 17. Consider the binary operator of exponentiation (on the integers, rationals, or reals). For almost all a and b we have $a^b \neq b^a$.

Example 18. We noted earlier that binary operators can act not only on numbers, but also on arbitrary elements, such as colors or other sets. Here we consider a set of geometric transformations which we can combine:

$$\begin{aligned} S \quad = \{ \quad & \text{rotate } 0^\circ, \text{rotate } 90^\circ, \text{rotate } 180^\circ, \text{rotate } 270^\circ \\ & \text{vertical mirror}, \text{horizontal mirror} \quad \} \end{aligned}$$

We can consider the binary operator of combining these geometric transformations by doing one and then doing the other. For example, consider reflecting a picture about a vertical mirror through its center and then rotating it by 90°, or rotating it by 180° and then reflecting it by about a horizontal mirror through its center. Spend a few minutes thinking about whether or not S is closed under this binary operator (HINT: it is not!).

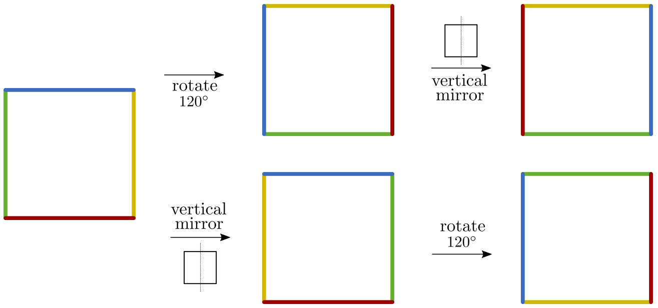


Figure 45: Square changed with a 90° rotation and with a reflection through a vertical mirror; the order in which these two operations are performed matters.

Of course, if you begin with an arbitrary picture, rotating it by 90° will give you a different result than flipping it about a vertical mirror. But what happens when we apply two of these transformations, but in different orders? Perform the following thought experiment. Take any two elements a and b from S and combine them, first performing a followed by b, and then performing b followed by a. Do you obtain the same result? Try performing this exercise for several choices of a and b.

If you spent several minutes performing the thought experiment, you will probably notice that in general $a \star b \neq b \star a$. In other words, the operation of combining geometric transformations is not commutative. Figure 45 illustrates what happens when we apply a 90° rotation and a reflection through a vertical mirror to a colored square in two different orders. Although we are performing the same two operations on the square, the final product depends on the order in which we perform them.

7.3 Groups

The study of symmetry has undergone tremendous change in the late 19th and early 20th centuries with the development of group theory, a part of an area called algebra (people who study algebra are called algebraists). Algebra and group theory has found applications in geometry, graph theory, physics, chemistry, architecture, crystallography, and countless other areas of modern science. There is hardly a discipline in which the study of symmetry, often with tools provided by group theory, has not played an important role.

In the previous two sections we have discussed shapes and their symmetries, and binary operators and several of their properties. The theory of groups will provide the link between these two topics, which might appear otherwise unrelated.

Remember that in Section 7.2 we considered several properties that a binary operator could have when acting on a given set. For example, closure describes the property of being able to combine two elements in a set to obtain another element also in the same set. We also considered identity elements and inverses, as well as the associative property. An important point that we made then is that not every set and binary operator possesses all of these properties. We saw some sets that were closed under an operator, for example, but which do not possess inverses, and other sets in which we could find an identity element, but for which not all elements have inverses.

A group is merely a choice of set S and binary operator $\star$ that satisfies four conditions.

Definition 32. *A* **group** *is a set G and operator $\star$ such that:*

- *(closure) G is closed under $\star$; i.e., if $a, b \in G$, then $a \star b \in G$.*
- *(identity) There exists an identity element $e \in G$; i.e., for all $a \in G$ we have $a \star e = e \star a = a$.*
- *(inverses) Every element $a \in G$ has an inverse in G; i.e., for all $a \in G$, there exists an element $a' \in G$ such that $a \star a' = a' \star a = e$.*
- *(associativity) The operator $\star$ acts associatively; i.e., for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.*

Although this definition sounds complicated, and perhaps even arbitrary, it turns out that many of the examples we have already considered are in fact groups; for the sake of time and focus we will generally not spend much time discussing the associative property.

Let us consider several examples. Most important for our connections to symmetries, it turns out that the set of symmetries of any geometric shape constitute a group when the binary operator is defined by defining $a \star b$ as "do a and then do b". (We briefly note, for the sake of completeness, that our conventions are in contrast to mathematical convention. In particular, most mathematicians would interpret $a \star b$ to mean first do b and then do a.)

Example 1. Let us consider the set $S = \{0, 1, 2, 3\}$ under addition mod 4. It is straightforward to see that this choice of set and binary operator constitute a group. (1) The set is closed under addition mod 4, as for any pair of numbers $a, b \in S$, their sum mod 4 is also an element of S. (2) The element/number 0 here is an identity element, since for any element $a \in S$, we have $a + 0 = 0 + a = a$. (3) Confirming inverses is slightly less straightforward, but it is not difficult to confirm. The inverse of 0 is 0 (itself), since $0 + 0 \equiv 0 \pmod 4$; the inverse of 1 is 3, the inverse of 2 is 2, and the inverse of 3 is 1, and combining any of these elements with its inverse (through addition mod 4) gives us the identity element 0. (4) Finally, modular addition is associative.

We can generalize this example to $\{0, 1, \ldots, m-1\}$ and addition modulo m, where m is a natural number. It is straightforward to see that addition modulo m is closed on this set, and that 0 can serve as the identity element, for any choice of m. The inverse of any element a this set is $m - a \pmod m$. For example, in mod 17, the inverse of 5 is $17 - 5 = 12$, which when added to 5 is congruent to 0 mod 17. Finally, as noted before, modular arithmetic is always associative.

Example 2. The set of all integers $\mathbb{Z}$ under addition is an example of a group, albeit one with an infinite number of elements in it. This choice of set and binary operator satisfies all four conditions to constitute a set.

Example 3. The same set of set might not be a group under a different operator. For example, the integers do not constitute a group under multiplication. Although 1 is good choice of identity element, almost no elements have an inverse. For example, the integer $a = 5$ has no "inverse" a' so that $a \times a' = 1$.

Example 4. Likewise, the same operator might not be a group if the set is changed. For example, even though $\mathbb{Z}$ constitutes a group under addition, the set of natural numbers $\mathbb{N}$ does not. Since every element is positive, there is certainly no identity element e such that $a + e = e + a = a$ for all $a \in \mathbb{N}$. Even if we add the number 0 to $\mathbb{N}$, i.e., even the the set $\mathbb{N} \cup \{0\}$, does not constitute a group since although it has an identity element, it does not have inverses for almost any of its elements.

Example 5. The set of *positive* rational numbers, which we call $\mathbb{Q}^+$ constitutes a group under multiplication. Multiplying any two positive rational numbers gives us another positive rational number. The number 1, which is of course a rational number, serves as the identity element, and for any element $a/b \in \mathbb{Q}^+$, the rational number b/a is its (multiplicative) inverse, since $\frac{a}{b}\frac{b}{a} = 1$.

Example 6. Groups do not need to be large or complicated. For example, consider the set $\{0\}$ under addition. It seems quite boring, but if you think about its properties will notice that it constitutes a group.

Example 7. Although the set $\{0, 1, 2, \ldots, m-1\}$ under addition modulo m constitutes a group, it does not under multiplication. To see this, consider that the number 1 is the identity element of such a group. Notice also that there is no element $a \in \{0, 1, 2, \ldots, m-1\}$ so that $a \times 0 = 0 \times a = 1$, so at least 0 does not have an inverse.

Example 8. Removing 0 from the set can sometimes help make $\{0, 1, 2, \ldots, m-1\}$ into a group under multiplication modulo m. Consider, for example, the set $\{1, 2, 3, 4\}$ under multiplication mod 5. The number 1 can serve as an identity element, and notice that every element has an inverse (can you see what they are?). Multiplication mod m is always associative, so this constitutes a group.

Example 9. However, removing 0 from the set does not always help. Consider, for example, the set $\{1, 2, 3, 4, 5\}$ under multiplication mod 6. The number 1 can serve as an identity element, but notice that not every element has an inverse. Indeed, most elements do not have an inverse. In particular notice that 2, 3, and 4, each of which shares factors in common with 6, do not have multiplicative inverses, while 1 and 5 do.

Group order

Occasionally we will want to have some way of measuring the "size" of a group. We use the word order to denote the number of elements in the associated set.

Definition 33. *The* **order** *of a group given by a set G and binary operator $\star$ is the number of elements in G, i.e., the order of G, sometimes written as $|G|$.*

We have seen several examples of finite groups, including sets $\{0, 1, 2, \ldots, m-1\}$ under addition modulo m. The order of such a group is m. A group that has only one element in it, such as $\{0\}$ under addition, is called a *trivial group*.

Groups of symmetries

The ultimate goal of this section was to see that symmetries of shapes can be studied carefully, using the tools of group theory. It turns out that many sets of symmetries constitute a group when the binary operator is defined as $a \star b =$ "do a and then do b". Let us look at several examples.

Example 1. Let us reconsider the set of all rotations of the equilateral triangle: $S = \{\text{rotate } 0°, \text{ rotate } 120°, \text{ rotate } 240°\}$. This is *not* the set of all symmetries, but it is a set of all rotational symmetries. Notice that we can combine any two of these symmetries to form a symmetry in this set. Notice also that rotating by 0° serves as the identity element, and that each of the rotations have an inverse. Finally, rotations in space are always associative. Using the definition of order, we can say that the order of the group of rotational symmetries of the equilateral triangle is 3. More generally, if we consider all n rotations of a regular polygon with n sides, then we get a group of order n.

Example 2. The set of all symmetries of a square also constitute a group under the operator of doing one symmetry and then doing another one. You might recall that the square has 8 different symmetries, four rotational ones and four mirror reflections. It might take some thinking to realize that combining any two of these symmetries will give us another symmetry in the group. It is also straightforward to see that the "do-nothing" rotation is an identity element, and also that that every symmetry can be reversed. Rotations are reversed by other rotations, and mirror reflection symmetries are always reverse themselves – if you take a reflection of a reflection (through the same mirror), then you always come back to the shape from which you began. More generally, if we consider all n rotations and all n reflections of a regular polygon with n sides, then we get a group with order $2n$.

Example 3. We can't always combine arbitrary symmetries to form a group. Consider for example the set of all mirror reflection symmetries of an equilateral triangle, or of a square. You will notice that combining any two mirror reflection symmetries will give us a symmetry not in the group. In fact, combining two mirrors will always give us a rotation. If you don't understand or believe me, take a square and label its four edges. Next, "reflect" it through one of the four mirror lines going through its center, and then reflect it again through another mirror line. You will see that the result is indeed a rotation. If you use the same mirror, then the result will be the same as the 0° rotation.

Example 4. The Platonic solids introduce symmetry groups that are substantially more complicated. In class we only considered rotational symmetries of these polyhedra, and we will not be concerned with the full group of symmetries. Let us begin by considering the cube. We can rotate the cube about axes that pass through two opposite face centers. Each of these axes support four distinct rotations, by 0°, 90°, 180°, or 270°. There are two different kinds of axes that also allow for rotations. In particular, we can also draw a line through opposite pairs of corners, allowing us to rotate the cube about them by 0°, 120°, or 240°. Finally, we can draw lines passing through centers of opposite edges. We can rotate the cube about these lines/axes either 0° or 180°.

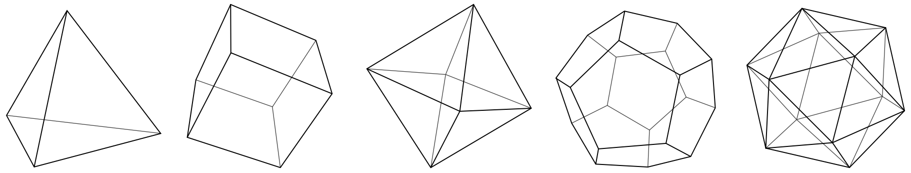


Figure 46: The five regular polyhedra, also known as the Platonic solids. Below is listed the number of vertices v, edges e, and faces f of each regular polyhedron, as well as the number of edges per face n and degree d of each vertex.

Commutative and non-commutative groups

One important idea that is not obvious at all is that the order of operations can matter, not always but often. To highlight the importance of this point, consider multiplication on the real numbers. For every pair of real numbers $x, y \in \mathbb{R}$ it is always the case that $x \times y = y \times x$. The same is true for addition and many other groups we have considered.

However, in many groups, the order in which we combine the elements matters. To see one such example, consider an equilateral triangle and its rotations. We have seen before that the set of symmetries of an equilateral triangle contain three rotations (including the one by 0°) and three mirror reflections. Does the order of applying these symmetries matter? Sometimes it does not. For example, consider the rotation by 120° and the rotation by 240°. The order in which we apply these symmetries does not matter.

However, consider the 120° rotation and a reflection through a vertical mirror. Figure 47 shows the intermediate and final results of performing these operations in two different orders. It is clear that here order matters.

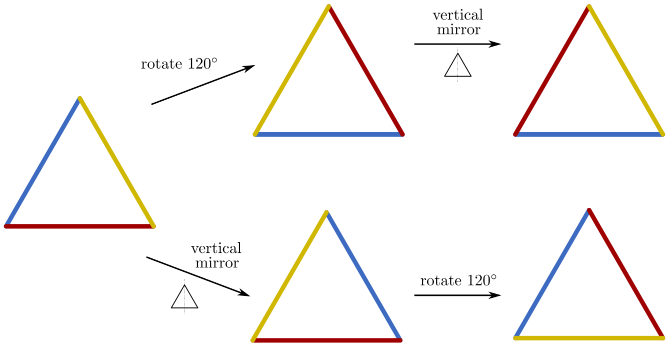


Figure 47: Equilateral triangle changed with a 120° rotation and with a reflection through a vertical mirror; the order in which these two operations are performed matters.

Groups in which the order does not matter, such as the integers, rationals, real numbers under addition or multiplication, the order does not matter, and $a + b = b + a$ and $a \times b = b \times a$ for any two elements. Such groups are called **commutative**, or Abelian, in honor of Niels Abel, a founding father of group theory. If we consider the set of rotational symmetries about a single axis of rotation, such as all rotations of a triangle, then that set will form a group which is commutative.

A more complete exploration of groups, even those associated with the Platonic solids, is beyond the scope of these notes. Additional information about this material can be found in the homework assignments and the posted solutions.

7.4 Symmetry Groups of Shapes

One of the primary applications of group theory is the study of symmetries of shapes of different kinds. Symmetries of shapes form groups, and this section will explore many such examples, including those associated with regular polygons and polyhedra.

Cyclic Groups

Consider the set of rotations of an equilateral triangle that we considered before. We have the set:

$$S = \{ \text{ rotate } 0^\circ, \text{rotate } 120^\circ, \text{rotate } 240^\circ \ \}, \tag{85}$$

which as we have seen before forms a group under the binary operation defined by performing one rotation and then another. For reasons that will become clear soon, from now onwards we will call this group C_3. Likewise, C_4 will be the group:

$$C_4 = \{ \text{ rotate } 0^\circ, \text{rotate } 90^\circ, \text{rotate } 180^\circ, \text{rotate } 270^\circ \ \}. \tag{86}$$

One thing we might notice about these two groups is that all elements of the group can be obtained by taking one element of the set, and combining it different numbers of times. For example, let us use r to denote the rotation by 90°. We can then rewrite C_4 as:

$$C_4 = \{ \ r^0, r^1, r^2, r^3 \ \}, \tag{87}$$

where powers of r indicate performing the same geometric operation (in this case rotations by 90°) multiple times. If we s to denote a rotation by 120°, then we can likewise describe C_3 as the set $\{s^0, s^1, s^2\}$.

Both of these examples illustrate the possibility of "generating" certain groups by using a single element of the group, and combining it different numbers of times. We have a special name for such groups:

Definition 34. *A* **cyclic group** *is a group that can be "generated" by combining a single element of the group multiple times. A cyclic group with n elements is commonly named C_n.*

Figure 48 illustrates several shapes with symmetry groups that are cyclic.

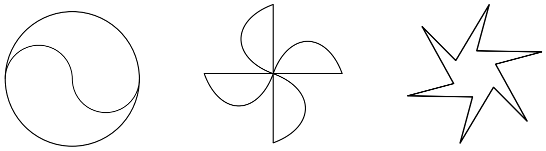


Figure 48: Shapes with associated symmetry groups C_2, C_4, and C_6.

The examples above might lead us to wonder whether all symmetry group can in fact be generated by repeatedly combining a single element. Is every symmetry group in fact cyclic? Simple consideration will show us that this is not the case.

Dihedral Groups

Let us reconsider, for example, the set of all symmetries of a square. In addition to four rotational symmetries ($0°, 90°, 180°, 270°$), the square also has four mirror reflection symmetries; the effects of applying these symmetries to a colored square can be seen in Figure 50. If the first square is identified with the identity element (0° rotation), then squares in the first row illustrate rotations, and all squares in the second row illustrate mirror reflections. It turns out that this set of rotations and reflections satisfy all criteria to form a group.

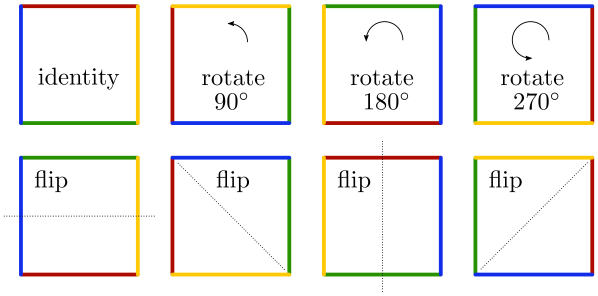


Figure 49: A single colored square transformed by rotations and mirror reflections; the set of all n rotation symmetries and n mirror reflection symmetries of a regular polygon with n sides make up the symmetry group of that polygon.

Knowing that the symmetries of a square constitute a group, we might wonder whether this group is cyclic. In other words, can all of these symmetries be obtained by combining a single element multiple times? In short, the answer is no. To help understand why this is, consider that repeating a mirror reflection returns a shape to its original position; i.e., every mirror reflection is its own inverse. Therefore, a single mirror reflection cannot possible generate any elements aside from the identity and itself. Likewise, a single rotation combined with itself many times could never produce a mirror reflection. To see why, notice that all elements in the top row of Figure 50 have the same "orientation". Specifically, red, yellow, green, blue all appear in the same order (clockwise). Rotations never change the orientation of a shape. In the bottom row, the four colors appear in a reversed order, which happens under any mirror reflection symmetry. In short, the symmetry group of a square is not cyclic.

Definition 35. *A* **dihedral group** *is a group that can be "generated" by combining a rotation symmetry and a mirror reflection multiple times. A dihedral group with n rotational and n mirror symmetries is commonly named D_n.*

Dihedral groups are often associated with regular polygons. In particular, the set of symmetries of every regular polygon with n sides forms the dihedral group D_n. Since this group contains n rotations and n reflection symmetries, the order of D_n is always $2n$.

Symmetry Groups of the Platonic Solids

The Platonic solids have symmetry groups that are even more complicated than either the cyclic or dihedral groups. One way to understand this is through consideration of their rotational symmetries. Until now all symmetry groups associated with shapes have a single axis of rotation. In both the cyclic and dihedral group, all rotational symmetries can be obtained by repeating a single rotation multiple times. This is not the case, however, for three-dimensional shapes including the Platonic solids.

[Notes here are incomplete.] However, we briefly consider one example. The cube has three different kinds of rotational symmetries.

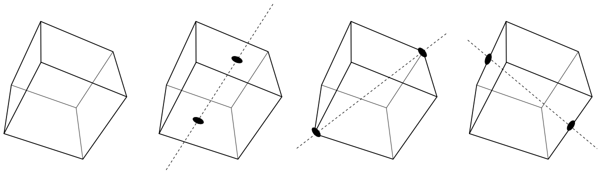


Figure 50: A cube and three different kinds of rotational symmetry axes.

1. We can draw lines through centers of opposite faces, and rotate the cube by multiples of 90° about these; there are three such pairs of faces, and hence three such axes of rotation.
2. We can also draw lines through opposite corners, and rotate the cube by multiples of 120° about these lines; there are four pairs of corners, and hence four such axes of rotation.
3. We can also draw lines through centers of opposite edges, and rotate the cube by multiples of 180° about these lines; there are six pairs of edges, and hence six such axes of rotation.

By themselves, these symmetries do not form a group, since in general combining these symmetries produce another symmetry not in this list. However, by combining these symmetries we can form a group. If we ignore any symmetries, the set of symmetries of a cube has 24 elements; if we include mirror reflections, the group of symmetries has 48 elements. [Notes here are incomplete.]