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: $S = \{\text{rotate } 0^\circ, \text{ rotate } 120^\circ, \text{ rotate } 240^\circ\}$. 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 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 symmetries of an equilateral triangle, or of a square. You will notice that combining any two mirror 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

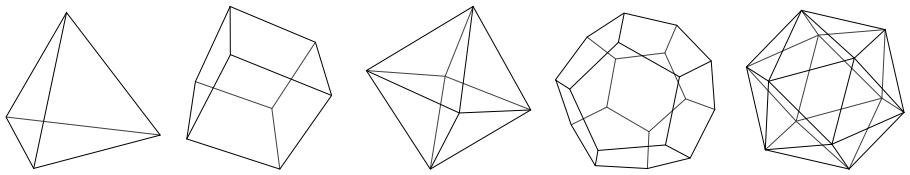

Figure 46: The five regular polyhedra, also known as the Platonic solids. Below is listed the number of vertices v, edges e, and faces f of each regular polyhedron, as well as the number of edges per face n and degree d of each vertex.

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°.

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 mirrors. 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

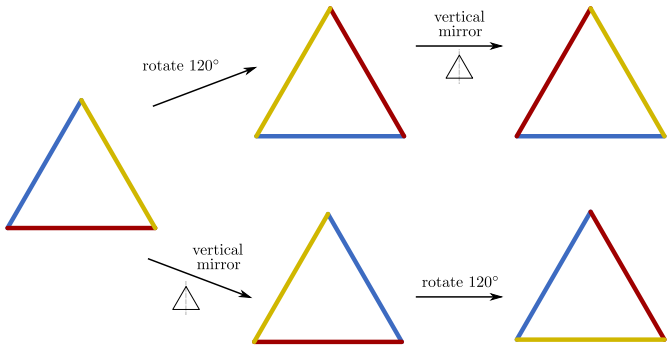

Figure 47: Equilateral triangle changed with a 120° rotation and with a reflection through a vertical mirror; the order in which these two operations are performed matters.

operations in two different orders. It is clear that here order 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.