Lecture Notes on Symmetry

MA 111 Spring 2009

Scott Taylor, Colby College

1. PRELIMINARIES

A **mapping** or **transformation** of a set X is a function which takes each point of X to some other point of X. A transformation is a **automorphism** or **symmetry** of X if it preserves a given "structure" of X. For example, automorphisms of the xy-plane, preserve distance: the distance between points A and B before the automorphism is the same as the distance between A' and B' after the automorphism (the automorphism takes A to A' and B to B'.) We always require our transformations and automorphisms to be "one-to-one". This means that two distinct points A and B are never mapped to the same point $A' = B'$.

Two important examples of situations where we care about automorphisms are:

(a) Symmetries of the plane (which preserve distance)
(b) Symmetries of a graph which preserve the relationship between vertices and edges.

We'll discuss symmetries of graphs more later, but we'll first study symmetries of the plane. It turns out that every symmetry of the plane is either a reflection (about some line), a rotation (about some point of with some angle), a translation (in some direction by some distance), or a combination of these.

Our first important example will concern symmetries of a square in the plane. This means we want to list all symmetries of the plane which take the square to itself. In other words, points on the square can be moved about within the square, but not outside the square. Two symmetries are considered to be the same if they have the same effect on the points of the square. For example a 90° rotation clockwise is the same as a 270° rotation counterclockwise, because all the points end up in the same spot. This will make more sense when we look at specific examples.

2. GROUPS

2.1. **Group Tables.** Consider the square below. On the left is the plain old square; on the right some axes of reflection are drawn. Reflecting the square about one of these axes produces a square which is indistinguishable from the first. We call the act of reflecting the square across one of these lines, a **reflection symmetry**.

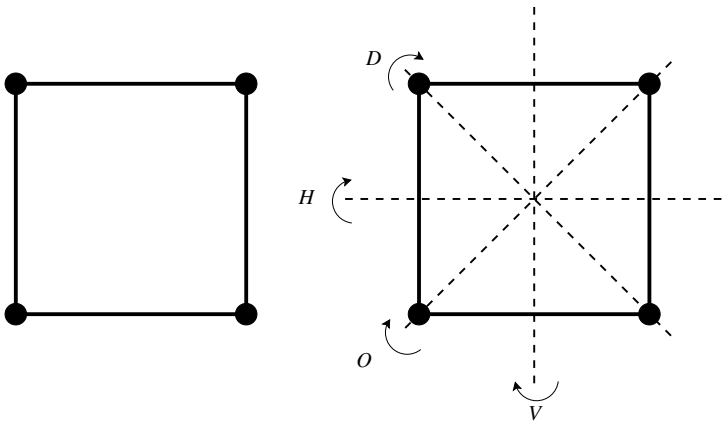

FIGURE 1. The symmetries of the square

.

In addition to the reflection symmetries, we can also rotate the square by multiples of 90° either clockwise or counter-clockwise. Denote a counterclockwise rotation of θ degrees by R_θ. Figure 2 shows the effects of repeatedly applying R_{90}. For example, performing R_{90} once moves the purple vertex from the upper right to the upper left and cycles the other colored vertices around "one notch".

At this point, we should be a little more precise. A **symmetry** of an object is a way of moving the object so that after the motion the object cannot be distinguished from the the way it was before the motion. When we discuss shapes (like a square) lying on the plane we will insist that the motion not change the distance between two arbitrary points. Sometimes, for other objects, we will not insist that distance remain unchanged. It will usually be clear from the context whether or not we assume distances are unchanged.

Even though a symmetry is a motion or action, we will usually think of it as an object of study in its own right. To be able to tell two different symmetries apart we will often decorate the object (e.g. the square) and

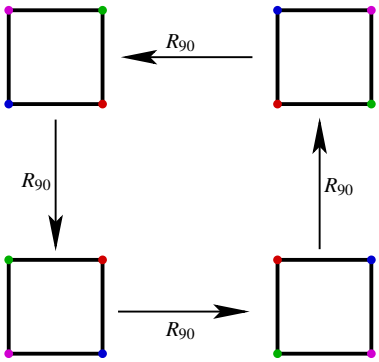

FIGURE 2. Applying R_{90} to the square. The vertices have been colored to exhibit the effect of R_{90}.

look at what happens to the decorations. For example, the rotation R_{90} moves the colors of the vertices counter-clockwise. Two symmetries are "the same" if they have the same effect on our decorations. For example, performing R_{90} and then performing R_{180} is the same as performing R_{270}. Similarly, performing R_{270} is the same as rotating the square by 90° in a *clockwise* direction.

So far, we have listed 7 symmetries of the square:

$$R_{90}, R_{180}, R_{270}, D, V, O, H.$$

In theory, we could produce new symmetries of the square by performing one of these symmetries. For example, performing R_{90} and then performing R_{90} again is the same as performing R_{180}. There is also the symmetry **I**, which consists of doing nothing at all. If S_1 and S_2 are symmetries, if we first perform S_1 and then perform S_2 we call the resulting symmetry $S_2 \circ S_1$. Notice that we should read this expression right to left.

Question: Is our list of symmetries: **I**, R_{90}, R_{180}, R_{270}, D, V, O, H complete?

Recall that D, V, O, and H are the reflections of the square about the lines indicated in Figure 1. Let's make a table:

S_2 \ S_1	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
$\mathbf{I}$								
R_{90}								
R_{180}								
R_{270}								
D								
V								
O								
H								

To fill in the table, notice that we must have $S \circ \mathbf{I} = S$ no matter what symmetry S is, since $\mathbf{I}$ means do nothing. Similarly, $\mathbf{I} \circ S = S$ no matter what symmetry S is. For example, $\mathbf{I} \circ R_{90} = R_{90}$ since rotating by 90° and then doing nothing is the same as rotating by 90°. This allows us to fill in the first row and the first column:

S_2 \ S_1	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
$\mathbf{I}$	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
R_{90}	R_{90}							
R_{180}	R_{180}							
R_{270}	R_{270}							
D	D							
V	V							
O	O							
H	H							

Next, notice that if we perform R_{90} and then perform R_{90} we have simply rotated the square 180°. That is, we have performed R_{180}. Using similar lines of reasoning we can fill in the upper left quadrant of the table:

S_2 \ S_1	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
$\mathbf{I}$	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
R_{90}	R_{90}	R_{180}	R_{270}	$\mathbf{I}$				
R_{180}	R_{180}	R_{270}	$\mathbf{I}$	R_{90}				
R_{270}	R_{270}	$\mathbf{I}$	R_{90}	R_{180}				
D	D							
V	V							
O	O							
H	H							

Now we can work on filling in the rest of the table. For example, to calculate $O \circ R_{270}$ we remember that this means that we rotate the square by 270° and then reflect over the off-diagonal axis. The left side of Figure 3 shows this operation. By examining the dots we see that $O \circ R_{270} = V$. The right side of Figure 3 shows that $R_{270} \circ O = H$. Notice that this means that

$$O \circ R_{270} \neq R_{270} \circ O.$$

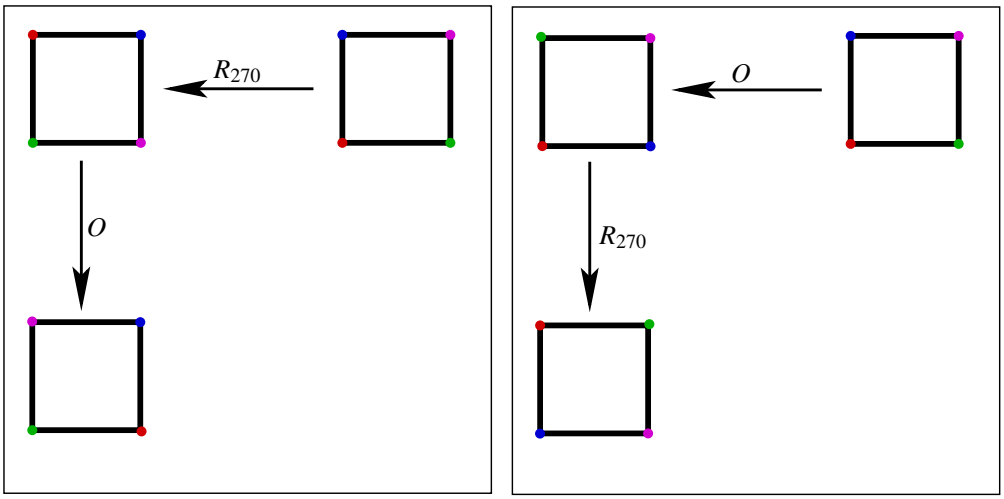

FIGURE 3. Calculating $O \circ R_{270}$ and $R_{270} \circ O$

Similar calculations allow us to fill in the rest of the table. See Table 1.

	S_1							
$S_2 \circ S_1$	**I**	R_{90}	R_{180}	R_{270}	D	V	O	H
I	**I**	R_{90}	R_{180}	R_{270}	D	V	O	H
R_{90}	R_{90}	R_{180}	R_{270}	**I**	H	D	V	O
R_{180}	R_{180}	R_{270}	**I**	R_{90}	O	H	D	V
S_2 R_{270}	R_{270}	**I**	R_{90}	R_{180}	V	O	H	D
D	D	V	O	H	**I**	R_{90}	R_{180}	R_{270}
V	V	O	H	D	R_{270}	**I**	R_{90}	R_{180}
O	O	H	D	V	R_{180}	R_{270}	**I**	R_{90}
H	H	D	V	O	R_{90}	R_{180}	R_{270}	**I**

TABLE 1. The group of symmetries of a square

Question: What patterns do you notice in the table?

Possible patterns include:
- every symmetry appears exactly once in each row and column.
- performing a reflection and then another reflection is the same as performing a rotation.
- For each symmetry, there is another symmetry which "undoes it".

The symmetries of the square are an example of what mathematicians call a **group**.

Definition 1. A **group** consists of a set G and an operation $\circ$ which combines two elements of G into a third element of G. That is, if a and b are in G then $a \circ b$ is also in G. Furthermore, we require the following properties to hold:

- (Associative) For any three elements a, b, c in G,
$$a \circ (b \circ c) = (a \circ b) \circ c.$$
- (Identity) There exists an element $\mathbf{I}$ in G (called the **identity element**) so that for every a in G,
$$a \circ I = I \circ a = a.$$
- (Inverses) For each a in G there exists some b in G so that
$$a \circ b = b \circ a = \mathbf{I}.$$
The element b is called the **inverse** of a and is sometimes written a^{-1}.

It need not be the case that for all a and b in X, $a \circ b = b \circ a$. That is, the group is not necessarily commutative. Indeed, the symmetries of the square are not commutative. Here is a fundamental observation which allows us to apply mathematics to the study of symmetry:

Theorem 1. For any object X, the set of symmetries of the object form a group. We denote the group $\mathtt{Sym}(X)$. The operation is simply: first do one symmetry and then do another symmetry.

Exercise 1. For the group of symmetries of the square do the following:

- Pick three elements a, b, c at random and show that
$$a \circ (b \circ c) = (a \circ b) \circ c.$$
- Explain how the fact that an identity exists shows up in the table.
The first row and the first column are exactly the same as the header column and the header row.
- Explain how the fact that each symmetry has an inverse symmetry shows up in the table.

Every row and every column contains **I**.

We will occasionally make use of the following terminology:

- The **integers** are the positive and negative whole numbers and zero:
$$\{\ldots,-2,-1,0,1,2,\ldots\}.$$
They are denoted by $\mathbb{Z}$.
- The **rational numbers** are all the numbers which can be written as fractions of two integers. $\frac{1}{2}$, 3.0000009, and -17 are examples of rational numbers. The set of rational numbers is denoted $\mathbb{Q}$.
- The set of **real numbers** is the set of all numbers on the number line. It includes the integers and rational numbers as well as other numbers like $\sqrt{2}$ and π. The set of real numbers is denoted $\mathbb{R}$.
- The set of all real numbers except for zero is denoted $\mathbb{R}^*$.

Exercise 2. Decide whether or not the following are groups.

(a) $\mathbb{Z}$ with the operation of $+$.
(b) $\mathbb{Z}$ with the operation of $-$.
(c) $\mathbb{R}$ with the operation of $+$.
(d) $\mathbb{R}$ with the operation of $\cdot$ (multiplication).
(e) $\mathbb{R}^*$ with the operation of $\cdot$.

(a), (c), and (e) are groups. (b) is not a group because subtraction is not associative. (d) is not a group because 0 does not have a multiplicative inverse. (There is no number x so that $0 \cdot x = 1$.)

Notice that the groups in the previous exercise are not described as the symmetries of an object. A common philosophy in mathematics is: If you want to study an object, study its group of symmetries; if you want to study a group find an object for which the group is a group of symmetries.

Exercise 3. Show that the rotations of the square form a group. (Consider **I** to be a rotation.)

If a group has only finitely many elements, in principle we can make up a group table like we did for the group of symmetries of a square. Here is another example. In this example the object will be three indistinguishable dots: ●●●. You should think of these points, which means that reflection about a horizontal line will not count as one of our symmetries. Our group will be the group of symmetries of these dots. We won't insist that the symmetry preserve the distance between the dots. One example of such a symmetry is swapping the first two dots. As with the square, we'll add some

colors to the dots: ●●●. This will enable us to keep track of the different behaviour of different symmetries.

To recap: our group is $\mathbb{G} = \mathtt{Sym}(●●●)$. We need names for the different symmetries of the dots. Denote the action of swapping the first two dots by $[1 \leftrightarrow 2]$. Notice that this changes the colors of the dots:

$$[1 \leftrightarrow 2](●●●) = ●●●.$$

We can also move the first dot to the second position, the second dot to the third position, and the third dot to the first position. Denote that symmetry as $[1 \rightarrow 2 \rightarrow 3 \rightarrow]$. Notice that this one also changes the colors:

$$[1 \rightarrow 2 \rightarrow 3 \rightarrow](●●●) = ●●●.$$

In the same vein, here is a list of more symmetries of the three dots:

$$\begin{gathered}\mathbf{I} \\ [1 \leftrightarrow 2] \\ [1 \leftrightarrow 3] \\ [2 \leftrightarrow 3] \\ [1 \rightarrow 2 \rightarrow 3 \rightarrow] \\ [1 \rightarrow 3 \rightarrow 2 \rightarrow]\end{gathered}$$

Is this list complete? The answer is "yes". Here's how to tell. Applying each symmetry to the colored dots ●●● produces a new way of coloring the dots. If two symmetries produce the same coloring, they have the same effect on the object (the uncolored dots) and so are considered to be the same symmetry. Given the initial coloring of the dots, no two of the symmetries in the list above produce the same coloring. All those symmetries are, therefore, different. But is the list complete? We still haven't answered that question. To do so, we'll argue that there are exactly 6 symmetries of ●●●. Since we have six distinct symmetries in our list, our list must be complete.

Each symmetry produces a unique coloring of the dots (given the initial coloring: ●●●. There are three ways of coloring the first dot, two ways of coloring the second, and one way of coloring the third. Thus there are six total ways of coloring the dots and, therefore, six total symmetries. Thus our list is complete and no symmetry is listed more than once.

We can now make up a group table for $\mathbb{G}$. To do so, we go through a process similar to what we did for the symmetries of the square. For example, to compute

$$[1 \leftrightarrow 2] \circ [1 \rightarrow 2 \rightarrow 3 \rightarrow].$$

Look at what it does to the colors:

$$[1 \leftrightarrow 2] \circ [1 \to 2 \to 3 \to](\bullet\bullet\bullet) = [1 \leftrightarrow 2](\bullet\bullet\bullet) = \bullet\bullet\bullet.$$

Notice that this is the same coloring as the one given by $[2 \leftrightarrow 3]$:

$$[2 \leftrightarrow 3](\bullet\bullet\bullet) = \bullet\bullet\bullet.$$

Thus,

$$[1 \leftrightarrow 2] \circ [1 \to 2 \to 3 \to] = [2 \leftrightarrow 3].$$

Challenge! Find a more efficient way of computing the effect of combining two symmetries of $\bullet\bullet\bullet$.

For the complete group table for $\mathbb{G}$, see Table 2.

Some groups are so common that they deserve special names. Let D_n denote the symmetry group of a regular n–gon. Thus, the symmetry group of the square (which we studied previously) is denoted D_4. The symmetry group of n indistinguishable dots is denoted $\mathbb{S}_n$. Thus, the symmetry group of three indistinguishable dots (which we just studied) is denoted $\mathbb{S}_3$.

Exercise 4.
(a) Show that every symmetry of 3 indistinguishable dots is also a symmetry of an equilateral triangle.
(b) Show that every symmetry of an equilateral triangle is also a symmetry of 3 indistinguishable dots.
(c) Explain why the previous two exercises show that D_3 is the same as $\mathbb{S}_3$.
(d) Show that D_n contains $2n$ symmetries.
(e) Show that $\mathbb{S}_n$ contains $n! = n(n-1)(n-2)\dots(3)(2)(1)$ symmetries.
(f) Explain why D_n is not the same as $\mathbb{S}_n$ for $n \geq 4$.

2.2. **Generators.** Although every (finite) group has a group table, for all but the smallest groups writing down the group table is very inefficient. A more efficient method is to write down the fewest number of elements possible so that every other group element is a combination of that small number of group elements. That small number of elements from which every other group element can be generated will be called a set of generators for the group.

To begin our discussion, we return to consideration of the group D_4, the symmetries of the square. We want to find a list of elements S in D_4 so that every element in D_4 can be written as a combination of those elements in our list. We say that S **generates** D_4 and that S is a set of **generators** for

S_2

$S_2 \circ S_1$	S_1					
	$\mathbf{I}$	$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \to 2 \to 3 \to]$	$[1 \to 3 \to 2 \to]$
$\mathbf{I}$	$\mathbf{I}$	$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \to 2 \to 3 \to]$	$[1 \to 3 \to 2 \to]$
$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 2]$	$\mathbf{I}$	$[1 \to 3 \to 2 \to]$	$[1 \to 2 \to 3 \to]$	$[2 \leftrightarrow 3]$	$[1 \leftrightarrow 3]$
$[1 \leftrightarrow 3]$	$[1 \leftrightarrow 3]$	$[1 \to 2 \to 3 \to]$	$\mathbf{I}$	$[1 \to 3 \to 2 \to]$	$[1 \leftrightarrow 2]$	$[2 \leftrightarrow 3]$
$[2 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \to 3 \to 2 \to]$	$[1 \to 2 \to 3 \to]$	$\mathbf{I}$	$[1 \leftrightarrow 3]$	$[1 \leftrightarrow 2]$
$[1 \to 2 \to 3 \to]$	$[1 \to 2 \to 3 \to]$	$[1 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \leftrightarrow 2]$	$[1 \to 3 \to 2 \to]$	$\mathbf{I}$
$[1 \to 3 \to 2 \to]$	$[1 \to 3 \to 2 \to]$	$[2 \leftrightarrow 3]$	$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 3]$	$\mathbf{I}$	$[1 \to 2 \to 3 \to]$

TABLE 2. The group table for $\mathbb{S}_3$.

D_4. Of course it is possible to just put every element of D_4 into S, but this is not very useful. We want S to be as small as possible.

First, notice, that there are two types of elements in D_4: reflections and rotations (count the identity as a rotation). Combining two reflections produces a rotation, and examing Table 1 shows that every rotation can be written as a combination of two reflections. Thus, the reflections generate D_4. We could, therefore, let S be the set of reflections: D, V, O, and H.

Question: What is the fewest number of reflections that will generate D_4?

We need at least two reflections, since combining a reflection with itself produces $\mathbf{I}$. Consider the reflections D and H. $H \circ D = R_{90}$ and so we can definitely obtain

$$\mathbf{I}, D, H, R_{90}.$$

Once we have R_{90}, we can obtain

$$R_{90}, R_{180}, \text{ and } R_{270}.$$

Exercise 5. Write R_{180} and R_{270} as combinations of D and H.

Question: Can we obtain all the reflections using just D and H?

Yes. We already have D and H, so we just need O and V. We also already know that we can obtain all the rotations. Notice that $R_{180} \circ D = O$ and $R_{270} \circ D = V$. Thus the reflections D and H generate all of D_4.

Exercise 6. (a) Show that D and V generate D_4.
(b) Show that R_{90} and any reflection generate D_4.
(c) Show that H and V do not generate D_4.
(d) Show that the rotations do not generate D_4.

For the last question, it may be helpful to notice that if you put arrows on the sides of the square so that they all point counter-clockwise around the square then a rotation will never change the fact that the arrows point counterclockwise. A reflection, however, does change the arrows from being counterclockwise to being clockwise. Thus, no combination of rotations can ever produce a reflection.

Exercise 7. Show that it is possible to generate D_n using only a reflection and a rotation. How many degrees must the rotation rotate? Does it matter what the reflection does?

Let's study the symmetric groups.

Exercise 8. What is the fewest number of elements of $\mathbb{S}_3$ that will generate $\mathbb{S}_3$? List several possibilities for generating sets with the fewest possible number of elements.

A **transposition** in a symmetric group $\mathbb{S}_n$ is a symmetry that swaps the position of two dots.

Theorem 2. The collection of all transpositions generates $\mathbb{S}_n$ for $n \geq 2$.

Proof. We must show that every permutation of n dots can be written as the combination of transpositions. This is clearly true for $n = 2$ and can easily be verified for $n = 3$ using Table 2.

Let T be in $\mathbb{S}_4$. Number the dots 1, 2, 3, 4. The effect of T on the dots can be written in the following form

1	2	3	4
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$T(1)$	$T(2)$	$T(3)$	$T(4)$

$T(1)$ is one of the numbers 1, 2, 3, or 4. Suppose first that $T(1) = 1$. Then T is a symmetry of the three dots labelled 2, 3, and 4 and therefore lives in $\mathbb{S}_3$. We have already seen that every symmetry in $\mathbb{S}_3$ can be written as a combination of transpositions. Thus, T can be written as a combination of transpositions.

Suppose that $T(1) \neq 1$. Let C be the 2–cycle $[1 \leftrightarrow T(1)]$. Let $S = C \circ T$. Then S can be described as:

1	2	3	4
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$T(1)$	$T(2)$	$T(3)$	$T(4)$
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
1	$C(T(2))$	$C(T(3))$	$C(T(4))$

Notice, therefore that S is a symmetry of dots 2, 3, and 4. It is, therefore a product of transpositions. Notice that $C \circ C = \mathbf{I}$. We have

$$S = C \circ T$$

Thus,

$$\begin{aligned} C \circ S &= (C \circ C) \circ T \\ C \circ S &= \mathbf{I} \circ T \\ C \circ S &= T. \end{aligned}$$

Thus, T is the combination of transpositions. A similar argument shows that every symmetry in $\mathbf{S}_5$ is the combination of transpositions. We then boot strap our way to conclude that every symmetry in $\mathbb{S}_n$ is a combination of transpositions for any $n \geq 2$. □

Exercise 9. How many transpositions are there in $\mathbb{S}_n$?

Exercise 10. Show that the following set of transpositions generate $\mathbb{S}_n$ for $n \geq 2$:

$$[1 \leftrightarrow 2]$$
$$[2 \leftrightarrow 3]$$
$$[3 \leftrightarrow 4]$$
$$\vdots$$
$$[n-1 \leftrightarrow n].$$

These are called **adjacent transpositions**.

Exercise 11. How many adjacent transpositions are there in $\mathbb{S}_n$?

2.3. **Relations.** Suppose that G is a group and that we have a list of generators $s_1, s_2, \ldots, s_n$ for G. Recall that this means that every element of the group can be written as a combination of the s_i and their inverses. Is this enough to specify the group? No – many different groups can be generated by n generators. To specify the which group we are discussing, we also need to list some **relations**. Relations are equations which tell us that certain combinations of the generators are equal to $\mathbf{I}$. Here is an example.

Suppose that G is a group with one generator s. Denote the combination of s with itself n times by s^n. Let s^{-n} denote the combination of s^{-1} with itself n times. Then the following list includes all the elements of G:

$$\ldots, s^{-4}, s^{-3}, s^{-2}, s^{-1}, \mathbf{I}, s^1, s^2, s^3, s^4, \ldots$$

There are infinitely many items in this list. If G has no relations then this is the list of elements in G with no repetitions. Suppose however, that G has the relation:

$$R1 : s^3 = \mathbf{I}$$

Then anytime we see $s \circ s \circ s$ we may cancel it (i.e. replace it with $\mathbf{I}$). For example, if $R1$ holds

$$s^8 = (s \circ s \circ s) \circ (s \circ s \circ s) \circ s \circ s = s \circ s = s^2$$

Some thought shows that if G has one generator (s) and the relation $R1$ then

$$G = \{\mathbf{I}, s, s^2\}.$$

We can write this as $G = \langle s | s^3 = \mathbf{I} \rangle$. Notice that if $s^3 = \mathbf{I}$, then $s^{-3} = \mathbf{I}$ since

$$s^{-3} \circ s^3 = s^{-3} \circ \mathbf{I} \Rightarrow \mathbf{I} = s^{-3}.$$

What happens if G has the relation $R1$ and the relation

$$R2 : s^4 = \mathbf{I}?$$

Notice then that:

$$s = s^4 \circ s^{-3} = s^4 \circ \mathbf{I} = \mathbf{I}$$

by first applying $R1$ and then applying $R2$. Thus, the group

$$\langle s | s^3 = \mathbf{I}, s^4 = \mathbf{I} \rangle$$

is just the group consisting only of the identity.

It turns out that every group has a presentation in terms of a list of generators and a list of relations. Here are some common group presentations:

C_n $\quad \langle \ s \ | \ s^n = \mathbf{I} \ \rangle$

D_n $\quad \langle \ s,t \ | \ s^n = \mathbf{I}, \quad t^2 = \mathbf{I} \ \rangle$

$$\mathbb{S}_n \qquad \left\langle \ s_1, s_2, \ldots, s_n \ \middle| \ \begin{array}{rcll} s_i^2 & = & \mathbf{I} & \\ s_i s_{i+1} s_i & = & s_{i+1} s_i s_{i+1} & \\ s_i s_j & = & s_j s_i & \text{if } |i-j| \neq 1 \end{array} \right\rangle$$

3. SUBGROUPS

Let G be a group with operation $\circ$. A subset H of G is a **subgroup** if H is a group with operation $\circ$.

Exercise 12. Show that the set of rotations in D_n is a subgroup of D_n. It is usually denoted C_n.

Exercise 13. Let A_n be the set of elements in S_n which can be written as a product of an even number of transpositions. It is called the alternating group of n dots. Show that A_n is a subgroup of S_n.

Exercise 14. Let x be an element of a group G. Show that the set of all combinations of x with itself and with its inverse is a subgroup of G. It is denoted by $\langle x \rangle$. Explain why $C_n = \langle x \rangle$ for some x in D_{2n}. Specify what x is.

Definition 2. The **order** of a finite group is simply the number of elements in the group.

We now come to the most important theorem in group theory.

Definition 3. Suppose that H is a subgroup of a finite group G. Then the order of G is divisible by the order of H.

For example, the order of D_n is twice the order of C_n.

To begin the proof of the theorem we need some more concepts. For an element g in G, denote by $[g]$ the set:

$$\{g \circ h : h \text{ is in } H\}.$$

S_2 \ S_1	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
$\mathbf{I}$	$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H
R_{90}	R_{90}	R_{180}	R_{270}	$\mathbf{I}$	H	D	V	O
R_{180}	R_{180}	R_{270}	$\mathbf{I}$	R_{90}	O	H	D	V
R_{270}	R_{270}	$\mathbf{I}$	R_{90}	R_{180}	V	O	H	D
D	D	V	O	H	$\mathbf{I}$	R_{90}	R_{180}	R_{270}
V	V	O	H	D	R_{270}	$\mathbf{I}$	R_{90}	R_{180}
O	O	H	D	V	R_{180}	R_{270}	$\mathbf{I}$	R_{90}
H	H	D	V	O	R_{90}	R_{180}	R_{270}	$\mathbf{I}$

TABLE 3. The cosets of C_4 in D_4

$\mathbf{I}$	R_{90}	R_{180}	R_{270}	D	V	O	H

TABLE 4. There are two cosets of C_4 in D_4.

$\mathbf{I}$	[12]	[13]	[14]	[23]	[24]
[34]	[12][23]	[13][32]	[12][24]	[14][42]	[13][34]
[14][43]	[23][34]	[24][43]	[12][34]	[13][24]	[14][23]
[12][24][43]	[12][23][34]	[13][32][24]	[13][34][42]	[14][42][23]	[14][43][32]

TABLE 5. The elements of A_4 inside $\mathbb{S}_4$.

The set $[g]$ is called the **coset** of G. If we have a group table for G, the set $[g]$ is simply the collection of all group elements in the row beginning with g which are also in a column headed by an element of H.

Here is an example. Consider the group D_4 with the subgroup C_4. Here is the group table for D_4. Each coset occurs in multiple rows. I have colored just one occurence of each coset. Different colors represent different cosets.

A more concise way of looking at the cosets is by listing each element of the group and coloring two elements the same if they are in the same coset. This is done in Table 4.

Let's find all the cosets of A_4 in $\mathbb{S}_4$. We begin by listing the elements of $\mathbb{S}_4$. To make the notation easier, we drop the arrows from the notation we've used previously. We write each element as the combination of transpositions (leaving out the $\circ$), to make it easy to tell if an element is in A_4 or not. The elements in A_4 have been shaded red. They also form one of our cosets.

Here is another example. Consider the element $x = [1234]$ in $\mathbb{S}_4$. Let $H = \langle x \rangle$. Find all the cosets of H in $\mathbb{S}_4$. Begin by listing the elements of H:

$$\begin{array}{rc} & \mathbf{I} \\ & [1234] \\ [1234][1234] = & [13][24] \\ [1234][1234][1234] = & [1432] \end{array}$$

The next lemma will be helpful in continuing our analysis:

Lemma 3. Let G be a finite group and H a subgroup. Then the following hold:

(a) If x is in the coset $[g]$ then $[x] = [g]$. (Different cosets have no elements in common.)
(b) H is a coset of H in G.
(c) All cosets have the same number of elements as H.

Proof. (1) Suppose that x is in the coset $[g]$. This means that there is an element h in H so that $g \circ h = x$. Notice that $g = x \circ h^{-1}$. We must show that every element in $[x]$ is in $[g]$ and every element of $[g]$ is in $[x]$. Suppose that y is in $[x]$. This means that there is an element h' in H so that $x \circ h' = y$. This means that $g \circ (h \circ h') = y$. Since H is a group, $h \circ h'$ is in H. Thus, y is in $[g]$. Now suppose that g' is in $[g]$. There exists h' so that $g' = g \circ h'$. This implies that $g' = (x \circ h^{-1}) \circ h'$. Thus, g' is in $[x]$.

(2) I claim that $[\mathbf{I}] = H$. By definition,

$$[\mathbf{I}] = \{y : \text{there exists some } h \text{ in } H \text{ with } I \circ h = y\}.$$

For every y, however, $\mathbf{I} \circ y = y$. Thus, $[\mathbf{I}] = H$.

(3) Let $[g]$ be a coset of H in G. We match every element of $[g]$ with an element of H and every element of H with an element of G so that different elements are not matched to the same element. Here is the matching: Let $g \circ h$ be an element of $[g]$ with h in H. Match $g \circ h$ with h. Notice that every element h in H is matched with some element in $[g]$. Notice that if $g \circ h$ is matched with h' then $g \circ h = g \circ h'$ and so $h = h'$. This shows that different elements of $[g]$ are matched with different elements of H. Thus $[g]$ and H have the same number of elements. □

Notice that since all the cosets of H in G are disjoint and since they all have the same number of elements, we automatically have proved Lagrange's theorem.

We can use these observations to study $H = \langle [1234] \rangle$ in $\mathbb{S}_4$. We can conclude, first of all, that H is one of our cosets. Here is a list of the elements of $\mathbb{S}_4$ with the elements of H colored in red.

I	[12]	[13]	[14]	[23]	[24]
[34]	[12][34]	[13][24]	[14][23]	[123]	[132]
[124]	[142]	[134]	[143]	[234]	[243]
[1234]	[1243]	[1324]	[1342]	[1423]	[1432]

By LaGrange's theorem we should expect $24/4 = 6$ other cosets. Let's begin by considering $\big[[12]\big]$. By calculation, we find

$$\begin{array}{rcl} [12][1234] & = & [234] \\ [12][[13][24] & = & [1324] \\ [12][1432] & = & [143] \end{array}$$

Let's color that coset blue.

I	[12]	[13]	[14]	[23]	[24]
[34]	[12][34]	[13][24]	[14][23]	[123]	[132]
[124]	[142]	[134]	[143]	[234]	[243]
[1234]	[1243]	[1324]	[1342]	[1423]	[1432]

Following the same pattern, it's not too hard to discover that these are the other cosets:

I	[12]	[13]	[14]	[23]	[24]
[34]	[12][34]	[13][24]	[14][23]	[123]	[132]
[124]	[142]	[134]	[143]	[234]	[243]
[1234]	[1243]	[1324]	[1342]	[1423]	[1432]

If G is a group and H is a subgroup of G, the number of cosets of H in G is called the **index** of H in G. The index of H in G is denoted $[G : H]$. Lagrange's theorem can be stated as

Theorem 4. (LaGrange) For a finite group G containing a subgroup H:

$$|H|[G : H] = |G|.$$

Exercise 15.
(a) Suppose that H is a subgroup of D_8. How many elements might H have?
(b) Suppose that H is a subgroup of $\mathbb{S}_4$. How many elements might H have?
(c) The index of A_n in $\mathbb{S}_n$ is two. How many elements does A_n have?
(d) Suppose that H is a subgroup of a cyclic group C_p where p is a prime number. How many elements might H have?

We have seen various ways of describing the groups D_n and $\mathbb{S}_n$ using different generating sets. In general, it is a difficult problem to explicitly describe a given group, whether or not it is a group of symmetries. Using an extension of LaGrange's theorem, though, we can learn somethings.

Definition 4. Suppose that G is a group of symmetries of an object X. Let x be a point of X. Define the orbit of x to be the set of all points y in X. such that there is a symmetry in G which takes x to y. Denote this set by $\texttt{orb}_G(x)$.

Let x be a vertex of the square. The group D_4 is the group of all symmetries of the square. A symmetry in D_4 takes x to another vertex, and we can send x to any vertex we want to by choosing an appropriate symmetry in D_4. Thus, $\texttt{orb}_{D_4}(x)$ is the set of vertices of the square.

The group $G = \{\mathbf{I}, R_{180}\}$ is a subgroup of D_8. The set $\texttt{orb}_G(x)$ consists of the vertex x and the vertex directly opposite it on the square.

Definition 5. Suppose that G is a group of symmetries of an object X. Let x be a point of X. The set of group elements g which don't move x is called the **stabilizer** of x in G. It is denoted $\texttt{stab}_G(x)$.

Let x be the upper left vertex of the square, then $\texttt{stab}_{D_4}(x) = \{\mathbf{I}, D\}$ since every element of D_4 except the identity and the diagonal reflection moves x to some other vertex. If x is the center of the square, then $\texttt{stab}_{D_4}(x) = D_4$, since no element of D_4 moves the center of the square.

Exercise 16. Prove that $\texttt{stab}_G(x)$ is a subgroup of G for any given point x.

Theorem 5. (Orbit-Stabilizer) Suppose that G is a group of symmetries of an object X. For any point x in X,

$$|\texttt{orb}_G(x)| \cdot |\texttt{stab}_G(x)| = |G|.$$

Proof. We simply need to show that $|\texttt{orb}_G(x)| = [G : \texttt{stab}_G(x)]$. Let $[g]$ be a coset of $\texttt{stab}_G(x)$ in G. Match the coset $[g]$ with the point $g(x)$ in $\texttt{orb}_G(x)$. Notice that if g and g' are both in $[g]$ then we have $g' = g \circ h$ for some h in $\texttt{stab}_G(x)$. Then $g'(x) = g \circ h(x)$. Since $h(x) = x$, $g'(x) = g(x)$ and so this matching is well defined. Notice also that ever point in the orbit of x is matched with some coset and that if $g(x) = g'(x)$ then $g^{-1} \circ g'(x) = x$. This implies that $g^{-1} \circ g$ is in $\texttt{stab}_G(x)$. It turns out that this implies that $[g] = [g']$.

Thus, each coset of $\texttt{stab}_G(x)$ is matched with one point in $\texttt{orb}_G(x)$ and different cosets are matched with different points. Since each point of the

orbit of x is matched with some coset, the size of $\mathtt{orb}_G(x)$ is equal to the number of cosets which is $[G : \mathtt{stab}_G(x)]$. □

Let's use this to do something interesting.

Let X be a cube in 3–space and let $G = \mathtt{Sym}(X)$. Let's determine how many symmetries are in G. Let x be a vertex of the cube. There is a symmetry which sends x to any other vertex that we want. Every symmetry of X must send vertices to vertices. The cube has 8 vertices, so $|\mathtt{orb}_G(x)| = 8$. Suppose that T is a symmetry of the square which doesn't move x. There are three edges coming into x and T must permute those in some way. It is not hard to see that all possibilities for permutations can be achieved. Furthermore, if T fixes x and all edges coming into x then T must be $\mathbf{I}$. To see this, recall that if a symmetry of 3–space fixes three points then it is the identity.

Thus,

$$|\mathtt{stab}_G(x)| = |\mathbb{S}_3| = 6.$$

Hence, by the orbit-stabilizer theorem, G has $8 \cdot 6 = 48$ elements.

The five platonic solids are the tetrahedron, the cube, the octahedron, the dodecahedron, and the iscosahedron.

Exercise 17. Look up pictures of each of the platonic solids and perform an analysis similar to what we just did to determine the orders of their groups of symmetries.

Some of the symmetries that we counted include reflections. Let $\mathtt{Sym}^+(X)$ denote the subgroup of $\mathtt{Sym}^+(X)$ which preserve the orientation of 3–space. Let $[g]$ and $[h]$ be cosets of this group in $\mathtt{Sym}(X)$ where both g and h reverse orientation. Notice that g^{-1} reverses orientation. Notice also that, $k = g^{-1} \circ h$ must preserve orientation; that is, $g \circ h$ is in $\mathtt{Sym}^+(X)$. The symmetry k^{-1} also preserves orientation. Thus,

$$h \circ k^{-1} \text{ is in } [h].$$

But

$$h \circ k^{-1} = h \circ (g^{-1} \circ h)^{-1} = h \circ h^{-1} \circ g = g.$$

Hence, $[g] = [h]$. This proves that there are at most two cosets of $\mathtt{Sym}^+(X)$ in $\mathtt{Sym}(X)$: $\mathtt{Sym}^+(X)$ and one other one $[g]$. Thus, the index of $\mathtt{Sym}^+(X)$ is either one or two in $\mathtt{Sym}^+(X)$. We can conclude, for example, that there are 24 orientation preserving symmetries of the cube. Figure 4 depicts three representative examples.

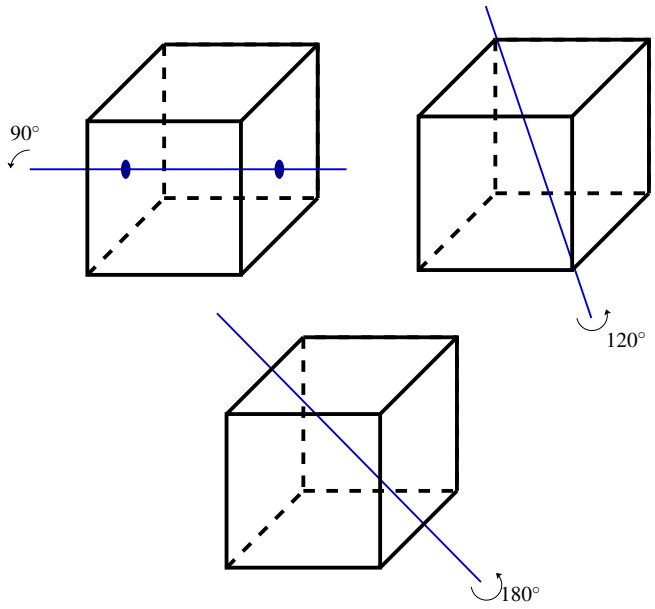

FIGURE 4. Examples of the three types of orientation preserving symmetries of the cube.