

Lecture Notes on Symmetry

MA 111 Spring 2010

Scott Taylor, Colby College

CONTENTS

1. Preliminaries	3
2. Groups	3
2.1. Group Tables	3
3. Interlude: Symmetry in Music	9
4. Other Examples of Groups	11
5. Interlude: Campanology	16
6. Subgroups	17
6.1. Subgroups as adding decoration	18
7. Generators	23
7.1. Generating the Dihedral Groups	23
7.2. Generating the Symmetric Groups	24
8. Interlude: Plain Bob Minimus	26
9. Even and Odd Symmetries in \mathbb{S}_n	28
10. Interlude: 15-Puzzle	32
11. The Alternating Groups	35
12. LaGrange's Theorem	37
12.1. Examples of LaGrange's Theorem in Practice	37
12.2. Cosets	38
13. The Orbit-Stabilizer Theorem	46
14. The Symmetries of \mathbb{R}^n for $n \leq 3$.	47
14.1. Classifying Isometries	47

14.2. Frieze Groups and Wallpaper Groups

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 . Here are two important points:

- Two transformations are the same if they have the same effects. (Thus, it doesn't matter *how* the transformation is performed, only what the result of the transformation is.
- We will only consider transformations which are “invertible”. This means that if T is a transformation, then there is another transformation S which “undoes” T . More about this later.

A transformation is a **automorphism** or **symmetry** of X if it preserves a given “structure” of X . Right now this is a very vague statement but as we see examples we will come to a clearer understanding of what this means.

Our first important example will concern symmetries of the plane that preserve the distance between points and which take a square to itself. For example, consider the rotation R_{180} of a square around its center by 180° counterclockwise. This is the same symmetry as “rotate 90° counterclockwise and then rotate another 90° counterclockwise. It is also the same as “rotate by 180° clockwise”.

We'll begin by listing 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.

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**.

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”.

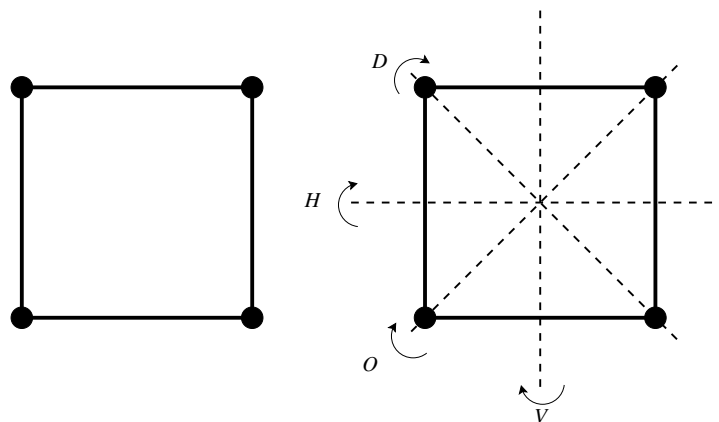


FIGURE 1. The symmetries of the square

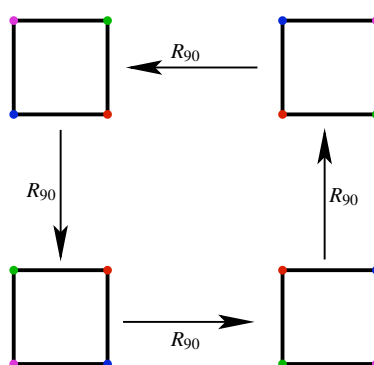


FIGURE 2. Applying R_{90} to the square. The vertices have been colored to exhibit the effect of R_{90} .

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 way it was before the motion. (Usually) 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 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 and then another. For example, performing R_{90} and then performing R_{90} again is the same as performing R_{180} . There is also the symmetry \mathbf{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: $\mathbf{I}, R_{90}, R_{180}, R_{270}, D, V, O, H$ 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_1							
		\mathbf{I}	R_{90}	R_{180}	R_{270}	D	V	O	H
S_2	\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_1							
		$S_2 \circ S_1$	I	R_{90}	R_{180}	R_{270}	D	V	O
S_2	I	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_1							
		$S_2 \circ S_1$	I	R_{90}	R_{180}	R_{270}	D	V	O
S_2	I	I	R_{90}	R_{180}	R_{270}	D	V	O	H
	R_{90}	R_{90}	R_{180}	R_{270}	I				
	R_{180}	R_{180}	R_{270}	I	R_{90}				
	R_{270}	R_{270}	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

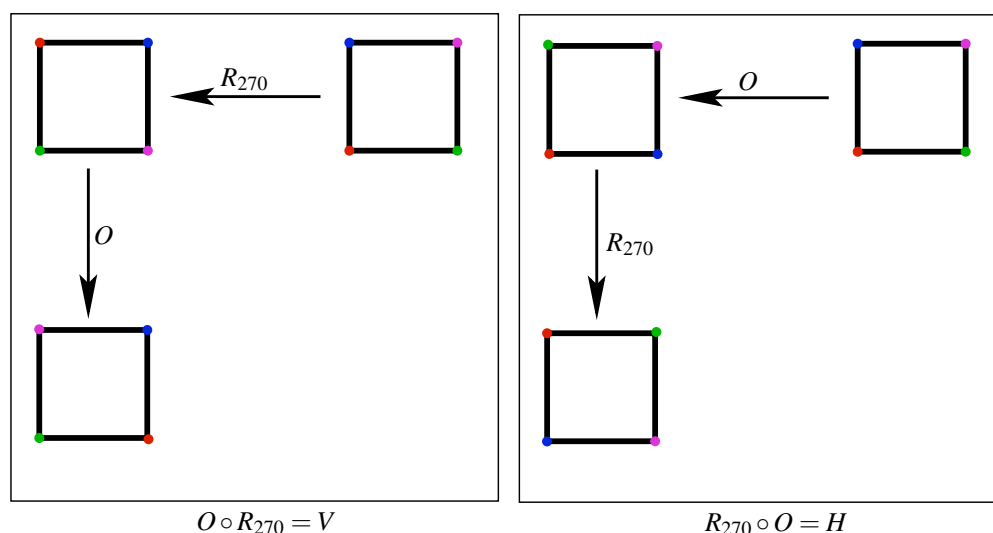
$$O \circ R_{270} \neq R_{270} \circ O.$$

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

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”.

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

		S_1							
		\mathbf{I}	R_{90}	R_{180}	R_{270}	D	V	O	H
S_2	\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 1. The group of symmetries of a square

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 such that the following properties to hold:

- (Closure) If a and b are in G , then $b \circ a$ is in G .
- (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 ,

$$a \circ \mathbf{I} = \mathbf{I} \circ a = a.$$

- (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 frequently 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 $\text{Sym}(X)$. 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 \mathbf{I} .

3. INTERLUDE: SYMMETRY IN MUSIC

Consider the “space” of Western Music. Symmetries of this space include “reflection in time”, reflection about a pitch, translation in time, translation in pitch (i.e. musical transposition). Composers have made use of all of these symmetries (and more!). Here are a few simple examples.


Example 1 Below is the theme for the “Crab Canon” from Bach’s *Musical Offering*. This is a canon where one player reads the music forwards and the other reads the music backwards. The theme is, therefore, symmetric in time about the midpoint of the composition. Notice that this does not mean that the theme itself is symmetrical.

Canones diversi
super thema regium.

Canon a 2.

1. 

Example 2 The excerpt below is from Bartok’s *Music for Strings, Percussion and Celeste* (mvt 1). What symmetry do you spot?¹



ppp

Example 3: Below is an excerpt from the middle of *Capriccio* K395 by Mozart. This passage is (approximately) symmetric under translation in time and reflection in pitch. Notice how the symmetry is broken at the end of the section.

¹You can read more about symmetry in Bartok’s music at <http://www.solomonsmusic.net/diss7.htm>



Example 4 Below is a tone row from Webern's Chamber Symphony. If we read it backwards we have a transposed version of what we get if we read it forwards. Thus, if we couldn't tell that it had been transposed, the row would be symmetric in time about its midpoint. Since it is transposed, it has a symmetry which is a combination of time reversal and pitch transposition.



Example 5 Below is the tone row from Schoenberg's Serenade (op 24, mvt 5). It is symmetric under the symmetry $T \circ R \circ I$, where I is inversion (turning it upside down), R is retrograde (playing it backwards), and T is a transposition.



4. OTHER EXAMPLES OF GROUPS

We will occasionally make use of the following terminology:

- The **integers** are the positive and negative whole numbers and zero:

$$\{\dots, -2, -1, 0, 1, 2, \dots\}.$$

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.

- \mathbb{Z} with the operation of $+$.
- \mathbb{Z} with the operation of $-$.
- \mathbb{R} with the operation of $+$.
- \mathbb{R} with the operation of \cdot (multiplication).
- \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.)

Exercise 4. Explain why the Western tonal system has as symmetries the rotations of a regular dodecagon. You may assume equal tempering so that two adjacent notes differ by exactly one semitone (half step). (Hint: A 440 Hz sounds a lot like A 880 Hz.)

Here is another example. In this example the object will be three indistinguishable points: $\bullet\bullet\bullet$. You should think of these as points (not dots with thickness), 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 points. We won't insist that the symmetry preserve the distance between the points. One example of an allowed symmetry is swapping the first two points.

As with the square, to distinguish the effects of different symmetries, we'll add some colors to the points: ●●●. This will enable us to keep track of the different behaviour of different symmetries.

To recap: our group is $\mathbb{G} = \text{Sym}(\bullet\bullet\bullet)$. We need names for the different symmetries of the points. Denote the action of swapping the first two points by $[1 \leftrightarrow 2]$. In our notation:

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

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

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

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

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

Is this list complete? The answer is “yes”. Here's how to tell. Applying each symmetry to the colored points ●●● produces a new way of coloring the points. If two symmetries produce the same coloring, they have the same effect and so are considered to be the same symmetry. Given the initial coloring of the points, 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 at most 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 points (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 points 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:

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

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,

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

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 points is denoted \mathbb{S}_n . Thus, the symmetry group of three indistinguishable points (which we just studied) is denoted \mathbb{S}_3 .

- Exercise 5.**
- Show that every symmetry of 3 indistinguishable points is also a symmetry of an equilateral triangle.
 - Show that every symmetry of an equilateral triangle is also a symmetry of 3 indistinguishable points.
 - Explain why the previous two exercises show that D_3 is “the same as” \mathbb{S}_3 .
 - Show that D_n contains $2n$ symmetries.
 - Show that \mathbb{S}_n contains $n! = n(n-1)(n-2)\dots(3)(2)(1)$ symmetries.
 - Explain why D_n is not the same as \mathbb{S}_n for $n \geq 4$.

Exercise 6. Write down all elements of \mathbb{S}_4 .

Exercise 7. In \mathbb{S}_4 there is a symmetry which interchanges the first two points and which interchanges the last two points. Explain why this is the same symmetry as the one where we first interchange the first two points and then we interchange the last two points.

As we progress we will be writing down lots of permutations, so let's make our notation more concise by dropping all the arrows. Thus, in \mathbb{S}_6 , instead

$S_2 \circ S_1$	I	$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$
I	I	$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$
$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 2]$	I	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$	$[2 \leftrightarrow 3]$	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	$[1 \leftrightarrow 3]$
$[1 \leftrightarrow 3]$	$[1 \leftrightarrow 3]$	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	I	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$	$[1 \leftrightarrow 2]$	$[2 \leftrightarrow 3]$
$[2 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	I	$[1 \leftrightarrow 3]$	$[1 \leftrightarrow 2]$
$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$	$[1 \leftrightarrow 3]$	$[2 \leftrightarrow 3]$	$[1 \leftrightarrow 2]$	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$	I
$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$	$[1 \rightarrow 3 \rightarrow 2 \rightarrow]$	$[2 \leftrightarrow 3]$	$[1 \leftrightarrow 2]$	$[1 \leftrightarrow 3]$	I	$[1 \rightarrow 2 \rightarrow 3 \rightarrow]$

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

of writing $[1 \rightarrow 3 \rightarrow 6 \rightarrow]$ we will write $[136]$. Also, we will frequently leave out the \circ when we combine symmetries. Thus, instead of writing $[136] \circ [243]$ we will write $[136][243]$.

5. INTERLUDE: CAMPANOLOGY

“To the ordinary man, in fact, the pealing of bells is a monotonous jangle and a nuisance, tolerable only when mitigated by remote distance and sentimental association. [But the change-ringer’s] passion – and it is a passion – finds its satisfaction in mathematical completeness and mechanical perfection, and as his bell weaves her way rhythmically up from lead to hinder place and down again, he is filled with the solemn intoxication that comes of intricate ritual faultlessly performed. – Dorothy L. Sayers, *The Nine Tailors*, 1934.

Cathedral bells in England (and elsewhere) come in different pitches. They are rung by pulling on ropes which swing the bells around. Typically, the bells are rung sequentially. For example, if there are four bells S, A, T, and B (in order of decreasing pitch), the bells might be rung in the order

S then A then T then B then S then A then T then B, etc.

The bells are very heavy and so it is not easy to radically alter the sequence (or “round”) in which they are rung. Usually, only two operations on the sequence in which the bells are rung are permitted: plain changes and cross changes. In a plain change, one pair of adjacent bells has their order swapped. In a cross change, more than one pair of adjacent bells may have their order swapped. For example:

One of the simplest changes is “the plain lead”. The “S” bell has been colored red, to make it easier to track its position in the round.

S	A	T	B	
A	S	B	T	
A	B	S	T	
B	A	T	S	
B	T	A	S	
T	B	S	A	
T	S	B	A	
S	T	A	B	

Notice that we are alternately applying the symmetries $g = [12][34]$ and $h = [23]$ to the round. Notice that the symmetries

$$\{\mathbf{I}, g, h \circ g, g \circ h \circ g, (h \circ g)^2, g \circ (h \circ g)^2, (h \circ g)^3, g \circ (h \circ g)^3\} = \{\mathbf{I}, [12][34], [1342], [14], [14][23], [13][24], [1243], [23]\}$$

form a group sitting inside \mathbb{S}_4 .

6. 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 8. Show that the set of rotations (including \mathbf{I}) in D_n is a subgroup of D_n . It is usually denoted C_n . Is the set of reflections a subgroup of D_n ?

Exercise 9. Let G be the symmetries of a circle. Show that the set of rotations in G is a subgroup of G .

One of the goals of this part of the course is to explain a particular relationship between the subgroups of a group and the group itself. To understand this relationship, it will be important to have at our disposal ways of creating subgroups of a given group. Here is a popular method, that will be generalized in the next section of these notes.

We begin with a bit of notation. Let G be a group with operation \circ and suppose that g is a symmetry in G . We can obtain new group elements by combining g with itself some number of times. For example, $g \circ g \circ g$. Denote the result of combining g with itself n times by g^n and denote the result of combining g^{-1} with itself n times by g^{-n} . For convenience, define $g^0 = \mathbf{I}$.

Exercise 10. Show that the following rules hold for all numbers $n, m \in \mathbb{Z}$.

- (a) $g^n \circ g^m = g^{n+m}$
- (b) The inverse of g^n is g^{-n} .

The previous exercise shows that the set $\langle g \rangle$ defined by

$$\langle g \rangle = \{\dots, g^{-3}, g^{-2}, g^{-1}, \mathbf{I}, g, g^2, g^3, \dots\}$$

is a subgroup of G .

Exercise 11. Let $g = [132][45]$ in \mathbb{S}_5 . Write down all the elements of $\langle g \rangle$.

Exercise 12. Let $g = [12][34]$ in \mathbb{S}_6 . Write down all the elements of $\langle g \rangle$.

If G is a finite group and if g is a symmetry in G then $\langle g \rangle$ must also be a finite group. The point of the next exercise is to show that *if* G is a finite group, then, for some $n \in \mathbb{N}$:

$$\langle g \rangle = \{\mathbf{I}, g, g^2, g^3, \dots, g^n\}$$

Exercise 13. Assume that G is a finite group and that $g \in G$. Let $H = \{\mathbf{I}, g, g^2, \dots\}$. Recall that $\langle g \rangle = \{\dots, g^{-3}, g^{-2}, g^{-1}, \mathbf{I}, g, g^2, g^3, \dots\}$. We wish to show that $H = \langle g \rangle$. We will do this by showing that each symmetry in H is also in $\langle g \rangle$ and that each symmetry of $\langle g \rangle$ is also in H .

- (a) Observe that each symmetry in H is also in $\langle g \rangle$.
 (b) Explain why even though the set

$$H = \{\mathbf{I}, g, g^2, g^3, \dots\}$$

looks like it has infinitely many symmetries in it, it can in fact have only finitely many symmetries.

- (c) Explain why the previous question implies that there are numbers $k, l \in \mathbb{N}$ with $k < l$ so that

$$g^k = g^l.$$

- (d) Explain why the previous question implies that $l - k > 0$ and $g^{l-k} = \mathbf{I}$.
 (e) Define $n = l - k$. For $m \in \mathbb{N}$, explain why the previous question implies that $g^{-m} = g^{n-m}$.
 (f) Explain why the previous parts show that $H = \langle g \rangle$.

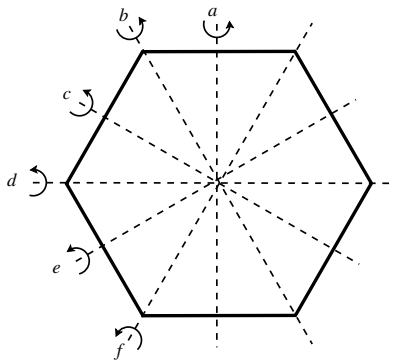
Exercise 14. Give an example of a subgroup of D_4 which is not equal to $\langle g \rangle$ for some g in D_4 .

6.1. Subgroups as adding decoration. If we are studying an object X (for example the hexagon below). We can find subgroups of the object by adding decorations and asking for all symmetries of X which preserve the decoration.

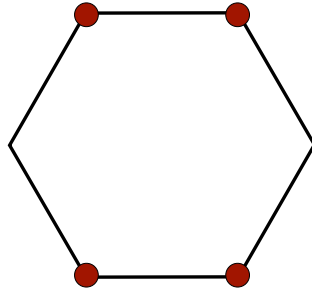
Consider for example the symmetries of a regular hexagon:

$$D_6 = \{\mathbf{I}, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, a, b, c, d, e, f\}$$

where $\{a, b, c, d, e, f\}$ are the reflections indicated in the diagram:



Paint four of the corners of the hexagon red, as below:



Then the symmetries of the hexagon which take red points to red points are:

$$H = \{\mathbf{I}, a, d, R_{180}\}.$$

H is a subgroup of D_6 .

Conversely, if we have a subgroup H of the symmetry group of X we can (sometimes) decorate X so that H is the symmetry group of the decorated X as follows.

- (a) Find a point p in X such that every symmetry of X (other than \mathbf{I}) moves p to some new point.
- (b) Add a decoration to p (say, color p red).
- (c) List the symmetries in H as

$$H = \{h_1, h_2, h_3, \dots\}.$$

- (d) Decorate all of the points

$$\{h_1(p), h_2(p), \dots\}$$

the same way that p is decorated.

Theorem 2. If it is possible to perform all of these steps, then H is exactly the symmetries of the decorated object X .

Proof. We must show that if g is a symmetry of the decorated object X , then g is a symmetry in H and, conversely, if h is a symmetry in H then h is a symmetry of the decorated object X . Let Dec be the set of all decorated points of X .

Claim 1: If g is a symmetry of the decorated object X then g is a symmetry in H .

The symmetry g takes all the points of Dec to other points of Dec . In particular, there exists h_j in H so that

$$g(p) = h_j(p).$$

This implies that

$$h_j^{-1} \circ g(p) = p.$$

In other words, the symmetry $h_j^{-1} \circ g$ does not move p . However, p was chosen so that every symmetry of X , other than \mathbf{I} moves p to some other point. Consequently,

$$h_j^{-1} \circ g = \mathbf{I}.$$

This implies that

$$g = h_j^{-1},$$

and so g is a symmetry in H .

Claim 2: If h_i is a symmetry in H then h_i is a symmetry of the decorated object X .

First of all, recall that H is a subgroup of the $\text{Sym}(X)$ and so h_i takes X to itself. It remains to show that h_i takes the set of decorated points Dec to itself. Suppose that $h_j(p)$ is a point in Dec . Then:

$$h_i(h_j(p)) = (h_i \circ h_j)(p).$$

Since H is a group, there exists k so that $h_i \circ h_j = h_k$. Thus,

$$h_i(h_j(p)) = h_k(p).$$

By the definition of Dec , $h_k(p)$ is a decorated point. Thus, h_i takes each decorated point of X to another decorated point of X . \square

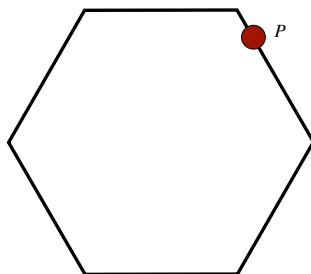
Here is an example: recall that the symmetries of the hexagon are

$$D_6 = \{\mathbf{I}, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, a, b, c, d, e, f\}$$

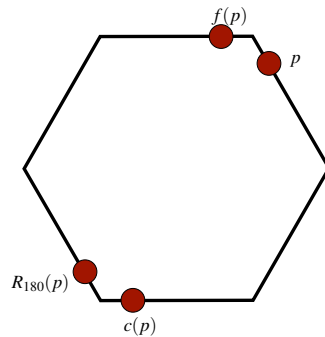
Let H be the subgroup

$$H = \{\mathbf{I}, c, f, R_{180}\}$$

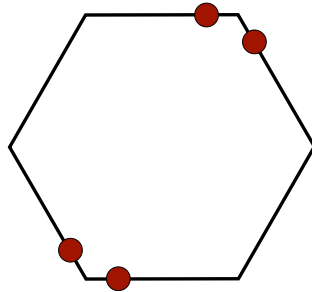
Pick a point p on the hexagon which is moved by every symmetry of D_6 other than \mathbf{I} .



Now decorate all the points $\text{Dec} = \{p, c(p), f(p), R_{180}(p)\}$



The subgroup H is exactly the symmetries of the decorated hexagon:



We are left with the question, “what keeps this method from working?” There are two obstructions:

- (a) There may not be a point p which is left unmoved by *all* the symmetries of X other than \mathbf{I} .
- (b) It may not be possible to “list” all the elements of H .

For an example where obstruction (a) arises, consider \mathbb{S}_n ($n \geq 3$) as the symmetries of a set X of n points. For each point in X , there exists a symmetry other than \mathbf{I} which doesn’t move the point. For an example where obstruction (b) arises consider the set of symmetries G of a circle X and let H be the set of rotations of the circle. At least abstractly there are ways around both obstructions but we won’t go into them.

Exercise 15. Let G be the group of symmetries of a circle X and let H be the rotations of X .

- (a) Show that for each point p on X there exists a symmetry in G other than \mathbf{I} which doesn’t move p .
- (b) Show that it is possible to add some decorations to the circle to create an object Y such that the symmetries of Y are exactly the symmetries in H . (Hint: Try adding arrows to the circle.)

We've looked at some examples of symmetry in music. For the most part those examples did not take rhythm or instrumentation into account. Taking those into account frequently reduces the symmetry group of that section of music to the trivial group $\{I\}$. Figure 4 below shows another example:



FIGURE 4. Notice that the copper lamp has both blue and green jewels. We could study the symmetries of the lamp where we ignore the color of the jewels. Call that symmetry group G . If we only consider symmetries which preserve the colors of the jewels (i.e. symmetries which take blue jewels to blue jewels and green jewels to green jewels) we get a symmetry group H . The symmetry group H is a subgroup of the symmetry group G .

7. GENERATORS

Although every (finite) group has a group table, for all but the smallest groups writing down the group table is very inefficient. For most groups, even writing down all the symmetries in the group is an arduous or impossible task. A more efficient method is to write down a collection S of symmetries such that every other symmetry in the group is a combination of symmetries in S and their inverses. That small number of elements from which every other group element can be generated will be called a set of generators for the group.

7.1. Generating the Dihedral Groups. 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 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 examining 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 **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 16. 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 17. (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 18. 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?

Exercise 19. Consider the subgroup C_n of D_n . (C_n consists of all rotational symmetries of a regular n -gon.) Explain how to find a symmetry S in C_n so that $C_n = \langle S \rangle$.

Exercise 20. Consider the set H of all rotations of a circle by $(2\pi k)/2^n$ degrees where k and n are integers. Show that H is a group and that there does not exist a symmetry S so that $H = \langle S \rangle$.

Exercise 21. Let C be the group of rotations of a circle. Does there exist a symmetry S in C so that $C = \langle S \rangle$?

7.2. Generating the Symmetric Groups.

Exercise 22. What is the fewest number of symmetries in \mathbb{S}_3 that will generate \mathbb{S}_3 ? List several possibilities for generating sets with the fewest possible number of elements.

A **cycle** in \mathbb{S}_n is a symmetry which moves a subset of the points in a way analogous to a rotation in D_n . For example, $[1 \rightarrow 3 \rightarrow 5 \rightarrow 4 \rightarrow]$ is a cycle in \mathbb{S}_5 . We will sometimes use $[5 \rightarrow]$ denote a cycle which doesn't move the 5th point. (Of course, 5 can be replaced by any other number.) A **transposition** is a cycle that swaps the position of two points. (Note: This notion of transposition is completely different from the notion of transposition in music.) For example, $[2 \leftrightarrow 5]$ is a cycle which swaps the second and fifth points.

The next theorem shows that the cycles generate \mathbb{S}_n .

Lemma 3. Given a permutation g in \mathbb{S}_n , it is possible to write

$$g = c_m \circ c_{m-1} \circ \dots \circ c_1$$

where each c_i is a cycle and each number of $\{1, \dots, n\}$ appears in exactly one cycle. Moreover, (up to the order in which c_1, c_2, \dots, c_m is written) there is a unique way of doing this.

Proof. To construct the list of cycles: Start with 1 and see where the first point goes to. Say it goes to 6. Write $[1 \rightarrow 6$. Then see where 6 goes to, say it goes to 3. Write $[1 \rightarrow 6 \rightarrow 3$ continue this process until we return to 1. Maybe we get $[1 \rightarrow 6 \rightarrow 3 \rightarrow 4 \rightarrow]$. Now take the smallest number from the list $\{1, 2, \dots, n\}$ and repeat the process. Then perhaps we get $[2 \rightarrow 5 \rightarrow 8 \rightarrow]$. Keep doing this until we've written down all the numbers in $\{1, \dots, n\}$. If the symmetry g doesn't move a point, say it doesn't move the 7th point, we will have a cycle of the form $[7 \rightarrow]$. \square

In fact, the transpositions themselves generate \mathbb{S}_n . To see this, observe that we only need to show that each cycle is a combination of transpositions.

Theorem 4. Suppose that g is a cycle of m points. Then g is the combination of $m - 1$ transpositions.

Proof. Suppose that

$$g = [a_1 a_2 a_3 \dots a_m]$$

is a cycle where a_1, \dots, a_m are numbers in $\{1, \dots, n\}$ with no number repeated more than once. Then it is easy to see that:

$$g = [a_1 a_2] \circ [a_2 a_3] \circ [a_3 a_4] \circ \dots \circ [a_{m-1} a_m].$$

\square

Exercise 23. Verify that $[13579] = [13][35][57][79]$.

Exercise 24. How many transpositions are there in \mathbb{S}_n ?

8. INTERLUDE: PLAIN BOB MINIMUS

One of the basic changes in campanology is Plain Bob Minimus. Each column of the following table shows the change Plain Bob Minimus for four bells. In each column a different bell has been colored to make its position in the round easier to track.

S	A	T	B	S	A	T	B	S	A	T	B	S	A	T	B
A	S	B	T	A	S	B	T	A	S	B	T	A	S	B	T
A	B	S	T	A	B	S	T	A	B	S	T	A	B	S	T
B	A	T	S	B	A	T	S	B	A	T	S	B	A	T	S
B	T	A	S	B	T	A	S	B	T	A	S	B	T	A	S
T	B	S	A	T	B	S	A	T	B	S	A	T	B	S	A
T	S	B	A	T	S	B	A	T	S	B	A	T	S	B	A
S	T	A	B	S	T	A	B	S	T	A	B	S	T	A	B
S	T	B	A	S	T	B	A	S	T	B	A	S	T	B	A
T	S	A	B	T	S	A	B	T	S	A	B	T	S	A	B
T	A	S	B	T	A	S	B	T	A	S	B	T	A	S	B
A	T	B	S	A	T	B	S	A	T	B	S	A	T	B	S
A	B	T	S	A	B	T	S	A	B	T	S	A	B	T	S
B	A	S	T	B	A	S	T	B	A	S	T	B	A	S	T
B	S	A	T	B	S	A	T	B	S	A	T	B	S	A	T
S	B	T	A	S	B	T	A	S	B	T	A	S	B	T	A
S	B	A	T	S	B	A	T	S	B	A	T	S	B	A	T
B	S	T	A	B	S	T	A	B	S	T	A	B	S	T	A
B	T	S	A	B	T	S	A	B	T	S	A	B	T	S	A
T	B	A	S	T	B	A	S	T	B	A	S	T	B	A	S
T	A	B	S	T	A	B	S	T	A	B	S	T	A	B	S
A	T	S	B	A	T	S	B	A	T	S	B	A	T	S	B
A	S	T	B	A	S	T	B	A	S	T	B	A	S	T	B
S	A	B	T	S	A	B	T	S	A	B	T	S	A	B	T

In a previous interlude we learned that the plain lead on four bells is the set of all permutations effected by the symmetries in the subgroup

$$H = \{\mathbb{I}, [12][34], [1342], [14], [14][23], [13][24], [1243], [23]\}$$

That subgroup is generated by $\{[12][34], [23]\}$. Notice that the first section of Plain Bob Minimus is simply the plain lead. In fact, each section of Plain Bob Minimus is the plain lead on four bells, just starting from a different round each time. To get between sections, the symmetry $[34]$ is used. All 24 permutations of 4 bells show up in Plain Bob Minimus. Thus,

$$\mathbb{S}_4 = \langle [12][34], [23], [34] \rangle.$$

Given our initial round of “S A T B”, each subsequent round is determined by a permutation that gets us from “S A T B” to the new round. For example, the round “T B S A” corresponds to the permutation $[13][24]$. Here is Plain Bob Minimus written with some permutation labels emphasizing a certain pattern:

I	
$[12][34]$	$= h_1$
$[13][42]$	$= h_2$
$[14]$	$= h_3$
$[14][23]$	$= h_4$
$[13][24]$	$= h_5$
$[1243]$	$= h_6$
$[23]$	$= h_7$
I \circ $[243]$	
$h_1 \circ [243]$	
$h_2 \circ [243]$	
$h_3 \circ [243]$	
$h_4 \circ [243]$	
$h_5 \circ [243]$	
$h_6 \circ [243]$	
$h_7 \circ [243]$	
I \circ $[234]$	
$h_1 \circ [234]$	
$h_2 \circ [234]$	
$h_3 \circ [234]$	
$h_4 \circ [234]$	
$h_5 \circ [234]$	
$h_6 \circ [234]$	
$h_7 \circ [234]$	

Notice that $[234]$ is the inverse of $[243]$. Thus, we can see from this table that

$$\mathbb{S}_4 = \langle h_1, h_7, [234] \rangle$$

Furthermore, we also can see the structure of the sections of Plain Bob Minimus. The first section is just the effect of applying the symmetries in H to the initial round “S A T B”. The second section is the effect of applying symmetries which are a combination of $[243]$ and the symmetries of H to “S A T B”. The third section is the effect of applying symmetries which are a combination of $[234]$ and the symmetries of H to “S A T B”.

9. EVEN AND ODD SYMMETRIES IN \mathbb{S}_n

Recall from the previous section that every symmetry in \mathbb{S}_n can be written as the combination of transpositions in \mathbb{S}_n . There are, however, lots of ways of writing a single symmetry as a combination of transpositions.

For example, consider $[12345]$ in \mathbb{S}_5 . Then

$$\begin{aligned} [12345] &= [12][23][34][45] \\ &= [34][25][15][24] \\ &= [34][13][25][13][15][24] \end{aligned}$$

We see from the example that there may be lots of different ways of writing a symmetry as a combination of transpositions. However, the following is a useful fact:

Theorem 5. A symmetry in \mathbb{S}_n can be written as a combination of either an even number of transpositions or as a combination of an odd number of transpositions, but not both.

The proof relies on the concept of “cycle number”, which we now define. Suppose that g is a symmetry in \mathbb{S}_n . Then g can be written as a combination of cycles. This can be done in such a way that each number from $\{1, 2, \dots, n\}$ appears in one of the cycles and no number appears more than once. The **cycle number** of g is equal to the number of cycles.

For example if $[125]$ is in \mathbb{S}_5 we can write

$$[125] = [125][3][4]$$

so the cycle number of $[125]$ in \mathbb{S}_5 is 3. The cycle number of $[125]$ in \mathbb{S}_8 is 6.

An observation which will be useful later is that, in \mathbb{S}_n , the cycle number of \mathbf{I} is n since

$$\mathbf{I} = [1][2][3] \dots [n].$$

The next lemma (or “helper theorem”) is the key to proving that each symmetry can be written as a combination of an odd number of transpositions or as a combination of an even number of transpositions, but not both.

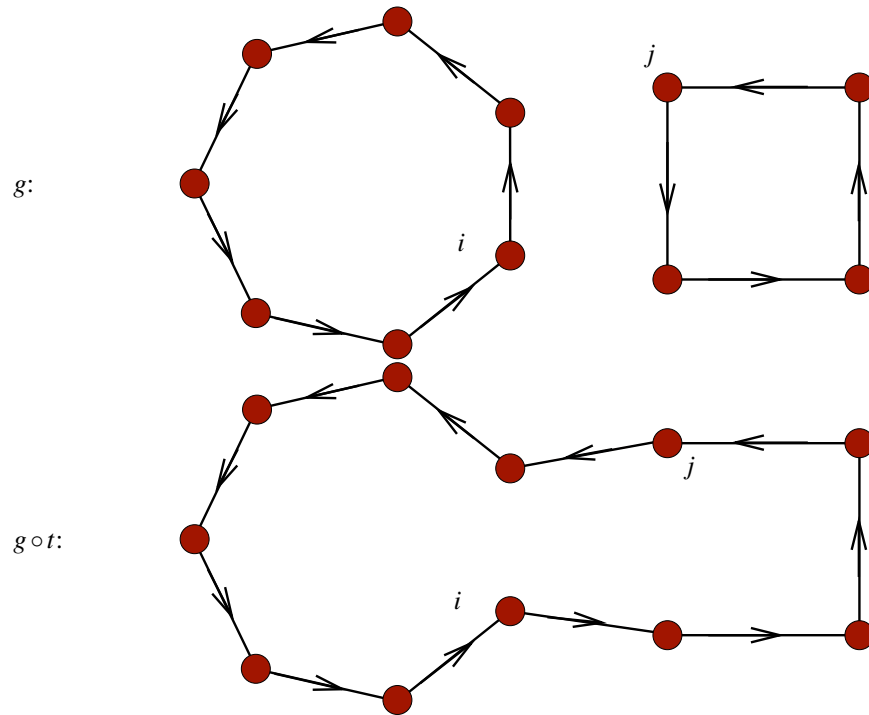
Lemma 6. Suppose that g is a symmetry in \mathbb{S}_n and that t is a transposition in \mathbb{S}_n . Then the cycle number of $g \circ t$ is exactly one more or exactly one less than the cycle number of g .

Proof of Lemma. We simply sketch the idea behind the proof. Assume that the transposition t swaps the point in position i and the point in position j .

Write g as the combination of cycles, so that each number from $\{1, 2, \dots, n\}$ appears in exactly one cycle. Remember that the cycle number of g is equal to the number of cycles.

Case 1: Points i and j are not in the same cycle of g .

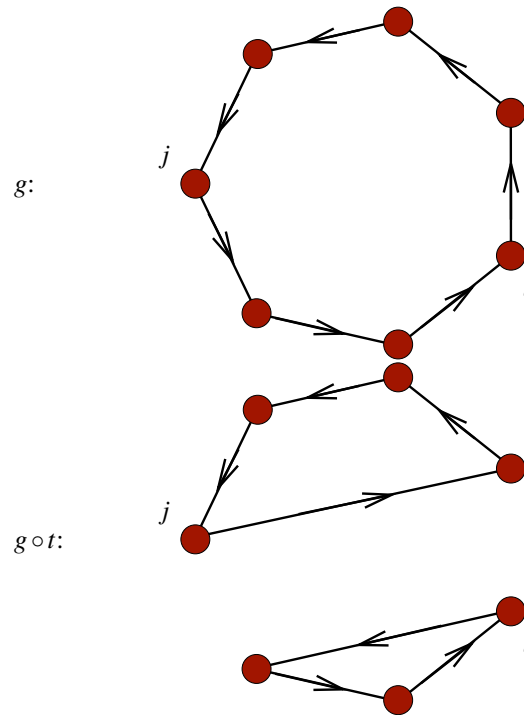
Contemplate this picture:



The cycles not containing points i and j are unaffected by the transposition t . We see that the cycle number of $g \circ t$ is one less than the cycle number of g .

Case 2: Points i and j are on the same cycle.

Contemplate this picture:



The cycles not containing i and j are unaffected by the transposition t . We see that the cycle number of $g \circ t$ is one more than the cycle number of g . \square

We can now prove the theorem that a symmetry g in \mathbb{S}_n can be written as a combination of an odd number of cycles or as a combination of an even number of cycles, but not both.

Proof of Theorem. Suppose that

$$g = t_1 \circ t_2 \circ \dots \circ t_k$$

where each t_i is a transposition. Then,

$$\mathbf{I} = g \circ t_k \circ t_{k-1} \circ \dots \circ t_2 \circ t_1.$$

Each time we apply a transposition to g the cycle number increases by one or decreases by one. The cycle number of \mathbf{I} is n . If you like you may think about a light switch. If the cycle number of g is odd, the light starts off. If the cycle number of g is even, the light starts on. If n (the cycle number of \mathbf{I}) is odd the light ends off. If n is even, the light ends on. For each transposition you see, flick the light switch once.

Thus the following are true:

- If the cycle number of g is odd and if n is odd, then there are an even number of transpositions.
- If the cycle number of g is odd and if n is even, then there are an odd number of transpositions.
- If the cycle number of g is even and if n is odd, then there are an odd number of transpositions.
- If the cycle number of g is even and if n is even, then there are an even number of transpositions.

We have written g as a combination of transpositions. We have shown that whether or not the number of transpositions is even or odd depends only on whether n is even or odd and on whether the cycle number of g is even or odd. \square

If a symmetry in \mathbb{S}_n can be written as a combination of an even number of transpositions, then we call it an **even permutation**. Otherwise it is an **odd permutation**. The set of all even permutations in \mathbb{S}_n is called the **alternating group of n points**. It is denoted \mathbb{A}_n . It turns out that \mathbb{A}_n is a subgroup of \mathbb{S}_n and that exactly half the symmetries of \mathbb{S}_n are in \mathbb{A}_n .

10. INTERLUDE: 15-PUZZLE



“People became infatuated with the puzzle and ludicrous tales are told of shopkeepers who neglected to open their stores; of a distinguished clergyman who stood under a street lamp all through a wintry night trying to recall the way he had performed the feat. The mysterious feature of the puzzle is that no one seems able to recall the sequence of moves whereby they feel sure they succeeded in solving the puzzle. Pilots are said to have wrecked their ships, engineers rush their trains past stations and business generally became demoralized. ... Farmers are known to have deserted their plows and I have taken one of such instances as an illustration of the above sketch”. – Sam Loyd

The 14-15 puzzle was marketed in the late 19th century by Sam Loyd, probably America’s greatest puzzle master of all time. It consisted of 15 squares in a 4×4 grid. There was one empty space (which we will think of as being square 16). A square adjacent to the empty square could be slid into it. The goal was to slide the squares around, so that the numbers appeared in order, like so:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

The version marketed by Loyd was called the 14–15 puzzle. It had an initial configuration of:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Loyd offered a \$1000 prize for the solution of the 14-15 puzzle. The prize was never collected, for the simple reason that it is impossible to solve!

Let's see why Loyd's puzzle is unsolvable. Let's say that a configuration of the puzzle is **valid** if there is a sequence of legal moves which converts that configuration into the solved configuration. If there is no such sequence of moves, the configuration is **invalid**. We will show that Loyd's starting position is invalid.

Each possible initial configuration of the puzzle is determined by a symmetry in \mathbb{S}_{16} which converts the solved configuration into the initial configuration. If g is a symmetry in \mathbb{S}_{16} producing a certain configuration, then if we perform a legal move on the configuration, there is a transposition t in \mathbb{S}_{16} so that $t \circ g$ is the symmetry corresponding to the new configuration.

To show that Loyd's puzzle cannot be solved, we complete the following four steps:

- Create a function F which takes in a symmetry in \mathbb{S}_{16} and spits out either $+1$ or -1 .
- Show that if a legal move is applied to a configuration, the value of F is unchanged.
- Show that F applied to the solved configuration is $+1$
- Show that F applied to Loyd's initial configuration is -1 .

Step 1: Create the function F .

F will be made up of two pieces: ε and δ .

Suppose that g is the symmetry in \mathbb{S}_{16} which produces the given configuration from the solved configuration. Define $\varepsilon(g) = +1$ if g is an even permutation, and define $\varepsilon(g) = -1$ if g is an odd permutation.

Suppose that in the initial position, square 16 is $x(g)$ squares to the left, and $y(g)$ squares up from square 16 in the solved position. Define $\delta(g)$ to be $+1$ if $x + y$ is even and define it to be -1 if $x + y$ is odd.

Define $F(g) = \varepsilon(g)\delta(g)$.

Exercise 25. For this initial position g , find $F(g)$.

1	4	2	3
8	5	6	7
9		11	12
13	15	14	10

Step 2: Show that F is unchanged under legal moves.

Suppose that a symmetry g in \mathbb{S}_{16} produces the initial configuration and that we apply a legal move to produce a new configuration. Then there is a transposition t in \mathbb{S}_{16} so that the symmetry $t \circ g$ produces the new configuration from the solved configuration. We wish to show that $F(g) = F(t \circ g)$.

If g is an even permutation, then $t \circ g$ is an odd permutation. If g is an odd permutation, then $t \circ g$ is an even permutation. Thus, $\varepsilon(g)$ has the opposite sign as $\varepsilon(t \circ g)$. That is, $\varepsilon(t \circ g) = -\varepsilon(g)$.

In a legal move, square 16 is moved up, down, left, or right one square. That is, either x or y (but not both) is increased or decreased by 1. Thus, if $x(g) + y(g)$ is even, then $x(t \circ g) + y(t \circ g)$ is odd. If $x(g) + y(g)$ is odd, then $x(t \circ g) + y(t \circ g)$ is even. That is, $\delta(t \circ g) = -\delta(g)$.

We conclude that

$$F(t \circ g) = (-\varepsilon(g))(-\delta(g)) = F(g).$$

Step 3: Show that F applied to the solved configuration is 1.

In this case, we have $\varepsilon(\mathbf{I}) = 1$ and $\delta(\mathbf{I}) = +1$, since $x(\mathbf{I}) + y(\mathbf{I}) = 0 + 0 = 0$.

Step 4: Show that F applied to Loyd's configuration is -1 .

Loyd's configuration is produced from the solved configuration by the symmetry $g = [14\ 15]$. This symmetry has $\varepsilon(g) = -1$ and $\delta(g) = 1$ since $x(g) + y(g) = 0$.

Exercise 26. Suppose that the initial configuration of the puzzle is produced from the solved configuration by an odd permutation of the 15 tiles (leaving the empty spot in the lower right corner). Show that this initial configuration is invalid.

It turns out that any configuration g of the puzzle for which $F(g) = 1$ is a configuration which can be converted into the solved configuration by legal moves. That is, the function F can tell us precisely whether or not a given configuration of the puzzle can be solved. We have shown that if $F(g) = -1$, then the puzzle cannot be solved. The proof that if $F(g) = 1$ then the puzzle can be solved is not much more difficult. It centers on showing that all 3-cycles of \mathbb{S}_{15} are contained in the subgroup of \mathbb{S}_{16} which leaves square 16 in the lower right corner and which consists of symmetries which are combinations of legal moves. The fact that 3-cycles generate \mathbb{A}_{15} is then used to show that any configuration which is an even permutation of squares 1 - 15 can be obtained by legal moves.

11. THE ALTERNATING GROUPS

The set of all even permutations in \mathbb{S}_n is denoted by \mathbb{A}_n .

Theorem 7. \mathbb{A}_n is a subgroup of \mathbb{S}_n and it has half the number of symmetries as \mathbb{S}_n . (That is, it contains $n!/2$ symmetries.)

Proof. Notice that $\mathbf{I} = [12][12]$, so that \mathbf{I} is a symmetry in \mathbb{A}_n . Suppose that g is a symmetry in \mathbb{A}_n so that

$$g = t_1 \circ t_2 \circ \dots \circ t_m$$

where each t_i is a transposition and m is an even number. Then,

$$g^{-1} = t_m^{-1} \circ \dots \circ t_2^{-1} \circ t_1^{-1} = t_m \circ \dots \circ t_2 \circ t_1.$$

This implies that g^{-1} is in \mathbb{A}_n . Finally suppose that

$$\begin{aligned} g &= t_1 \circ t_2 \circ \dots \circ t_m \\ h &= s_1 \circ s_2 \circ \dots \circ s_k \end{aligned}$$

are in \mathbb{A}_n with each t_i and s_j a transposition and m and k even. Then,

$$g \circ h = t_1 \circ t_2 \circ \dots \circ t_m \circ s_1 \circ s_2 \circ \dots \circ s_k.$$

Notice that we have written $g \circ h$ as a combination of $m + k$ transpositions. Since m and k are both even, $m + k$ is even. Consequently, $g \circ h$ is in \mathbb{A}_n . We conclude that \mathbb{A}_n is a subgroup of \mathbb{S}_n .

To see that \mathbb{A}_n has half the symmetries of \mathbb{S}_n , consider the function $f: \mathbb{S}_n \rightarrow \mathbb{S}_n$ given by:

$$f(g) = [12] \circ g.$$

Notice that f takes even permutations to odd permutations and odd permutations to even permutations. Suppose that g and h are permutations in \mathbb{S}_n such that

$$f(g) = f(h).$$

Then,

$$\begin{aligned} f(g) &= f(h) \\ ([12] \circ g) &= [12] \circ h \\ ([12] \circ ([12] \circ g)) &= ([12] \circ ([12] \circ h)) \\ ([12] \circ [12]) \circ g &= ([12] \circ [12]) \circ h \\ g &= h. \end{aligned}$$

We conclude that f takes different symmetries to different symmetries. Since after applying f every even permutation becomes an odd permutation, the number of even permutations is less than or equal to the number of odd permutations. Also, since after applying f every odd permutation becomes an even permutation, the number of odd permutations is less than

or equal to the number of even permutations. Hence, the number of even permutations is the same as the number of odd permutations. Since every symmetry in \mathbb{S}_n is either an even permutation or an odd permutation and since there are the same number of each, the number of symmetries in \mathbb{A}_n is half the number of symmetries of \mathbb{S}_n . \square

- Exercise 27.** (a) Show that $[123]$ is an even permutation in \mathbb{S}_4 and that $[1234]$ is an odd permutation.
- (b) Consider the subgroup $H = \langle [123], [12][56] \rangle$ in \mathbb{S}_8 . Explain why $[1234]$ is not a symmetry in H . (That is, explain why $[1234]$ cannot be written as a combination of $[123]$ and $[12][56]$ and their inverses.)
- (c) Show that the symmetries $[12][34]$ and $[123]$ generate \mathbb{A}_4 .

12. LAGRANGE'S THEOREM

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

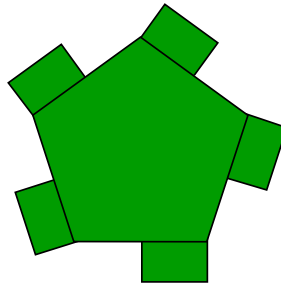
Theorem 8 (Preliminary version of LaGrange's Theorem). Suppose that H is a subgroup of a finite group G . Then the number of symmetries in G is a multiple of the number of symmetries in H .

12.1. **Examples of LaGrange's Theorem in Practice.** You might wish to verify the following examples of the relationship indicated by LaGrange's theorem.

- (a) The number of symmetries in D_n is twice the number of symmetries in C_n .
- (b) The number of symmetries in S_n is twice the number of symmetries in A_n .
- (c) The number of symmetries in S_4 is three times the number of permutations in the plain lead on four bells.
- (d) The number of symmetries in D_4 is four times the number of symmetries in the subgroup $\{\mathbf{I}, H\}$.
- (e) The number of symmetries in D_6 is three times the number of symmetries in the subgroup $\{\mathbf{I}, a, d, R_{180}\}$ where a and d are the reflections of the hexagon about vertical and horizontal lines respectively.

Here are some consequences of LaGrange's theorem:

- Exercise 28.**
- (a) Suppose that H is a subgroup of D_8 . How many symmetries might H contain?
 - (b) Suppose that H is a subgroup of S_4 . How many symmetries might H contain?
 - (c) Suppose that H is a subgroup of a cyclic group D_p where p is a prime number. How many symmetries might H contain?
 - (d) Use the previous problem to show that every possible way of decorating the object below will result in an object with either no non-trivial symmetries or with 5 rotational symmetries (including the trivial symmetry \mathbf{I}).



- (e) Show that \mathbb{S}_5 has no subgroups containing exactly 7, 9, or 17 symmetries.

The remainder of this section will be taken up with the proof of LaGrange's Theorem. Throughout, let G be finite group and let H be a subgroup of G . We wish to show that there is a number k so that

$$\# \text{ of symmetries in } G = k \cdot (\# \text{ of symmetries in } H).$$

The first step is to figure out what the number k could be.

12.2. **Cosets.** For an element g in G , denote by gH the set:

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

That is, gH is the set of all symmetries in G which can be obtained by first performing a symmetry in H and then performing the symmetry g . The set gH is called the **left coset** of H in G containing g .

As you might guess, there are also right cosets of H in G . For g a symmetry in G , the **right coset** of H in G containing g is

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

Exercise 29. Explain why the three sections of the change Plain Bob Minor for 4 bells are exactly the three right cosets of the plain lead in \mathbb{S}_4 .

In general, gH is *not the same* as Hg . If I don't specify whether I am talking about left cosets or right cosets, I will mean *left cosets*.

Example 1. In this example, let $G = D_4$ and let $H = C_4$ the subgroup of rotations.

- (a) Find the coset of C_4 in D_4 containing R_{90} .

We do this by listing the symmetries in C_4 on the right and then combining each of them with our chosen symmetry R_{90} .

$$\begin{array}{r|l|l}
 & C_4 & \\
 \hline
 R_{90} \circ \mathbf{I} & = & R_{90} \\
 R_{90} \circ R_{90} & = & R_{180} \\
 R_{90} \circ R_{180} & = & R_{270} \\
 R_{90} \circ R_{270} & = & \mathbf{I}
 \end{array}$$

Thus the coset of C_4 in D_4 containing R_{90} is

$$R_{90}C_4 = \{R_{90}, R_{180}, R_{270}, \mathbf{I}\}.$$

What matters is the symmetries in the list, not the order in which they are listed. Notice that the coset we just found is exactly C_4 .

Exercise 30. Show that if g is any rotation in D_4 , then $gC_4 = C_4$.

(b) Find the coset of C_4 in D_4 containing the symmetry V .

We do this by listing the symmetries in C_4 on the right and then combining each of them with our chosen symmetry V .

$$\begin{array}{r|l|l}
 & C_4 & \\
 \hline
 V \circ \mathbf{I} & = & V \\
 V \circ R_{90} & = & O \\
 V \circ R_{180} & = & H \\
 V \circ R_{270} & = & D
 \end{array}$$

Thus, the coset of C_4 in D_4 containing V is

$$VC_4 = \{V, O, H, D\}.$$

Exercise 31. Show that if g is any reflection in D_4 , then the coset gC_4 is exactly the same as VC_4 .

We conclude that C_4 has two distinct cosets inside D_4 . One of the cosets is equal to C_4 itself (i.e. consists of the rotations.) and the other coset consists of all the reflections.

The next lemma simplifies the process of finding all the distinct cosets.

Lemma 9. Let G be a finite group and let H be a subgroup. Then any two left cosets of H in G either contain all the same symmetries (i.e. they are equal) or they have all different symmetries.

Proof. Let a and b be symmetries in G and suppose that aH and bH have a symmetry in common. This means that there exist symmetries h_1 and h_2 in H such that

$$a \circ h_1 = b \circ h_2.$$

Notice that this means that $a = b \circ (h_2 \circ h_1^{-1})$ and $b = a \circ (h_1 \circ h_2^{-1})$.

We need to show that they have all their symmetries in common. We do this by showing that every symmetry in aH is also in bH and that every symmetry in bH is also in aH .

Step 1: Show that every symmetry in aH is also in bH .

Suppose that g is a symmetry in aH . This means that there exists a symmetry h_3 in H so that $g = a \circ h_3$. Since $a = b \circ (h_2 \circ h_1^{-1})$, we have

$$g = b \circ (h_2 \circ h_1^{-1}) \circ h_3.$$

By the associative property:

$$g = b \circ (h_2 \circ h_1^{-1} \circ h_3)$$

Since H is a group, $h_2 \circ h_1^{-1} \circ h_3$ is a symmetry in H . Since bH consists of all symmetries which are created by combining a symmetry in H with b , g is in bH . Since g was an arbitrary symmetry in aH , we have shown that every symmetry in aH is also a symmetry in bH .

Step 2: Show that every symmetry in bH is also a symmetry in aH .

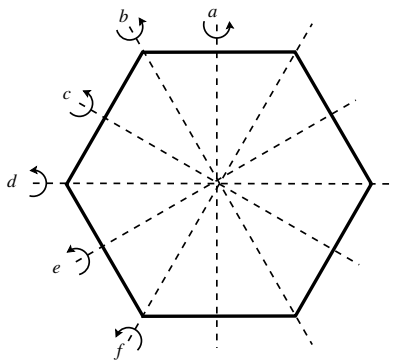
This step is left as an exercise. □

Exercise 32. Complete Step 2 in the proof above.

Example 2. Here are the symmetries of a regular hexagon:

$$D_6 = \{\mathbf{I}, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, a, b, c, d, e, f\}$$

where $\{a, b, c, d, e, f\}$ are the reflections indicated in the diagram:



Let H be the subgroup $\{\mathbf{I}, a, d, R_{180}\}$. Find all the (distinct) left cosets of H in D_6 .

Our strategy is to pick a symmetry in g , calculate the coset gH . Then pick a symmetry not in gH , calculate the coset containing that symmetry and repeat. Once we write down a symmetry in G , as part of a coset calculation we never need to calculate the coset containing that symmetry. This is

because by the lemma above, its coset will just be one of the cosets we've already written down.

We begin by calculating the coset containing \mathbf{I} :

$$\begin{array}{r|l|l} & H & \\ \hline \mathbf{I} \circ \mathbf{I} & = & \mathbf{I} \\ \mathbf{I} \circ a & = & a \\ \mathbf{I} \circ d & = & d \\ \mathbf{I} \circ R_{180} & = & R_{180} \end{array}$$

So one of the cosets of H in D_6 is just H itself.

Now pick a symmetry not in H , say the reflection b :

$$\begin{array}{r|l|l} & H & \\ \hline b \circ \mathbf{I} & = & b \\ b \circ a & = & R_{60} \\ b \circ d & = & R_{240} \\ b \circ R_{180} & = & e \end{array}$$

So one of the cosets of H in D_6 is $\{b, R_{60}, R_{240}, e\}$.

Now pick a symmetry in D_6 that we haven't yet seen. Say, the reflection c :

$$\begin{array}{r|l|l} & H & \\ \hline c \circ \mathbf{I} & = & c \\ c \circ a & = & R_{120} \\ c \circ d & = & R_{300} \\ c \circ R_{180} & = & f \end{array}$$

So another coset of H in D_6 is $\{c, R_{120}, R_{300}, f\}$.

Since every symmetry in D_6 appears in one of the cosets we have written down, we can stop. We conclude that H has three distinct left cosets in D_6 . They are:

$$\begin{aligned} & \{\mathbf{I}, a, d, R_{180}\} \\ & \{b, R_{60}, R_{240}, e\} \\ & \{c, R_{120}, R_{300}, f\} \end{aligned}$$

Lemma 10. Suppose that G is a finite group and that H is a subgroup of G . Then one of the cosets of H in G is H itself.

Proof. The coset of H in G containing \mathbf{I} must be H . □

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 3. The even symmetries inside \mathbb{S}_4 .

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 4. The two cosets of \mathbb{A}_4 inside \mathbb{S}_4 are colored differently.

Example 3. Find all the (left) cosets of \mathbb{A}_4 in \mathbb{S}_4 .

We begin by listing the elements of \mathbb{S}_4 in Table 3. We write each element as the combination of transpositions, to make it easy to tell if an element is in \mathbb{A}_4 or not. The symmetries in \mathbb{A}_4 have been shaded red. They also form one of our cosets.

Let's pick a symmetry in \mathbb{S}_4 which is not in \mathbb{A}_4 . Let's pick $[12]$. Now calculate $[12]\mathbb{A}_4$ by combining each symmetry in \mathbb{A}_4 with $[12]$:

$$\begin{aligned}
 [12] \circ \mathbf{I} &= [12] \\
 [12] \circ [12][23] &= [23] \\
 [12] \circ [13][32] &= [13] \\
 [12] \circ [12][24] &= [24] \\
 [12] \circ [14][42] &= [14] \\
 [12] \circ [13][34] &= [1342] \\
 [12] \circ [14][43] &= [1432] \\
 [12] \circ [23][34] &= [1234] \\
 [12] \circ [24][43] &= [1243] \\
 [12] \circ [12][34] &= [34] \\
 [12] \circ [13][24] &= [1324] \\
 [12] \circ [14][23] &= [1423]
 \end{aligned}$$

Notice, that between \mathbb{A}_4 and $[12]\mathbb{A}_4$ we have gotten all the symmetries in \mathbb{S}_4 . Thus, there are two cosets of \mathbb{A}_4 in \mathbb{S}_4 . Notice that both cosets contain exactly the same number of symmetries. If we color the symmetries of \mathbb{S}_4 corresponding to the cosets of \mathbb{A}_4 we have Table 4.

The previous examples suggest the following theorem.

Theorem 11 (LaGrange's Theorem for real). Let G be a finite group of symmetries and suppose that H is a subgroup. Then:

$$\# \text{ of symmetries in } G = (\# \text{ of left cosets of } H \text{ in } G) \cdot (\# \text{ of symmetries in } H).$$

The proof of LaGrange's theorem. LaGrange's theorem follows from the following three claims. The first two were proven earlier as lemmas.

- (1) If two left cosets have any symmetry in common, they are the same coset. (Left cosets partition G .)
- (2) H is the coset of H in G containing \mathbf{I} .
- (3) All left cosets have the same number of elements as H .

Claim (1) means that we can sort the symmetries in G into boxes corresponding to the left cosets of H in G .

g_1H	g_2H	g_3H	g_4H
g_5H	g_6H	g_7H	g_8H
g_9H	$g_{10}H$	$g_{11}H$	$g_{12}H$

In this example, there are 12 (different) left cosets of H in G . Each symmetry in H is in one of the boxes representing one of the cosets. No symmetry is in more than one coset.

Claim (2) means that one of the left cosets of H in G is exactly H .

H	g_2H	g_3H	g_4H
g_5H	g_6H	g_7H	g_8H
g_9H	$g_{10}H$	$g_{11}H$	$g_{12}H$

In this example, there are 12 (different) left cosets of H in G . Each symmetry in H is in one of the boxes representing one of the cosets. No symmetry is in more than one coset. H is one of the cosets.

Claim (3) means that all the cosets contain the same number of symmetries. This means that all the cosets contain the same number of symmetries as H .

# H symmetries	# H symmetries	# H symmetries	# H symmetries
# H symmetries	# H symmetries	# H symmetries	# H symmetries
# H symmetries	# H symmetries	# H symmetries	# H symmetries

In this example, there are 12 cosets of H in G . Each coset has the same number of symmetries as H . Since every symmetry in G is in a coset and since no two different cosets have a symmetry in common, this means that G has 12 times as many symmetries as does H .

Here is a proof of Claim 3:

Proof of Claim 3. Let gH be a coset of H in G . We match every symmetry in gH with a symmetry in H and every symmetry in H with a symmetry in gH so that different symmetries are matched to different symmetries. Here is the matching: Let $g \circ h$ be a symmetry in gH where h is some symmetry in H . Match $g \circ h$ with h . \square

In addition to proving LaGrange's theorem, cosets are useful when we are looking for ways to generate a group. Here is an updated proof that D_n is generated by a rotation and a reflection.

Theorem 12. D_n can be generated by a rotation and a reflection.

Proof. The subgroup C_n consists of all the rotations in D_n . It is generated by the smallest rotation, call it R_θ . By LaGrange's theorem, C_n has two cosets in D_n . One of the cosets is C_n . Everything in C_n can be obtained by combining R_θ with itself. The other coset contains all the reflections in D_n . Let a be one of the reflections, the coset is then aC_n . By definition, aC_n consists of combinations of a with symmetries in C_n . Each symmetry in C_n is a combination of R_θ , so every symmetry in D_n is a combination of a with R_θ (some number of times). \square

Exercise 33. (a) Show that S_n can be generated by the set of all even permutations plus any odd permutation.

(b) Suppose that G is a finite group and that H is a subgroup of G with k left cosets. Let h_1, \dots, h_n be a generating set for H and let x_2, \dots, x_k

be a choice of symmetry from each coset of H in G other than H .
Show that $G = \langle h_1, \dots, h_n, x_1, \dots, x_n \rangle$.

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.

13. THE ORBIT-STABILIZER THEOREM

Definition 2. 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 $\text{orb}_G(x)$.

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, $\text{orb}_{D_4}(x)$ is the set of vertices of the square.

The group $G = \{\mathbf{I}, R_{180}\}$ is a subgroup of D_4 . The set $\text{orb}_G(x)$ consists of the vertex x and the vertex directly opposite it on the square.

Definition 3. 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 $\text{stab}_G(x)$.

Let x be the upper left vertex of the square, then $\text{stab}_{D_4}(x) = \{\mathbf{I}, D\}$ 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 $\text{stab}_{D_4}(x) = D_4$, since no element of D_4 moves the center of the square.

Exercise 34. Prove that $\text{stab}_G(x)$ is a subgroup of G for any given point x .

Theorem 13. (Orbit-Stabilizer) Suppose that G is a group of symmetries of an object X . For any point x in X ,

$$\begin{aligned} & \# \text{ of symmetries in } G = \\ & (\# \text{ of points in } \text{orb}_G(x)) \cdot (\# \text{ of symmetries in } \text{stab}_G(x)) \end{aligned}$$

Proof. We simply need to show that $(\# \text{ of points in } \text{orb}_G(x))$ is equal to the number of left cosets of $\text{stab}_G(x)$ in G . Let gH be a coset of $H = \text{stab}_G(x)$ in G . Match the coset gH with the point $g(x)$ in $\text{orb}_G(x)$. Notice that if g and g' are both in gH then we have $g' = g \circ h$ for some h in $\text{stab}_G(x)$. 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 every 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 $\text{stab}_G(x)$. It turns out that this implies that $gH = g'H$.

Thus, each coset of H is matched with one point in $\text{orb}_G(x)$ and different cosets are matched with different points. Since each point of the orbit of x is matched with some coset, the size of $\text{orb}_G(x)$ is equal to the number of cosets. \square