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 $n \geq 2$. $\square$

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 $n \geq 2$:

$$\begin{gathered} [1 \leftrightarrow 2] \\ [2 \leftrightarrow 3] \\ [3 \leftrightarrow 4] \\ \vdots \\ [n-1 \leftrightarrow n]. \end{gathered}$$

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:

$C_n \qquad \langle\ s \ \mid\ s^n = \mathbf{I}\ \rangle$

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

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

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:

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

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.

S_1

S_2

$S_2 \circ S_1$	$\mathbf{I}$	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 $\mathbb{S}_4$.

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 **??**.

Let's find all the cosets of A_4 in $\mathbb{S}_4$. We begin by listing the elements of $\mathbb{S}_{\not\trianglerighteq}$. 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

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

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