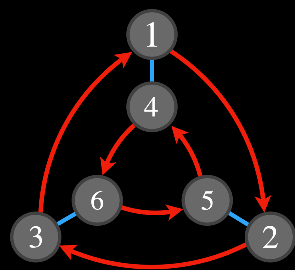
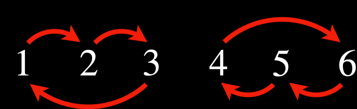
Cayley's Theorem states that any group can be represented as a group of permutations, or rearrangements of its elements.

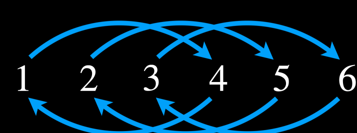
We start with this diagram for the symmetric group S_3. The nodes are numbered 1 through 6 in order to make it easy to talk about permutations.



The red arrows move from 1 to 2, 2 to 3, 3 to 1, 4 to 6, 6 to 5 and 5 to 4. The blue arrows interchange the node pairs. And yes, even though they don't have arrow heads we will still call them arrows.

The permutations representing what is happening in the diagram look like this, and show the exact same thing that is happening in the diagram.





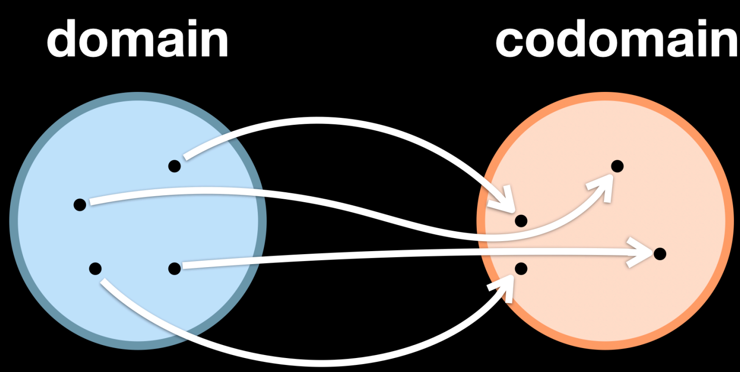
This makes the entire group consist of 2 permutations.

One acts like a rotation. This permutation cycles the elements, behaving like a 120-degree rotation of an equilateral triangle. We'll call that a red permutation. The other acts like a flip. This permutation swaps elements acting like a mirror image. This one is a blue permutation.

When you consider all possible combinations (or products) of the red and blue permutations, you generate a **group**.

The group generated by the red and blue permutations has the same order (which are six elements) and the same structural relationships among its elements as S_3.

This means there's a one-to-one correspondence between the two. One-to-one, or injective, relationship means each element in the first set (domain) is paired with a unique element in the second set (codomain).



Because there's a one-to-one correspondence the group generated by the red and blue permutations is **isomorphic** to S_3.

The diagram of S_3 which we drew earlier represents right multiplication.

The term "right multiplication" is used when the element b is multiplied to the right side of a, denoted as a×b.

The S_3 diagram shows us all the possible ways to rearrange, or permeate, the objects, but it's less obvious than it would be if we used multiplication tables.

Let's take V_4 as an example, with elements labeled 1 2 3 4 for simplicity.

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

1 is the identity element for any ***a***. Each element is its own inverse.

$$1 \cdot a = a \cdot 1 = a$$

$$a \cdot a = 1$$

Rows represent the first element in the multiplication (or the left factor). Columns represent the second element in the multiplication (or the right factor).

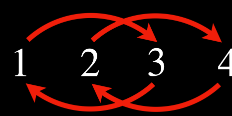
When you look at a specific column in the multiplication table, you're seeing the results of right
multiplication by the element at the top of that column.

For example, the column labeled 3 shows the results of $a \cdot 3$ for each element ***a*** in the group.

If we analyze each case of column 3, we notice that the column is simply a reordering of the numbers 1 through 4, a permutation.

$$1 \cdot 3 = 3$$
$$2 \cdot 3 = 4$$
$$3 \cdot 3 = 1$$
$$4 \cdot 3 = 2$$

The right multiplication by "3" effectively permutes the elements of the group.



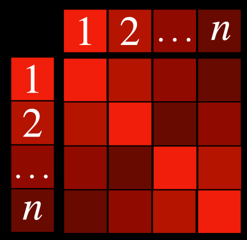
From a multiplication table, we can create a permutation for each element of the group. And vice versa, out of the permutations, we can make a multiplication table. They both have to behave in the same way, and are therefore isomorphic.

And this is **Cayley's Theorem**: every group is isomorphic to a collection of permutations.

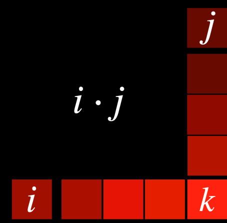
In order to prove that, say we have a group ***G*** with ***n*** elements.

$$G = \{1 \ldots n\}$$

The element labeled 1 is the identity element of the group.

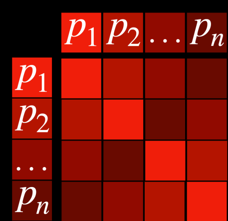


Each cell at the intersection of row *i* and column *j* contains the product *i*×*j*, according to the group operation. Each element is labeled *k* .

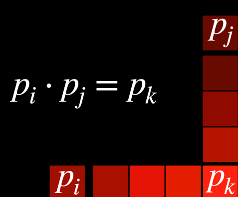


Thus, we have that $i \cdot j = k$.

Now, we can create another table.



We have a similar thing happen, with row p_i and column p_j, the intersection of which is p_k.



The equation $p_i \cdot p_j = p_k$ means that composing permutation p_i with p_j results in permutation p_k.

Now, consider how the permutations treat the identity element from the original group.

If we take p_k and apply it to *1*, it will be the same thing as saying $k \cdot 1$. And of course, anything times the identity element results in the element itself, so *k*.

The same thing is true if we take $p_i \cdot p_j$ and apply it to 1 $p_i \cdot p_j(1)$, which is the exact same thing as multiplying 1 by i and then j: $1 \cdot i \cdot j$.

Since we saw that $p_i \cdot p_j = p_k$, it means that $p_k(1)$ and $p_i \cdot p_j(1)$ will lead us to the same answer. Since $p_i \cdot p_j$ is $i \cdot j$ and $p_k(1)$ is *k*, we have $i \cdot j = k$.

So, equations like $p_i \cdot p_j = p_k$ from the table of permutations we made, is a faithful representation of the original table *i* · *j* = *k*.

We provide a specific example, with elements 1 2 3 4, 1 being the identity.

We define each permutation as this:

$$p_1(g) = 1 \cdot g = g$$
$$p_2(g) = 2 \cdot g$$
$$p_3(g) = 3 \cdot g$$
$$p_3(g) = 3 \cdot g$$
$$p_4(g) = 4 \cdot g$$

Since $p_1(g) = 1 \cdot g = g$ it maps every element to itself

$$p_1(1) = 1$$
$$p_1(2) = 2$$
$$p_1(3) = 3$$
$$p_1(4) = 4$$

The same can be done with p_3 and p_4 for example:

$p_3(g) = 3 \cdot g$	$p_4(g) = 4 \cdot g$
$p_3(1) = 3 \cdot 1 = 3$	$p_4(1) = 4 \cdot 1 = 4$
$p_3(2) = 3 \cdot 2 = 4$	$p_4(2) = 4 \cdot 2 = 3$
$p_3(3) = 3 \cdot 3 = 1$	$p_4(3) = 4 \cdot 3 = 2$
$p_3(3) = 3 \cdot 4 = 2$	$p_4(4) = 4 \cdot 4 = 1$

<u>Comment</u>: Please, if you find this document useful, let us know. Or if you found typos and things to improve, let us know as well. Your feedback is very important to us, since we are working hard every single day to deliver the best material possible. For contacting us: dibeos.contact@gmail.com