

## Lesson 4

### SYMMETRIC GROUPS

So far we've talked about two main classes of groups – cyclic groups which can be generated by a single element, and dihedral groups which arise from the rotational and mirror symmetry of regular polygons. Now we want to learn about a third class of groups, the symmetric groups.

The symmetric group  $S_n$  is essentially the group of all permutations that can be made of a set of  $n$  objects. There are a couple of things, though, that we should realize at the start. First, this is yet another example of a group acting on a set. Our underlying set  $X$  is a set containing  $n$  objects, and our group  $S_n$  is the group of all permutations we can make of those  $n$  objects. For example, if  $X = \{a, b, c\}$ , then the group  $S_3$  represents the number of permutations we can make of these three letters. In this case, if  $(a, b, c) \in S_3$ , then we'll interpret that permutation as meaning the letter  $a$  becomes  $b$ , the letter  $b$  changes to  $c$ , and the letter  $c$  becomes  $a$ . This permutation would, thus, change  $abc$  to  $bca$ .

A question we want to ask now, however, is how many elements are in a group like  $S_n$ ? Fortunately, this is easy to answer. Just consider  $S_3$  acting on  $X = \{a, b, c\}$ . If we want to count up how many different permutations there are of the three letters  $a$ ,  $b$ , and  $c$ , then we just need to think about how we would construct a single permutation. To do this we need to pick a first letter and then a second letter and then the third letter. However, when we start, we have 3 choices for the first letter, and then only 2 choices left for the second letter, and then just 1 choice for the third letter. Thus, the number of distinct permutations we can make from these three letters is  $3 \cdot 2 \cdot 1 = 6$ . Furthermore, we can easily list all six permutations.

*abc acb bac bca cab cba*

Additionally, we have a special notation for a product like  $3 \cdot 2 \cdot 1$ . We call it “3 factorial,” and we write it as  $3! = 3 \cdot 2 \cdot 1$ . You might recall that  $D_3$ , the group of rotational and mirror symmetries of an equilateral triangle, also contains six elements. Since we can think of the rotations and reflections in  $D_3$  as creating permutations of the three vertices and since the number of permutations in  $D_3$  is the same as the total number of possible permutations of three objects, it must follow that  $D_3$  is isomorphic to  $S_3$ . Thus,  $D_3$  and  $S_3$  are essentially the same group expressed through different notations, and in mathematics we denote the fact that they are isomorphic by writing  $D_3 \cong S_3$ .

$$D_3 \cong S_3 = \{(), (1, 2, 3), (1, 3, 2), (1, 2), (2, 3), (1, 3)\}$$

## Lesson 4

Since  $D_3 \cong S_3$ , an obvious question to ask is are symmetric groups always basically the same as dihedral groups? Well, the answer is no, and all we have to do to see that is to determine the size of  $S_4$ , the group of permutations of 4 objects. Let's let our set of objects be  $X = \{1, 2, 3, 4\}$ , and once again let's think about how many permutations we can make of these four objects. If we are constructing a single permutation, then we have 4 choices for the first number, 3 choices for the next one, 2 choices for the third number, and only 1 choice left for the last number. Hence, the number of permutations we can make of four objects is  $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ , and, thus,  $|S_4| = 24$ . Since  $|D_4| = 8$ , it should be clear that  $D_4$  is not isomorphic to  $S_4$ . However, since the elements of both groups represent permutations of four objects, we can consider  $D_4$  to be a subgroup of  $S_4$ . And more generally, we always have that  $|S_n| = n!$ , and  $D_n$  is always a subgroup of  $S_n$ .

Now let's examine something rather interesting. First, consider these three permutations -  $(1, 2, 3)$ ,  $(1, 4)$ , and  $(5, 6)$ . The latter two permutations,  $(1, 4)$ , and  $(5, 6)$ , are called transpositions since each one switches only two elements. We also say that those two particular permutations are disjoint since they move entirely different elements, and when two permutations are disjoint, they commute with one another. In other words,  $(1, 4)(5, 6) = (5, 6)(1, 4)$ . On the other hand,  $(1, 2, 3)$  and  $(1, 4)$  are not disjoint and they do not commute with one another since when we multiply left to right,  $(1, 2, 3)(1, 4) = (1, 2, 3, 4)$ , but  $(1, 4)(1, 2, 3) = (1, 4, 2, 3)$ .

Now for the good part. Every permutation can be written as a product of transpositions, and there's an easy way to do it. We'll illustrate with the permutation  $(1, 2, 3)$  from  $S_3$ . All you have to do is write  $(1, 2, 3) = (1, 2)(1, 3)$ . And now there are two things to notice. First, the transpositions on the right are not disjoint, and second, we have an even number of transpositions. In general, we'll call a permutation an even permutation if it can be written as the product of an even number of transpositions, and we'll call a permutation an odd permutation if it can be written as an odd number of transpositions using the method indicated above. The identity,  $( )$ , is somewhat of a special case, and we'll simply define it as also being an even permutation. By the way, there exists a theorem that says that if you can write a permutation as a product of transpositions in more than one way, then all those various ways will contain either an even number of transpositions or an odd number of transpositions. And now what is quite remarkable is that the set of all even permutations in  $S_n$  forms a subgroup of  $S_n$  that we call the alternating group,  $A_n$ . To verify that this is a subgroup, it suffices to show that the product of two even permutations is even. The reason this is all you need to show is because (1) we get the associative law for free since we're already working within a group, and (2) if your group is finite, then if we pick any even permutation and start multiplying it by itself over and over again, you will eventually begin repeating values. In particular, before you repeat your original value, you will get a product that is equal to the identity, and that means that the product before that one is the inverse of your even permutation. And now, it should be obvious that the product of any two even permutations is an even permutation since if you multiply an even number of transpositions by an even number of

## Lesson 4

transpositions, you still have an even number of transpositions. Thus, the set of even transpositions is closed under multiplication, and for any finite group, closure under multiplication is all you need to verify to show that some subset of the group forms a subgroup. Here now are the elements in the alternating group  $A_3$ .

$$A_3 = \{(), (1,2,3) = (1,2)(1,3), (1,3,2) = (1,3)(1,2)\}$$

Notice that this subgroup contains 3 elements, and that is half of the 6 elements in  $S_3$ , and that is no accident. In any symmetric group  $S_n$ , half of the elements will be even permutations and half will be odd. Thus, it is always true that  $\frac{|S_n|}{|A_n|} = 2$ .

And finally, note that in any finite group  $G$  of permutations, the even permutations will always form a subgroup. We can take any subset  $X$  of a group  $G$  and generate a subgroup  $H$  of  $G$  just by constructing all finite products of powers of elements in  $X$ . In this case, if  $X$  is the set of even permutations in  $G$ , then all finite products of even permutations will result in an even permutation, and so  $X$  is already a subgroup of  $G$ , and I call this the *even subgroup of  $G$*  or  $Even(G)$ .

And finally, one important bit of information in closing is that  $D_3 \cong S_3$  is the smallest example one can find of a nonabelian group. In other words,  $|D_3| = |S_3| = 6$ , and any group of smaller order will automatically be abelian!