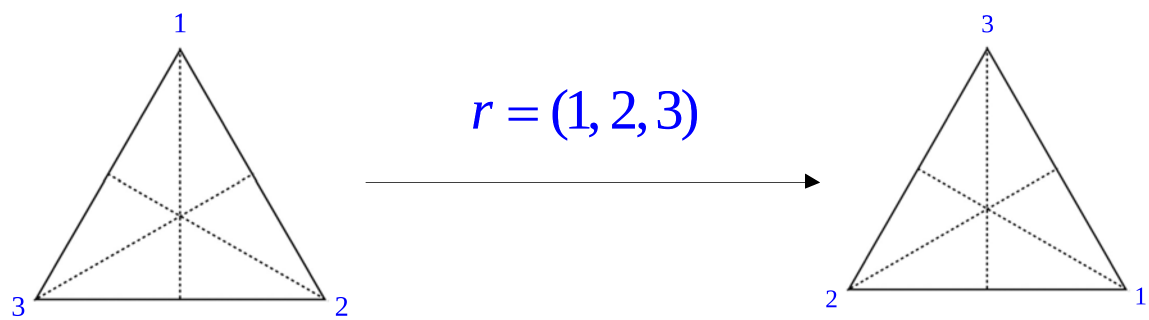
Lesson 1

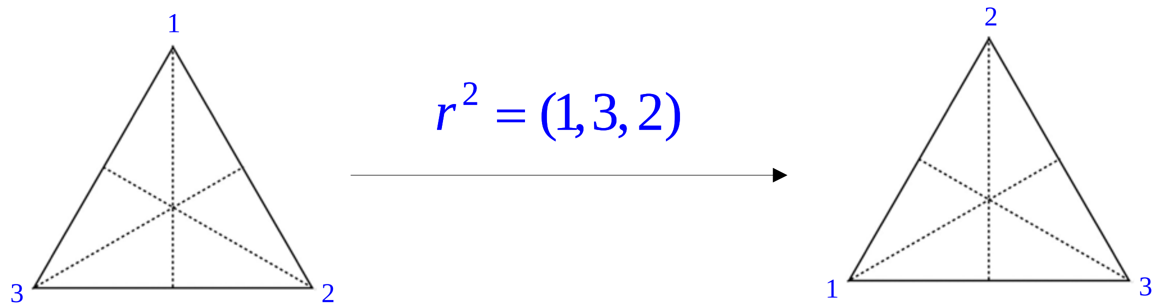
WHAT'S A GROUP?

What is a "group?" Well, that's a question we can begin to answer in several different ways. First and foremost, we can say that groups are composed of cycles and that's why groups are so important, because we find cycles everywhere in life! For example, we have the cycle of the seasons where winter becomes spring which turns into summer and then fall, and then the cycle begins itself anew. We call this a cycle of length four. Similarly, the transition from day to night and back again gives us a cycle of length two since it involves only two states, day and night. And on a personal level, we may describe a typical day as waking up, eating breakfast, going to work, eating lunch, going back to work, coming home, eating dinner, watching TV, going to bed, and then repeating everything again the next day. This gives us a slightly longer cycle of length nine since we have nine distinct states we are cycling between.

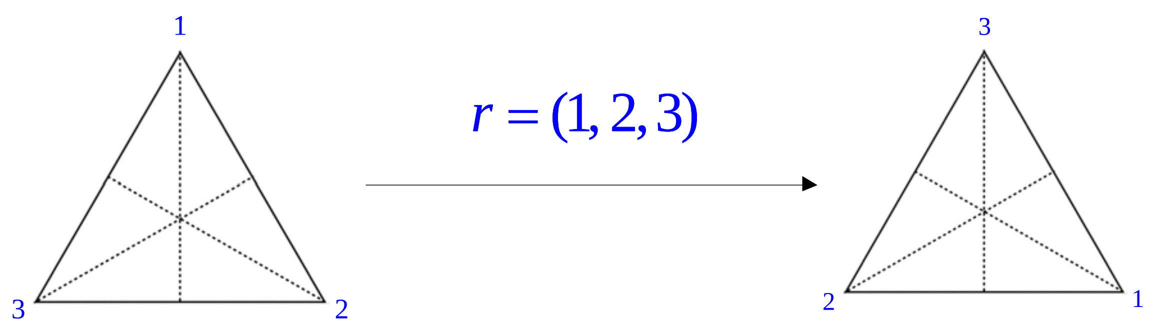
Here's one way to picture a cycle. Suppose we take an equilateral triangle, label the vertices with the numbers 1, 2, & 3, and then we rotate the whole diagram clockwise around the center of the triangle through an angle of $120°$. This will create a cycle where 1 goes to where 2, 2 goes to the place of 3, and 3 goes to 1. A common notation we use for this maneuver is $r=(1,2,3)$. You will also see this frequently written as $r=(1\ 2\ 3)$ without the use of commas as separators, but since software packages that have been developed for group theory use the commas, I will do the same. Additionally, the letter "*r*" stands for "rotation, and we are doing the type of rotation that moves 1 to 2, 2 to 3, and 3 back to 1. Furthermore, notice that we can also write the cycle $(1,2,3)$ as either $(2,3,1)$ or $(3,1,2)$.



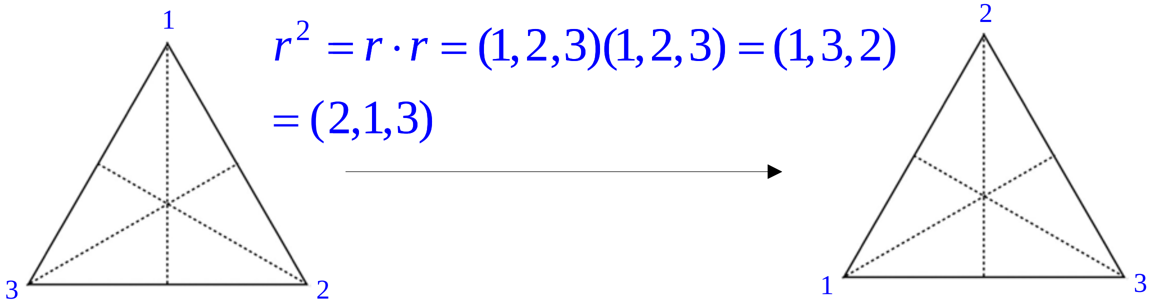
If we do this maneuver twice, then we call it "r-squared" and 1 goes to position 3, 2 to 1, and 3 to 2, and, again, we can write $r^2=(1,3,2)$ as either $(3,2,1)$ or $(2,1,3)$. This is illustrated by the following diagram.



Notice that we can also interpret a cycle such as $r = (1,2,3)$ as a permutation of the numerals 1, 2, & 3. In other words, to say that 1 moves to position 2, 2 moves to position 3, and 3 moves to position 1 is just another way of stating that we are replacing the arrangement 123 with the arrangement 312. Thus, we also think of groups as composed of permutations.



There is an easy way to multiply permutations together. We just simply follow one permutation by another. For example, if $r = (1,2,3)$, then $r^2 = r \cdot r = (1,2,3)(1,2,3)$. Now these days, many people do this multiplication from left to right, but be aware that many other people also do it from right to left, and, in general, that can give a different result. In particular, in many YouTube videos (including those on my webpage) you will see this multiplication done from right to left. Nonetheless, if we're multiplying from left to right, then here's how we do it. In the first permutation, 1 goes to 2, and in the second permutation, 2 goes to 3. Hence, when we follow one by the other, we get that 1 goes to 3, $1 \to 3$. Now we'll continue with 3. The first permutation sends 3 to 1, but the second permutation sends 1 to 2. Hence, when combined, we have that 3 goes to 2, $3 \to 2$. And finally, the first permutation sends 2 to 3, and the second sends 3 to 1. Thus, in combination we have 2 going to 1, $2 \to 1$. In our cycle notation for this permutation we have $r^2 = r \cdot r = (1,2,3)(1,2,3) = (1,3,2)$. Of course, since we are doing $(1,2,3)(1,2,3)$, you will get the same result regardless of whether you multiply from left to right or right to left. However, this is not what happens in general. For example, when we multiply $(1,2,3)(2,3)$ left to right, we get $(1,2,3)(2,3) = (1,3)$, but when we multiply right to left we get $(1,2,3)(2,3) = (1,2)$. Thus, be clear on how the person you are watching is doing their multiplication, and for more examples, see the videos that follow this lesson!



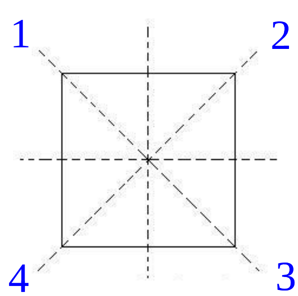
$$r^2 = r \cdot r = (1,2,3)(1,2,3) = (1,3,2)$$
$$= (2,1,3)$$

Notice, again, that the cycle, or permutation, $(1,3,2)$ means the same thing as $(2,1,3)$. The former says 1 goes to 3, 3 to 2, and 2 to 1, while the latter says 2 goes to 1, 1 to 3, and 3 to 2. It's the exact same set of instructions just written in a different order! Also, if we do our rotation three times, then notice that this will take 1 to 1, 2 to 2, and 3 to 3. We call this result the "identity rotation" or more simply, the identity. The rationale for this name is that doing three rotations is equivalent to doing nothing at all, and, thus, none of the numbers change their identity. We can express this in cycle notation as follows. (Remember to multiply left to right!)

$$r^3 = r \cdot r^2 = (1,2,3)(1,3,2) = (1)(2)(3) = ()$$

The expression $(1)(2)(3)$ is the classic way of saying 1 remains 1, 2 remains 2, and 3 remains 3. However, because of software programs that are now available to help with these computations, it is becoming more common to use their notation, ( ), to represent the identity. Also, since $r \cdot r^2 = ()$, we say that r^2 is the inverse of *r*, and we write $r^{-1} = r^2 = (1,3,2)$. Notice that $r^{-1} = (1,3,2) = (2,1,3) = (3,2,1)$, and, in general, if we have a cycle like $r = (1,2,3)$, then we can always form its inverse by writing everything in reverse order such as $r^{-1} = (3,2,1)$.

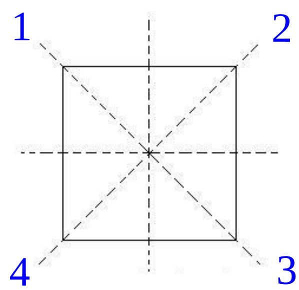
So, at this point, we can say that groups are composed of cycles, and that cycles can also be thought of as permutations. Let's now look at a third way to think of groups which is in terms of symmetry. We'll illustrate the relationship between groups and symmetry by this time using a square.



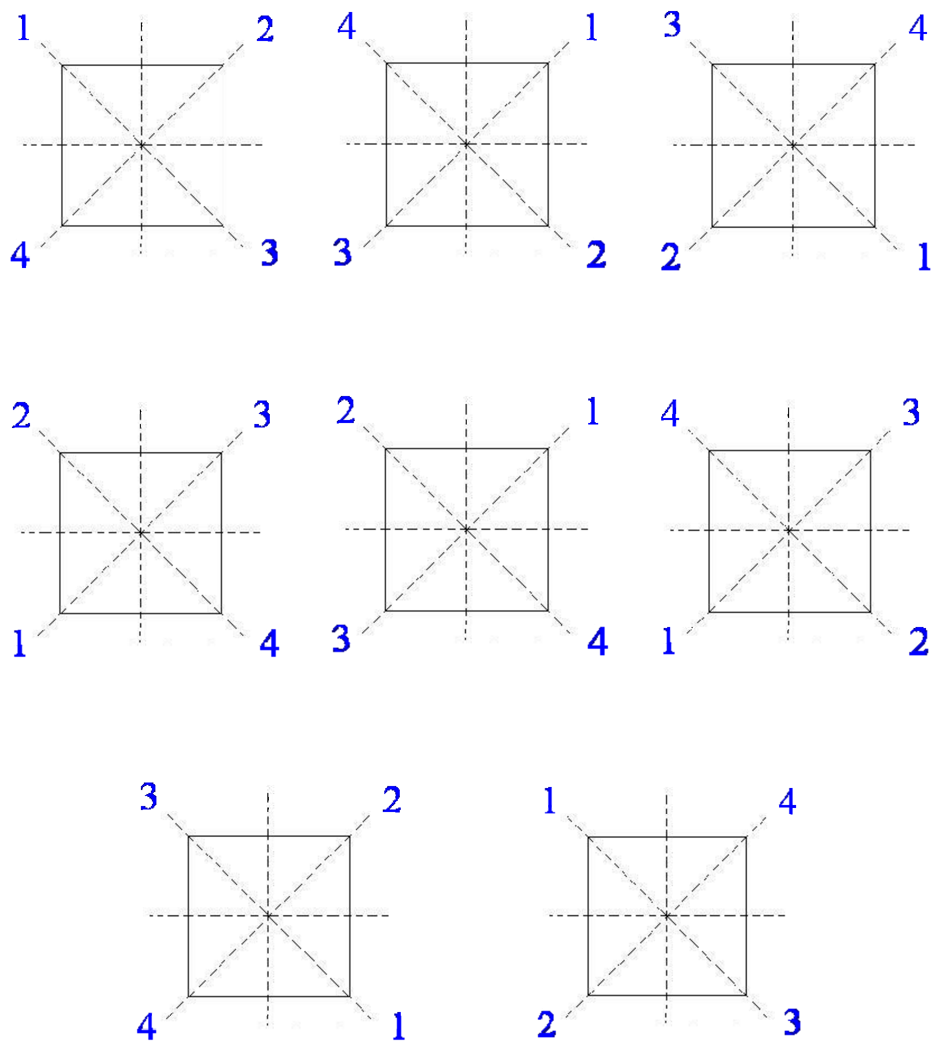
If we ignore the labeling of the vertices, then rotations about the center through successive angles of $90°$ will always leave the square looking exactly the same as it does now, and we can say that the rotation represented by $r = (1,2,3,4)$ generates a cyclic group of four elements or states for the square. This happens because this square possesses symmetry, so let's take a minute to talk about what the word symmetry actually means. Symmetry simply means that there is some kind of pattern present that repeats itself. For example, below you see a picture in which the head of a clown is repeated four times. The symmetry of the image is present in the repetition of this pattern.

We can also imagine moving the clown in position 1 on the left to position 2 in the center, the clown in position 2 to position 3 on the right, the clown in position 3 to position 4, and the clown in position 4 over to position 1. If we do this, then nothing really seems to change in the image. Notice, too, that this cycle is exactly the same kind of cycle of length four that we used to describe our rotations of the square above, i.e. $(1,2,3,4)$. Thus, moving our clown heads around in a cycle is, in an abstract way, the same as rotating our square through multiples of $90°$. That's because both the row of clowns and the square possess a symmetry that can be described in terms of the same cycle of length four, $(1,2,3,4)$.

However, there is one important way in which our square is different from our clown diagram in terms of symmetry. In particular, our square not only exhibits rotational symmetry, it also possesses what we call "mirror symmetry." In other words, there are four axes of symmetry that we may reflect the square about, and the result is once again that when done, our diagram will look unchanged. Thus, look at our square again, but this time focus on the four axes of symmetry that have been drawn inside.



If we use the labels on our vertices, we can follow the result of each rotation or reflection, and then we can discover by trial and error that there are eight possible states our square can wind up in. These are illustrated below.



The first four squares represent the results of doing rotations through multiples of $90°$ in the clockwise direction, and the following four squares represent what happens when you flip the square around each of the indicated axes of symmetry. Furthermore, each of the eight possible states can be represented in cycle notation as indicated below, and remember that ( ) means do nothing at all.

$$(), (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,2)(3,4), (1,4)(2,3), (1,3), (2,4)$$

The full symmetry associated with the clown faces, however, is actually greater than that of the symmetry of the square because if we labele the clowns first, second, third, and fourth, then there are going to be twenty-four arrangements of the clowns in a row that look identical. This is because we have 4 choices regarding which clown to put first, 3 choices for which to put second, 2 choices for the third clown, and only one choice left for the fourth clown. Hence, in all there will be $4 \cdot 3 \cdot 2 \cdot 1 = 24$ possible choices or ways to arrange the clowns, and, consequently, a row of four identical clowns possesses, in this sense, greater symmetry than that of a square.

Well, hopefully from the above you can see that groups are going to arise every time we encounter cycles or permutations or symmetry. There's another way, however, to talk about groups, and that is in terms of algebraic properties. In particular, here is a much more formal mathematical definition of a group.

Definition: A group is a nonempty set of objects *G* with some sort of "multiplication" defined such that the following algebraic properties are present:

1. (closure) If *a* and *b* are elements of *G*, then *ab* (*a* times *b*) is an element of *G*.

2. (associative law) If *a*, *b*, and *c* are elements of *G*, then $(ab)c = a(bc)$.

3. (existence of an identity element) There exists an element *e* in *G* such that if *a* is any element in *G*, the $ea = a = ae$.

4. (existence of inverses) If *a* is any element in *G*, then there exists an element a^{-1} (a-inverse) in *G* such that $aa^{-1} = e = a^{-1}a$.

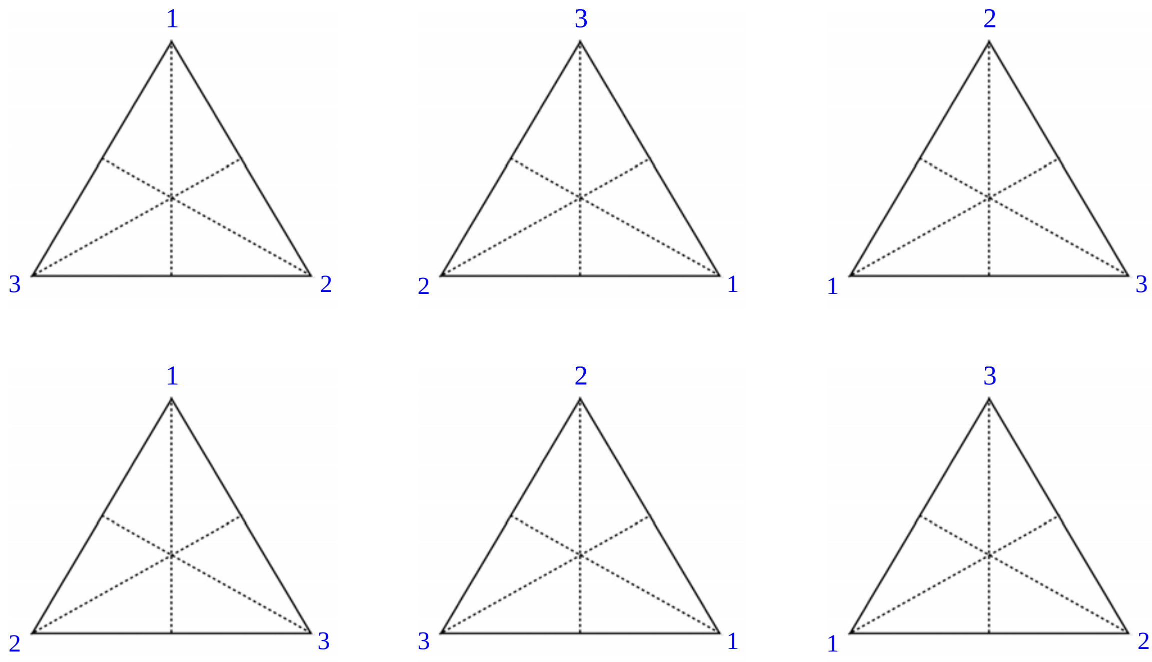
We use the word "group" because, like the word "set," it is a synonym for a collection. However, the difference between a group and a set is that a group is a collection with a multiplication defined on it that obeys the four properties listed above.

In mathematics, groups are so powerful because many different kinds of sets with a defined operation for combining elements wind up conforming to these group properties, and that means that a single theorem about groups can apply to many different situations at once. And to make this a little more concrete, here are some examples of things that are groups.

Example 1: If we take the set of integers, $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and let our operation be ordinary addition of integers, then all of the properties for a group are defined. In this group, the identity element is zero, and we know from experience that, for instance, $0+2=2=2+0$. We also know from experience that the associative property holds. For example, $(1+2)+3=1+(2+3)$. Additionally, the inverse of 2 is just -2 since $2+(-2)=0$.

Example 2: If we let our set be the collection of positive rational numbers (ratios of positive integers) and if we let our operation be the ordinary multiplication of numbers, then this also forms a group. Our identity element this time is the number 1 since, for instance, $1\cdot 2 = 2 = 2\cdot 1$. Also, the inverse of 2 is $2^{-1} = \frac{1}{2}$ since $2\cdot\frac{1}{2} = 1$.

Example 3: If we go back to the symmetries of our equilateral triangle, then recall that there are six possible states that our triangle can be in, and all of these states can be attained via rotations and flips.



Furthermore, we can describe these moves as:

$e = ()$

$r = (1,2,3)$

$r^2 = (1,3,2)$

$f_1 = (2,3)$

$f_2 = (1,2)$

$f_3 = (1,3)$

Additionally, we "multiply" two moves together simply by following one by the other. This set of all possible states along with the indicated multiplication forms a group. Just remember, though, that in our example we are doing all our multiplication in order from left to right. Thus, for example,

$$rf_2 = (1,2,3)(1,2) = (1)(2,3) = (2,3)$$

and,

$$f_2 r = (1,2)(1,2,3) = (1,3)(2) = (1,3)$$

Notice, too, that in this instance, $rf_2 \neq f_2r$. When something like this happens, we say that our group is non-commutative. In other words the commutative property $(ab = ba)$ fails to hold. Another term that is often used in place of "commutative" is "abelian," after the great Norwegian mathematician Niels Henrik Abel whose work helped lead to the development of group theory. Thus, we also say that our group of symmetries for the equilateral triangle is nonabelian. However, if it is true for some particular group *G* that $ab = ba$ for all elements *a* and *b* that are in *G*, then we say that the group *G* is commutative or abelian.

Above we have given three different examples of groups, and as I've already mentioned, the power of group theory lies in the fact that any single theorem we prove about groups will apply equally to each of these three different scenarios. For example, much later on we will prove that every group has only one identity element and we'll prove that every element in a group has only one inverse. Again, these results apply immediately to all possible groups as well as to the three examples above, and, thus, we don't have to mathematically reinvent the wheel each time we move from one group to another.

To recap, the important points in the chapter are that groups can be described in terms of cycles, permutations, symmetries, or algebraic properties. Furthermore, cycles and symmetry are everywhere, and that means that groups are everywhere. You just need to let yourself become aware of all the various cycles in your life and all the symmetries or repetitions of patterns that you encounter on a daily basis in order to understand how intimately groups are intertwined with our lives. So if you haven't thought about this before, begin now!