Lesson 11

INTRODUCTION TO COMMUTATORS

Recall that we defined the conjugate of a by b as $b^{-1}ab$, and we pointed out that if a and b commute, then this results in the statement that $b^{-1}ab = a$. Another way to write this last equation is as $a^{-1}b^{-1}ab = e = \text{the identity}$. We get this last equation simply by multiplying both sides of the former equation on the left by a^{-1}. Hence, if a and b commute with one another, then $a^{-1}b^{-1}ab$ gives us back the identity element. But on the other hand, if a and b don't commute with one another, then $a^{-1}b^{-1}ab$ gives us back some other element c that is different from the identity.

In group theory, we call the expression $a^{-1}b^{-1}ab$ the <u>commutator of *a* and *b*</u>, and we denote it by $[a,b] = a^{-1}b^{-1}ab$. You should be aware, though, that some authors define the commutator of a and b as $[a,b] = aba^{-1}b^{-1}$, and so you should always check the definition that is being used in any book or paper on this topic. However, ultimately it doesn't matter so much which definition we use because we are primarily interested in the subgroup generated by the commutators within a group, and we derive the same subgroup either way. This subgroup is known as either the commutator subgroup or the derived group, and it is essentially a measure of how far a group is from being abelian. For example, if our group G is abelian so that every element commutes with every other element, then the commutator subgroup of G is the identity which in cycle notation we denote by ( ). On the other hand, if G is not abelian, then the size of the commutator subgroup and the ratio of the number of elements in G to the number in the commutator subgroup serve as an indicator of how far the group G is from being abelian.

In puzzles such as Rubik's cube, commutators find additional applications. For example, if we take two permutations a and b and form their commutator $a^{-1}b^{-1}ab$, then even if a and b don't commute with one another, there is a good chance that at least part of the scrambling produced by $a^{-1}b^{-1}$ is undone by following it by ab. And this is exactly what we want to happen when we are trying to solve Rubik's cube. In other words, we want maneuvers that move just a few cubelets and leave the rest right where they are. As an example, if we let $a = (1,2,3)(4,5,6)$ and $b = (6,7,8)(9,10)$, then notice first that the only element that the cycles defining a have in common with those of b is the element 6. In other words, while a and b together create a permutation of the numbers 1 through 10, the number 6 is the only one that both a and b individually move. Thus, there is a good chance that the commutator of a by b will leave the majority of the numbers from 1 to 10 fixed. And when we do the math, this is exactly what happens!

$$a^{-1}b^{-1}ab = (6,5,4)(3,2,1)(10,9)(8,7,6)(1,2,3)(4,5,6)(6,7,8)(9,10) = (4,6,7)$$