CONJUGATES AND COMMUTATORS

If G is a group, and $x, a \in G$, then the element axa^{-1} is called a *conjugate* of x.

Additionally, if H is a subgroup of G, $H \leq G$, then we can define the conjugate of the whole subgroup as $aHa^{-1} = \{axa^{-1} \mid x \in H\}$. And now we claim that if H is a subgroup of G, then so is aHa^{-1}. We'll prove this is the case just for finite groups since that is our primary interest.

Theorem: If G is a finite group, H is a subgroup of G, and $a \in G$, then aHa^{-1} is also a subgroup of G.

Proof: Since G is a finite group, it suffices to show that aHa^{-1} is closed under multiplication. Thus, suppose that $b, c \in aHa^{-1}$. Then there exist x and y in H such that $b = axa^{-1}$ and $c = aya^{-1}$. Hence, $bc = (axa^{-1})(aya^{-1}) = a(xy)a^{-1} \in aHa^{-1}$ since $xy \in H$. Therefore, aHa^{-1} is a subgroup of G. □

We've mentioned previously that some subgroups have the special property that $aHa^{-1} = H$ for all $a \in G$, and when this happens, we say that the subgroup is a normal subgroup and write $H \triangleleft G$. What our theorem above shows is that even if $aHa^{-1} \neq H$, then aHa^{-1} will still be a subgroup of G. Also, if the only normal subgroups of a group G are G and $\{e\}$, then we call G a *simple group*.

Recall now our earlier discussion of Sylow p-subgroups where our theorem said that if p^n is the highest power of a prime p that divides into the order of our group G, then G will have a subgroup of order p^n, a Sylow p-subgroup. We'll now state our second and third Sylow Theorems.

The Second Sylow Theorem: Let G be a finite group, and let p be a prime that divides the order of G. Then all Sylow p-subgroups of G are conjugate to one another.

The Third Sylow Theorem: The number of Sylow p-subgroups of a finite group G is a divisor of the order of G.

Hence, from this it follows that if our Sylow p-subgroup is not normal, then we can find all of the Sylow p-subgroups just by taking conjugates of a single Sylow p-subgroup. If we go back to our multiplication table for S_3, we can easily verify that all the subgroups of order 2 are conjugate.

	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$

For example, we have three subgroups of order 2. Namely, $\left\{ \begin{matrix} (1)(2)(3) \\ (1\quad 2) \end{matrix} \right\}$, $\left\{ \begin{matrix} (1)(2)(3) \\ (1\quad 3) \end{matrix} \right\}$, and $\left\{ \begin{matrix} (1)(2)(3) \\ (2\quad 3) \end{matrix} \right\}$. If we now create some conjugates by multiplying $\left\{ \begin{matrix} (1)(2)(3) \\ (1\quad 2) \end{matrix} \right\}$ by $(1\quad 3)$ and $(2\quad 3)$ [Note that each of these elements is its own inverse], then we obtain:

$(1\quad 3)\left\{ \begin{matrix} (1)(2)(3) \\ (1\quad 2) \end{matrix} \right\}(1\quad 3) = \left\{ \begin{matrix} (1)(2)(3) \\ (2\quad 3) \end{matrix} \right\}$ and $(2\quad 3)\left\{ \begin{matrix} (1)(2)(3) \\ (1\quad 2) \end{matrix} \right\}(2\quad 3) = \left\{ \begin{matrix} (1)(2)(3) \\ (1\quad 3) \end{matrix} \right\}$. Thus, the other two groups are conjugate to the first, and hence, they are all conjugate to each other

The second concept we want to look at is that of a commutator. Basically, if $x, y \in G$, then the *commutator* of x and y is the product $xyx^{-1}y^{-1}$. Notice that if G is an abelian group or if x and y commute with one another, then $xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = e$, the identity element in G. On the other hand, if x and y don't commute with one another, but if their corresponding permutations don't have much in common, then their commutator probably won't result in too many changes. For example, let's suppose that $X = (1\ \ 2\ \ 3)(4\ \ 5\ \ 6)$ and $Y = (6\ \ 7\ \ 8)(9\ \ 10)$. Then $X^{-1} = (6\ \ 5\ \ 4)(3\ \ 2\ \ 1)$ and $Y^{-1} = (10\ \ 9)(8\ \ 7\ \ 6)$. The only item both X and Y permute is 6, and their commutator is,

$$\begin{aligned} XYX^{-1}Y^{-1} &= (1\ \ 2\ \ 3)(4\ \ 5\ \ 6)(6\ \ 7\ \ 8)(9\ \ 10)(6\ \ 5\ \ 4)(3\ \ 2\ \ 1)(10\ \ 9)(8\ \ 7\ \ 6) \\ &= (5\ \ 6\ \ 8) \end{aligned}$$

Thus, even though our permutations don't commute, the commutator still undoes quite a bit of what gets moved around.

$$XYX^{-1}Y^{-1} = (1\quad 2\quad 3)(4\quad 5\quad 6)(6\quad 7\quad 8)(9\quad 10)(6\quad 5\quad 4)(3\quad 2\quad 1)(10\quad 9)(8\quad 7\quad 6)$$
$$= (5\quad 6\quad 8)$$

Now let's suppose that we take all the commutators in our group and form all possible, finite products with them. This will generate a subgroup of G that we call the *commutator subgroup*. Again, if G is abelian, then this commutator subgroup will simply be the identity. However, if G is not abelian, then we can think of the commutator subgroup as measuring how far from being abelian it actually is. Thus, in general, we might say that more abelian the group is, the smaller its commutator subgroup, and the less abelian it is, the larger its commutator subgroup. For S_3, the commutator subgroup is the same as its single Sylow 3-subgroup, $\left\{\begin{matrix} (1)(2)(3) \\ (1\ \ 2\ \ 3) \\ (1\ \ 3\ \ 2) \end{matrix}\right\}$.