Math 476 - Abstract Algebra 1
Day 16 Group Assignment **Name:**________________________________

Lagrange's Theorem

1. Consider the group D_6, the symmetries of a regular hexagon (see page 277 in your textbook).

   (a) What is the order of D_6? List out every divisor of $|D_6|$.

   (b) For each positive divisor d of $|D_6|$, determine whether or not D_6 has a subgroup of order d.

   (c) Does D_6 have any subgroups whose order is **not** a divisor of D_6?

Theorem 26.11 (Lagrange's Theorem): If G is a finite group and H a subgroup of G, then the order of H divides the order of G

Although we will give a formal proof of this theorem, the following activity will help us see why this theorem is true.

2. Let G be a finite group, let $a \in G$, and let H be a subgroup of G. The left coset aH is defined as follows: $aH = \{ah : h \in H\}$. Let $\varphi : aH \to H$ be the function defined via $\varphi(ah) = h$.

   (a) Show that φ is a one to one function.

   (b) Show that φ is an onto function.

   (c) Parts (a) and (b) above show that φ is a bijection. What does this tell us about the number of elements in aH for any $a \in G$?

   (d) Since G is the disjoint union if its cosets (they are generated by an equivalence relation), what does this tell us about how $|H|$ related to $|G|$?

Note: The converse to Lagrange's Theorem is **not** true. Lagrange's theorem ensures that the order of any subgroup divides the order of the group. However, there are cases where the order of G has a divisor d, but there ends up **not** being any subgroups of that order. To see this, consider A_4. As we saw in DGW 14, $|A_4| = 12$. However, if you examine this group closely, you can show that it has no subgroups of order 6. We **do** have the following *partial* converse to Lagrange's Theorem.

Corollary 26.13: Let G is a finite group of order n with $n > 1$. Then there is a prime integer p such that G contains a subgroup of order p.

Proof: Let G be a group of order $n > 1$ with identity e. Since $n > 1$, we can choose an element $a \neq 1$ in G. Let $H = \langle a \rangle$. Since G has finite order, we may apply Lagrange's Theorem to G and H to conclude that $|a| = |H|$ divides n. Then $|a| = d$ for some divisor d of n. Since H is cyclic, by Theorem 23.7, H has exactly one subgroup of order k for each positive divisor k of d. Since every subgroup of H is also a subgroup of G, we can conclude that G has a subgroup of order k for every positive divisor k of d. in particular, if p is a prime that divides d, G has a subgroup of order p. $\square$.

Corollary 26.14: Let G be a finite group of order $|G| = n$ with identity element e. Then $a^n = e$ for every $a \in G$.

3. Give a brief (but clear) explanation for why this Corollary is true.

Definition 26.15: Let G be a group and H a subgroup of G. The **index** of H in G is the number of distinct left cosets of H in G.

We denote the index of H in G as $[G : H]$. When G is a finite group, we have: $[G : H] = \dfrac{|G|}{|H|}$. Please note that we can apply definition 26.15 to infinite groups (but the division property stated here does not make sense). To see this, think about $G = \mathbb{Z}$ and $H = \mathbb{E} = 2\mathbb{Z}$.

4. For each of the following, find $[G : H]$.

   (a) $G = \mathbb{Z}_{16}$ $H = \langle [4] \rangle$

   (b) $G = S_3$, $H = \langle (1, 2) \rangle$

5. Let G be a group of order p, where p is prime, and let H be a subgroup of G. What does Lagrange's Theorem allow us to conclude about possibilities for the order of H? How many subgroups does G have?

6. Let G be a group of order p, where p is prime, and let $a \in G$. What must be true about $|a|$? Explain. Based on this, what conclusions can we draw about G? Must G be Abelian? Must G be cyclic? Explain.