Lecture 10

We will start by proving Lagrange's theorem.

Recall

Theorem [Lagrange's Theorem] Let G be a finite group and $H \leq G$. Then $|H| \,\big|\, |G|$.

Proof Let $a_1H, a_2H, \ldots, a_kH$ denote the distinct left cosets of H in G. Then from the Lemma proved in Lec. 9, we know that the set of all left cosets of H in G partitions G, i.e.,

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH \qquad \text{—— } (*)$$

Property (4) from the Lemma tells us that all the cosets are disjoint and Property (6) tells us that $|a_iH| = |H| \quad \forall \quad 1 \leq i \leq k$

So counting sizes on both sides of $(*)$, we get

$$|G| = |a_1H| + \cdots + |a_kH|$$

$$= \underbrace{|H| + \cdots + |H|}_{k\text{-times}}$$

$$\Rightarrow \quad k = \frac{|G|}{|H|} \quad \Rightarrow \quad |H| \mid |G|$$

$\boxed{/\!/\!/}$

Remark Let's clearly understand what Lagrange's theorem is saying! If you have a group G with $|G| = n$, then any subgroup of G must have order which divides n. So for example if $|G| = 12$, then we can say beforehand that a set H with $|H| = 8$ or $|H| = 10$ cannot be a subgroup as $8 \nmid 12$ and $10 \nmid 12$. However,

the converse of Lagrange's theorem is false.

i.e., there might not be subgroups of G whose order are divisors of $|G|$. e.g. if $|G|=12$, G might or might not have a subgroup of order 6, even though $6 \mid 12$. We'll see an explicit counterexample soon.

Let's see various corollaries of Lagrange's theorem.

__Corollary 1__ If G is a finite group and $H \leq G$ then the index of H in G is $\frac{|G|}{|H|}$, i.e.,
$$|G:H| = \frac{|G|}{|H|}.$$

__Proof__ Recall from previous lecture that $|G:H|$ was defined as the number of distinct left cosets of H in G. From the proof of the theorem we observe $|G:H| = k$ and hence

$$|G:H| = \frac{|G|}{|H|}.$$

$\boxed{///}$

Corollary 2 In a finite group G, $\text{ord}(a) \mid |G|$ $\forall$ $a \in G$.

Proof Recall that $\forall\, a \in G$, $\langle a \rangle$ is a subgroup of $|G|$. Also $\text{ord}(a) = |\langle a \rangle|$ $\Rightarrow$ by Lagranges theorem, $\text{ord}(a) \mid |G|$.

$\boxed{///}$

Corollary 3 Groups of prime order are cyclic, i.e., if $|G| = p$ for a prime p $\Rightarrow$ G is cyclic.

Proof Suppose $|G| = p$. Let $a \in G$, $a \neq e$. Then $|\langle a \rangle| \,\big|\, |G|$ $\Rightarrow$ either $|\langle a \rangle| = 1$ or $|\langle a \rangle| = p$ as p is a prime. But $|\langle a \rangle| \neq 1$ $\Rightarrow$ $|\langle a \rangle| = p$ and hence $G = \langle a \rangle$ and is cyclic.

Corollary 4. Let G be a finite group and let $a \in G$. Then $a^{|G|} = e$.

Proof Left as an exercise.

$\blacksquare$

Corollary 5 [Fermat's Little Theorem]

For every integer a and every prime p, $a^p \equiv a \mod p$. (Recall modular arithmetic from MATH 135).

Proof If $p \mid a \Rightarrow a \equiv 0 \mod p \Rightarrow a^p \equiv a \mod p$.

If $p \nmid a \Rightarrow a \in U(p)$ [Recall the group of units in $\mathbb{Z}_p$]. Since $|U(p)| = p-1 \Rightarrow$ from Lagrange's theorem (or Corollary 4) $a^{p-1} \equiv 1 \mod p$

$\Rightarrow \quad a^p \equiv a \mod p.$

$\blacksquare$

Lagrange's Theorem imposes severe restrictions on the possible order of subgroups. The next theorem also places powerful limits on the existence of certain subgroups.

Theorem Let G be a group and H and K be two finite subgroups of G. Define the set

$$HK = \{ hk \mid h \in H,\ k \in K \}. \text{ Then } |HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof: It looks by looking at the set HK that it should have $|H| \cdot |K|$ elements. However it might happen in the group G that $h_1 k_1 = h_2 k_2$ where $h_1 \neq h_2$ and $k_1 \neq k_2$, so there might be overcounting. We would like to show that the extent to which this overcounting occurs.

Let $x \in H \cap K$. Then for any $h \in H$ and $k \in K$

$$hk = (hx)(x^{-1}k) \quad \text{and} \quad hx \in HK \text{ and } x^{-1}k \in HK$$

$\Rightarrow$ every element in HK is represented by atleast $|H \cap K|$ times.

If $h_1 k_1 = h_2 k_2 \Rightarrow x = h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$

$\Rightarrow \quad h_1 = h_2 x$ and $k_2 = x k_1$. So every element in HK is represented exactly by $|H \cap K|$ products $\Rightarrow |HK| = \dfrac{|H||K|}{|H \cap K|}$.

$\square$

An example of using Lagrange's Theorem and the theorem above is Problem 8 on your assignment 2.