Lecture 9: Lagranges theorem

Lagranges theorem: Let G be a finite group and let H be a subgroup of G then Lagranges thm. states that $|H| \,\big|\, |G|$.

Proof: If $H = G$ then the result is trivial. If H is a proper subgroup of G then let $g_1 \in G$, $g_1 \notin H$ and consider the set $g_1 H = \{g_1 h : h \in H\}$. We have two claims

(i) $g_1 H \cap H = \phi$

(ii) $|g_1 H| = |H|$

To prove (i) assume that $h \in g_1 H \cap H$, then $h = g_1 h_1$ for some $h_1 \in H \Rightarrow g_1 = h h_1^{-1}$

But this is a contradiction since by hypothesis $g_1 \notin H$. Therefore $g_1 H \cap H = \phi$

To show (ii) we check that the mapping $\Phi : H \to g_1 H$ given by $h \mapsto g_1 h$ is a 1-1 and onto mapping. (check!).

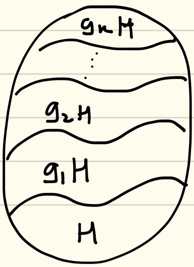
Next let $g_2 \in G$, $g_2 \notin H$ and $g_2 \notin g_1 H$ then again we have the claims

(iii) $g_2 H \cap H = \phi$, $g_2 H \cap g_1 H = \phi$

(iv) $|g_2 H| = |H|$

Proof of $g_2 H \cap H = \phi$ goes along the same lines as before. To show that $g_1 H \cap g_2 H = \phi$ assume by the way of contradiction that it is not so, then $\exists$ an elemet $g_1 h \in g_1 H$ such that it also belongs to $g_2 H$ $\therefore g_1 h = g_2 h'$ for some $h, h' \in H$. Thefore $g_2 = g_1 h (h')^{-1}$ $\Rightarrow g_2 \in g_1 H$ which is a contradiction. So, $g_1 H \cap g_2 H = \phi$. Claim (iv) can be shown similar to claim (ii).

Continuing in this manner till we exhaust all the elements of G (this has to happen since G is finite) we get a partition of G as shown



Then counting the elements of G we get

$$|G| = |H| + |g_1 H| + |g_2 H| + \cdots + |g_k H|$$

$$|G| = |H| + k|H| \quad (\text{since } |g_i H| = |H|)$$

$$|G| = (k+1) H$$

$\therefore$ $|H| \,\big|\, |G|$ as required.

Applications of Lagrange's theorem:

Corollary 1: Let G be a group and Let $x \in G$ then $|\langle x \rangle| \mid |G|$

Corollary 2: Let G be a group of prime order then then G is cyclic.

Proof: Let $x \in G$ s.t. $x \neq e$ and consider $\langle x \rangle$. By corollary 1 $|\langle x \rangle| \mid |G|$. Since $|G|$ is prime $|\langle x \rangle| = 1$ or $|\langle x \rangle| = |G|$. Since $x \neq e \Rightarrow |\langle x \rangle| = |G|$. Therefore x generates G and G is cyclic

Corollary 3: Let G be a group and x be any element of G then $x^{|G|} = e$.

Proof: Let m be the order of x. From corollary 1 $m \mid |G|$, so $|G| = km$ for some $m \in \mathbb{Z}$. So $x^{|G|} = x^{mk} = (x^m)^k = e^k = e$.

Consider the set $\mathbb{Z}_n^*$ consisting of elements that are less than n and relatively prime to n. For eg $\mathbb{Z}_8^* = \{1,3,5,7\}$. $\mathbb{Z}_{20}^* = \{1,3,7,9,11,13,17,19\}$. This forms a group under multiplication modulo n. (check!). The order of this group is $\Phi(n)$ the Euler Phi function.

Corollary 4: (Euler's theorem) If $\gcd(x,n) = 1$ then $x^{\Phi(n)} \equiv 1 \bmod n$

Proof: $x \in \mathbb{Z}_n^*$ (modulo n) then from corollary 3 $x^{\Phi(n)} = 1$

Corollary 5: (Fermat's Little theorem) If p is a prime and x is not a multiple of p then $x^{p-1} \equiv 1 \bmod p$.

Proof: Apply Eulers theorem with $n = p$ noting that $\Phi(p) = p-1$.