1 Lagrange's Theorem

Consider $\mathbb{Z}_{12}$

$\langle 3\rangle = \{0, 3, 6, 9\}$

$1 \notin \langle 3\rangle$

Let us add 1 to each element of $\langle 3\rangle$ and denote this set as $1\langle 3\rangle$

$1\langle 3\rangle = \{1, 4, 7, 10\}$

$2 \notin \langle 3\rangle \cup 1\langle 3\rangle$

$2\langle 3\rangle = \{2, 5, 8, 11\}$

We observe that the sets $\langle 3\rangle, 1\langle 3\rangle$ and $2\langle 3\rangle$ are disjoint.

and $\langle 3\rangle \cup 1\langle 3\rangle \cup 2\langle 3\rangle = \mathbb{Z}_{12}$.

All the 3 sets above have 4 elements.

$\Rightarrow o(\langle 3\rangle)$ divides $o(\mathbb{Z}_{12})$.

Let G be a finite group and H be a proper subgroup of G.

Consider aH where $a \notin H$.

Let $x \in H \cap aH$, then $x = ah_1 = h_2$ for some $h_1, h_2 \in H$.

$\Rightarrow \quad a = h_2 h_1^{-1} \in H; \ \Rightarrow\Leftarrow$

$\Rightarrow \quad H \cap aH = \emptyset$

In the set aH, $\quad ah_1 = ah_2 \Rightarrow h_1 = h_2 \quad \Rightarrow \quad |aH| = |H|$.

Consider $b \in G$ such that $b \notin H$ and $b \notin aH$

Then $H \cap bH = \emptyset$.

Let $x \in aH \cap bH \quad \Rightarrow \quad x = ah_1 = bh_2$ for some $h_1, h_2 \in H$.

$\Rightarrow b = ah_1 h_2^{-1}, \quad \Rightarrow \quad b \in aH \quad \Rightarrow\Leftarrow$

So $aH \cap bH = \emptyset$.

Since G is finite we stop when we are left with no elements of G

G has been partitioned into a collection of disjoint subsets of G all of equal size, that of H.

This construction proves what we state as :

- *Lagrange's Theorem*:
  If G is a finite group and H is a subgroup of G then $o(H)|o(G)$.

- *Corollary* 1:
  Let $a \in G$. Then $a^{o(G)} = e$.

- *Corollary* 2:
  If $o(G) = p$ a prime then G is a cyclic group.

Cosets

Let H be a subgroup of a group G.

Consider the collection of sets $\{aH|\ a \in G\}$.
We observed the following:

- Not all the sets in this collection are distinct.

- Either $aH = bH$ or $aH \cap bH = \emptyset$ for $a, b \in G$ and

- $G = \cup_{a \in G} aH$

Def.
Left coset: Let H be a subgroup of G and $a \in G$. A left coset of H in G is a subset aH of G given by $aH = \{ah|h \in H\}$.

We can similarly define the right coset as the set Ha.

Note: For a non-abellian group we may not have $aH = Ha$.

- *Eg.* 2   Multiplication $(\mod 7)$

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

  $H = \{1, 6\}$ is a subgroup of $\mathbb{Z}_7^*$.

- The distinct left cosets of H are
  $H = 6H = \{1, 6\},\ \ 2H = 5H = \{2, 5\},\ \ 3H = 4H = \{3, 4\}$

- Since this group is abellian the left cosets are same as the respective right cosets.

Cosets establishes an equivalence relation amongst the elements of the group.

- Let us define a relation on G.
  $a \sim b$ if $a \in bH$.

- We can show that this is an equivalence relation.   exercise

- The equivalence classes are the cosets of H in G.

  If $x \in [a]$ then $x \in aH, \ \Rightarrow \ [a] \subseteq aH$
  If $x \in aH$ then $x \sim a, \ \Rightarrow \ x \in [a] \ \Rightarrow \ aH \subseteq [a]$
  $\implies [a] = aH$.

- Note that the right cosets induce a different equivalence relation on G.
  The equivalence classes induced by it are the right cosets and they are in general different from the left cosets.

- *Def.* **Index**
  Let H be a subgroup of a group G. Index of H in G denoted as $[G : H]$ is defined as the number of distinct left(or right) cosets of H in G.

- If G is finite then
  $$[G : H] = \frac{o(G)}{o(H)}$$
  Index of H in G is also denoted as $i_G(H)$.