Def: Let G be a group, H a subgroup. Define the index of H in G

$[G:H]$ = # of (unique) left cosets of H in G

Ex] $G = \mathbb{Z}_6$, $H = \{0,3\}$

$$[G:H] = 3$$

Thm] Let H be a subgroup of G.

# of left cosets of H in G = # right cosets of H in G.

Proof: $\mathcal{L}_H$ - set of left cosets, R_H - set of right cosets

want to define a bijection $\phi : \mathcal{L}_H \to R_H$

If $gH \in \mathcal{L}_H$ let $\phi(gH) = Hg^{-1}$

this is well defined since if $g_1H = g_2H$ are different rep. of the same coset

then $Hg_1^{-1} = Hg_2^{-1}$ by Lemma.

$\therefore$ well defined

1-1 : Suppose $\phi(a_1H) = \phi(a_2H)$

$\Rightarrow Ha_1^{-1} = Ha_2^{-1} \Rightarrow a_1H = a_2H$ by (same) Lemma onto: For any $Hg \in R_H$ we have that

$$\phi(g^{-1}H) = H(g^{-1})^{-1} = Hg \quad \therefore \phi \text{ is onto}$$

$\therefore$ ϕ is a bijection $|S_H| = |R_H|$ ∎.

Lagrange's Theorem

Thm) Let G be a finite group, H a subgroup of G.
Then

$$\frac{|G|}{|H|} = [G:H] = \#\text{ distinct (left/right) cosets of } H \text{ in } G.$$

In particular $|H| \mid |G|$.

Proof:

The group G is partitioned into $[G:H]$ distinct cosets. Each coset has $|H|$ elements.

$\therefore$ $|G| = [G:H]\,|H|$. ∎

corollary) Suppose G is a finite group, $g \in G$.
Then $|g| \mid |G|$. That is "the order of an element divides the order of the group".

Proof:

Apply Lagrange's Thm. to $H = \langle g \rangle$.

Corollary) Let $|G| = p$ for p prime. Then G is cyclic and is generated by any $g \in G$ s.t. $g \neq e$.

Proof: Let $g \in G$, $g \neq e$.

Then $|g| \mid |G| \Rightarrow |g| > 1$ (since $g \neq e$) and $|g| \leq |G|$

$\Rightarrow |g| = |G| \therefore G = \langle g \rangle$. ∎

Cor.) Let H and K be subgroups of G, $|G| < \infty$ Such that $K \subseteq H \subseteq G$, Then $[G:K] = [G:H][H:K]$.

Proof:

$$[G:K] = \frac{|G|}{|K|} = \underbrace{\frac{|G|}{|H|}}_{[G:H]} \underbrace{\frac{|H|}{|K|}}_{[H:K]} = [G:H][H:K].$$ ∎

Note: The converse o Lagranges Theorem is false, i.e. there may not exist subgroups of all orders which divide $|G|$

Consider A_4, $|A_4| = 12$, by Lagranges theorem we could have subgroups of orders $1, 2, 3, 4, 6$

Prop.) A_4 has no subgroups of order 6.

Proof. Suppose H is a subgroup of order 6

$\Rightarrow [A_4 : H] = 2$

$\Rightarrow$ H has two cosets, one of which is $eH = H = He$.

$\therefore A_4 = H \underset{\text{disjoint union}}{\amalg} gH = H \amalg Hg \quad \forall g \notin H$

Take $g \notin H$ consider

$g^2 H$, either $g^2 H = H$ or $g^2 H = gH$

if $g^2 H = gH \Rightarrow gH = H \Rightarrow g \in H$, contradiction

$\Rightarrow g^2 H = H$

$\Rightarrow g^2 \in H \quad \forall g \in A_4$

Suppose $g^3 = e \Rightarrow g^2 = g^{-1} \Rightarrow g^2 \in H$ then

$g^{-1} \in H$

$\Rightarrow g \in H$

$\Rightarrow \forall g \in A_4$ s.t. $g^3 = e$ are in H

There are 8 3-cycles in A_4 $\therefore$ all these

3-cycles, and the identity, are in H

$\Rightarrow |H| \geq 9$

but $|H| = 6$ was assumed

$\therefore$ a contradiction. $\blacksquare$.

$$hH = eH = H \qquad \forall h \in H.$$