Recall

$aH = \{ah \mid h \in H\}$ is left coset

$Ha = \{ha \mid h \in H\}$ right coset

Lemma

Let $H \leq G$

Every left or right coset of H in G has the same cardinality as H

Proof

Let $a \in G$. Define $\phi : H \to aH$

$\phi(h) = ah$

for $h \in H$

Notice ϕ-injective bcs

$\forall h_1, h_2 \in H \quad \phi(h_1) = \phi(h_2) \iff h_1 = h_2$

ϕ-surjective

$\forall h' \in H \quad \phi(h) = ah \quad$ for $h = h'$

so ϕ-bijective, hence

$$|H| = |aH|$$

Similarly, $|H| = |Ha|$

Theorem of Lagrange

Let G be a finite group & $H \leq G$

Then $|H| \,\Big|\, |G|$ ("divides")

Proof

let $|G| = n$

$|H| = m$

By the lemma,

$\forall g \in G$, $|gH| = |Hg| = |H| = m$

Let k be the # of left/right cosets

Since $\forall i = 1..k$ $\quad g_i H \neq \emptyset$
$j = 1..k$

$$g_i H \cap g_j H \neq \emptyset$$

$$\bigcup_{i=1}^{k} g_i H = G$$

$$n = |G| = |g_1 H| + |g_2 H| + \dots + |g_k H|$$

$$= m + m + \dots + m$$

$$= km = k|H|$$

so $\quad m = |H| \mid |G| = n$

$$k \mid |G| = n$$

Definition

Let $H \leq G$

The **index** of H in G denoted

$$(G:H)$$

is the # of left/right cosets of H in G

If G is finite

$$|G| = (G:H) \cdot |H|$$

<u>Example</u>

Find the index of H in G

1) $H = \langle 3 \rangle \leq G = \mathbb{Z}_6$

$$(G:H) = \frac{|G|}{|H|} = \frac{|\mathbb{Z}_6|}{|\langle 3 \rangle|} = 6/2 = 3$$

(3 left + right cosets that coincide)

Corollary 1

Every group of prime order is cyclic

Proof

Let G be a group of a prime order p.

Let $a \in G$ s.t. $a \neq e$.

Then $|\langle a \rangle| \geq 2$, by L.T.

$$|\langle a \rangle| \,\Big|\, |G| = p, \text{ hence}$$

$|G| = |\langle a \rangle| = p$ which means

$G = \langle a \rangle$ so G is cyclic

Note: Every cyclic group of order n

is isomorphic to $\mathbb{Z}_n$, every group of prime order p is isomorphic to $\mathbb{Z}_p$

Therefore, there is a unique group of prime order p – $\mathbb{Z}_p$

Corollary 2

The order of an element of a finite group divides the order of the group

Proof

Let G be a finite group &
let $a \in G$ of order n

Then $\forall k < n$, $a^k \neq e \wedge a^n = e$
Since $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$

$$|\langle a \rangle| = n \quad \text{by L.T.}$$
$$n = |\langle a \rangle| \mid |G|$$