Proof of Lagrange's Theorem

Definition: Let H be a subgroup of a group G. The *index* of H in G, written $\boxed{[G : H]}$, is the number of left (or right) cosets of H in G if this number is finite. If it is not finite, H is said to have infinite index.

Example:

$\in G = D_3$

- If H is the group of rotations of the triangle, H has index 2 in D_3. H has 3 elts, 2 cosets so $[G:H]=2$
- $n\mathbb{Z}$ has index n in $\mathbb{Z}$. $a+n\mathbb{Z}$ $a=0,1,\dots,n-1$
- If $H = \{e, (12)\}$ in D_3, then H has index 3.

$[G:H]=3.$

$G = \mathbb{R}^* = \{x \in \mathbb{R}, x \neq 0\}$. operation is multiplication.

$H = \{+1, -1\}$. $r \in \mathbb{R}^*$ $rH = \{r, -r\}$.

$r \in \mathbb{R}^*$, $r > 0$ rH

$rH = sH \Rightarrow \{r, -r\} = \{s, -s\} \Leftrightarrow r = \pm s$

$\Leftrightarrow r = s$ when $r, s > 0$.

Theorem: Let G be a finite group and H a subgroup. Then

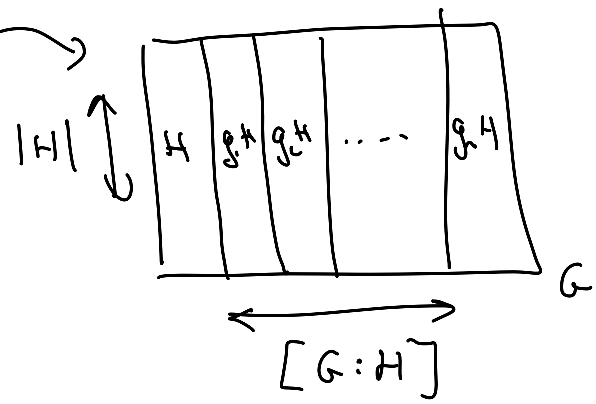
$$\underline{|G|} = \underbrace{|H|}_{}\,\underbrace{[G : H]}_{}.$$

order index

In particular the order of H divides the order of G.

Proof: Each (left) coset of H in G has the same number of elements as H. More specifically the map $f : H \to gH$ defined by $f(h) = gh$ is bijective.

if $|gH| = |H|$



- f is injective.

injective

$f(h_1) = f(h_2) \Rightarrow gh_1 = gh_2$

$\Rightarrow h_1 = h_2$

using

$(g^{-1} \cdot gh_1) = g^{-1}gh_2$

- f is surjective

if $x \in gH$, $x = gh$ for some h.

$f(h) = gh = x.$

This means that G is the disjoint union of $[G : H]$ sets, each with $|H|$ elements, proving the result.

Corollary: The order of an element of a group is a divisor of the order of the group.

$g \in G$

order(g) = $\langle g \rangle$

$|\langle g \rangle| \,\Big|\, |G|$ by Lagrange's theorem.

$\mathbb{Z}_{12}$ order $(3) = 4$ $4 \cdot 3 \equiv 0 \ (12)$

index $\langle 3 \rangle = 3$

order $\langle 3 \rangle = 4$.

Corollary: If $|G|$ is a prime number, then G is a cyclic group and any non-identity element is a generator of G.

$|G| = p$ p prime.

$\alpha \in G$, $\alpha \neq 1$.

order(α) must divide p.

order $(\alpha) = p$.

$|\langle \alpha \rangle| = p$ $[G : \langle \alpha \rangle] = 1$

$\langle \alpha \rangle = G$.

Corollary: Suppose $K \subset H \subset G$ are subgroups. Then

$$[G : K] = [G : H][H : K].$$

Proof:

$$\underline{[G : K]} = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = \underline{[G : H]}\underline{[H : K]}$$