Lagrange's Theorem

P. Reany

March 16, 2024

Abstract

Lagrange's Theorem states that the order of a subgroup of a finite group must divide the order of the group. The proof of this theorem relies heavily on the fact that every element of a group has an inverse.

1 Theorem Statement

Let G be a finite group with $|G|$ its order. Let H be a subgroup of G with $|H|$ its order. Then

$$|H| \,\big|\, |G| \,. \tag{1}$$

2 Proof

For specificity, let's assume that $|H| = m$, then, with the group identity element represented as e, we have that

$$H = \{e, h_1, h_2, \ldots, h_{m-1}\} \,. \tag{2}$$

Next, let g be an element of G that is not in H. Then

$$gH = g\{e, h_1, h_2, \ldots, h_{m-1}\} \equiv \{g, gh_1, gh_2, \ldots, gh_{m-1}\} \,, \tag{3}$$

where gH is a set but not a group in itself. Why? (Hint: it has no identity element.) Also, note that for any $g \in G$, $g \in gH$.

Claim: The set gH has no elements in common with H. Proof by contradiction. Assume that the two sets do have a common element. Say that gh_i in gH is equal to some element in H, namely h_j. Then

$$gh_i = h_j \,. \tag{4}$$

Multiplying on the right by h_i^{-1} we get

$$g = h_j h_i^{-1} \,. \tag{5}$$

But $h_j h_i^{-1}$ is an element of H, implying that $g \in H$, which we had assumed is not true. Contradiction. Hence, the sets gH and H have no common elements.

Definition: The set gH is said to be a *left coset* of H.

Now choose another element of G, namely g', which is not in the set $gH \cup H$. Then we need to show that the set $g'H$ has no common element with $gH \cup H$. How do we know this to be true? By the previous argument, we know that $g'H$ has no common element with H. But does it have a common element with gH? Let's assume that it does. Then for some $g'h_i \in g'H$ and for some $gh_j \in gH$

$$g'h_i = gh_j \,. \tag{6}$$

Which leads to

$$g' = gh_j h_i^{-1} \in gH \,, \tag{7}$$

which is a contradiction because we had assumed that $g' \notin gH$.

Obviously, every element of G, say g', will be in exactly one of the cosets of H, namely $g'H$. But we already know that $g' \in g'H$. Then under what condition are these two cosets are equal? Namely,

$$g'H = gH \,, \tag{8}$$

where we are treating $g'H$ and gH as sets? For this to be true, then there must exist some elements h_i and h_j such that

$$g'h_i = gh_j \,, \tag{9}$$

from which we get that

$$g^{-1}g' = h'_j h_i^{-1} \in H \,. \tag{10}$$

Thus $g'H$ and gH are the same set if and only if g and g' quotient by an element of H.

Clearly, all the elements of G are placed in exactly one coset of H. And every coset has the same size, namely m. Therefore

$$|G| = km \,, \tag{11}$$

for some positive integer k. Just as clearly, $k = |G|/m$.

Therefore, we have proved that for G a finite group and H a subgroup of G, then the order of H divides the order of G.

By the way, the number k is the number of left cosets of H in G, which is sometimes represented by the symbol $[G, H]$ or $|G, H|$, and is called the *index* of H in G. Sometimes we see the relation

$$[G, H] = \frac{|G|}{|H|} \,. \tag{12}$$