Lagrange's Theorem: Statement and Proof

Paul D. Humke

April 5, 2002

Abstract

Lagrange's Theorem is one of the central theorems of Abstract Algebra and it's proof uses several important ideas. This is some good stuff to know!

Before proving Lagrange's Theorem, we state and prove three lemmas.

Lemma 1. *If G is a group with subgroup H, then there is a one to one correspondence between H and any coset of H.*

PROOF. Let C be a left coset of H in G. Then there is a $g \in G$ such that $C = g * H$.[1] Define $f : H \to C$ by $f(x) = g * x$.

1. f is one to one.

   If $x_1 \neq x_2$, then as G has cancellation, $g * x_1 \neq g * x_2$. Hence, $f(x_1) \neq f(x_2)$.

2. f is onto.

   If $y \in C$, then since $C = g * H$, there is an $h \in H$ such that $y = g * h$. It follows that $f(h) = y$ and as y was arbitrary, f is onto.

This completes the proof of Lemma 1. □

Lemma 2. *If G is a group with subgroup H, then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 * H = g_2 * H$ is an equivalence relation.*

PROOF. The essence of this proof is that $\sim$ is an equivalence relation because it is defined in terms of *set equality* and equality for sets is an equivalence relation. The details are below.

- $\sim$ is reflexive.

  Let $g \in G$ be given. Then, $g*H = \{g*h : h \in H\}$ and as this set is well defined, $g*H = g*H$.

[1] We use "$*$" to represent the binary operation in G.

- $\sim$ is symmetric.

  Let $g_1, g_2 \in G$ with $g_1 \sim g_2$. Then by the definition of $\sim$, $g_1 * H = g_2 * H$. That is, $\{g_1 * h : h \in H\} = \{g_2 * h : h \in H\}$ and as set equality is symmetric, $\{g_2 * h : h \in H\} = \{g_1 * h : h \in H\}$. Hence, $g_2 \sim g_1$ and as g_1 and g_2 were arbitrary, $\sim$ is symmetric.

- $\sim$ is transitive.

  Let $g_1, g_2, g_3 \in G$ with $g_1 \sim g_2$ and $g_2 \sim g_3$. Then,

$$g_1 * H = \{g_1 * h : h \in H\} = \{g_2 * h : h \in H\} = g_2 * H$$

  and

$$g_2 * H = \{g_2 * h : h \in H\} = \{g_3 * h : h \in H\} = g_3 * H.$$

  As set equality is transitive, it follows that

$$g_1 * H = \{g_1 * h : h \in H\} = \{g_3 * h : h \in H\} = g_3 * H,$$

  or $g_1 * H = g_3 * H$. That is, $g_1 \sim g_3$, and as $g_1, g_2, g_3 \in G$ are arbitrary, $\sim$ is transitive.

This complete the proof of the lemma. □

Lemma 3. *Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.*

PROOF. To prove the lemma, we show that $A \subset B$ and $B \subset A$. As A and B are arbitrarily labeled, it suffices to show the former.

Let $a \in A$. As $A \cap B \neq \emptyset$, there is a $c \in A \cap B$. As A is an equivalence class of $\sim$ and both a and c are in A, it follows that $a \sim c$. But as $a \sim c$, $c \in B$ and B is an equivalence class of $\sim$, it follows that $a \in B$. □

Armed with these three lemmas we proceed to the main result.

Theorem 1. *[Lagrange's Theorem] If G is a finite group of order n and H is a subgroup of G of order k, then $k|n$ and $\frac{n}{k}$ is the number of distinct cosets of H in G.*

PROOF. Let $\sim$ be the left coset equivalence relation defined in Lemma 2. It follows from Lemma 2 that $\sim$ is an equivalence relation and by Lemma 3 any two distinct cosets of $\sim$ are disjoint. Hence, we can write

$$G = (g_1 * H) \cup (g_2 * H) \cup \cdots \cup (g_\ell * H)$$

where the $g_i * H$, $i = 1, 2, \ldots, \ell$ are the disjoint left cosets of H guaranteed by Lemma 3.

By Lemma 1, the cardinality of each of these cosets is the same as the order of H, and so

$$\begin{aligned} |G| &= |g_1 * H| + |g_2 * H| + \cdots + |g_\ell * H| \\ &= \underbrace{|H| + |H| + \cdots + |H|}_{\ell \text{ summands}} \\ &= \ell \cdot |H| = \ell \cdot k. \end{aligned}$$

This completes the proof. □