Lagrange's Theorem

Akhil Jalan

Feb 10, 2017

Introduction and Definitions

Claim: Let G be a group and $H \leq G$ a subgroup. Let $|G| = n$ and $|H| = m$ for some $m, n \in$
ZZ^+. Then $m|n$.

We will make use of cosets of H. A **left coset of H** aH is $\{a * h : h \in H\}$. Similarly, a **right coset of H** Ha is $\{h * a : h \in H\}$.

Lemma 1

If $a, b \in G$ are distinct, then $aH = bH$ or $aH \cap bH = \emptyset$.

Proof: Suppose that $aH \cap bH \neq \emptyset$. Then for some $h_i, h_j \in H$, we know $ah_i = bh_j$. This implies $a = bh_j h_i^{-1}$ and implies $b = ah_i h_j^{-1}$. Then $aH \subseteq bH$ since for any $ah_k \in aH$, we know $ah_k = (bh_j h_i^{-1})h_k = b(h_j(h_i)^{-1}h_k) \in bH$. And by symmetry, $bH \subset aH$. So either $aH = bH$ or $aH \cap bH = \emptyset$.

Lemma 2

For any $a \in G$ the coset $|aH| = |H|$.

Proof: Consider aH for some $a \in G$. By Lemma 1, set is either the same as H itself (we compare aH to $eH = H$) or totally disjoint from it. If it is the same as H then it has the same size, namely m. If it is totally disjoint from m, then each element is of the form ah_i for some $h_i \in H$. Then we have $ah_1 = ah_2 \Rightarrow h_1 = h_2$ by left cancellation. So $h_1 \neq h_2 \Rightarrow ah_1 \neq ah_2$ by contrapositive. So right multiplication by each element of H yields a unique value, and $|aH| = |H|$.

Main Proof

If $G = \{g_1, ..., g_n\}$ then the cosets $g_1H, ..., g_nH$ are exhaustive of G. For any $g' \in G$ we know that at the least, $g' \in g'H$.

By Lemma 1, the cosets are either equal or distinct. By Lemma 2, they are all of the same size. By our argument just above, they are exhaustive of G. Therefore, the left cosets of H partition G, and there must be $\frac{n}{m}$ of them. Then $m|n$.

Remark

This theorem is perhaps poorly stated, because most of the significance comes from the realization that membership in a left coset of H (and by symmetric arguments, a right coset) is an equivalence relation on G itself. These cosets form a very natural partition of the group. We might find it useful to make the following corollaries.

Corollary 1

If the order of a group G is a prime $p \in \mathbb{N}$ then the only subgroups of G are $\{e\}$ (the **trivial subgroup**) and G itself.

Proof: Suppose that G is a group of prime order. Then no nontrivial proper subgroup of G can exist, because it would have to have an order which divides p.

Corollary 2

Membership in a coset aH is an equivalence relation on G.

Proof: Every element $g \in G$ exists in one coset, and only one coset, by the main proof. So clearly there is an equivalence relation of belonging to the same coset, which we can denote $\sim$.

i. Reflexive: $a \sim a$ since $a \in gH \leftrightarrow a \in gH$.

ii. Symmetric: $a \sim b$ means "a is in the same coset as b" so clearly b is in the same coset as a. So $b \sim a$.

iii. Transitive: If $a \sim b$ and $b \sim c$ then a is in the same coset as b which is in the same coset as c. So a, c are in the same coset. We conclude $a \sim c$.

Corollary 3

The cosets aH, Ha are subgroups of G iff $a \in H$.

Proof: We'll prove for aH, since it is entirely symmetric for both sides.

$\Leftarrow$: Suppose that $a \in H$. Then since $ae = a \in aH$, this means by Lemma 1 that $aH = H$. $aH = H$ is a subgroup.

$\Rightarrow$: Suppose that aH is a subgroup. Then we know $ah_i = e$ for some $h_i \in H$. By uniqueness of inverses, $h_i = a^{-1}$. But if $a^{-1} \in H$, then so is a by closure under inverses.