Lagrange's Theorem

James Pagan

Abstract

I found this proof in about nine hours in June, knowing nothing except the group axioms. The key was, rather than analyzing subgroups directly, to focus on constructing possible groups around a given subgroup. The idea of cosets — or as I called them, "projections" — arised naturally. The following is my old proof verbatim, although I changed my older projection notation; my current proofwriting style is more mature.

1 Lagrange's Theorem

Theorem 1. *If H is a subgroup of the finite group G, then $|H|$ divides $|G|$.*

Proof. Let the elements of G be $x_1, x_2, \ldots, x_{|G|}$; for any $x \in G$, we define the **projection** of H by x as $Hx = \{hx \mid h \in H\}$.

Lemma 1. *If a and b are elements of G, then either $Ha = Hb$ or $Ha \cap Hb = \varnothing$.*

Proof. Suppose that Ha and Hb are not disjoint — namely, there exist some $h, g \in G$ such that $ha = gb$. We thus have that $a = h^{-1}gb$, and $b = g^{-1}ha$; as H is a subgroup, $h^{-1}g$ and $g^{-1}h$ are in H.

Now, let fa and fb be any elements of Ha and Hb respectively. We have that $fa = fh^{-1}gb$, so every element in Ha is an element of Hb, and $fb = fg^{-1}ha$, so every element of Hb is an element of Ha. Then $Ha = Hb$, as desired.

Thus, projections are either equal or disjoint.

Lemma 2. *For any element $x \in G$, $|Hx| = |H|$.*

Proof. We establish a bijection between Hx and H. For any $x \in G$, let $f_x : H \to Hx$ be $f_x(h) = hx$. By the definition of Hx, fx is surjective. Now suppose that for any $a, b \in H$, we have $ax = bx$. Multiplying by x^{-1} yields $ha = hb$, so $f_x$is injective. Then there is a bijection between Hx and H, which implies $|Hx| = |h|$.

We claim that $Hx_1 \cup Hx_2 \cup \cdots \cup Hx_{|G|} = G$.

Proof. We show that both sides are subsets of each other. Note that every element of Hx is an element of G (by $G's$ closure), so $Hx_1 \cup \cdots \cup Hx_{|g|} \subseteq G$. Now, note that G's identity e is in H; then for all x in G, $x = ex$ is in Hx. Then every element of G is contained in some projection of H, and the $G \subseteq Hx_1 \cup \cdots \cup Hx_{|G|}$. Therefore, both sides are equal.

We now claim that the order of $Hx_1 \cup Hx_2 \cup \cdots \cup Hx_{|G|}$ is a multiple of $|H|$. We prove this by induction.

Base case: By Lemma 2, Hx_1 has order H — it is thus a multiple of $|H|$.

Inductive step: Suppose $Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$ is a multiple of H for some integer $n \in \{1, 2, \ldots, |G| - 1\}$. These bounds guarantee that Hx_{n+1} exists. Now, if there exists an integer r such that $Hx_r = Hx_{n+1}$, we have that

$$|Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n \cup Hx_{n+1}| = |Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n|.$$

If no such r exists, Lemma 1 guarantees that Hx_{n+1} is disjoint from every single $Hx_1, Hx_2, \ldots, Hx_n$. Therefore,

$$|Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n \cup Hx_{n+1}| = |Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n| + |H|.$$

In either case, our inductive hypothesus guarantees that $Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n \cup Hx_{n+1}$ is a multiple of $|H|$.

We thus have that the order of $Hx_1 \cup Hx_2 \cup \cdots Hx_{|G|}$ is a multiple of H. This may be equivalently stated as $|G|$ is a multiple of $|H|$. Therefore, if H is a subgroup of the finite group G, $|H|$ divides $|G|$. $\square$