Lecture 8: Proof of Lagrange's Theorem

Recall these two items from Lecture 7:

Theorem

(Lagrange's Theorem) Let G be a finite group with a subgroup H. Then the order of H divides the order of G.

Definition Let H be a subgroup of a group G (with binary operation $\star$). Then the left coset of H in G determined by x, which is denoted xH or $x \star H$, is the set

$$xH = \{x \star h : h \in H\}.$$

Key property of left cosets

This is Lemma 2.1.7 in the lecture notes.

Lemma Suppose that g_1 and g_2 are elements of a group G and that H is a subgroup of G. Then either the cosets g_1H and g_2H are equal to each other or they are disjoint from each other, i.e. their intersection is empty, they have no element in common.

Note: Since g_1H and g_2H are *sets* (subsets of G), what it means to say that they are equal is that they have exactly the same elements. A standard way to show that two sets A and B are equal is to show that every element of A belongs to B (so $A \subseteq B$) and that every element of B belongs to A (so $B \subseteq A$).

Proof

If g_1H and g_2H have no element in common then there is nothing to do.

So suppose that these two sets *do* have at least one element in their intersection. This means that there are elements h_1 and h_2 of H for which

$$g_1h_1 = g_2h_2.$$

We must deduce that the sets g_1H and g_2H are equal.

First we show that $g_1H \subseteq g_2H$.

Choose an element of g_1H. It is g_1h for some $h \in H$.

Now

$$g_1h_1 = g_2h_2 \Longrightarrow g_1 = g_2h_2h_1^{-1},$$

so we can write $g_1h = g_2h_2h_1^{-1}h = g_2\underbrace{\left(h_2h_1^{-1}h\right)}_{\in H}$.

So $g_1h \in g_2H$ and $g_1H \subseteq g_2H$.

Proof (continued)

Starting with $g_1 h_1 = g_2 h_2$ and rewriting it as $g_2 = g_1 h_1 h_2^{-1}$, we can use the same approach to prove the oppostite inclusion $g_2 H \subseteq g_1 H$. We conclude that the left cosets of H determined by different elements of G are identical if they intersect at all. $\square$

It is this property that allows to prove Lagrange's Theorem by establishing that G is the union of the distinct left cosets of H, each of which has the same number of elements as H. The number of these cosets is called the index of H in G, denoted by $[G : H]$. If G is finite, then

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