GROUP THEORY PROOFS

AKASH DHIRAJ

We omitted these proofs in the main lecture for the sake of time and presentation.

1. Lagrange's Theorem

Proposition 1.1. *For $H \leq G$ and cosets g_1H and g_2H, $g_1H = g_2H$ or $g_1H \cap g_2H = \varnothing$.*

Proof. If $g_1H \cap g_2H = \varnothing$, we're done. So, suppose there exists $g \in g_1H \cap g_2H$. Then, there exists $h_1, h_2 \in H$ such that $g = g_1h_1 = g_2h_2$. We'll show $g_1H \subseteq g_2H$. Consider arbitrary $g_1h \in g_1H$. Then, our result follows since $g_1h = g_2h_2h_1^{-1}h \in g_2H$. By applying a symmetric argument, we may show $g_2H \subseteq g_1H$ and conclude $g_1H = g_2H$. ■

Proposition 1.2. *For $H \leq G$, all cosets of H have the same cardinality*

Proof. Consider the coset g_1H. It suffices to show $|g_1H| = |H|$. We'll do this by constructing a bijection $f : g_1H \to H$ such that $f(g_1h) = h$. We obtain the inverse $g : H \to g_1H$ via $g(h) = g_1h$. Recall that bijectivity and invertibility are equivalent to conclude the desired result. ■

Proposition 1.3. *For $H \leq G$, every $g \in G$ belongs in a coset of H.*

Proof. Recall $e \in H$. Then, $g = ge \in gH$. ■

Finally!

Corollary 1.4 (Lagrange's Theorem)**.** *Let G be a group and $H \leq G$. Let n be the number of cosets of H. When $|G|$ is finite, $|G| = n|H|$.*

Proof. Let n be the number of cosets. By Proposition 1.3, we note that $G = \bigcup_{i=1}^{n} g_iH$ for $g_1, \ldots, g_n \in G$. Then, by Propositions 1.2 and 1.3,

$$|G| = |g_1H| + |g_2H| + \cdots + |g_nH| = n|H|.$$

■

2. Orbit-Stabilizer Theorem

We'll start with a prelimary definition.

Definition 2.1 (Coset Space)**.** Suppose $H \leq G$. Then, the *coset space* is

$$G/H \coloneqq \{gH \mid g \in G\},$$

where $gH \coloneqq \{gh \mid h \in H\}$. The elements of G/H are called *cosets* of H.

Theorem 2.2 (Orbit-Stabilizer Theorem)**.** *Let the finite group G act on the finite set X. For $x \in X$, $|\mathcal{O}(x)| \times |G_x| = |G|$.*

Proof. We'll conclude the desired result by constructing a bijection from $f : G/G_x \to \mathcal{O}(x)$. This works because, by Corollary 1.4, $|G/G_x| = |G|/|G_x|$. For $gG_x \in G/G_x$, we'll define f such that $f(gG_x) = gx$. But, our cosets can have multiple representations: that is, we can find $g' \in G$ such that $g \neq g'$ and $gG_x = g'G_x$. In this case, we need to make sure our map gives us the same output regardless of the representation we choose. Otherwise. our map isn't well-defined. We'll note that

$$gG_x = g'G_x \implies \exists h, h' \in G_x,\ gh = g'h' \implies g^{-1}g' = h\,(h')^{-1} \in G_x.$$

Now, we have that $g^{-1}g'x = x \implies g'x = gx \implies f(gG_x) = f(g'G_x)$. We can go back to showing f is bijective now. Surjectivity follows trivially since if $x_1 \in \mathcal{O}(x)$, there exists $g_1 \in G$ such that $g_1x = x_1$. Hence, $f(g_1G_x) = x_1$. Injectivity is slightly more tricky. Suppose $f(g_1G_x) = f(g_2G_x)$, i.e. $g_1x = g_2x$. Then, $g_1^{-1}g_2x = x \implies g_1^{-1}g_2 \in G_x$. Let $g_1^{-1}g_2 = h$. Rearranging, we obtain $g_2e = g_1h$. This means the cosets g_1G_x and g_2G_x have non-empty intersection, and, hence, by Proposition 1.1, we conclude $g_1G_x = g_2G_x$ and f is injective. ■

Email address: akashdhiraj2019@gmail.com

Math Circle