Section 10: Cosets and Lagrange's Theorem

Definition 0.1. Let H be a subgroup of a group G. The subset $aH = \{ah \mid h \in H\}$ is the **left coset of H containing** a and the subset $Ha = \{ha \mid h \in H\}$ is the **right coset of H containing** a.

Example 0.2. Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. What are the left cosets of H?

We are looking for all possible subsets aH where $a \in \mathbb{Z}_6$. We can just enumerate these over possible elements of $\mathbb{Z}_6$:

- $a = 0$ or $a = 3$: $aH = H = \{0, 3\}$ (Fact: if $a \in H$, because H is closed, $aH = H$)
- $a = 1$ or $a = 4$: $aH = \{1, 4\}$
- $a = 2$ or $a = 5$: $aH = \{2, 5\}$

Lemma 0.3. *Let H be a subgroup of G. Every (left or right) coset of H has the same number of elements as H.*

Proof. Let $a \in G$ and aH be the left coset containing a (the proof for the right coset will be the same). We want to show that H and aH has the same number of elements. To do this, we will define an onto and one-to-one function $\phi : H \to aH$ by $\phi(h) = ah$.[1] This is one-to-one because, if $\phi(h_1) = \phi(h_2)$, then $ah_1 = ah_2$, so $h_1 = h_2$. This is onto because every element in aH is of the form ah for some $h \in H$, and $\phi(h) = ah$. Therefore, ϕ is a bijection, so H and aH have the same number of elements. □

Lemma 0.4. *Let aH and bH be two left cosets of H. If $aH \neq bH$, then $aH \cap bH = \emptyset$ (in other words, aH and bH have no elements in common). The same holds for the right cosets.*

Proof. If $aH \cap bH$ is non-empty, then there exists $x \in G$ such that $x \in aH$ and $x \in bH$, then by definition $x = ah_1$ and $x = bh_2$, so $ah_1 = bh_2$. Multiplying by h_2^{-1}, we get $b = ah_1h_2^{-1}$. Because H is closed, the element $h = h_1h_2^{-1} \in H$, so $b = ah \in aH$. Therefore, $bH = (ah)H$, but $hH = H$ because $h \in H$, so $bH = aH$. □

Summarizing, if H is a subgroup of G,

- Every element $a \in G$ is contained in some coset of H.
- The distinct cosets of H divide G into blocks and no two of these blocks overlap.
- All of the cosets have the same number of elements.

With this in mind, we can prove the following important theorem. Recall that the **order** of a group (or subgroup) is the number of elements in the group (or subgroup), and this is denoted by $|G|$ or $|H|$.

Theorem 0.5 (Lagrange's Theorem)**.** *Let H be a subgroup of a finite group G. Then, the order of H divides the order of G.*

[1] This is the same proof as what we did to show the number of even permutations was the same as the number of odd permutations in S_n!

Proof. Let G have order n and H have order m. Let $H, a_1H, a_2H, \ldots, a_{k-1}H$ be the k distinct cosets of H. By the previous lemmas, each coset has order m, every element of G appears in exactly one coset, and there are k cosets, so $n = mk$. Therefore, m divides n. □

With the example from the worksheet, we see that D_4 has order 8 and is a subgroup of S_4, and there are 3 distinct cosets, and $24 = 8 \cdot 3$. Lagrange's Theorem says this always happens: (size of group) = (size of subgroup) × (number of cosets).

This theorem has so many important consequences that we will talk about today and Friday.

Corollary 0.6. If G is a finite group and $a \in G$ is any element, then the order of a divides the order of G.

Proof. The order of a is the smallest positive integer such that $a^m = e$, which is equivalent to saying the order of the subgroup $\langle a \rangle$ is m. By Lagrange's Theorem, m divides the order of G. □

Example 0.7. Let G be a group with six elements. This corollary says that, for any $a \in G$, the order of a divides 6. So, $\text{ord}(a) = 1, 2, 3$ or 6. We an actually say even more: if $\text{ord}(a) = 1$, then $a = e$. If $\text{ord}(a) = 6$, then $\langle a \rangle = \{e, a, a^2, a^3, a^4, a^5\} \subset G$, so $\langle a \rangle = G$ and G is cyclic.[2]

We know another group of order 6: S_3! All of the elements of S_3 have order $1, 2$, or 3 (order 1: ι, order 2: transpositions, like (12), order 3: cycles of length 3, like (123)). Here is a fact that you should think about: if G is a group of order 6 and no element of G has order 6, then $G \cong S_3$.

Corollary 0.8. If G is a finite group of prime order p, then G is cyclic.

Proof. The previous corollary implies that, if a is any non-identity element of G, then $\text{ord}(a) = p$, so $\langle a \rangle = G$, so G is cyclic. □

We'll close the day with one new definition.

Definition 0.9. Let H be a subgroup of a finite group G. The **index** of H in G, denoted $(G : H)$, is the number of left cosets of H in G.

With this, Lagrange's Theorem could be stated as $|G| = |H|(G : H)$.

[2] Fact: we've seen this before, but let's say it again: a group G of order n is cyclic if and only if G contains an element of order n.