3.2: Cosets and Lagrange's Theorem

Alex L.

October 9, 2024

Def: The **order** of a finite group is how many elements are in the group. The order is an important group invariant to study.

Theorem: Lagrange's Theorem If G is a finite group and $H \leq G$, then the order of H divides the order of G, and the number of cosets of G/H is equal to $\frac{|G|}{|H|}$

Proof: Let the order of H be n, and the number of left cosets of H in G be k. The left cosets of H, gH, form k disjoint subsets, each with size n, so the total size of G is kn, therefore, if $|H| = n$, and $|G/H| = k$ (because the quotient group is the group of cosets), then $|G/H| = \frac{|G|}{|H|}$.

Def: If G is a group and $H \leq G$, the number of left cosets of H in G is called the **index** of H in G, and is denoted $|G : H|$.

Corrolary: If G is a finite group and $x \in G$, the order of x divides the order of G. Additionally, $x^{|G|} = 1$ for all $x \in G$

Proof: The order of x is equal to the order of the group generated by x, $| < x > |$. If we let that group equal H, then by Lagrange's Theorem, $|G|$ is a multiple of the order of x, meaning the second statement holds.

Corrolary: If G is a group of prime order p, then G is cyclic, hence $G \simeq Z_p$

Proof: Cyclic means a group that can be generated by a single element, and by extension, that element has the same order as the entire group. Let $x \in G$ and $x \neq 1_G$. Then, by the previous corrolary, the order of the group generated by x must divide $|G|$, but it can't be 1 because x is not the identity. Therefore, since $|G|$ is prime, $| < x > | = |G|$, and the group is cyclic.