Subgroups and Lagrange’s Theorem

Definition: Let $H \subset G$ a subset of a group $G$. We say that $H$ is a subgroup of $G$ if $1 \in H$ and if $h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$.

Remark: If $H$ is a subgroup of $G$, then $h_1, h_2 \in H \Rightarrow h_1^{-1} \in H$ and $h_1 h_2 \in H$.

Examples: 1) If $x \in G$, then the cyclic subgroup $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ generated by $x$ is a subgroup of $G$.

2) If $G$ is abelian, and if $m \in \mathbb{N}$, then the set $G[m] := \{x \in G : x^m = 1\}$ is a subgroup of $G$.

Note: If $G = (\mathbb{Z}/n\mathbb{Z})^\times$, then $G[n - 1] = \mathcal{P}_n$.

Theorem 2 (Lagrange) Let $H$ be a subgroup of a finite group $G$. Then $#H | #G$.

Remark: Note that if $H = \langle x \rangle$, then $#H = \text{ord}(x)$ by Theorem 2.1, so Lagrange’s Theorem generalizes property (P3) of Theorem 2.2.