42

3. (6 points) STATE and PROVE Lagrange's Theorem.

If H is a subgroup of the finite group G, then the order of H divides the order of G.

Proof For each $x \in G$, let $Hx = \{hx \mid h \in H\}$.

Claim 1 If x and y are in G with $Hx \cap Hy$ non-empty, then $Hx = Hy$.

Pf suppose $h_1x = h_2y$ for $h_i \in H$. We show $Hx \subseteq Hy$. A typical element of Hx is hx for $h \in H$. We see $hx = h_1 h_1^{-1} h_2 y \in Hy$. Now we show $Hy \subseteq Hx$. A typical element of Hy is hy for some $h \in H$. We see $hy = h h_2^{-1} h_1 x \in Hx$.

Claim 2 There exist $x_1, \dots, x_r \in H$ with every element of G in exactly one of the cosets $Hx_1, Hx_2, \dots, Hx_r$. Pf Start with $x_1 = id$. Find as many mutually disjoint cosets $Hx_1, \dots, Hx_r$ as possible. Observe $G = Hx_1 \cup \dots \cup Hx_r$. Otherwise, there exists $x \in G$ with $x \notin Hx_1 \cup \dots \cup Hx_r$. We see from Claim 1 that $Hx_1, \dots, Hx_r, Hx$ are mutually disjoint. This contradicts the hypothesis that $Hx_1, \dots, Hx_r$ is as large a mutually disjt set of cosets as possible. Thus $G = Hx_1 \cup \dots \cup Hx_r$

Claim 3 $|H| = |Hx|$ for all $x \in G$.

Pf Consider the function $\varphi: H \to Hx$ given by $\varphi(h) = hx$. We see φ is 1-1 (if $\varphi(h_1) = \varphi(h_2)$ then $h_1x = h_2x$ $\therefore h_1 = h_2$) and onto. So H + Hx have been put in a one-to-one correspondence.

Thus $|H| = |Hx|$

G has been partitioned into r disjoint sets. Each set has $|H|$ elements. $\therefore$ $|G| = r|H|$.