69 ~~60~~

4. DEFINE *normal subgroup.*

The subgroup N of the group G is <u>normal</u> if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

8

5. STATE Lagrange's Theorem. If H is a subgroup of the finite group G, then then $|H| \mid |G|$.

<u>Proof</u> Observe that if two right cosets Hx_1 & Hx_2 have any elements in common, then $Hx_1 = Hx_2$. (If $h_1x_1 = h_2x_2$, then $Hx_1 \subseteq Hx_2$ because $hx_1 = hh_1^{-1}h_2x_2 \in Hx_2$ and $Hx_2 \subseteq Hx_1$ because $hx_2 = hh_2^{-1}h_1x_1 \in Hx_1$.) It follows that we may find $x_1, \dots, x_r \in G$ so that G is the disjoint union of $Hx_1 \cup \dots \cup Hx_r$.
Observe that H and Hx have the same number of elements for each coset Hx. (The function $H \to Hx$, which is given by $h \mapsto hx$, is one to one and onto.) Thus $|G| = |H|r$.

6. STATE the lemma from number theory about linear combinations and greatest common divisors. Let d be the greatest common divisor of the integers m and n. Then there exist integers a and b with $am+bn = d$.

<u>Proof</u> Let $H = \{am+bn \mid a \text{ and } b \in \mathbb{Z}\}$. It is easy to check that H is a subgroup of $\mathbb{Z}$, and therefore, H is a cyclic group. (see Problem 9) Let h generate H. Since $h \in H$, we have integers a and b with $h = am+bn$. The gcd of m and n divides both m and n so $d \mid h$. On the other hand, m and n are both in H so h divides m and h divides n. Thus h is a common divisor of m and n and therefore $h \le$ the greatest common divisor of m and n. so $h \le d$ and $d \mid h$ with d and h both positive. This can happen only if $h = d$ and therefore $d \in H$ so $d = am+bn$ for some integers a and b.