Proof of Lagrange's theorem:

The left cosets partition $G$.
(By #1 and 3 from yesterday)

Say there are $r$ left cosets
so $G = a_1H \cup a_2H \cup \ldots \cup a_rH$
But by #5, \( |\alpha_i + \Pi| = |\Pi| \neq i \)

So \( |G| = \sum |\alpha_i + \Pi| = r \cdot \Pi \)

\[ \Rightarrow |G| = r |\Pi| \]

\[ \Rightarrow |\Pi| |G| \quad \text{and} \quad |G : \Pi| = \frac{|G|}{|\Pi|} \]
eg if $|G| = 30$, and $H \leq G$,

then $|H| = 31, 2, 3, 5, 6, 10, 15, 30$.

Cor 1. $|a| \mid |G|$  \hspace{1cm} n \mid 16!$, doesn't mean $G$ has an element of order $n$.

Since $|a| = |<a>|$ and $<a> \leq G$.

\textbf{Note} just because $n \mid 16!$ doesn't mean $G$ has a subgroup of order $n$.

eg $G = \text{binary strings of length } n$ under $+$. 
Cor 2. if $|G|$ is prime, the $G$ is cyclic. Reason: if $x \neq e$, $x \in G$ then $|x| \mid |G|$, but $|G|$ is prime so $|x| = |G|$, so $\langle x \rangle = G$

Cor 3. $a^{|a|} = e \quad \forall \ a \in G$

since $|a| \mid |G|$, so $a^{|a|} = e^{k \cdot |a|} = e^{|a|} = e$
Cor. 4. (Fermat’s little theorem)

\[ \forall a \in \mathbb{Z}, \forall p \text{ prime}, \]
\[ a^p \mod p = a \mod p \]

Proof: \[ a = pm + r \quad w/ 0 \leq r < p \]

So \[ a = r \mod p, \quad a^p \mod p = r^p \mod p \]
Thus it suffices to show that
\[ r^p \mod p = r \mod p \quad \text{for } 0 \leq r < p \]
If \( r = 0 \), we're done.
Otherwise, \( r \in U(p) = \{1, \ldots, p-1\} \)
since \( p \) is prime.
by Cor 3,
\[ r \mid u(p) \]
\[ r^{|u(p)|} = 1 \]

\[ \Rightarrow r^{p-1} = 1 \Rightarrow r^{p-1} \cdot r = r \in U(p) \]

\[ r^p = r \mod u(p) \text{ where we reduce mod } p \]
so \[ r^p = r \mod p \]

\[ \checkmark (\Rightarrow a^p \mod p = a \mod p) \]
Def: Let $G \leq S_R$ where $R$ is a set.

$S_R$ is the group of permutations on a set $R$, and $G$ is a subgroup of $S_R$, i.e. it is a group of permutations on $R$.

The stabilizer of $i \in R$ is

$\text{Stab}_G(i) = \{ \phi \in G \mid \phi(i) = i \}$

(note these are elements of $G$)

The orbit of $i \in R$ under $G$ is

$\text{Orb}_G(i) = \{ \phi(i) \mid \phi \in G \}$

(note $\text{Orb}_G(i)$ is a subset of $R$)