**Last time:** Classified gps H order $p^2$

**Sylow Thms**

C a finite gp, $|G| = p^e m$ with $e \geq 1$ an int and $p \nmid m$.

A Sylow $p$ subgp of $G$ is a subgp $H$ of $G$ with order $p^e$.

**Thm 1** If $G$ has size $p^e m$ with $e \geq 1$ and $\gcd(p, m) = 1$, then $G$ contains a subgp $H$ of order $1H1 = p^e$.

**Cor** Suppose $p \mid |G|$. Then $\exists x \in G$ with $\ord(x) = p$.

**Pf:** Let $H \subseteq G$ be a sylow $p$ subgp. Then $1H1 = p^e$.

HW question $\Rightarrow$ $H$ contains elt $A$ order $p$.

$y \in H$ arbitrary w/ $y \neq 1$. Then $\ord(y) = p^c$ for some $c$.

$x = y^{p^c}$ has order $p$.

**Thm 2** $G$ a finite gp w/ $p \mid |G|$, 

a) The Sylow $p$ subgps of $G$ are all conjugate

b) Every $p$- subgp of $G$ is contained in some Sylow $p$- subgp
Cor: If there is just one Sylow \( p \)-subgroup \( H \) of \( G \), then \( H \) must be normal.

**Thm 3** \( |G| = p^e m \) with \( \gcd(p, m) = 1 \). Let \( S \) denote

the number of Sylow \( p \)-subgroups. Then

\* \( S \) divides \( m \)
\* \( S \equiv 1 \mod p \).

**Cor** Suppose \( |G| = p^e q \) with \( p, q \) distinct primes, and \( p > q \).

Then \( G \cong C_p \times C_q \).

**Pf:** Let \( H \) be a Sylow \( p \)-subgroup.

Let \( K \) be a Sylow \( q \)-subgroup.

The \# of Sylow \( p \)-subgroups \( \equiv 1 \mod p \) and \( \) divides \( q \).

\[ \Rightarrow \text{\# of Sylow } p \text{-subgroup } = 1 \Rightarrow H \text{ is normal.} \]

Now \( H \cdot K = \mathbb{S}_3 \) b/c any \( e \) in \( H \cdot K \) has order dividing \( p \) and \( q \).

Moreover \( \text{mult: } H \times K \to G \) is bijective.

\( \text{b/c it's injective b/c } H \cdot K = \mathbb{S}_3 \) and both sides have size \( pq \).

\[ \Rightarrow G = H \times K, \text{ f: } K \to \text{Aut}(H) \text{ (action of } K \text{ on } H) \text{ by conjugation} \]

\[ \cong C_p \times C_q. \]
What are the possible actions of $C_q$ on $C_p$?

**Prop.** $\text{Act}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^X$

**Pf:** Suppose $r \in (\mathbb{Z}/n\mathbb{Z})^X$. Define

$$\phi_r : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

as $\phi_r(k) = r \cdot k$.

$\phi_r$ is a gp homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ because

$$\phi_r(k + k') = r(k + k') = r \cdot k + r \cdot k' = \phi_r(k) + \phi_r(k')$$

Also, $\phi_r$ is an isomorphism $\iff r \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $rs \equiv 1 \text{ mod } n$.

Then $\phi_s \circ \phi_r = \phi_r \circ \phi_s : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the identity map.

Conversely, suppose $r \in \text{Act}(\mathbb{Z}/n\mathbb{Z})$.

Then $\phi(1) = r$ for some $r \in \mathbb{Z}/n\mathbb{Z}$.

$\phi$ gp hom $\iff \phi(k) = r \cdot k \ \forall k \in \mathbb{Z}/n\mathbb{Z}$.

$\phi$ bijective $\iff \exists s \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\phi(s) = 1$.

But, $\phi(s) = rs \equiv 1 \text{ mod } n$.

$\implies r \in (\mathbb{Z}/n\mathbb{Z})^\times$. 
Finally, the bijection $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ is a group.

$C_m \cong C_n$ by gp homom.

$\phi: C_m \rightarrow \text{Aut}(C_n) = (\mathbb{Z}/n\mathbb{Z})^*$

$\{1, y, y^2, \ldots, y^{m-1}\}$

There is a bijective correspondence between

$\{\text{actions of } C_m \text{ on } C_n \text{ by gp homomorphisms}\}
\leftrightarrow
\{\text{elts } r \in (\mathbb{Z}/n\mathbb{Z})^* \text{ with } r^m \equiv 1 \mod n\}$

*Proof:* If $r \in (\mathbb{Z}/n\mathbb{Z})^*$ with $r^m \equiv 1 \mod n$, then

$C_m \cong C_n \text{ via } y^j \ast (k) = r^j k. \quad \forall \in C_m \in \mathbb{Z}/n\mathbb{Z}$

*Example:* $C_7 \not\cong C_3$ with $\phi: C_3 = \langle y, y^2 \rangle \rightarrow \text{Aut}(\mathbb{Z}/7\mathbb{Z})$

$\phi(y) = 2$

Also: $\phi(y) = 4$
Cor: a) Every gp of order 15 is cyclic.

b) There are two isom class of gps of order 6, namely $S_3$ and $C_3 \times C_2 \cong C_6$.

c) There are two isom class of gps of order 21, namely $C_7 \times C_3 \cong C_{21}$ and $C_7 \times C_3 \cong C_{21}$ with $\phi$ as in the example above.

Pf: a) $G$ a gp of order 15.

- $G \cong C_5 \times C_3$.

However: $\phi : C_3 \rightarrow \text{Aut}(C_5) = \left( C_3 \right)^{\times} / \text{size 3}$

has size 4

must be trivial

$\Rightarrow G \cong C_5 \times C_3 \cong C_{15}$

b) $G$ a gp of order 6.

- $G \cong C_3 \times C_2$.

$\phi : C_2 \rightarrow \text{Aut}(C_3) = \left( C_3 \right)^{\times} / \text{cycle of order 2}$

If $\phi$ is trivial, $G \cong C_3 \times C_2$

If $\phi$ is non-trivial, $G \cong C_3 \times C_2 \Rightarrow G \cong S_3$.

Recall: $D_2 \cong S_2$, also $D_n \cong C_n \times C_2$. 
Recall $D_3 \cong S_3$, also $D_n \cong C_n \times C_2$

c) $G$ has order 21. Then $G \cong C_7 \times C_3$

$\phi : C_3 = \{1, y, y^2\} \rightarrow \left( \mathbb{Z}/7\mathbb{Z} \right)^*$$

Possible $\phi$'s:
- $\phi(y) = 1$ \& $\phi$ trivial
  - $\phi(y) = 2$
  - $\phi(y) = 4$

First case, $\phi$ trivial, given $G \cong C_7 \times C_3 \times C_{21}$

Claim: Find two $\phi$'s give non-abelian group

Proof: Define $y' = y^2$ in $C_7$.

Then $C_7 = \{1, y, y^2, \ldots, y^6\} = \{1, y', (y')^2\}$.

If $\phi(y) = 4$ then $\phi(y') = \phi(y^2) = 2$.

$\Rightarrow C_7 \times \{1, y, y^2\} \cong C_7 \times \{1, y, y^2\}$. (1)

\[ \phi(y) = 4 \]
\[ \phi'(y') = 2 \]