Last time, let $H, N$ be two groups with $H$ acting on $N$ by group homomorphisms: we have an action $H \times N \to N$

$$a \cdot (n_1, n_2) = (a \cdot n_1, a \cdot n_2) \quad \forall n_1, n_2 \in N, a \in H$$

Then the binary operation $\ast : (N \times H) \times (N \times H) \to N \times H$

$$(n_1, a_1) \ast (n_2, a_2) = (n_1 a_1, a_1 a_2), \quad a_1, a_2$$

is associative and makes the set $N \times H$ into a group.

Example: $H = \text{GL}(n, \mathbb{R}), \ N = \mathbb{R}^n, \ A \ast V = AV \ \forall A \in \text{GL}(n, \mathbb{R}), V \in \mathbb{R}^n$

$$\mathbb{R}^n \times \text{GL}(n, \mathbb{R}) \simeq \{ \begin{pmatrix} A & V \\ 0 & 1 \end{pmatrix} \in \text{GL}(n+1, \mathbb{R}) \mid A \in \text{GL}(n, \mathbb{R}) \}$$

The group of affine transformations of $\mathbb{R}^n$.

Example: $H = \text{O}(n), \ N = \mathbb{R}^n$

$$\mathbb{R}^n \times \text{O}(n) = \{ \begin{pmatrix} A & V \\ 0 & 1 \end{pmatrix} \in \text{GL}(n+1, \mathbb{R}) \mid A \in \text{O}(n) \}$$

The group of rigid motions of $\mathbb{R}^n$

$$T : \mathbb{R}^n \to \mathbb{R}^n \mid \|T_x - T_y\|_2 = \|x - y\|_2 \quad \forall x, y \in \mathbb{R}^n$$

Here $\|x\|_2 = \sqrt{\sum x_i^2}$, the Euclidean distance.

Example: let $G$ be any abelian group. Then

$$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} \quad \forall a, b \in G$$

$\Rightarrow \text{inv} : G \to G, \ a \mapsto a^{-1}$ is an isomorphism.

$$(a^{-1})^{-1} = a \quad \forall a \in G. \Rightarrow \text{inv} \circ \text{inv} = \text{id}$$

$\Rightarrow \text{inv} \in \text{Aut}(G)$ has order $2$.

$\Rightarrow$ we get a action of $\mathbb{Z}_2$ on $G$ by

$$[k] \ast a = a^k \quad \forall a \in G, \ k \in \mathbb{Z}_2 \subseteq \{1, 0\}$$

We get a semidirect product $G \rtimes \mathbb{Z}_2$ with multiplication

$$(a, [k]) \ast (b, [k]) = (a b^{-1}, [k + k])$$

Note: if $G = \mathbb{Z}_n$, $\mathbb{Z}_n \rtimes \mathbb{Z}_2 \simeq D_n$
Reason
Let \( p = (1,1), \tau = (10,11), \tau^2 = (10,01) \)
\[
p^n = (n,1), (01) = (n,0) = (0,0) = (01,01)
\]
\[
\tau \times p = (10,11) \times (11,00) = (10,11)(11,00) = (11,10) = (1,1,01)
\]
\[
p^{-1} \times \tau = (11,10) \times (01,1) = (11,10)(01,1) = (11,01) = (11,01)
\]
So \( \tau \times p = p^{-1} \times \tau \).

Our next goal: Sylow theorems

Recall A group \( G \) acts on itself by conjugation \( g \cdot x = gxg^{-1} \), \( x \in G \).
Equivalently, we have a homomorphism \( c : G \rightarrow \text{Aut}(G) \), \( g \mapsto c_g \) where \( c_g(x) = gxg^{-1} \).

Note If \( H \) is a subgroup of \( G \), then \( \forall g \in G \)
\[
c_g(H) = \{ ghg^{-1} \mid h \in H \} = c_h(H)
\]
Also a subgroup of \( G \) (and \( c_g : H \rightarrow c_g(H) \) is an iso)

Definition Two subgroups \( H_1, H_2 \leq G \) are conjugate \( \text{(in } G \text{)} \)
if \( \exists g \in G \) such that \( gH_1g^{-1} = H_2 \)

Definition Let \( H \) be a subgroup of \( G \). The normalizer \( N_G(H) \) of \( H \) in \( G \) is
\[
N_G(H) = \{ g \in G \mid gHg^{-1} = H \}
\]
Note \( G \) acts on \( \mathcal{P}(G) = \) the set of subsets of \( G \) by \( g \cdot S = gSg^{-1} = c_g(S) \).
\[
N_G(H) = \{ g \in G \mid gH = H \} = \text{stab}(H)
\]
\( \therefore N_G(H) \) is a subgroup of \( G \). Also \( \forall g \in N_G(H) \)
\[
gHg^{-1} = H \Rightarrow H \leq N_G(H) \)
Definition: Let G be a finite group, p prime, \( |G| = p^n m \), \( \text{gcd}(p, m) = 1 \).

A subgroup \( P \) of \( G \) is a Sylow \( p \)-subgroup if \( |P| = p^n \).

If \( H \) is a subgroup of \( G \) and \( |H| = p^k \) then \( H \) is called a \( p \)-subgroup of \( G \).

Remark: If \( H \leq G \), \( |G| = p^n m \), and \( |H| = p^k \) then \( p^k \mid p^n m \).

Lagrange's theorem. So \( p \)-Sylow subgroups are the largest \( p \)-subgroups.

Theorem (Sylow theorems #1, 2 and 3): Let \( G \) be a finite group, \( p \) prime, \( p \mid |G| \).

1) If \( p^k \mid |G| \) then \( G \) has a subgroup \( H \) with \( |H| = p^k \).

In particular, \( p \)-Sylow Theorem exact.

2) Let \( H \leq G \) be a \( p \)-subgroup, \( P \) a \( p \)-Sylow subgroup of \( G \). Then \( \exists a \in G \) s.t. \( aHa^{-1} \subseteq P \). In particular, any two \( p \)-Sylow subgroups are conjugate.

3) Let \( n_p = \# \) of \( p \)-Sylow subgroups of \( G \), \( P \leq G \) a \( p \)-Sylow subgroup.

Then (i) \( n_p \mid [G : P] = |G/P| \)

(ii) \( n_p = 1 \mod p \)

(iii) \( n_p = [G : N_G(P)] \) where \( N_G(P) = \) the normalizer of \( P \) in \( G \).  

Example: Suppose \( p, q \) are two primes with \( p > q \). Then

(i) if \( q \mid (p-1) \) then any group \( G \) of order \( pq \) is cyclic.

(ii) if \( q \mid (p-1) \) then any group \( G \) of order \( pq \) is either cyclic or isomorphic to \( \mathbb{Z}_p \times \mathbb{Z}_q \). (for some action of \( \mathbb{Z}_q \) on \( \mathbb{Z}_p \)).

Proof: Let \( G \) be a group with \( |G| = pq \).

By Cauchy's Theorem, \( G \) has elements of order \( p \) and of order \( q \).

\( \Rightarrow \exists \) subgroups \( P, Q \) of \( G \) of order \( p \) and \( q \), respectively.
\[ P n Q < P \text{ and } P n Q < G. = | P n Q | \varphi \text{ and } | P n Q | \psi. \]

Since \( p, q \) are distinct primes, \( | P n Q | = 1 \).

\[ n_p | [G:p] = p^q = q \rightarrow n_p = q \text{ or } 1. \]

But \( n_p \equiv 1 \text{ mod } p \) and \( q < p \). So \( n_p \neq q \). \( \therefore \) \( n_p = 1 \).

\( P \) is a unique \( p \)-Sylow subgroup of \( G \).

\( P \) in a unique \( p \)-Sylow subgroup of \( G \).

On the other hand, \( \forall g \in G \), \( g P g^{-1} \) is also a \( p \)-Sylow \( \rho \)-subgroup of \( G \).

\[ \rightarrow g P g^{-1} = \rho \forall g \in G, \text{ i.e. } P \triangleleft G. \]

Consider \( f: P \times Q \rightarrow G, f(a,b) = ab. \]

\[ f(a_1, b_1) = f(a_2, b_2) \Rightarrow a_1 b_1 = a_2 b_2 \Rightarrow a_2^{-1} a_1 = b_2 b_1^{-1} \in P n Q. \]

\( \therefore \) \( f \) is injective. Since \( | P \times Q | = | P | \times | Q | = pq \text{ and } | G | = pq \).

\( f \) is a bijection. \( \Rightarrow G = P Q. \)

We've seen: \( G = PQ, P \triangleleft G \) and \( P n Q = \{ e \} \). \( \Rightarrow G \cong P \times Q. \)

\( \therefore \) \( G \cong Z_p \times Z_q \), for some homomorphism \( \mu: Z_q \rightarrow Aut(Z_p). \)

Note: \( ker \mu < Z_q \) so \( | ker \mu | | q \Rightarrow ker \mu = Z_q \text{ or } 1(0) \).

If \( ker \mu = Z_q \), \( \forall 1k \in Z_q, \forall 1l \in Z_p \text{ and } \mu(1k)(1l) = \mu((kl)) = \mu(1) = 1 \).

\( \Rightarrow Z_p \times Z_q \cong Z_p \times Z_q \cong Z_{pq}. \)

If \( | ker \mu | = 1, \mu \) is injective. \( \Rightarrow \mu(Z_q) = Z_q \).

\( \Rightarrow q = | Z_q | = | \mu(Z_q) | | Aut(Z_p) |. \)

\textbf{Homework}: \( \forall n \text{ } Aut(Z_n) = Z_n^\times = \{ k | k \in Z_n \text{ and } [k][k] = 1 \text{ for some } i \in Z_n \}. \)

\( \Rightarrow | Aut(Z_p) | = | Z_p^\times | = p - 1. \)

So \( q \neq (p - 1), \mu \) cannot be injective. \( \Rightarrow \mu((Z_q)) = 1 \).

\( \Rightarrow G \cong Z_{pq}. \)