Lecture 19
Sylow’s Theorems
Last time:

Definition
Let $G$ be a group with $|G| = p^\alpha m$, where $p$ is prime and $p \nmid m$. A subgroup of order $p^\alpha$ is called a **Sylow $p$-subgroup** of $G$. $\text{Syl}_p(G)$ is the set of Sylow $p$-subgroups and $n_p = n_p(G) = |\text{Syl}_p(G)|$.

Theorem (Sylow’s Theorem)

1. **Sylow $p$-subgroups of $G$ exist**, i.e. $\text{Syl}_p(G) \neq \emptyset$.
2. **If $P$ is a Sylow $p$-subgroup of $G$ and $Q$ is any $p$-subgroup of $G$, then $Q$ is contained in some conjugate of $P$. In particular, any two Sylow $p$-subgroups of $G$ are conjugate in $G$.**
3. **The number of Sylow $p$-subgroups of $G$ satisfies**

   $$n_p \equiv 1 \pmod{p}, \quad \text{and} \quad n_p = |G : N_G(P)|$$

   for any Sylow $p$-subgroup $P$. 
More from last time:

**Corollary**

Let $P$ be a Sylow $p$-subgroup of $G$. Then the following are equivalent:

1. $P$ is the unique Sylow $p$-subgroup of $G$, i.e., $n_p = 1$.
2. $P$ is normal in $G$.
3. $P$ is characteristic in $G$ (from the exam!)
4. All subgroups generated by elements of the $p$-power order are $p$-groups, i.e. if $X \subseteq G$ such that $|x|$ is a power of $p$ for all $x \in X$, then $\langle X \rangle$ is a $p$-group.
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

**Claim:** If $q \not\equiv 1 \pmod{p}$, then $G \cong Z_{pq}$. 
Back to $|G| = pq$

Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

**Claim:** If $q \not\equiv 1 \pmod{p}$, then $G \cong Z_{pq}$.

**Proof.**
Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$.
Always, $n_q = 1$ so $Q \trianglelefteq G$. Since $n_p \mid q$, either $n_p = q$ or 1.
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

**Claim:** If $q \not\equiv 1 \pmod{p}$, then $G \cong Z_{pq}$.

**Proof.**

Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$. Always, $n_q = 1$ so $Q \trianglelefteq G$. Since $n_p \mid q$, either $n_p = q$ or $1$.

If $q \not\equiv 1 \pmod{p}$, then $p = 1$. So $P \trianglelefteq G$. 
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

**Claim:** If $q \not\equiv 1 \pmod{p}$, then $G \cong Z_{pq}$.

**Proof.**

Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$.

Always, $n_q = 1$ so $Q \trianglelefteq G$. Since $n_p \mid q$, either $n_p = q$ or 1.

If $q \not\equiv 1 \pmod{p}$, then $p = 1$. So $P \trianglelefteq G$.

Let $P = \langle x \rangle$ and $Q = \langle y \rangle$.

Then $x^{-1}y^{-1}xy \in P \cap Q = 1$ (so $PQ = QP$ has order $pq$).
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

**Claim:** If $q \not\equiv 1 \pmod{p}$, then $G \cong Z_{pq}$.

**Proof.**

Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$.

Always, $n_q = 1$ so $Q \trianglelefteq G$. Since $n_p | q$, either $n_p = q$ or 1.

If $q \not\equiv 1 \pmod{p}$, then $p = 1$. So $P \trianglelefteq G$.

Let $P = \langle x \rangle$ and $Q = \langle y \rangle$.

Then $x^{-1}y^{-1}xy \in P \cap Q = 1$ (so $PQ = QP$ has order $pq$).

So $|xy| = pq$ and so $G \cong Z_{pq}$. 

$\square$
Direct products

Recall that the direct product of two groups \((G, \star)\) and \((H, \diamond)\) is

\[
G \times H = \{(g, h) \mid g \in G, h \in H\}
\]

with multiplication

\[
(g, h)(g', h') = (g \star g', h \diamond h').
\]
Direct products

Recall that the direct product of two groups \((G, \star)\) and \((H, \diamond)\) is

\[
G \times H = \{(g, h) \mid g \in G, h \in H\}
\]

with multiplication

\[
(g, h)(g', h') = (g \star g', h \diamond h').
\]

You showed that \(G \times (H \times K) \cong (G \times H) \times K\), so we can easily talk about the direct product of a finite collection of groups

\[
(G_1, \star_1), (G_2, \star_2), \ldots, (G_n, \star_n).
\]
Direct products

Recall that the direct product of two groups \((G, \star)\) and \((H, \Diamond)\) is

\[ G \times H = \{(g, h) \mid g \in G, h \in H\} \]

with multiplication

\[(g, h)(g', h') = (g \star g', h \Diamond h').\]

You showed that \(G \times (H \times K) \cong (G \times H) \times K\), so we can easily talk about the direct product of a countable collection of groups

\[(G_1, \star_1), (G_2, \star_2), \ldots \]
Direct products

Recall that the direct product of two groups \((G, \star)\) and \((H, \diamond)\) is

\[G \times H = \{(g, h) \mid g \in G, h \in H\}\]

with multiplication

\[(g, h)(g', h') = (g \star g', h \diamond h').\]

You showed that \(G \times (H \times K) \cong (G \times H) \times K\), so we can easily talk about the direct product of a countable collection of groups

\[(G_1, \star_1), (G_2, \star_2), \ldots\]

Proposition

If \(G_1, \ldots, G_n\) are groups, their direct product is a group of order \(|G_1||G_2| \ldots |G_n|\).
Proposition

Let \( G_1, G_2, \ldots, G_n \) groups and let \( G = G_1 \times G_2 \times \cdots \times G_n \).

1. For each fixed \( i \), the set
   \[
   \{(1, \ldots, 1, \underbrace{g}_{i^{th} \text{ component}}, 1, \ldots, 1) \mid g \in G_i\} \subseteq G
   \]
   is a normal subgroup isomorphic to \( G_i \) with
   \[
   G/G_i \cong G_1 \times \cdots G_{i-1} \times G_{i+1} \times G_n.
   \]
Proposition

Let $G_1, G_2, \ldots, G_n$ groups and let $G = G_1 \times G_2 \times \cdots \times G_n$.

1. For each fixed $i$, the set
\[
\{(1, \ldots, 1, g, 1, \ldots, 1) \mid g \in G_i\} \subseteq G
\]

is a normal subgroup isomorphic to $G_i$ with
\[
G/G_i \cong G_1 \times \cdots G_{i-1} \times G_{i+1} \times G_n.
\]

2. For each fixed $i$ define the projection
\[
\pi_i : G \to G_i \quad \text{by} \quad (g_1, \ldots, d_n) \mapsto g_i.
\]
Then $\pi_i$ is a surjective homomorphism with
\[
\ker \pi_i = \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots g_n \mid g_j \in G_j\} \cong G/G_i.
\]
Proposition

Let $G_1, G_2, \ldots, G_n$ groups and let $G = G_1 \times G_2 \times \cdots \times G_n$.

1. For each fixed $i$, the set
   $$\{(1, \ldots, 1, g_{i}, 1, \ldots, 1) \mid g \in G_i\} \subseteq G$$
   is a normal subgroup isomorphic to $G_i$ with
   $$G/G_i \cong G_1 \times \ldots G_{i-1} \times G_{i+1} \times G_n.$$

2. For each fixed $i$ define the projection
   $$\pi_i : G \to G_i \text{ by } (g_1, \ldots, d_n) \mapsto g_i.$$
   Then $\pi_i$ is a surjective homomorphism with
   $$\ker \pi_i = \{(g_1, \ldots g_{i-1}, 1, g_{i+1}, \ldots g_n | g_j \in G_j\} \cong G/G_i.$$

3. If $x \in G_i$ and $y \in G_j$ for some $i \neq j$ then $xy = yx$. 
Definition

1. A group $G$ is **finitely generated** if there is a finite subset $A$ of $G$ such that $G = \langle A \rangle$. 
Definition

1. A group $G$ is **finitely generated** if there is a finite subset $A$ of $G$ such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of $r$ copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the **free abelian group of rank** $r$. 

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)

Let $G$ be a finitely generated abelian group. Then

1. $G \cong \mathbb{Z}^{r_1} \times \mathbb{Z}^{n_1} \times \cdots \times \mathbb{Z}^{n_s}$ for some integers $r_1, n_1, \ldots, n_s$ such that $r_1 \geq 0$ and $n_1 | n_2 | \cdots | n_s$.

2. The expression in (1) is unique.
Definition

1. A group $G$ is **finitely generated** if there is a finite subset $A$ of $G$ such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of $r$ copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the **free abelian group of rank** $r$.

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)

*Let $G$ be a finitely generated abelian group. Then*

1. $$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$
   *for some integers $r, n_1, \ldots, n_s$ such that $r \geq 0$ and $2 \leq n_1 | n_2 | \cdots | n_s$.***
Definition

1. A group $G$ is finitely generated if there is a finite subset $A$ of $G$ such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of $r$ copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the free abelian group of rank $r$.

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)

Let $G$ be a finitely generated abelian group. Then

1. 

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

for some integers $r, n_1, \ldots, n_s$ such that $r \geq 0$ and $2 \leq n_1 | n_2 | \cdots | n_s$.

2. The expression in (1) is unique.