Last time: Centralizers and conjugacy classes

Let $G$ act on itself by conjugation, and let $a \in G$. Denote by $\mathcal{K}_a$ the conjugacy class in $G$ containing $a$.

We had

$$\mathcal{K}_g = \{ \text{elements of } G \text{ conjugate to } g \}$$

$$|\mathcal{K}_g| = |G : C_G(g)|$$

$$|G| = \sum_{g \in G} |G : C_G(g)|$$

(where $G$ a set of distinct representatives of the conjugacy classes)

Note that for all $z \in Z(G)$, we have $|\mathcal{K}_g| = 1$, and so $|G : G_z| = 1$.

Theorem (Class equation)

The size of any conjugacy class $\mathcal{K}_a$ is equal to the index of $C_G(a)$, and therefore

$$|G| = |Z(G)| + \sum_{a_i \in A} |G : C_G(a_i)|,$$

where $A$ is a set of distinct representatives of the conjugacy classes.
Two powerful pieces of information when used together for finite groups:

1. \(|G| = |Z(G)| + \sum_{a_i \in A} |G : C_G(a_i)|\) (class equation), and
2. \(|Z(G)|\) and \(|G : C_G(a_i)|\) divide \(|G|\) (Lagrange).

For example:

**Theorem**

*If \(G\) is a group with \(|G| = p^\alpha\) for \(p\) prime and \(\alpha > 1\), then \(G\) has non-trivial center.*

**Corollary**

*If \(|G| = p^2\), then \(G\) is abelian. More precisely, \(G \cong Z_{p^2}\) or \(G \cong Z_p \times Z_p\).*
Last time: Sylow $p$-subgroup

Definition
Let $G$ be a group and let $p$ be a prime.

1. A group of order $p^\alpha$ for some $\alpha \geq 0$ is called a $p$-group. Subgroups of $G$ that are $p$-groups are called $p$-subgroups.

2. If $G$ is a group of order $p^\alpha m$ where $p \nmid m$, then a subgroup of order $p^\alpha$ is called a Sylow $p$-subgroup of $G$.

3. The set of Sylow $p$-subgroups of $G$ will be denoted by $\text{Syl}_p(G)$ and the number of Sylow $p$-subgroups of $G$ will be denoted by $n_p(G)$ (or just $n_p$ when $G$ is clear from context).

Example: Consider $D_{12}$: $|D_{12}| = 12 = 2^2 \cdot 3$ and $D_{12}$ has subgroups

$\langle r^3, s \rangle$  $\langle r^3, sr \rangle$  $\langle r^3, sr^2 \rangle$  of order 4

and

$\langle r^2 \rangle$  of order 3
Suppose \( |G| = p^\alpha m \), where \( p \) is prime and \( p \nmid m \). Let 
\( \text{Syl}_p(G) = \{ P \leq G \mid |P| = p^\alpha \} \) and \( n_p = n_p(G) = |\text{Syl}_p(G)| \).

Last time:

**Lem.** Let \( P \in \text{Syl}_p(G) \). If \( Q \) is any \( p \)-subgroup of \( G \), then 
\( Q \cap N_G(P) = Q \cap P \).

**Thm.** If \( G \) is a finite abelian group and \( p \) is a prime divisor of \( |G| \), then \( G \) contains an element of order \( p \).

**Theorem (Sylow’s Theorem)**

1. Sylow \( p \)-subgroups of \( G \) exist, i.e. \( \text{Syl}_p(G) \neq \emptyset \).
Suppose $|G| = p^\alpha m$, where $p$ is prime and $p \nmid m$. Let $\text{Syl}_p(G) = \{P \leq G \mid |P| = p^\alpha\}$ and $n_p = n_p(G) = |\text{Syl}_p(G)|$.

**Last time:**

**Lem.** Let $P \in \text{Syl}_p(G)$. If $Q$ is any $p$-subgroup of $G$, then $Q \cap N_G(P) = Q \cap P$.

**Thm.** If $G$ is a finite abelian group and $p$ is a prime divisor of $|G|$, then $G$ contains an element of order $p$.

**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 $P$. 
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 $G$, meaning it is set-wise fixed by any automorphism of $G$.
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.
Example

Let $G$ be a finite group and let $p$ be a prime.

1. If $p 
mid |G|$, the Sylow $p$-subgroup of $G$ is the trivial group.
   If $|G| = p^\alpha$, $G$ is the unique Sylow $p$-subgroup of $G$. 
Example

Let $G$ be a finite group and let $p$ be a prime.

1. If $p \nmid |G|$, the Sylow $p$-subgroup of $G$ is the trivial group. If $|G| = p^\alpha$, $G$ is the unique Sylow $p$-subgroup of $G$.

2. A finite abelian group has unique Sylow $p$-subgroup for each prime $p$. This subgroup consists of all elements $x$ whose order is a power of $p$. This is sometimes called the $p$-primary component of the abelian group.
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$. 

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

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

Since $n_q = 1 + kq$ and $n_q | p$, we must have $k = 0$. So $Q \leq G$. 

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

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

Since $n_q = 1 + kq$ and $n_q \mid p$, we must have $k = 0$. So $Q \trianglelefteq G$.

Now, since $n_p \mid q$, either $n_p = q$ or 1.
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

Let $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_p(G)$.

Since $n_q = 1 + kq$ and $n_q \mid p$, we must have $k = 0$. So $Q \subseteq G$.

Now, since $n_p \mid q$, either $n_p = q$ or $1$.

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

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

Then $x^{-1}y^{-1}xy \in P \cap Q = 1$. 
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.

Let $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_p(G)$.

Since $n_q = 1 + kq$ and $n_q \mid p$, we must have $k = 0$. So $Q \trianglelefteq G$.

Now, 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 $|xy| = pq$ and so $G \cong Z_{pq}$.
Let $|G| = pq$ with $p$ and $q$ prime with $p < q$.
Let $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_p(G)$.
Since $n_q = 1 + kq$ and $n_q \mid p$, we must have $k = 0$. So $Q \trianglelefteq G$.

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

Otherwise, $p \mid q - 1$ and we can use this to build a non-abelian group of order $pq$. 
Direct products

Let

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

be groups. Then the **direct product** of these groups is the set

\[G_1 \times G_2 \times \cdots = \{(g_1, g_2, \ldots) \mid g_i \in G\}\]

with binary operation

\[(g_1, g_2, \ldots) \star (g'_1, g'_2, \ldots) = (g_1 \star_1 g'_1, g_2 \star_2 g'_2, \ldots).\]
Direct products

Let

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

be groups. Then the direct product of these groups is the set

\[G_1 \times G_2 \times \cdots = \{(g_1, g_2, \ldots) \mid g_i \in G\}\]

with binary operation

\[(g_1, g_2, \ldots) \star (g'_1, g'_2, \ldots) = (g_1 \star_1 g'_1, g_2 \star_2 g'_2, \ldots).\]

Once we’re comfortable with the fact that different coordinates have their own binary operations, we can stop writing the stars like before:

\[(g_1, g_2, \ldots)(g'_1, g'_2, \ldots) = (g_1g'_1, g_2g'_2, \ldots)\]

(unless \(\star_i\) is +, in which case you should still write +).
Direct products

Let

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

be groups. Then the direct product of these groups is the set

\[G_1 \times G_2 \times \cdots = \{(g_1, g_2, \ldots) \mid g_i \in G\}\]

with binary operation

\[(g_1, g_2, \ldots) \star (g'_1, g'_2, \ldots) = (g_1 \star_1 g'_1, g_2 \star_2 g'_2, \ldots).\]

Once we’re comfortable with the fact that different coordinates have their own binary operations, we can stop writing the stars like before:

\[(g_1, g_2, \ldots)(g'_1, g'_2, \ldots) = (g_1 g'_1, g_2 g'_2, \ldots)\]

(unless \(\star_i\) is \(+\), in which case you should still write \(+\)).

Proposition

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

Proposition

Let $G_1, \ldots, G_n$ be groups, and let $G = G_1 \times \cdots \times G_n$. Fix $i \in [n]$.

1. The set
   \[ \hat{G}_i = \{(1, \ldots, 1, \underbrace{g, 1, \ldots, 1}_{i^{th} \text{ component}}, 1, \ldots, 1) \mid g \in G_i\} \subseteq G \]
   is a normal subgroup isomorphic to $G_i$. Identify $G_i$ with this subgroup (i.e. just write $G_i$ instead of $\hat{G}_i$, even though they’re slightly different a priori). Then
   \[ G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times G_n. \]
Direct products

Proposition

Let $G_1, \ldots, G_n$ be groups, and let $G = G_1 \times \cdots \times G_n$. Fix $i \in [n]$.

(1) The set
$$\hat{G}_i = \{(1, \ldots, 1, \underbrace{g}_{i^{th} \text{ component}}, 1, \ldots, 1) \mid g \in G_i\} \subseteq G$$

is a normal subgroup isomorphic to $G_i$. Identify $G_i$ with this subgroup (i.e. just write $G_i$ instead of $\hat{G}_i$, even though they’re slightly different a priori). Then
$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times G_n.$$

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

Proposition

Let $G_1, \ldots, G_n$ be groups, and let $G = G_1 \times \cdots \times G_n$. Fix $i \in [n]$.

(1) The set

$$\hat{G}_i = \{(1, \ldots, 1, g, 1, \ldots, 1) \mid g \in G_i\} \subseteq G$$

is a normal subgroup isomorphic to $G_i$. Identify $G_i$ with this subgroup (i.e. just write $G_i$ instead of $\hat{G}_i$, even though they’re slightly different a priori). Then

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times G_n.$$  

(2) For each fixed $i$ define the projection

$$\pi_i : G \to G_i \text{ by } (g_1, \ldots, g_n) \mapsto g_i.$$  

Then $\pi_i$ is a surjective homomorphism with

$$\ker(\pi_i) = \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) \mid g_j \in G_j\} \cong G/G_i.$$  

(3) If $x \in G_i$ and $y \in G_j$ for some $i \neq j$ then $xy = yx$. So if $x_i \in G_i$ for $i = 1, \ldots, n$, then $(x_1 x_2 \cdots x_n)^\ell = x_1^\ell x_2^\ell \cdots x_n^\ell$, and so $|x_1 \cdots x_n| = \text{lcm}(|x_1|, \ldots, |x_n|)$. 

Direct products of cyclic groups

Proposition

Let $m, n \in \mathbb{Z}^+$. 

1. $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.

2. If $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}}$. 
Direct products of cyclic groups

Proposition

Let \( m, n \in \mathbb{Z}^+ \).

1. \( Z_m \times Z_n \cong Z_{mn} \) if and only if \( (m, n) = 1 \).

2. If \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) then \( Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}} \).

Recall, for groups \( A, B, \) and \( C \),

\[ A \times B \cong B \times A \quad \text{and} \quad (A \times B) \times C \cong A \times (B \times C). \]
Direct products of cyclic groups

Proposition

Let \( m, n \in \mathbb{Z}^+ \).

1. \( Z_m \times Z_n \cong Z_{mn} \) if and only if \((m, n) = 1\).

2. If \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) then \( Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}} \).

Recall, for groups \( A, B, \) and \( C \),

\[
A \times B \cong B \times A \quad \text{and} \quad (A \times B) \times C \cong A \times (B \times C).
\]

Examples:

\[
Z_2 \times Z_3 \cong Z_6
\]
Direct products of cyclic groups

Proposition

Let \( m, n \in \mathbb{Z}^+ \).

1. \( Z_m \times Z_n \cong Z_{mn} \) if and only if \((m, n) = 1\).

2. If \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) then \( Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}} \).

Recall, for groups \( A, B, \) and \( C \),

\[
A \times B \cong B \times A \quad \text{and} \quad (A \times B) \times C \cong A \times (B \times C).
\]

Examples:

\[
Z_2 \times Z_3 \cong Z_6, \quad \text{but} \quad Z_6 \times Z_4 \ncong Z_{24}.
\]
Direct products of cyclic groups

Proposition

Let $m, n \in \mathbb{Z}^+$. 

1. $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.
2. If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}}$.

Recall, for groups $A$, $B$, and $C$,

$$A \times B \cong B \times A \quad \text{and} \quad (A \times B) \times C \cong A \times (B \times C).$$

Examples:

$$Z_2 \times Z_3 \cong Z_6, \text{ but } Z_6 \times Z_4 \not\cong Z_{24}$$

Note: $Z_6 \times Z_4$ is not cyclic!
Direct products of cyclic groups

Proposition

Let \( m, n \in \mathbb{Z}^+ \).

1. \( Z_m \times Z_n \cong Z_{mn} \) if and only if \( (m, n) = 1 \).
2. If \( n = p_1^{\alpha_1} \ldots p_k^{\alpha_k} \) then \( Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}} \).

Recall, for groups \( A, B, \) and \( C \),

\[
A \times B \cong B \times A \quad \text{and} \quad (A \times B) \times C \cong A \times (B \times C).
\]

Examples:

\[
Z_2 \times Z_3 \cong Z_6, \quad \text{but} \quad Z_6 \times Z_4 \not\cong Z_{24}
\]

Note: \( Z_6 \times Z_4 \) is not cyclic!

Since \( 24 = 8 \times 3 = 2^3 \times 3 \), we have

\[
Z_{24} \cong Z_{2^3} \times Z_3.
\]
Direct products of cyclic groups

Proposition

Let \( m, n \in \mathbb{Z}^+ \).

1. \( Z_m \times Z_n \cong Z_{mn} \) if and only if \( (m, n) = 1 \).

2. If \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) then \( Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}} \).

Recall, for groups \( A, B, \) and \( C, \)

\[ A \times B \cong B \times A \quad \text{and} \quad (A \times B) \times C \cong A \times (B \times C). \]

Examples:

\[ Z_2 \times Z_3 \cong Z_6, \text{ but } Z_6 \times Z_4 \not\cong Z_{24} \]

Note: \( Z_6 \times Z_4 \) is not cyclic!

Since \( 24 = 8 \times 3 = 2^3 \times 3, \) we have

\[ Z_{24} \cong Z_{2^3} \times Z_3. \]

Can: break \( Z_n \) into maximal \( Z_{p^\alpha} \)'s, or merge \( Z_{p^\alpha} \) with \( Z_{q^\beta} \) (\( p \neq q \)).

Cannot: break \( Z_{p^\alpha} \)'s down any further, or merge \( Z_{p^\alpha} \) with \( Z_{p^\beta} \).
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 $r \in \mathbb{Z}_{\geq 0}$, 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. $G \cong \mathbb{Z}^{r_1} \times \mathbb{Z}^{n_2} \times \cdots \times \mathbb{Z}^{n_s}$ for some integers $r, n_1, n_2, \ldots, n_s$ such that $r \geq 0$ and $n_1 \leq n_2 \leq \cdots \leq n_s$.

2. The expression in (1) is unique. (Presented without proof).
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 $r \in \mathbb{Z}_{\geq 0}$, 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 $2 \leq n_s | \cdots | n_2 | n_1$. 

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 $r \in \mathbb{Z}_{\geq 0}$, 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 $2 \leq n_s | \cdots | n_2 | n_1$.*

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

*(Presented without proof).*