Last time: Group actions.

A group action of a group $G$ on a set $A$ is a map from 
$$G \times A \rightarrow A \quad (g, a) \mapsto g \cdot a$$

that satisfies

$$g \cdot (h \cdot a) = (gh) \cdot a \quad \text{and} \quad 1 \cdot a = a \quad \text{(structure preserving)}$$

for all $g, h \in G$, $a \in A$. We say $G$ acts on $A$, denoted $G \subseteq A$.

Examples:

1. The dihedral group acts on the set of symmetric states a regular $n$-gon can occupy by rotations and flips.
2. The symmetric group $S_X$ acts on $X$ by permutation.
3. Any group $G$ acts on itself (let $A = G$) in several ways:
   - left regular action: $g \cdot a = ga$
   - right multiplication: $g \cdot a = ag^{-1}$
   - conjugation: $g \cdot a = gag^{-1}$
A **group action** of a group $G$ on a set $A$ is a map from

$$G \times A \to A \quad (g, a) \mapsto g \cdot a$$

that satisfies

$$g \cdot (h \cdot a) = (gh) \cdot a \quad \text{and} \quad 1 \cdot a = a \quad \text{(structure preserving)}$$

for all $g, h \in G$, $a \in A$. We say $G$ acts on $A$, denoted $G \acts A$.

**Examples:**

1. The dihedral group acts on the set of symmetric states a regular $n$-gon can occupy by rotations and flips.
2. The symmetric group $S_X$ acts on $X$ by permutation.
3. Any group $G$ acts on itself (let $A = G$) in several ways:
   - **left regular action:** $g \cdot a = ga$
   - **right multiplication:** $g \cdot a = ag^{-1}$
   - **conjugation:** $g \cdot a = gag^{-1}$

   Note: The way we’ve been writing the action $(g \cdot a)$ is called a **left action**. Sometimes it can be better to write

   $$a \cdot g \quad \text{means } g \text{ is acting from the right.}$$
Last time: Group actions.

A group action of a group $G$ on a set $A$ is a map from

$$G \times A \to A \quad (g, a) \mapsto g \cdot a$$

that satisfies

$$g \cdot (h \cdot a) = (gh) \cdot a \quad \text{and} \quad 1 \cdot a = a \quad \text{(structure preserving)}$$

for all $g, h \in G$, $a \in A$. We say $G$ acts on $A$, denoted $G \acts A$.

Examples:

1. The dihedral group acts on the set of symmetric states a regular $n$-gon can occupy by rotations and flips.
2. The symmetric group $S_X$ acts on $X$ by permutation.
3. Any group $G$ acts on itself (let $A = G$) in several ways:
   - left regular action: $g \cdot a = ga$
   - right multiplication: $g \cdot a = ag^{-1}$
   - conjugation: $g \cdot a = gag^{-1}$

Note: The way we’ve been writing the action $(g \cdot a)$ is called a left action. Sometimes it can be better to write

$$a \cdot g \quad \text{means } g \text{ is acting from the right.}$$

The right regular action is $a \cdot g = ag$. (Different from the left action of right multiplication!)
Theorem
A group action is equivalent to a homomorphism
\[ G \rightarrow S_A \]
\[ g \mapsto \sigma_g \text{ defined by } \sigma_g(a) = g \cdot a. \]

In other words, given a homomorphism, you get an action, and vice versa.
Theorem

A group action is equivalent to a homomorphism

\[ G \to S_A \]
\[ g \mapsto \sigma_g \quad \text{defined by } \sigma_g(a) = g \cdot a. \]

In other words, given a homomorphism, you get an action, and vice versa.

Some vocabulary/facts:

(1) The trivial action is \( g \cdot a = a \), i.e \( \sigma_g = 1 \) for all \( g \in G \).
Theorem
A group action is equivalent to a homomorphism

\[ G \to S_A \]

\[ g \mapsto \sigma_g \quad \text{defined by } \sigma_g(a) = g \cdot a. \]

In other words, given a homomorphism, you get an action, and vice versa.

Some vocabulary/facts:
(1) The trivial action is \( g \cdot a = a \), i.e \( \sigma_g = 1 \) for all \( g \in G \).
(2) If the map \( g \mapsto \sigma_g \) is injective, we say the action is faithful.
Theorem
A group action is equivalent to a homomorphism

\[ G \to S_A \]
\[ g \mapsto \sigma_g \quad \text{defined by } \sigma_g(a) = g \cdot a. \]

In other words, given a homomorphism, you get an action, and vice versa.

Some vocabulary/facts:
(1) The trivial action is \( g \cdot a = a \), i.e \( \sigma_g = 1 \) for all \( g \in G \).
(2) If the map \( g \to \sigma_g \) is injective, we say the action is faithful.
(3) The kernel of an action is the set \( \{ g \in G \mid g \cdot a = a \quad \forall a \in A \} \).
   The kernel of a \( G \)-action is a subgroup of \( G \).
Theorem
A group action is equivalent to a homomorphism
\[ G \to S_A \]
\[ g \mapsto \sigma_g \text{ defined by } \sigma_g(a) = g \cdot a. \]

In other words, given a homomorphism, you get an action, and vice versa.

Some vocabulary/facts:
1. The trivial action is \( g \cdot a = a \), i.e. \( \sigma_g = 1 \) for all \( g \in G \).
2. If the map \( g \to \sigma_g \) is injective, we say the action is faithful.
3. The kernel of an action is the set \( \{ g \in G \mid g \cdot a = a \quad \forall a \in A \} \).
   The kernel of a \( G \)-action is a subgroup of \( G \).
4. The stabilizer of an element \( s \in A \) is the set \( G_s = \{ g \in G \mid g \cdot s = s \} \). This is also a subgroup of \( G \).
Theorem
A group action is equivalent to a homomorphism

\[ G \rightarrow S_A \]
\[ g \mapsto \sigma_g \quad \text{defined by } \sigma_g(a) = g \cdot a. \]

In other words, given a homomorphism, you get an action, and vice versa.

Some vocabulary/facts:
(1) The trivial action is \( g \cdot a = a \), i.e \( \sigma_g = 1 \) for all \( g \in G \).
(2) If the map \( g \mapsto \sigma_g \) is injective, we say the action is faithful.
(3) The kernel of an action is the set \( \{ g \in G \mid g \cdot a = a \quad \forall a \in A \} \).
   The kernel of a \( G \)-action is a subgroup of \( G \).
(4) The stabilizer of an element \( s \in A \) is the set \( G_s = \{ g \in G \mid g \cdot s = s \} \). This is also a subgroup of \( G \).
(5) On the homework:
   "\( a \sim b \) if there is some \( g \) for which \( g \cdot a = b \)"
   is an equivalence relation. The orbit of an element \( s \in A \) is the
   equivalence class of \( a \), \( \bar{a} = \{ a \in A \mid g \cdot s = a \text{ for some } g \in G \} \).
Types of groups we know

Numbers: \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times \)

Matrices: \((M_n(F), +), \text{GL}_n(F)\), where \(F = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \text{ or } \mathbb{F}_p\).

Modular groups: \(\mathbb{Z}/n\mathbb{Z}\) and \((\mathbb{Z}/n\mathbb{Z})^\times\)

Dihedral groups: \(D_{2n} = \langle r, s \mid s^2 = r^n = 1, rs = sr^{-1} \rangle\)

Symmetric groups: \(S_n = \{\text{permutations of } 1, \ldots, n\}\)

Quaternians: \(Q_8 = \langle i, j, k, -1 \mid \cdots \rangle\)

Finite groups, infinite groups, abelian groups

Types of subgroups we know

Kernels of homomorphisms, of group actions

Images of homomorphisms

The center (elements of \(G\) which commute with everything in \(G\).)

Centralizers (elements of \(G\) which commute \textit{w} everything in \(A \subseteq G\))

Normalizers (elements of \(G\) which \textit{setwise} commute with \(A \subseteq G\))

Stabilizers (given a group action on \(A\), the elements of \(G\) which fix elements of a set \(S \subseteq A\))
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{ x^\ell \mid \ell \in \mathbb{Z} \} = \langle x \rangle.$$
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$ 

Additive notation: $H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle$. 

Examples:

- $\mathbb{Z}$ is generated by $\bar{1}$.
- $\mathbb{Z}$ is generated by $1$.

Non-example: $S_3$ is not cyclic. Check: This group consists of:
  1. the identity, which only generates itself;
  2. two-cycles, $p_{ij}$, which only generate themselves and the identity;
  3. three-cycles $p_{1ij}$, which only generate $p_{1ij}$, $p_{1ji}$, and $1$. 

Cyclic groups

A group $H$ is **cyclic** if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$  

Additive notation:  

$$H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$  

Examples:  

$$\mathbb{Z}/n\mathbb{Z}$$ is generated by $\bar{1}$
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which $H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle$.

Additive notation: $H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle$.

Examples:

$\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$

$\mathbb{Z}$ is generated by $1$
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$

Additive notation:

$$H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$

Examples:

- $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$
- $\mathbb{Z}$ is generated by $1$

Non-example:

$S_3$ is not cyclic.
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$  

Additive notation:  

$$H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$  

Examples:  

$\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$  

$\mathbb{Z}$ is generated by $1$  

Non-example:  

$S_3$ is not cyclic.  

Check: This group consists of

1. the identity, which only generates itself;
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$ 

Additive notation: $H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle$.

Examples:

$$\mathbb{Z}/n\mathbb{Z} \text{ is generated by } 1$$

$$\mathbb{Z} \text{ is generated by } 1$$

Non-example:

$S_3$ is not cyclic.

Check: This group consists of

1. the identity, which only generates itself;
2. two-cycles, $(i \ j)$, which only generate themselves and the identity;
Cyclic groups

A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$ 

Additive notation: $H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle$.

Examples:

$$\mathbb{Z}/n\mathbb{Z}$$ is generated by $1$

$$\mathbb{Z}$$ is generated by $1$

Non-example:

$S_3$ is not cyclic.

Check: This group consists of

1. the identity, which only generates itself;
2. two-cycles, $(i \ j)$, which only generate themselves and the identity; and
3. three-cycles $(1 \ i \ j)$, which only generate $(1 \ i \ j)$, $(1 \ j \ i)$, and $1$.  


Order

If the generator has finite order, then the cyclic group is finite, and is presented as
\[ \text{mult} : \mathbb{Z} \rightarrow \mathbb{Z} \]

Example: The integers modulo \( n \) are cyclic and finite,
\[ \mathbb{Z}/n\mathbb{Z} \]

If the generator has infinite order, then there are no relations, and the cyclic group is countably infinite.
Example: The integers are cyclic and infinite,
\[ \mathbb{Z} \]

Proposition
If \( H \) is cyclic, then \( |H| = |\mathbb{Z}| \).
More specifically,
1. \( |H| = n \) iff \( x^n = 1 \) and \( 1, x, x^2, ..., x^{n-1} \) are all distinct,
2. \( |H| = \infty \) iff \( x^a \neq x^b \) for all \( a \neq b \).

Proof.
(Same argument as in your homework: read p. 55)
Order

If the generator has finite order, then the cyclic group is finite, and is presented as

\[ \text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle. \]
Order

If the generator has finite order, then the cyclic group is finite, and is presented as

\[ \text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle. \]

**Example:** The integers modulo \( n \) are cyclic and finite,

\[ \mathbb{Z}/n\mathbb{Z} = \langle x = \bar{1} \mid nx = \bar{0} \rangle. \]
Order

If the generator has finite order, then the cyclic group is finite, and is presented as

\[
\text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle.
\]

**Example:** The integers modulo \( n \) are cyclic and finite,

\[
\mathbb{Z}/n\mathbb{Z} = \langle x = \bar{1} \mid nx = \bar{0} \rangle.
\]

If the generator has infinite order, then there are no relations, and the cyclic group is *countably infinite*.
Order

If the generator has finite order, then the cyclic group is finite, and is presented as

\[ \text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle. \]

Example: The integers modulo \( n \) are cyclic and finite,

\[ \mathbb{Z}/n\mathbb{Z} = \langle x = \bar{1} \mid nx = \bar{0} \rangle. \]

If the generator has infinite order, then there are are no relations, and the cyclic group is *countably infinite*.

Example: The integers are cyclic and infinite,

\[ \mathbb{Z} = \langle 1 \rangle. \]
Order

If the generator has finite order, then the cyclic group is finite, and is presented as

\[ \text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle. \]

Example: The integers modulo \( n \) are cyclic and finite,

\[ \mathbb{Z}/n\mathbb{Z} = \langle x = \bar{1} \mid nx = \bar{0} \rangle. \]

If the generator has infinite order, then there are are no relations, and the cyclic group is \textit{countably infinite}.

Example: The integers are cyclic and infinite,

\[ \mathbb{Z} = \langle 1 \rangle. \]

Proposition

\[ \text{If } H = \langle x \rangle, \text{ then } |H| = |x|. \]
**Order**

If the generator has finite order, then the cyclic group is finite, and is presented as

\[
\text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle.
\]

**Example:** The integers modulo \( n \) are cyclic and finite,

\[
\mathbb{Z}/n\mathbb{Z} = \langle x = 1 \mid nx = 0 \rangle.
\]

If the generator has infinite order, then there are no relations, and the cyclic group is *countably infinite*.

**Example:** The integers are cyclic and infinite,

\[
\mathbb{Z} = \langle 1 \rangle.
\]

**Proposition**

If \( H = \langle x \rangle \), then \(|H| = |x|\). More specifically,

1. \(|H| = n \iff x^n = 1 \text{ and } 1, x, x^2, \ldots, x^{n-1} \text{ are all distinct},
2. \(|H| = \infty \iff x^a \neq x^b \text{ for all } a \neq b\).
Order

If the generator has finite order, then the cyclic group is finite, and is presented as

\[
\text{mult: } \langle x \mid x^n = 1 \rangle \quad \text{add: } \langle x \mid nx = 0 \rangle.
\]

Example: The integers modulo \( n \) are cyclic and finite,

\[
\mathbb{Z}/n\mathbb{Z} = \langle x = \bar{1} \mid nx = \bar{0} \rangle.
\]

If the generator has infinite order, then there are are no relations, and the cyclic group is *countably infinite*.

Example: The integers are cyclic and infinite,

\[
\mathbb{Z} = \langle 1 \rangle.
\]

Proposition

If \( H = \langle x \rangle \), then \( |H| = |x| \). More specifically,

(1) \( |H| = n \) iff \( x^n = 1 \) and \( 1, x, x^2, \ldots, x^{n-1} \) are all distinct,

(2) \( |H| = \infty \) iff \( x^a \neq x^b \) for all \( a \neq b \).

Proof. (Same argument as in your homework: read p. 55)
Cyclic groups are unique

Theorem

Any two cyclic subgroups of the same order are isomorphic.
Cyclic groups are unique

Theorem
Any two cyclic subgroups of the same order are isomorphic.
In particular,

1. if \( n \in \mathbb{Z}_{>0} \) and \( \langle x \rangle \) and \( \langle y \rangle \) are both cyclic groups of order \( n \), then

\[
\varphi : \langle x \rangle \to \langle y \rangle \\
x^k \mapsto y^k
\]

is a well-defined bijective homomorphism,
Cyclic groups are unique

Theorem
Any two cyclic subgroups of the same order are isomorphic.
In particular,

1. if \( n \in \mathbb{Z}_{>0} \) and \( \langle x \rangle \) and \( \langle y \rangle \) are both cyclic groups of order \( n \), then

\[
\varphi : \langle x \rangle \rightarrow \langle y \rangle \\
x^k \mapsto y^k
\]

is a well-defined bijective homomorphism, or

2. if \( \langle x \rangle \) is an infinite cyclic group, then the map

\[
\varphi : \mathbb{Z} \rightarrow \langle x \rangle \\
k \mapsto x^k
\]

is a well defined bijective homomorphism.
Cyclic groups are unique

**Theorem**

Any two cyclic subgroups of the same order are isomorphic.

In particular,

1. if $n \in \mathbb{Z}_{>0}$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order $n$, then
   \[
   \varphi : \langle x \rangle \to \langle y \rangle \\
   x^k \mapsto y^k
   \]
   is a well-defined bijective homomorphism, or

2. if $\langle x \rangle$ is an infinite cyclic group, then the map
   \[
   \varphi : \mathbb{Z} \to \langle x \rangle \\
   k \mapsto x^k
   \]
   is a well defined bijective homomorphism.

**Notation:** Let $\mathbb{Z}_n$ be the cyclic group of order $n$. 
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$

(2) $\langle r^2 \rangle = \{r^{2\ell} \mid \ell \in \mathbb{Z}\} = \{\ldots, r^0, r^2, \ldots\}$

(3) $\langle r^3 \rangle = \{r^{3\ell} \mid \ell \in \mathbb{Z}\} = \{\ldots, r^0, r^3, \ldots\}$

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\}$

(5) $\langle rs \rangle = \{rs^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, rs^{-2}, rs^{-1}, rs^0, rs^1, rs^2, \ldots\}$

(6) $\langle r^2s \rangle = \{r^{2\ell}s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^0s^{-2}, r^2s^{-1}, rs^0, rs^2, \ldots\}$

(7) $\langle r^3s \rangle = \{r^{3\ell}s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^0s^{-3}, r^3s^{-2}, rs^0, rs^3, \ldots\}$

Note that $p_{rsq}^2 = r^2s^2 = rsrs^{-1} = r$. So $\langle rs \rangle = \{r^k, s^k \mid \ell \in \mathbb{Z}\}$.
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{ r^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots \}$

$$= \{ 1, r, r^2, r^3 \}, \text{ since } r^4 = 1, \text{ so that } r^{4k+\ell} = r^\ell.$$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{ r^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots \} = \{ 1, r, r^2, r^3 \}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle$

(Same as (1))

(3) $\langle r^3 \rangle$

(4) $\langle s \rangle = \{ s^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, \ldots \} = \{ 1, s, s^2, s^3 \}$, since $s^2 = 1$, so that $r^{4k+\ell} = r^\ell$.

(5) $\langle rs \rangle = \{ rs^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, rs^{-2}, rs^{-1}, 1, rs, rs^2, rs^3, \ldots \}$

Note that $rs^2 = rsrs = rr^3 = r^3$.

So $\langle rs \rangle = \{ 1, rs, rs^2, rs^3 \}$.

Recall we showed that $|r^m| = 2$ for any $m$!

(6) So similarly, $\langle r^2 \rangle$

(7) $\langle 1 \rangle$ (Notation).
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$

$= \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

1. $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$
   
   $= \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

2. $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

3. $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots \} = \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots \} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots \}$.
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

1. $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$
   \[= \{1, r, r^2, r^3\}, \text{ since } r^4 = 1, \text{ so that } r^{4k+\ell} = r^\ell.\]

2. $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}.$

3. $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\}$
   \[= \{\ldots, r^{-2}, r^{-1}, 1, r^3, r^2, r^1, 0, \ldots\}\]
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$

$= \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\}$

$= \{\ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$.

(Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\} = \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\} = \{\ldots, r^{-2}, 1, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$.

(Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots \}$

= $\{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k + \ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots \} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots \}$

= $\{\ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots \} = \{1, r, r^2, r^3\}$.

(Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots \}$

= $\{1, s\}$, since $s^2 = 1$, so that $r^{2k + \ell} = r^\ell$. 

(5) Note that $p^{rsq_2} = rsrs = rr$.

So $\langle rs \rangle = \{t, rsu\}$.

Recall we showed that $|r^m| = 2$ for any $m \neq 0$. 

(6) So similarly, $\langle r^2s \rangle$ and $\langle r^3s \rangle$.
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$
   = $\{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\}$
   = $\{\ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$.
   (Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\}$
   = $\{1, s\}$, since $s^2 = 1$, so that $r^{2k+\ell} = r^\ell$.

(5) $\langle rs \rangle = \{(rs)^\ell \mid \ell \in \mathbb{Z}\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$
   $= \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\}$
   $= \{\ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$.
   (Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\}$
   $= \{1, s\}$, since $s^2 = 1$, so that $r^{2k+\ell} = r^\ell$.

(5) $\langle rs \rangle = \{(rs)^\ell \mid \ell \in \mathbb{Z}\}$
   $= \{\ldots, (rs)^{-2}, (rs)^{-1}, 1, (rs), (rs)^2, (rs)^3, (rs)^4, \ldots\}$
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

1. $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\} = \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

2. $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

3. $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\} = \{\ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$. (Same as (1))

4. $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\} = \{1, s\}$, since $s^2 = 1$, so that $r^{2k+\ell} = r^\ell$.

5. $\langle rs \rangle = \{(rs)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, (rs)^{-2}, (rs)^{-1}, 1, (rs), (rs)^2, (rs)^3, (rs)^4, \ldots\}$. Note that $(rs)^2 = rsrs = rr^{-1}ss = 1$. 

Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{ r^l \mid l \in \mathbb{Z} \} = \{ \ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots \}$
   $= \{ 1, r, r^2, r^3 \}$, since $r^4 = 1$, so that $r^{4k+l} = r^l$.

(2) $\langle r^2 \rangle = \{ (r^2)^l \mid l \in \mathbb{Z} \} = \{ \ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots \} = \{ 1, r^2 \}$.

(3) $\langle r^3 \rangle = \{ (r^3)^l \mid l \in \mathbb{Z} \} = \{ \ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots \}$
   $= \{ \ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots \} = \{ 1, r, r^2, r^3 \}$.

(Same as (1))

(4) $\langle s \rangle = \{ s^l \mid l \in \mathbb{Z} \} = \{ \ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots \}$
   $= \{ 1, s \}$, since $s^2 = 1$, so that $r^{2k+l} = r^l$.

(5) $\langle rs \rangle = \{ (rs)^l \mid l \in \mathbb{Z} \}$
   $= \{ \ldots, (rs)^{-2}, (rs)^{-1}, 1, (rs), (rs)^2, (rs)^3, (rs)^4, \ldots \}$

Note that $(rs)^2 = rsrs = rr^{-1}ss = 1$. So $\langle rs \rangle = \{ 1, rs \}$.  

(Same as (1))
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$

$= \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\}$

$= \{\ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$.

(Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\}$

$= \{1, s\}$, since $s^2 = 1$, so that $r^{2k+\ell} = r^\ell$.

(5) $\langle rs \rangle = \{(rs)^\ell \mid \ell \in \mathbb{Z}\}$

$= \{\ldots, (rs)^{-2}, (rs)^{-1}, 1, (rs), (rs)^2, (rs)^3, (rs)^4, \ldots\}$

Note that $(rs)^2 = rsrs = rr^{-1}ss = 1$. So $\langle rs \rangle = \{1, rs\}$.

Recall we showed that $|r^m s| = 2$ for any $m$!
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{ r^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots \}$
   $\quad = \{ 1, r, r^2, r^3 \}$, since $r^4 = 1$, so that $r^{4k+\ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots \} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots \}$
   $\quad = \{ \ldots, r^{-2}, r^1, 1, r^3, r^2, r^1, 0, \ldots \} = \{1, r, r^2, r^3\}$.
   (Same as (1))

(4) $\langle s \rangle = \{ s^\ell \mid \ell \in \mathbb{Z} \} = \{ \ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots \}$
   $\quad = \{1, s\}$, since $s^2 = 1$, so that $r^{2k+\ell} = r^\ell$.

(5) $\langle rs \rangle = \{(rs)^\ell \mid \ell \in \mathbb{Z} \}$
   $\quad = \{ \ldots, (rs)^{-2}, (rs)^{-1}, 1, (rs), (rs)^2, (rs)^3, (rs)^4, \ldots \} \ldots$
Note that $(rs)^2 = rsrs = rrr^{-1}ss = 1$. So $\langle rs \rangle = \{1, rs\}$.
Recall we showed that $|r^m s| = 2$ for any $m$!

(6) So similarly, $\langle r^2 s \rangle = \{1, r^2 s\}$ and $\langle r^3 s \rangle = \{1, r^3 s\}$.
Cyclic subgroups

Example: What are the cyclic subgroups of $D_8$?

(1) $\langle r \rangle = \{r^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, r^{-1}, 1, r, r^2, r^3, r^4, \ldots\}$
   $= \{1, r, r^2, r^3\}$, since $r^4 = 1$, so that $r^{4k + \ell} = r^\ell$.

(2) $\langle r^2 \rangle = \{(r^2)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-2}, 1, r^2, r^4, r^6, \ldots\} = \{1, r^2\}$.

(3) $\langle r^3 \rangle = \{(r^3)^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, r^{-6}, r^{-3}, 1, r^3, r^6, r^9, r^{12}, \ldots\}$
   $= \{\ldots, r^{-2}, r^{-1}, 1, r^3, r^2, r^1, 0, \ldots\} = \{1, r, r^2, r^3\}$. (Same as (1))

(4) $\langle s \rangle = \{s^\ell \mid \ell \in \mathbb{Z}\} = \{\ldots, s^{-2}, s^{-1}, 1, s, s^2, s^3, s^4, \ldots\}$
   $= \{1, s\}$, since $s^2 = 1$, so that $r^{2k + \ell} = r^\ell$.

(5) $\langle rs \rangle = \{(rs)^\ell \mid \ell \in \mathbb{Z}\}$
   $= \{\ldots, (rs)^{-2}, (rs)^{-1}, 1, (rs), (rs)^2, (rs)^3, (rs)^4, \ldots\} \ldots$
   Note that $(rs)^2 = rsrs = rr^{-1}ss = 1$. So $\langle rs \rangle = \{1, rs\}$.
   Recall we showed that $|r^m s| = 2$ for any $m$!

(6) So similarly, $\langle r^2 s \rangle = \{1, r^2s\}$ and $\langle r^3 s \rangle = \{1, r^3s\}$.

(7) $\langle 1 \rangle = \{1\} = 1$ (Notation).
Cyclic subgroups

You try: What are the cyclic subgroups of $S_4$?