Lecture 11: Cyclic groups

Recall: $G$ a group, $H \leq G$ is a subgroup of $G$ if
(i) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$
(ii) $h \in H \Rightarrow h^{-1} \in H$.

This gives us a way to construct lots of groups: as subgroups of other groups.

Ex: $C^* = \mathbb{C} \backslash \{0\}$ is a group under multiplication.
$z = a + bi$, $\bar{z} = a - bi$, $|z| = \sqrt{a^2 + b^2}$, $z^{-1} = \frac{\bar{z}}{|z|^2}$.

$C^* = \{ z \in \mathbb{C} | |z| = 1 \}$ "Unit complex numbers" $U$ also known as $U(1)$ or $S^1$.

Any $z \in U$ can be written in polar form as
$z = e^{i\Theta} = \cos\Theta + i \sin\Theta$, for some $\Theta \in \mathbb{R}$.
Then multiplication takes the form $e^{i\alpha}e^{i\beta} = e^{i(\alpha + \beta)}$ and $e^{2\pi i} = 1$.

$U$ is a subgroup: $z_1, z_2 \in U$, $z_1 e^{i\Theta_1}, z_2 e^{i\Theta_2}, z_1 z_2 = e^{i(k+1)} \in U$.
$z \in U$, $z = e^{i\Theta}$, $z^{-1} = e^{-i\Theta} \in U$.

Another subgroup is, for $n \in \mathbb{N}$,
$C_n = \{ e^{2\pi ik/n} | k \in \mathbb{Z} \}$: $C_2 = \{ -1, 1 \}$, $C_4 = \{ 1, i, -1, -i \}$
(check it.)

Proposition 2.2.8: Let $G$ be a group and let $H_\alpha \leq G$ be a subgroup for each $\alpha \in \mathcal{I}$ ($\mathcal{I}$ some indexing set).
Then $\bigcap_{\alpha \in \mathcal{I}} H_\alpha = \{ g \in G | (\forall \alpha)(g \in H_\alpha) \}$ is a subgroup $\alpha \in \mathcal{I}$
as well. "The intersection of subgroups is a subgroup."
Proof:

(i) Let \( h_1, h_2 \in \bigcap_{\alpha \in J} H_\alpha \) for all \( \alpha \in J \), \( h_1, h_2 \in H_\alpha \). Since \( H_\alpha \) is a subgroup, \( h_1 h_2 \in H_\alpha \) for all \( \alpha \in J \), and \( h_1 h_2 \in \bigcap_{\alpha \in J} H_\alpha \).

(ii) Let \( h \in \bigcap_{\alpha \in J} H_\alpha \). For all \( \alpha \in J \), \( h \in H_\alpha \). Since \( H_\alpha \) is a subgroup, \( h^{-1} \in H_\alpha \). So for all \( \alpha \in J \), \( h^{-1} \in H_\alpha \). So \( h^{-1} \in \bigcap_{\alpha \in J} H_\alpha \).

Recall: An isomorphism from \( G \) to \( H \) is a bijective function \( \varphi : G \to H \) such that \( \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \) for all \( g_1, g_2 \in G \). We say \( G \) and \( H \) are isomorphic, \( G \cong H \), if there is an isomorphism between them.

Ex: \( G \cong H = \{ \langle g \rangle \mid g \in G \} \leq \text{Sym}(G) \) Cayley's Thm.

Ex: \( C_n = \{ e^{2\pi i k/n} \mid k \in \mathbb{Z}^+ \} \leq (\mathbb{C}^*, \cdot) \) and \( \langle \mathbb{Z}_n \rangle \) are isomorphic.

\( \varphi : \mathbb{Z}_n \to C_n \) is defined by \( \varphi([k]) = e^{2\pi i k/n} \).

Why is it well defined? If \([k] = [k']\), then \( k \equiv k' \mod n \), so \( n \mid (k' - k) \), so \( k' - k = q n \) so \( k' = k + qn \). But then \( e^{2\pi i k/n} = e^{2\pi i (k + qn)/n} = e^{2\pi i k/n} e^{2\pi i qn} = e^{2\pi i k/n} e^{2\pi i qn} = e^{2\pi i k/n} \) since \( e^{2\pi i qn} = (e^{2\pi i})^q = 1^q = 1 \).

Why bijective? Fact: every \( z \in C_n \) can be written as \( e^{2\pi i k/n} \) for a unique \( k \in \{0, 1, 2, \ldots, n-1\} \).

Why isomorphism?

\( \varphi([k] + [l]) = \varphi([k+l]) = e^{2\pi i (k+l)/n} = e^{2\pi i k/n} e^{2\pi i l/n} e^{2\pi i k/n} = \varphi([k]) \varphi([l]) \).
If $A \leq G$, $A \neq \emptyset$ is any subset of $G$, we can construct a subgroup:

$$\langle A \rangle = \text{intersection of all subgroups } H \leq G \text{ such that } A \leq H$$

$\langle A \rangle$ is called the subgroup generated by $A$.

For $a \in G$, $a^k = a \cdot a \cdot \ldots \cdot a$, $a^0 = e$, $a^{-k} = (a^{-1})^k$ for $k > 0$.

Then $a^k a^l = a^{k+l}$ for all $k, l \in \mathbb{Z}$.

**Proposition**

If $A = \{a^3\}$ consists of a single element $a \in G$, then $\langle A \rangle = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle$.

**Proof:**

Indeed $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is a group, since $a^k a^l = a^{k+l}$

So $\langle a \rangle$ is a subgroup of $G$ containing $A = \{a^3\}$, so $\langle A \rangle \subseteq \langle a \rangle$.

On the other hand, any subgroup of $G$ containing $a$ must contain all powers $a^k$, $k \in \mathbb{Z}$, so $\langle a \rangle \subseteq \langle A \rangle$, and $\langle a \rangle = \langle A \rangle$.

**Def.** $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is called the cyclic subgroup generated by $a$. If $\langle a \rangle = G$, we say that $G$ is a cyclic group. $a$ is then called a generator for $G$.

**Ex.** In $(\mathbb{Z}, +)$: $\langle d \rangle = \{kd \mid k \in \mathbb{Z}\} = \langle -d \rangle$.

$\langle 1 \rangle = \mathbb{Z}$ so $\mathbb{Z}$ is cyclic, generated by $1$.

In $(\mathbb{Z}_2, +)$: $\langle [3] \rangle = \{[0], [3], [6], [9]\}$
For $a \in G$, $\langle a \rangle \leq G$ is either finite or infinite.

The order of $a$, $o(a)$, is the number of elements of $\langle a \rangle$.

Eq. \[ \exists j \in \mathbb{Z} \quad o([2]) = 4. \]
\[ 10 \in \mathbb{Z} \quad o(10) = \infty. \]

**Proposition 2.2.20:** Let $G$ be a group, $a \in G$. Then

(i) if $o(a) = \infty$, $\varphi : \mathbb{Z} \to \langle a \rangle \quad \varphi(k) = a^k$

is an isomorphism.

(ii) if $o(a) = n \in \mathbb{N}$, $\varphi : \mathbb{Z}_n \to \langle a \rangle \quad \varphi([k]) = a^k$

is an isomorphism.

We will prove this next time, but the first step is

**Lemma:** If $o(a) = n < \infty$, then $n$ is the smallest natural number such that $a^n = e$, and $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.\[ \]

**Proof:** If $o(a) = n < \infty$, there are $k, l \in \mathbb{Z}$ such that $k < l$ and $a^k = a^l$. Then $e = a^{-k} a^k = a^{-k} a^l = a^{l-k}$ and $l - k > 0$. So let $n$ be the smallest such that $a^n = e$. Then $\{e, a, a^2, \ldots, a^{n-1}\}$ are all distinct. (Homework)

Any $k \in \mathbb{Z}$ can be written as $k = qn + r$ with $0 \leq r < n$, and then $a^k = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = e a^r = a^r$. So $\langle a \rangle \leq \{e, a, a^2, \ldots, a^{n-1}\}$, and in fact they are equal.