Last time: 1) Proved: A finite set $X$ & $\sigma \in \text{Aut}(X)$ can be written uniquely (up to order) as a product of disjoint cycles.
2) defined group actions.

Today: back to order of an element of a group.

**Proposition 11.1** Let $G$ be a group, $g \in G$, $g \neq e$.

$\varphi : \mathbb{Z} \rightarrow \langle g \rangle$, $\varphi(k) = g^k$ the corresponding homomorphism. Then either

1) $\varphi$ is an isomorphism (and $g$ has infinite order)

or 2) $\exists n > 0$ so that

$\overline{\varphi} : \mathbb{Z}/n \rightarrow \langle g \rangle$, $\overline{\varphi}(lk) = g^k$ in a well-defined isomorphism (and $g$ has order $n$).

**Proof:** 1) If $\varphi$ is 1-1, then $\varphi$ is an isomorphism.

$\varphi$ is also onto and $\varphi^{-1} : \langle g \rangle \rightarrow \mathbb{Z}$ preserves multiplication.

Suppose $\varphi$ is not 1-1. Then $\exists k, l \in \mathbb{Z}$ sit, $k \neq l$ and $g^k = \varphi(k) = \varphi(l) = g^l$.

May assume: $k > l$. Then

$g^{k-l} = g^k \cdot g^{-l} = (g^k)(g^l)^{-1} = e$

$\Rightarrow \exists m > 0$ st $g^m = e$.

Let $S = \{ m \in \mathbb{Z} | \exists m > 0, g^m = e \}$

By well-ordering $\exists n = \min S$.

We'd like to define $\overline{\varphi} : \mathbb{Z}/n \rightarrow \langle g \rangle$ by $\overline{\varphi}(lk) = g^k$, $\overline{\varphi}(lk) = \varphi(k)$.

Need to check: (a) $\overline{\varphi}$ is well-defined.

(b) $\overline{\varphi}$ is a homomorphism (c) $\overline{\varphi}$ is an isomorphism.
Suppose $|k| = |k'|$ in $\mathbb{Z}/n$. Then $k-k' = qn$ for some $q \in \mathbb{Z}$, i.e., $k = k' + qn$.

$$g^k = \phi(k) = \phi(k' + qn) = \phi(k') \cdot \phi(qn) = g^{k'} \cdot g^{qn} = g^{k'} \cdot (g^n)^q = g^{k'} \cdot e^q = g^{k'}$$

$\Rightarrow \phi$ is well-defined.

(a) If $\phi$ has order 6, then $\phi[27] = [18]$ and $g^2 = g^6$

(b) $\phi([k] + [l]) = \phi([k+l]) = \phi(k + l) = \phi(k) \cdot \phi(l)$

$$= \phi([k]) \cdot \phi([l])$$

$\Rightarrow \phi$ is a homomorphism.

(c) $\phi$ is onto since $g^k = \phi([k])$.

Suppose $\phi([k]) = \phi([l])$ and $k > l$.

Then $g^k = \phi([k]) = \phi([l]) = g^l$

$\Rightarrow g^{k-l} = e$

$\Rightarrow k-l \in S$ and $k-l = q \cdot n + r$

for some $0 \leq r < n$. If $r > 0$ then

$$g^r = \phi(r) = \phi(k - l - q \cdot n)$$

$$= \phi(k) \cdot \phi(l) \cdot \phi(q \cdot n)^{-1}$$

$$= e \cdot (\phi(n)^q)^{-1} = e \cdot (e^q)^{-1} = e.$$

$\Rightarrow r \in S$ and $r < \min S$.

Contradiction.

$\therefore r = 0$

$\Rightarrow nq = k-l$

$\Rightarrow n \mid k-l$

$\Rightarrow [k] = [l] \in \mathbb{Z}/n$.

$\Rightarrow \phi$ is 1-1.

$\therefore \phi$ is an isomorphism. $\square$
Remarks 1) If \( g \in G \) has order \( n \), \( 0 < n < \infty \)

Then, since \( \overline{\varphi} : \mathbb{Z}/n \to \langle g \rangle \) is a bijection
\[
\overline{\varphi}(0) = e, \quad \overline{\varphi}(1) = g, \quad g^{n-1} = \overline{\varphi}(\mathbb{Z}/[n-1])
\]
are all distinct.

2) We can picture the relation between \( \varphi \) and \( \overline{\varphi} \) as follows:

\[
\begin{array}{cc}
\mathbb{Z} & \varphi \rightarrow \langle g \rangle \\
\downarrow \pi & \\
\mathbb{Z}/n & \overline{\varphi} \text{ and } \pi_{\omega}
\end{array}
\]

This graphically says: \( \overline{\varphi} \circ \pi = \varphi \)

And indeed, \( \forall k \in \mathbb{Z} \)
\[
\varphi(k) = \overline{\varphi}(1k) = \overline{\varphi}(\pi(k)) = (\overline{\varphi} \circ \pi)(k).
\]

We now generalize 11.1 to arbitrary homomorphisms.
We start with a definition.

Def: Let \( \varphi : G \to H \) be a homomorphism. The kernel of \( \varphi \) is the set
\[
\ker \varphi = \{ g \in G \mid \varphi(g) = e_H \}.
\]

Proposition 11.2 \( \text{ (kernels measure injectivity)} \)

Let \( \varphi : G \to H \) be a homomorphism. Then

\( \forall a, b \in G \)
\[
\varphi(a) = \varphi(b) \iff ab^{-1} \in \ker \varphi.
\]

In particular: \( \ker \varphi = \{ e_G \} \iff \varphi \) is injective.

Proof:
\[
ab^{-1} \in \ker \varphi \iff e_H = \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(ab)
\]
\[
\implies e_H = \varphi(ab) = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a)
\]
Suppose \( \ker \psi = \{e_0\} \) and \( \psi(a) = \psi(b) \).

Then \( ab^{-1} \in \ker \psi \Rightarrow ab^{-1} = e_0 \Rightarrow a = b \).

Conversely suppose \( \psi \) is injective and \( a \in \ker \psi \).

Then \( \psi(a) = e_H = \psi(e_0) \).

Injectivity of \( \psi \Rightarrow a = e_0 \). \( \Rightarrow \ker \psi = \{e_0\} \).

---

**Lemma 11.3** Let \( \psi: G \to H \) be a homomorphism. Then

1) \( \ker \psi \) is a subgroup of \( G \)
2) \( \forall g \in G, \forall a \in \ker \psi \Rightarrow gag^{-1} \in \ker \psi \)

**Proof**

(1) \( \forall a,b \in \ker \psi \)

\[ \psi(ab^{-1}) = \psi(a)(\psi(b)^{-1}) = \psi(a)(\psi(b))^{-1} = e_H e_H^{-1} = e_H \]

\( \Rightarrow ab^{-1} \in \ker \psi \).

\( \Rightarrow \ker \psi \) is a subgroup.

(2) \( \forall a \in \ker \psi, \forall g \in G \)

\[ \psi(gag^{-1}) = \psi(g) \psi(a) \psi(g^{-1}) = \psi(g) e_H \psi(g^{-1}) = e_H \]

\( \Rightarrow gag^{-1} \in \ker \psi \).

---

**Def** A subgroup \( N \) of a group \( G \) is **normal** if \( \forall g \in G, \forall a \in N \Rightarrow gag^{-1} \in N \).

---

**Note** If \( G \) is abelian then any subgroup is normal:

\( \forall g \in G, \forall a \in N \Rightarrow gag^{-1} = g g^{-1} a = a \in N \).

---

**Ex** \( \text{det} : GL(2, \mathbb{R}) \to \mathbb{R}^* \) is a homomorphism.

\( \Rightarrow \text{SL}(2, \mathbb{R}) : = \ker(\text{det}) \) is a normal subgroup.