Last class:

An isomorphism \( \Phi \) is a map
\[
\Phi : G \rightarrow \bar{G} , \quad G, \bar{G} \text{ groups}
\]
Satisfying
- 1-1 and onto (i.e., bijection between \( G \) and \( \bar{G} \))
- \( \Phi(ab) = \Phi(a) \Phi(b) \) for all \( a, b \) in \( G \)

We say that the groups \( G \) and \( \bar{G} \) are isomorphic (notation: \( G \cong \bar{G} \)) if there exists an isomorphism \( \Phi : G \rightarrow \bar{G} \)
Have seen:
1. \((\mathbb{R}, +)\) and \((\mathbb{R}^+, \cdot)\) are isomorphic groups
   \[ \Phi(x) = e^x \quad \text{isom. } \mathbb{R} \rightarrow \mathbb{R}^+ \]
2. If \(a \in G, \ \text{ord}(a) = \infty \Rightarrow \langle a \rangle \cong \mathbb{Z} \)
   \[ \text{ord}(a) = n \Rightarrow \langle a \rangle \cong \mathbb{Z}_n \]

Important Question:
Given two groups \(G\) and \(\bar{G}\), are they isomorphic?
- To prove that they are isom.: Find an isom. \(\Phi: G \rightarrow \bar{G}\)
- To disprove "": Use properties of isomorphisms to show that no isom. \(G \rightarrow \bar{G}\) can exist.

Example: Have seen. If \(G\) abelian, \(\frac{G}{G} \cong \bar{G}\)
\[ \Rightarrow \mathbb{Z}_6 \text{ and } S_3 \text{ are not isom.} \]
Properties of isomorphisms
(numbers as in Theorem 6.2 in book).

2) \( \phi(a^n) = \phi(a)^n \)
   (proof by induc. on \( n \):
   \( n=2 \):
   \[
   \phi(a^2) = \phi(a \cdot a) = \phi(a) \cdot \phi(a) = \phi(a)^2
   \]
   \( n>2 \):
   \[
   \phi(a^n) = \phi(a^{n-1} \cdot a) = \phi(a^{n-1}) \cdot \phi(a) = \phi(a)^{n-1} \cdot \phi(a)
   \]

4) isomorphisms preserve order of group elements
   i.e. \( \text{ord } \phi(a) = \text{ord } a \) \( \forall a \in G \)
   (proof: let \( n = \text{ord } a \)
    \[
    \phi(a)^n = \phi(a^{n}) = \phi(e) = e
    \]
    identity of \( G \)
    \[
    \Rightarrow \text{ord } \phi(a) \mid n
    \]
    let \( 0 < j < n \): \( \phi(a)^j = \phi(a^j) = \phi(e) = e \) by assumpt
    \[
    \phi \text{ is 1-1!}
    \]
    \[
    \text{ord } \phi(a) \geq n \]
    \( @ e \square \Rightarrow \) claim
7) \( G \) finite \( \Rightarrow \) \( G \) and \( \overline{G} \) have same \# elements of every order.

Example: Is \( U(8) \cong \mathbb{Z}_4 \)?

\( U(8) = \{ 1, 3, 5, 7 \} \Rightarrow |U(8)| = |\mathbb{Z}_4| = 4 \)

Additional check: use 7

have already checked: \( \text{ord}(3) = \text{ord}(5) = \text{ord}(7) = 2 \)

\( \Rightarrow \) \( U(8) \) has \( \boxed{3} \) elements of order 2

\( \mathbb{Z}_4 \):

\( \text{ord}(1) = 4 \)
\( \text{ord}(2) = 2 \) 
\( \text{ord}(3) = 4 \) 

by prop. 7 \( \Rightarrow \) \( \mathbb{Z}_4 \neq U(8) \)

Another result: \( G \) cyclic, \( G \cong \overline{G} \) \( \Rightarrow \) \( \overline{G} \) cyclic

Proof: There exists an isomorphism \( \phi: G \rightarrow \overline{G} \)

let \( a \) be a generator, i.e. \( G = \langle a \rangle \)
\[ G = \{ a^j \}, \; j \in \mathbb{Z} \]
\[ \bar{G} = \overline{\phi(G)} = \{ \overline{\phi(a^j)} \}, \; j \in \mathbb{Z} \]
\[ \overline{\phi} \text{ surjective.} \]
\[ = \{ \overline{\phi(a)^j} \}, \; j \in \mathbb{Z} \]
\[ = \langle \overline{\phi(a)} \rangle \]
\[ \Rightarrow \bar{G} \text{ is cyclic with generator } \overline{\phi(a)}. \]
Automorphisms

An autom $\alpha$ is an isomorphism from $G$ to itself.

Example: $G = (\mathbb{R}, +)$, $\alpha(x) = -x$

Obviously $\alpha: \mathbb{R} \to \mathbb{R}$

Only need to check it is an isom:

$x \to -x$ is 1-1 and onto

$\alpha(x+y) = -(x+y) = -x - y = (-x) + (-y) = \alpha(x) + \alpha(y)$
Lemma: Let $G$ be a group, $a \in G$

Define map $\alpha_a : G \rightarrow G$

$$g \mapsto aga^{-1}$$ (conjugation by $a$)

$\Rightarrow \alpha_a$ is an automorphism

Proof: Obviously $\alpha_a(g) = aga^{-1} \in G$

enough to show: $\alpha_a$ is an isomorphism:

1-1: assume $\alpha_a(g) = \alpha_a(h)$

$aga^{-1} = aha^{-1}$

use cancellation properties!

$ga^{-1} = ha^{-1}$ (left cancellation)

$g = h$ (right cancellation)
Let \( h \in G \) need to find \( g \in G \) s.t. \( \alpha_a(g) = h \)

\( \Rightarrow \quad a g a^{-1} = h \)

\( \iff \quad g = a^{-1} h a \)

\( \Rightarrow \quad g = a^{-1} h a \) does the job

\[ \alpha_a(gh) = a g h a^{-1} = a \alpha_a(g) \alpha_a(h) = a g a^{-1} h a a^{-1} = a g h a^{-1} = \alpha_a(gh) \]

**Def:** An autom. of the form \( \alpha_a \) is called an inner automorphism.
Examples

1. \( G \) abelian
   \[
   a_a(g) = a g a^{-1} = a a^{-1} g = g
   \]
   \( \Rightarrow a_a = \text{id} \) for all \( a \in G \)

2. \( G = S_3 \) \( a = (12) \)

   Recall:
   \[
   \pi(a_1 \ldots a_r)^{-1} = (\pi(a_1) \pi(a_2) \ldots \pi(a_r))^{-1}
   \]

   \[
   \Rightarrow a_{(12)}(12) = (21) = (12)
   \]
   \[
   a_{(12)}(13) = (23)
   \]
   \[
   a_{(12)}(23) = (13)
   \]
   \[
   a_{(12)}(123) = (12)(123)(12)^{-1} = (213) = (132) = a_{(12)}(123)
   \]
   \[
   a_{(12)}(132) = (123)
   \]