Chapter 10

**Defn:** Let $G$, $\overline{G}$ be groups. A **homomorphism** from $G$ to $\overline{G}$ is a map $\phi : G \rightarrow \overline{G}$ that preserves the group operation, meaning for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b)$$

**Defn:** The **kernel** of a homomorphism $\phi : G \rightarrow \overline{G}$ is

$$\text{Ker } \phi = \{g \in G : \phi(g) = e_{\overline{G}}\}$$

where $e_{\overline{G}}$ is the identity of $\overline{G}$.

**Obs:** An isomorphism is just a homomorphism that is one-to-one and onto. When $\phi$ is an isomorphism, $\text{Ker } \phi = \{e\}$.

**Ex:** The map $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ given by $\phi(x) = x \mod n$ is a homomorphism.

$$\text{Ker } \phi = \{x \in \mathbb{Z} : x \mod n = 0\} = \langle n \rangle$$

**Ex:** The map $\phi : S_n \rightarrow \mathbb{Z}_2$ given by

$$\phi(\alpha) = \begin{cases} 0 & \alpha \text{ even permutation} \\ 1 & \alpha \text{ odd permutation} \end{cases}$$

is a homomorphism. $\text{Ker } \phi = \{\alpha \in S_n : \alpha \text{ even} \} = A_n$

**Ex:** The map $\phi : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$ given by $\phi(x) = 1/x$

is a homomorphism. $\text{Ker } \phi = \{x \in \mathbb{R} \setminus \{0\} : 1/x = 1\} = \{1, 1\}$
Thm 10.1: Let \( \phi: G \to \overline{G} \) be a homomorphism. Then

1. \( \phi(e) = \overline{e} \) \( \leftarrow \) identity of \( \overline{G} \)
2. \( \phi(g^n) = \phi(g)^n \) for all \( g \in G, n \in \mathbb{Z} \)
3. If \( g \) has finite order, \( (\text{order of } \phi(g)) \mid (\text{order of } g) \)
4. \( \ker \phi \) is a subgroup of \( G \)
5. For all \( a, b \in G \), \( \phi(a) = \overline{b \phi(b)} \) \( \iff \) \( a \ker \phi = b \ker \phi \)
6. If \( \phi(a) = \overline{a} \) then \( \phi^{-1}(\overline{a}) = \exists g \in G : \phi(g) = \overline{a}^3 = a \ker \phi \)

\[ \text{Pf: } 1)(2) \text{ true by same argument as Thm 6.2.} \]
3. If \( g \) has order \( n \) then
\[
\phi(g)^n = \phi(g^n) = \phi(e) = \overline{e}
\]
So order of \( \phi(g) \) divides \( n \) by Cor 2 of Thm 4.1.

4. By \( \phi \mathrel{\in} \ker \phi \), So \( \ker \phi \) is nonempty.
Now suppose \( a,b \in \ker \phi \), meaning \( \phi(a) = \overline{e} = \phi(b) \). Then
\[
\phi(ab^{-1}) = \phi(a) \phi(b^{-1}) = \overline{e} \overline{b} = \overline{e} \overline{b} = \overline{e}
\]
By \( \phi \) is a homomorphism
\( a b^{-1} \in \ker \phi \). Thus \( \ker \phi \) is a subgroup
(by One-Step Subgroup Test)

5. \( a \ker \phi = b \ker \phi \iff b^{-1} a \in \ker \phi \) (by lem 7.1)
\[ \iff \phi(b^{-1} a) = \overline{e} \] (definition of \( \ker \phi \))
\[ \iff \phi(b^{-1}) \phi(a) = \overline{e} \] (since \( \phi \) is homomorphism)
\[ \iff \phi(b^{-1} a) = \overline{e} \] (by 2)
\[ \iff \phi(a) = \overline{b} \] (by multiplying on left by \( \phi(b) \))

6. For \( g \in G, \phi(g) = \overline{a} \iff \phi(g) = \phi(a) \) (since \( \phi(e) = \overline{a} \))
\[ \iff g \ker \phi = a \ker \phi \] (by 5)
\[ \iff g \in \ker \phi \] (by lem 7.1)

Therefore \( \exists g \in G : \phi(g) = \overline{a}^3 = a \ker \phi \). \( \square \)
Thm 10.2: Let $G, \bar{G}$ be groups and let $H$ be a subgroup of $G$. If $\phi : G \rightarrow \bar{G}$ is a homomorphism then:

A. $\phi(\langle H \rangle) = \langle \phi(h) : h \in H \rangle$ is a subgroup of $\bar{G}$
B. $H$ cyclic $\Rightarrow \phi(\langle H \rangle)$ cyclic. In fact $H = \langle a \rangle \Rightarrow \phi(\langle H \rangle) = \langle \phi(a) \rangle$
C. $H$ abelian $\Rightarrow \phi(\langle H \rangle)$ abelian
D. $H$ normal in $G \Rightarrow \phi(\langle H \rangle)$ normal in $\phi(G)$
E. $|\langle H \rangle| \mid |H|
F. if $K$ is a subgroup of $\bar{G}$, then $\phi^{-1}(K) = \{ g \in G : \phi(g) \in K \}$ is a subgroup of $G$
G. if $K$ is a normal subgroup of $\bar{G}$ then $\phi^{-1}(K)$ is a normal subgroup of $G$

Proof: (A) (B) (C) true by same argument in proof of Thm 6.3
D. For any $\phi(h) \in \phi(H)$ and $\phi(g) \in \phi(H)$ we have $\phi(g) \phi(h) \phi(g)^{-1} = \phi(g) \phi(h) \phi(g)^{-1} = \phi(ghg^{-1})$. Since $H$ is normal we know $ghg^{-1} \in H$. Therefore $\phi(g) \phi(h) \phi(g)^{-1} = \phi(g) \phi(h) \phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$. By the Normal Subgroup Test, we conclude $\phi(H)$ is normal in $\phi(G)$
E. Set $n = |H|!$ and enumerate the elements of $H$ as $\{ h_1, h_2, \ldots, h_n \}$. By (D) of the previous theorem, we can pick $a_1, a_2, \ldots, a_n \in H$ satisfying $\phi(a_1) = h_1, \phi(a_2) = h_2, \ldots, \phi(a_n) = h_n$. Therefore since $\phi(H) = \{ h_1, \ldots, h_n \}$, the sets $\phi^{-1}(a_1), \ldots, \phi^{-1}(a_n)$ partition $H$. Also, $\phi^{-1}(a_1) = a_1$. 


Let $\psi : H \to \phi(H)$ be the restriction of $\phi$ to $H$. Then $\psi$ is a homomorphism from $H$ onto $\phi(H)$. Thm 10.1 tells us that for every $\bar{h} \in \phi(H)$ the set of preimages $\psi^{-1}(\bar{h})$ has cardinality $|\ker \psi|$. Therefore $|H| = |\ker \psi| \cdot |\phi(H)|$ and $|\phi(H)|$ divides $|H|$.

Since $\phi(e) = \bar{e} \in R$, we have $e \in \psi^{-1}(R)$ and therefore $\psi^{-1}(R)$ is nonempty.

Now suppose $a, b \in \psi^{-1}(R)$. Then $\phi(a), \phi(b) \in R$ so $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} \in R$ (since $R$ is a subgroup).

Therefore $ab^{-1} \in \psi^{-1}(R)$. We conclude $\psi^{-1}(R)$ is a subgroup (by One-Step Subgroup Test).

Consider any $g \in G$ and $a \in \psi^{-1}(R)$. Since $R$ is normal in $G$ and $\phi(a) \in R$, we have $\phi(g)\phi(a)\phi(g)^{-1} \in R$.

Therefore $\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in R$.

Which implies $gag^{-1} \in \psi^{-1}(R)$. We conclude $\psi^{-1}(R)$ is normal in $G$ (by Normal Subgroup Test).

Cor: If $\phi : G \to \bar{G}$ is any homomorphism then $\ker \phi$ is a normal subgroup of $G$.

Pf: Set $\bar{K} = \{e \in \bar{G}\}$. Then $\bar{K}$ is a normal subgroup of $\bar{G}$. See Thm 10.2\(\odot\) $\ker \phi = \psi^{-1}(R)$ is normal in $G$. $\Box$
Ex: Define $\phi: \mathbb{Z}_{21} \to \mathbb{Z}_{21}$

$$\phi(x) = 3x \mod 21$$

Then $\phi$ is a homomorphism since

$$3(x+y) \mod 21 = 3x + 3y \mod 21 = (3x \mod 21) + (3y \mod 21)$$

Given that $\phi(0) = 18$, find all $x \in \mathbb{Z}_{21}$ satisfying $\phi(x) = 18$.

The kernel of $\phi$ is

$$\ker \phi = \{0, 7, 14, 21\}$$

Since $\phi(0) = 18$, we have

$$\phi^{-1}(18) = \{x \in \mathbb{Z}_{21} : \phi(x) = 18\} = \{0, 7, 14, 21\}$$

Ex: Suppose $\phi: \mathbb{Z}_{28} \to \mathbb{Z}_{49}$ is a homomorphism satisfying $\phi(9) = 14$.

Determine $\phi(x)$, the image of $\phi$, kernel of $\phi$, and $\phi^{-1}(14)$.

In $\mathbb{Z}_{28}$, $9+9+9 = 27$ is the inverse of 1.

So $\phi(27) = \phi(9) + \phi(9) + \phi(9) = 42$ is the inverse of $\phi(1)$.

In other words

$$\phi(1) = \phi(-1) = \phi(27) = \phi(9 + 9 + 9) = \phi(9) + \phi(9) + \phi(9) = 14 + 14 + 14 = 42$$

The 12, 14, 27 is inverse of 1 in $\mathbb{Z}_{28}$ since $\phi$ is a homomorphism.

In $\mathbb{Z}_{49}$, the inverse of 42 is 7, so $\phi(1) = 7$. 
Then for any \( x \in \mathbb{Z}_{28} \), we have
\[
\phi(x) = \phi(1+1+\ldots+1) = \phi(0)+\phi(1)+\ldots+\phi(7) \quad \xRightarrow{\text{addition}} \quad 7+7+\ldots+7
\]
\[
= 7 \times \mod 49
\]
So \( \phi(x) = 7x \mod 49 \)

Since \( \mathbb{Z}_{28} = \langle 1 \rangle \), Thm 10.2.8 tells us
\[
\text{image of } \phi = \phi(\mathbb{Z}_{28}) = \phi(\langle 1 \rangle) = \langle \phi(1) \rangle = \langle 7 \rangle
\]

Since \( \phi(x) = 0 \) iff 49 divides \( 7x \), iff 7 divides \( x \)
\[\text{Ker } \phi = \{0, 7, 14, 21\}^3\]

We previously saw \( \phi(27) = 42 \), so
\[
\phi^{-1}(42) = 27 + \text{Ker } \phi = 27 + 3 \times \{0, 7, 14, 21\}
\]
\[
= \{27, 34, 41, 48, 3\}.
\]