Chapter 10

<u>Defn</u>: Let $G, \overline{G}$ be groups. A <u>homomorphism</u> from G to $\overline{G}$ is a map $\phi : G \to \overline{G}$ that preserves the group operation, meaning

$$\forall a,b \in G \quad \phi(ab) = \phi(a)\phi(b)$$

<u>Defn</u>: The <u>kernel</u> of a homomorphism $\phi : G \to \overline{G}$ is

$$\operatorname{Ker}\phi = \{g \in G : \phi(g) = \overline{e}\}$$

↖identity of $\overline{G}$

<u>Obs</u>: An isomorphism is just a homomorphism that is one-to-one and onto. When ϕ is an isomorphism, $\operatorname{Ker}\phi = \{e\}$.

<u>Ex</u>: The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(x) = x \bmod n$ is a homomorphism.

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

<u>Ex</u>: The map $\phi : S_n \to \mathbb{Z}_2$ given by

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

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

<u>Ex</u>: The map $\phi : \mathbb{R}\setminus\{0\} \to \mathbb{R}\setminus\{0\}$ given by $\phi(x) = |x|$ is a homomorphism. $\operatorname{Ker}\phi = \{x \in \mathbb{R}\setminus\{0\} : |x| = 1\} = \{-1, 1\}$

Thm 10.1: Let $\phi: G \to \bar{G}$ be a homomorphism. Then

① $\phi(e) = \bar{e}$ ← identity of $\bar{G}$.

② $\phi(g^n) = \phi(g)^n$ for all $g \in G$, $n \in \mathbb{Z}$

③ If g has finite order, (order of $\phi(g)$) | (order of g)

④ Ker ϕ is a subgroup of G

⑤ for all $a, b \in G$, $\phi(a) = \phi(b) \Leftrightarrow a\,\mathrm{Ker}\,\phi = b\,\mathrm{Ker}\,\phi$

⑥ if $\phi(a) = \bar{a}$ then $\phi^{-1}(\bar{a}) = \{g \in G : \phi(g) = \bar{a}\} = a\,\mathrm{Ker}\,\phi$

Pf: ①② true by same argument in Thm 6.2.

③ If g has order n then

$$\phi(g)^n \overset{②}{=} \phi(g^n) = \phi(e) \overset{①}{=} \bar{e}$$

So order of $\phi(g)$ divides n by Cor 2 of Thm 4.1

④ By ① $e \in \mathrm{Ker}\,\phi$, so Ker ϕ is nonempty.

Now suppose $a, b \in \mathrm{Ker}\,\phi$, meaning $\phi(a) = \bar{e} = \phi(b)$. Then

$$\phi(ab^{-1}) \underset{\substack{\uparrow \\ \phi \text{ is a homomorphism}}}{=} \phi(a)\phi(b^{-1}) \overset{②}{=} \phi(a)\phi(b)^{-1} = \bar{e}(\bar{e})^{-1} = \bar{e}$$

so $ab^{-1} \in \mathrm{Ker}\,\phi$. Thus Ker ϕ is a subgroup (by One-Step Subgroup Test)

⑤ $a\,\mathrm{Ker}\,\phi = b\,\mathrm{Ker}\,\phi \overset{\text{Lem. 7.A}}{\Longleftrightarrow} b^{-1}a \in \mathrm{Ker}\,\phi$ (by Lem 7.A)

$\Longleftrightarrow \phi(b^{-1}a) = \bar{e}$ (definition of Ker ϕ)

$\Longleftrightarrow \phi(b^{-1})\phi(a) = \bar{e}$ (since ϕ is homomorphis

$\Longleftrightarrow \phi(b)^{-1}\phi(a) = \bar{e}$ (by ②)

$\Longleftrightarrow \phi(a) = \phi(b)$ (by multiplying on left by $\phi(b$

⑥ For $g \in G$, $\phi(g) = \bar{a} \Longleftrightarrow \phi(g) = \phi(a)$ (since $\phi(a) = \bar{a}$)

$\Longleftrightarrow g\,\mathrm{Ker}\,\phi = a\,\mathrm{Ker}\,\phi$ (by ⑤)

$\Longleftrightarrow g \in \mathrm{Ker}\,\phi$ (by Lem 7.A)

Therefore $\{g \in G : \phi(g) = \bar{a}\} = a\,\mathrm{Ker}\,\phi$. $\square$

Thm 10.2: Let $G, \overline{G}$ be groups and let H be a subgroup of G. If $\phi : G \to \overline{G}$ is a homomorphism then:

Ⓐ $\phi(H) = \{\phi(h) : h \in H\}$ is a subgroup of $\overline{G}$

Ⓑ H cyclic $\Rightarrow$ $\phi(H)$ cyclic. In fact $H = \langle a \rangle \Rightarrow \phi(H) = \langle \phi(a) \rangle$

Ⓒ H abelian $\Rightarrow$ $\phi(H)$ abelian

Ⓓ H normal in $G \Rightarrow \phi(H)$ normal in $\phi(G)$

Ⓔ $|\phi(H)|$ divides $|H|$

Ⓕ if $\overline{K}$ is a subgroup of $\overline{G}$, then
$\phi^{-1}(\overline{K}) = \{g \in G : \phi(g) \in \overline{K}\}$ is a subgroup of G

Ⓖ if $\overline{K}$ is a normal subgroup of $\overline{G}$ then
$\phi^{-1}(\overline{K})$ is a normal subgroup of G

Pf: Ⓐ Ⓑ Ⓒ true by same argument in proof of Thm 6.3

Ⓓ For any $\phi(h) \in \phi(H)$ and $\phi(g) \in \phi(G)$ we have
$\phi(g)\phi(h)\phi(g)^{-1} \overset{\textcircled{2}}{=} \phi(g)\phi(h)\phi(g^{-1}) = \phi(ghg^{-1})$.
Since H is normal we know $ghg^{-1} \in H$. Therefore
$\phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$. By the Normal Subgroup Test, we conclude $\phi(H)$ is normal in $\phi(G)$.

~~Ⓔ Set $m = |\phi(H)|$ and enumerate the elements of $\phi(H)$ as $\phi(a_1), \phi(a_2), \dots, \phi(a_m)$. By Ⓒ of the previous theorem $\bar{a}_1, a_2, \dots, a_m$. Pick $a_1, a_2, \dots, a_m \in H$ satisfying $\phi(a_1) = \bar{a}_1$, $\phi(a_2) = \overline{a_2}$, $\dots$, $\phi(a_m) = \bar{a}_m$. The set Since $\phi(H) = \{\bar{a}_1, \dots, \bar{a}_m\}$, the sets $\phi^{-1}(\bar{a}_1), \dots, \phi^{-1}(\bar{a}_m)$ partition H. Also, $\phi^{-1}(\bar{a}_i) = a_i$~~

Ⓔ Let $\psi : H \to \phi(H)$ be the restriction of ϕ to H. Then ψ is a homomorphism from H onto $\phi(H)$. Thm 10.1⑥ tells us that for every $\bar{h} \in \phi(H)$ the set of preimages $\psi^{-1}(\bar{h})$ has cardinality $|\text{Ker } \psi|$. Therefore $|H| = |\text{Ker } \psi| \cdot |\phi(H)|$ and $|\phi(H)|$ divides $|H|$.

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

Now suppose $a, b \in \phi^{-1}(\bar{K})$. Then $\phi(a), \phi(b) \in \bar{K}$ so

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} \in \bar{K} \text{ (since } \bar{K} \text{ is a subgroup).}$$

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

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

$$\phi(g)\phi(a)\phi(g)^{-1} \in \bar{K}.$$

Therefore

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in \bar{K}$$

which implies $gag^{-1} \in \phi^{-1}(\bar{K})$. We conclude $\phi^{-1}(\bar{K})$ is normal in G (by Normal Subgroup Test).

□

<u>Cor</u>: If $\phi : G \to \bar{G}$ is any homomorphism then $\text{Ker } \phi$ is a normal subgroup of G.

<u>Pf</u>: Set $\bar{K} = \{\bar{e}\}$. Then $\bar{K}$ is a normal subgroup of $\bar{G}$. So by Thm 10.2Ⓖ $\text{Ker } \phi = \phi^{-1}(\bar{K})$ is normal in G. □

Ex: Define $\phi : \mathbb{Z}_{21} \to \mathbb{Z}_{21}$

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

Then ϕ is a homomorphism since

$$3(x+y) \bmod 21 = 3x+3y \bmod 21 = (3x \bmod 21) \overset{\substack{\text{addition in } \mathbb{Z}_{21} \\ \downarrow}}{+} (3y \bmod 21)$$

Given that $\phi(6) = 18$, find all $x \in \mathbb{Z}_{21}$ satisfying $\phi(x) = 18$.

The kernel of ϕ is

$$\text{Ker}\,\phi = \{0, 7, 14\}$$

Since $\phi(6) = 18$ we have

$$\begin{aligned}\phi^{-1}(18) = \{x \in \mathbb{Z}_{21} : \phi(x) = 18\} &= 6 + \text{Ker}\,\phi \\ &= 6 + \{0, 7, 14\} \\ &= \{6, 13, 20\}\end{aligned}$$

Ex: Suppose $\phi : \mathbb{Z}_{28} \to \mathbb{Z}_{49}$ is a homomorphism satisfying $\phi(9) = 14$.
Determine $\phi(x)$, the image of ϕ, kernel of ϕ, and $\phi^{-1}(42)$

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

$$-\phi(1) \underset{\substack{\uparrow \\ \text{Thm 10.1 ②}}}{=} \phi(-1) \underset{\substack{\uparrow \\ \text{27 is inverse} \\ \text{of 1 in } \mathbb{Z}_{28}}}{=} \phi(27) = \phi(9+9+9) \underset{\substack{\uparrow \\ \text{since } \phi \text{ is a} \\ \text{homomorphism}}}{=} \phi(9)+\phi(9)+\phi(9) = 14+14+14 = 42$$
)

In $\mathbb{Z}_{49}$, the inverse of 42 is 7, so $\phi(1) = 7$

Then for any $x \in \mathbb{Z}_{28}$ we have

$$\begin{aligned}\phi(x) = \phi(\overbrace{1+1+\cdots+1}^{x \text{ summands}}) &= \overbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}^{x \text{ summands}} \quad \leftarrow \text{addition mod } 49 \\ &= 7+7+\cdots+7 \\ &= 7x \mod 49\end{aligned}$$

So $\phi(x) = 7x \mod 49$

Since $\mathbb{Z}_{28} = \langle 1 \rangle$, Thm 10.2Ⓑ 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

$$\text{Ker}\,\phi = \{0, 7, 14, 21\}$$

We previously saw $\phi(27) = 42$, so

$$\begin{aligned}\phi^{-1}(42) = 27 + \text{Ker}\,\phi &= 27 + \{0, 7, 14, 21\} \\ &= \{27, 34, 41, 48\}.\end{aligned}$$

Thm 10.3 (First Isomorphism Theorem):

Let $\phi : G \to \overline{G}$ be a group homomorphism

Then the map

$$\begin{aligned} G/\text{Ker}\,\phi &\longrightarrow \phi(G) \\ g\,\text{Ker}\,\phi &\longmapsto \phi(g)\end{aligned}$$

is an isomorphism and $G/\text{Ker}\,\phi \approx \phi(G)$

Pf: Define $\psi: G/\text{Ker}\,\phi \to \phi(G)$ by $\psi(g\text{Ker}\,\phi) = \phi(g)$.
(It makes sense to define ψ in this way since
Thm 10.1 ⑤ tells us $a\text{Ker}\,\phi = b\text{Ker}\,\phi \Longrightarrow \phi(a) = \phi(b)$)
We check ψ is an isomorphism.

(One-to-one) If $\psi(a\text{Ker}\,\phi) = \psi(b\text{Ker}\,\phi)$
then $\phi(a) = \psi(a\text{Ker}\,\phi) = \psi(b\text{Ker}\,\phi) = \phi(b)$
and Thm 10.1 ⑤ tells us $a\text{Ker}\,\phi = b\text{Ker}\,\phi$.

(Onto) Every element of $\phi(G)$ is of the form $\phi(g)$ for some $g \in G$ and we have

$$\phi(g) = \psi(g\text{Ker}\,\phi)$$

(Preserves group operation)

$$\begin{aligned}\psi(a\text{Ker}\,\phi \cdot b\text{Ker}\,\phi) &= \psi(ab\text{Ker}\,\phi)\\ &= \phi(ab) = \phi(a)\phi(b)\\ &= \psi(a\text{Ker}\,\phi)\psi(b\text{Ker}\,\phi) \quad \square\end{aligned}$$

Thm 10.4 : Every normal subgroup is the kernel of some homomorphism:
if N is a normal subgroup of G then
N is the kernel of the homomorphism
$\phi: G \to G/N$ defined by $\phi(g) = gN$.

Pf: ϕ is a homomorphism because $\phi(ab) = abN = aNbN = \phi(a)\phi(b)$.
Finally, $\phi(g) = N$ (the identity of G/N)
$\iff gN = N \overset{\text{Lem 7.A}}{\iff} g \in N$. Thus $\text{Ker}\,\phi = \{g \in G : \phi(g) = N\} = N$. $\square$