Lecture 21

In this lecture, we'll prove the First Isomorphism Theorem which has many important consequences. Before stating the theorem, let's see why, intuitively, it should be true.

Proposition 1 (Properties of Kernel)

Let $\varphi : G \to \overline{G}$ be a homomorphism and $\ker(\varphi)$ be its kernel. Then

1) $\ker(\varphi) \triangleleft G$.

2) $\varphi(a) = \varphi(b) \iff a\ker(\varphi) = b\ker(\varphi)$.

3) If $\varphi(g) = \bar{g}$, then $\varphi^{-1}(\bar{g}) = \{x \in G \mid \varphi(x) = \bar{g}\}$
$= g\ker\varphi$.

4) If $|\ker\varphi| = n$, then φ is an n-to-1 mapping from $G \to \overline{G}$.

5) If φ is onto then φ is an isomorphism $\Leftrightarrow$ $\ker(\varphi) = \{e\}$.

Proof 1) We have already proved this.

2) This is saying that two elements in G have same image in $\bar{G}$ $\Leftrightarrow$ the cosets $a\ker\varphi$ and $b\ker\varphi$ are the same.

Suppose $a\ker\varphi = b\ker\varphi$. Then

$a = bg$ where $g \in \ker\varphi$. Then $\varphi(a) = \varphi(bg)$
$= \varphi(b)\varphi(g) = \varphi(b)\bar{e}$ (as $g \in \ker\varphi$).

So $\varphi(a) = \varphi(b)$.

Suppose $\varphi(a) = \varphi(b)$. We want to show that $a\ker\varphi = b\ker\varphi$. From Lec. 9 we know that

$a\ker\varphi = b\ker\varphi \Leftrightarrow b^{-1}a \in \ker\varphi$.

Now $\varphi(b^{-1}a) = \varphi(b^{-1})\varphi(a) = \varphi(b)^{-1}\varphi(a) = \bar{e}^{-1}\bar{e}$
$= \bar{e}$

So $b^{-1}a \in \ker\varphi$. Thus $a\ker\varphi = b\ker\varphi$.

3) This is saying that if $\varphi(g) = \bar{g}$, then the inverse image of $\bar{g}$ is the coset $g\ker\varphi$.

We'll prove $\varphi^{-1}(\bar{g}) \subseteq g\ker\varphi$ and

$g\ker\varphi \subseteq \varphi^{-1}(\bar{g})$

If $x \in \varphi^{-1}(\bar{g}) \Rightarrow \varphi(x) = \bar{g} = \varphi(g)$

So from 2) $x\ker\varphi = g\ker\varphi \Rightarrow x \in g\ker\varphi$

$\Rightarrow \varphi^{-1}(\bar{g}) \subseteq g\ker\varphi$.

Now let $gb \in g\ker\varphi$ for $b \in \ker\varphi$. Then

$\varphi(gb) = \varphi(g)\cdot\varphi(b) = \varphi(g)\cdot\bar{e} = \varphi(g) \Rightarrow$

$gb \in \varphi^{-1}(\bar{g})$. So, $g\ker\varphi \subseteq \varphi^{-1}(\bar{g})$. Hence the statement.

4) This is saying if $|\ker\varphi| = n$, then exactly

n elements in G have the same image in $\overline{G}$.

Recall from Lec. 9 that for any coset $g\ker\varphi$,

$|g\ker\varphi| = |\ker\varphi| = n$.

So 4) follows.

5) Suppose φ is onto. φ is already a homomorphism. So we need to prove that φ is one-to-one $\Leftrightarrow$ $\ker(\varphi) = \{e\}$.

But this follows from 4).

$\square$

So from the above proposition, we observe that $\ker\varphi$ is sort of "preventing" (or "hindering") φ to be an isomorphism. So it seems that if we somehow, "collapse" all the elements of $\ker\varphi$ then φ might be an isomorphism.

But collapsing really means taking quotient by $\ker\varphi$. So, if we can take quotient by $\ker\varphi$ and somehow get a group, then the result might be isomorphic to $\overline{G}$.

But $\ker(\varphi) \triangleleft G$, so $\dfrac{G}{\ker\varphi}$ is indeed a group!

<u>Theorem</u> [First Isomorphism Theorem]

Let $\varphi : G \to \overline{G}$ be an onto homomorphism.

Then $\dfrac{G}{\ker(\varphi)} \cong \overline{G}$.

<u>Proof</u> Let us define $T : \dfrac{G}{\ker\varphi} \to \overline{G}$ by

$$T\left(g\ker\varphi\right) = \varphi(g)$$

Let's remember the second principle.

Whenever you define a map from a quotient group to another group, alway check that it is well-defined.

why? Because elements in a quotient group are cosets, and we have seen that $a \neq b$ in G can still give $a\,\mathrm{Ker}\,\varphi = b\,\mathrm{Ker}\,\varphi$. So we want to make sure that if two elements are same in $\frac{G}{\mathrm{Ker}\,\varphi}$, then their image under T are also same.

<u>T is well-defined.</u>

Let $a\,\mathrm{Ker}\,\varphi = b\,\mathrm{Ker}\,\varphi$. Then from 2) in Prop. 1, we know that $\varphi(a) = \varphi(b)$, i.e.,

$$T(a\,\mathrm{Ker}\,\varphi) = T(b\,\mathrm{Ker}\,\varphi).$$

<u>T is one-to-one</u>

Let $T(a\ker\varphi) = T(b\ker\varphi)$. Then

$\varphi(a) = \varphi(b) \Rightarrow$ from 2) Prop. 1

$a\ker\varphi = b\ker\varphi$.

<u>T is onto</u>

Since φ is onto $\Rightarrow$ for $\bar{g} \in \bar{G}$ $\exists$ $g \in G$ s.t.

$\varphi(g) = \bar{g}$. So $T(g\ker\varphi) = \varphi(g) = \bar{g}$.

<u>T is a homomorphism</u>

Let $a\ker\varphi, b\ker\varphi \in \frac{G}{\ker\varphi}$

Then
$$
\begin{aligned}
T\big((a\ker\varphi)(b\ker\varphi)\big) &= T(ab\ker\varphi) \\
&= \varphi(ab) = \varphi(a)\varphi(b) \\
&= T(a\ker\varphi)T(b\ker\varphi)
\end{aligned}
$$

Thus T is an isomorphism and hence

$$\frac{G}{\ker\varphi} \cong \overline{G}.$$

$\blacksquare$

Remark If $\varphi : G \to \overline{G}$ is not onto then the above theorem becomes $\dfrac{G}{\ker\varphi} \cong \varphi(G)$.

Corollary If $\varphi : G \to \overline{G}$ is a homomorphism where $|G| < \infty$, $|\overline{G}| < \infty$, then $|\varphi(G)| \,\big|\, |\overline{G}|$ and $|\varphi(G)| \,\big|\, |G|$

Proof Note that $\varphi(G) \leq \overline{G} \Rightarrow$ from Lagrang-
-es theorem, $|\varphi(G)| \,\big|\, |G'|$.

Also from the Remark above

$$\frac{G}{\ker\varphi} \cong \varphi(G) \Rightarrow \frac{|G|}{|\ker\varphi|} = |\varphi(G)|$$

$$\Rightarrow \quad |\varphi(G)| \,\big|\, |G|.$$

$\blacksquare$

Examples :-

1) Consider $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by

$$\varphi(a) = a \bmod n \quad , a \in \mathbb{Z}.$$

Then φ is onto and $\ker(\varphi) = \langle n \rangle$

So $$\frac{\mathbb{Z}}{\langle n \rangle} \cong \mathbb{Z}_n .$$

Theorem Let G be a group and $Z(G)$ be the center of G. Then $\frac{G}{Z(G)} \cong \mathrm{Inn}(G)$.

Proof :- We'll use the First Isomorphism theorem.

Define $T : G \to \mathrm{Inn}(G)$ by

$T(g) = \varphi_g$, the inner automorphism induced by g.

Clearly T is onto. Let's find $\ker(T)$.

Let $a \in \ker T$, i.e, $T(a) = I$ where I is the identity automorphism of G. Also, by definition $T(a) = \varphi_a$. So for $g \in G$,

$$\varphi_a(g) = a g a^{-1} = g$$

$$\Rightarrow \quad ag = ga \quad \Rightarrow \quad a \in Z(G)$$

So $\quad \mathrm{Ker}(T) \subseteq Z(G)$.

We've already seen that for $g \in Z(G)$, φ_g, the inner automorphism induced by g is I.

So $\quad Z(G) \subseteq \mathrm{Ker}(T)$.

Thus $\quad Z(G) = \mathrm{Ker}(T)$

So by the first isomorphism theorem,

$$\frac{G}{Z(G)} \cong \mathrm{Inn}(G).$$

$\square$

We'll end this lecture by proving that every normal subgroup of a group is actually a kernel of some isomorphism.

Theorem [Normal subgroups are kernels]

Let $N \triangleleft G$. Then N is the kernel of some homomorphism of G. More precisely, the map

$$\varphi : G \to \frac{G}{N}, \quad \varphi(g) = gN \text{ has kernel } N.$$

Proof Since $N \triangleleft G \Rightarrow \frac{G}{N}$ is a group.

Consider $\varphi : G \to \frac{G}{N}$ by $\varphi(g) = gN$

φ is onto. Also $\varphi(gh) = ghN = gNhN = \varphi(g)\varphi(h)$

So φ is a homomorphism. Let $h \in \ker(\varphi)$, i.e,

$\varphi(h) = N \Leftrightarrow hN = N \Leftrightarrow h \in N$. So

$\ker(\varphi) \subseteq N$ and clearly $N \subseteq \ker(\varphi)$.

So $\ker(\varphi) = N$.

$\boxtimes$

Remark :- The map $\varphi : G \to G/N$ by

$\varphi(g) = gN$ is called the natural homomorphism from G to G/N.