Sec 1: 1st Isomorphism Thm

- **1st Iso Thm:**
  Let $f: G \to H$ is a group homomorphism with $K = \ker f$
  Note that we've proven that $\ker f \lhd G$, so $G/K = \{xK \mid x \in G\}$ is a group (called quotient group).

- Let $i: G/K \longrightarrow \mathrm{Im}(f)$ be defined by
  $gK \longmapsto f(g)$ for all $gK \in G/K$.

  Then i is an isomorphism.

- Prove that i is well-defined:
  We need to show that if $aK = bK$ then $i(aK) = i(bK)$.
  Suppose $aK = bK$.
  Then for some $k \in K$, $ak \overset{(*)}{=} b$.
  So

$$
\begin{aligned}
i(aK) &= f(a) \\
&= f(a)\, e \\
&= f(a) f(k) && \text{since } k \in K = \ker f \\
&= f(ak) && \text{since } f \text{ is a homomorphism} \\
&= f(b) && \text{by } (*) \\
&= i(bK) && \text{by def of } i.
\end{aligned}
$$

1. Prove that i is a homomorphism:
   We need to show that $i(aK \cdot bK) = i(aK)\, i(bK)$.
   Recall from the def of quotient groups that $aK \cdot bK \overset{\text{def}}{=} abK$.

$$
\begin{aligned}
i(aK \cdot bK) &= i(abK) && \text{by def of the binary operation of } G/K. \\
&= f(ab) && \text{by def of } i \\
&= f(a) f(b) && \text{since } f \text{ is a homomorphism} \\
&= i(aK)\, i(bK) && \text{by def of } i. \ \boxed{1}
\end{aligned}
$$

2. Prove that i is surjective:
   We need to show that for each $h \in \overbrace{\mathrm{Im}(f)}^{\text{codomain}}$, there is $gK \in \overbrace{G/K}^{\text{domain}}$ with $i(gK) = h$.

   Let $y \in \mathrm{Im}(f)$. By def, $\mathrm{Im}(f) = \{f(g) \mid g \in G\}$, so there is $x \in G$ with $f(x) = y$

   Then $i(xK) = f(x) = y$. $\boxed{2}$

3. Prove that $\bar{\iota}$ is injective:
We need to show that $\bar{\iota}(aK) = \bar{\iota}(bK)$ implies $aK = bK$.

Suppose $\bar{\iota}(aK) = \bar{\iota}(bK)$.
Then $f(a) = f(b)$ by def of $\bar{\iota}$

Then $[f(b)]^{-1} f(a) = e$ by left multiplication on both sides

Then $f(b^{-1}) f(a) = e$ by Prop 1 of basic homomorphism properties

Then $f(b^{-1}a) = e$ since f is a homomorphism

So $b^{-1}a \in \ker f = K$ by def of $\ker f$.

So $b^{-1}aK = K$ (we've seen that $x \in \underbrace{H}_{\text{subgroup}} \Rightarrow xH = H$)

We claim that $aK = bK$. To prove this, it's enough to show $b \in aK$.

To show $b \in aK$, note that there is $k \in K$ with $b^{-1}ak = e$.
Then $ak = b$, so $b \in aK$. $\boxed{3}$

4. Example: Prove that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Recall that $\mathbb{Z}_n \overset{\text{def}}{:=} \{0, 1, 2, 3, \dots, n-1\}$

$$n\mathbb{Z} \overset{\text{def}}{:=} \{\text{integer multiples of } n\}$$
$$= \{nz \mid z \in \mathbb{Z}\}$$
$$= \{\dots, -n, 0, n, 2n, 3n, \dots\}$$

Define $f: \mathbb{Z} \longrightarrow \mathbb{Z}_n$
by $z \longmapsto z \pmod n$

Let $K \overset{\text{def}}{:=} \ker f = \{\text{integer multiples of } n\} = n\mathbb{Z}$.

The elements of $\underbrace{\mathbb{Z}/K = \mathbb{Z}/n\mathbb{Z}}_{\text{quotient group}}$ are the cosets

$0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $2 + n\mathbb{Z}$, ..., $n+1 + n\mathbb{Z}$
K, $1 + K$, $2 + K$, ..., $n+1 + K$

By the 1st Isomorphism Thm, $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im}(f)$.
But $\operatorname{Im}(f) = \mathbb{Z}_n$, so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. $\boxed{4}$