Section 13  The Fundamental Theorem of Group Homomorphisms

Def. Let \( \phi : (G, \cdot) \rightarrow (G', \#) \) be a homomorphism of \( G \) into \( G' \). Let \( \epsilon \) be the identity of \( (G, \#) \).

Let \( K = \{ x \in G \mid (x) \phi = \epsilon \} \).

\( K \) is called the kernel of \( \phi \).

\( \text{Theorem 1} \) \( K \) is a normal subgroup of \( G \).

**Note:** \( aK \) is a left coset of \( K \) where \( a \in G \).

Recall \( aK = \{ ak \mid aK \in K \} \). Then \( (aK) \phi = (a) \phi \# (b) \phi \)

\( = (a) \phi \# (b) \phi = (a) \phi \# \epsilon = (a) \phi \# \epsilon = (a) \phi \) is a left coset.

\( \text{Theorem 2} \) Let \( \phi : G \rightarrow G' \) be a homomorphism, where \( G \) and \( G' \) are groups. Suppose \( K = \text{Kernel of } \phi \). Then \( G/K \cong G' \).

In particular the mapping \( \tilde{\phi} : (G/K, \#) \rightarrow (G', \#) \) defined by

\( (aK) \tilde{\phi} = (a) \phi \) \( \forall aK \in G/K \).

Moreover \( \tilde{\phi} \) is a well-defined 1-1 mapping of \( G/K \) onto \( G' \) and the kernel of \( \tilde{\phi} \) is \( K \). More importantly, \( \tilde{\phi} \) is a homomorphism, i.e., \( [(aK) \# (bK)] \tilde{\phi} = (aK) \tilde{\phi} \cdot (bK) \tilde{\phi} \) \( \forall aK, bK \in G/K \).

\( \text{Note: This means } |G/K| = |G'| \). In particular if \( G \) is finite, then \( |G| \) divides \( |G'| \).

**Theorem 3** Let \( H \) be a normal subgroup of \( (G, \cdot) \). Define \( \gamma : G \rightarrow G/H \) by \( (x) \gamma = xH \) \( \forall x \in G \). Then \( \gamma \) is a homomorphism of \( G \) onto \( G/H \) and the kernel of \( \gamma \) is \( H \).

Putting Theorem 2 and Theorem 3 together, we have that
Up to isomorphism, the set of homomorphic images of $G$ (i.e., the set of groups $\overline{G}$ for which $\exists$ a homomorphism $\psi$ from $G$ onto $\overline{G}$) is $\mathcal{G} / \mathcal{H}$, where $\mathcal{H}$ is a normal subgroup of $G$.

Note: $\psi$ is called the canonical or natural mapping of $G$ onto $G / \mathcal{H}$.

Theorem 2 and Theorem 3 together form the Fundamental Theorem of Group Homomorphisms along with the following diagram:

\[
\begin{array}{ccc}
G & \xrightarrow{\phi} & \overline{G} \\
\downarrow{\gamma} & & \downarrow{\gamma} \\
G / \mathcal{H} & \xrightarrow{\psi} & \end{array}
\]

where
- $\phi$ is a given homomorphism of $G$ onto $\overline{G}$ with kernel $\mathcal{H}$.
- $\gamma$ is the canonical mapping given by $\gamma(x) = x + \mathcal{H}$, $\forall x \in G$.
- $\psi$ is the mapping given by $\psi(a + \mathcal{H}) = \phi(a)$, $\forall a \in G$.

Then $\gamma \circ \psi = \phi$

and we say the above diagram is commutative.

One other observation:

We have the groups $\big( \mathbb{Z} / \langle n \rangle, \ast \big)$ and $\big( \mathbb{Z}_n, +_n \big)$.

The elements of $\mathbb{Z} / \langle n \rangle$ are of the form $a + \langle n \rangle = a + kn$, $\forall k \in \mathbb{Z}$.

This means $\mathbb{Z} / \langle n \rangle = \mathbb{Z}_n$ as sets.

This also means $a + \langle n \rangle \ast (b + \langle n \rangle) = (a + b) + \langle n \rangle$ by definition of $\ast$.

This means $\ast$ and $+_n$ are the exact same operation.

Thus, the groups $\big( \mathbb{Z} / \langle n \rangle, \ast \big)$ and $\big( \mathbb{Z}_n, +_n \big)$ are exactly the same.