Definition 10.1 (Homomorphism)**.** *For any group G and $\overline{G}$, a* ***homomorphism*** *is a mapping from G to $\overline{G}$ that preserves structure. That is, $\forall a\ b \in G, \phi(ab) = \phi(a)\phi(b)$.*

Definition 10.2 (Kernel of Homomorphism)**.** *The* ***kernel*** *of a homomorphism $\phi : G \to \overline{G}$ is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by* $\operatorname{Ker} \phi$

The following lemmas assumes $\phi : G \to \overline{G}$ is a homomorphism.

Lemma 10.1 (Homomorphism Preserves identity)**.** $\phi(e_G) = e_{\overline{G}}$.

Proof. $\phi(g) = \phi(eg) = \phi(e)\phi(g)$, by cancellation, $\phi(e) = e_{\overline{G}}$. □

Lemma 10.2 (Homomorphism Preserves Inverse)**.** $\forall g \in G, \phi(g^{-1}) = \phi(g)^{-1}$.

Proof. $e_{\overline{G}} = \phi(e_G) = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$, then $\phi(g)^{-1} = \phi(g^{-1})$. □

Lemma 10.3 (Homomorphism Preserves Power)**.** $\forall g \in G, n \in Z, \phi(g^n) = \phi(g)^n$.

Proof. Induction on n.

- Base: $\phi(g^0) = \phi(g)^0$ by Lemma 10.1.
- Negative Direction:

$$
\begin{aligned}
&\phi(g^{-(n+1)}) \\
=&\phi(g^{-n-1}) \\
=&\phi(g^{-n}g^{-1}) \\
=&\phi(g^{-n})\phi(g^{-1}) \\
=&\phi(g^{-n})\phi(g)^{-1} \\
=&\phi(g)^{-n}\phi(g)^{-1} && \text{(By induction hypothesis)} \\
=&\phi(g)^{-(n+1)}
\end{aligned}
$$

- Positive Direction: Similarly to the negative direction.

□

Lemma 10.4 (Image of Homomorphism is Subgroup)**.** $\phi(G) = \{\phi(g) \mid g \in G\}$ *is subgroup of $\overline{G}$.*

Proof. By three-steps:

- $\phi(e) \in \phi(G)$
- For any $\phi(a)\ \phi(b) \in \phi(G)$, $\phi(a)\phi(b) = \phi(ab) \in \phi(G)$.
- For ang $\phi(a) \in \phi(G)$, $\phi(a)^{-1} = \phi(a^{-1}) \in \phi(G)$.

$\square$

Lemma 10.5 (Homomorphism on Order). *For any $g \in G$, if $|g|$ is finite, $|\phi(g)|$ divides $|g|$; If $|G|$ is finite, $|\phi(g)|$ divides $|g|$ and $|\phi(G)|$.*

Proof. Let $|g| = n$, $\phi(g)^n = \phi(g^n) \to \phi(g)^n = e$, then $|\phi(g)|$ divides n.

Since $|G|$ is finite, so is $|g|$, and we proved $|\phi(g)|$ divides $|g|$. Since $\phi(G)$ is a subgroup of $\overline{G}$ and $\phi(g) \in \phi(G)$, $|\phi(g)|$ divides $|\phi(G)|$. $\square$

Lemma 10.6 (Kernel is Subgroup). $\operatorname{Ker}\phi$ *is a subgroup of G.*

Proof. By three-steps:

- $\phi(e) = e$ so $e \in \operatorname{Ker}\phi$.
- For any $a\ b \in \operatorname{Ker}\phi$, $\phi(ab) = \phi(a)\phi(b) = e$ so $ab \in \operatorname{Ker}\phi$.
- For any $a \in \operatorname{Ker}\phi$, $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$ so $a^{-1} \in \operatorname{Ker}\phi$.

$\square$

Lemma 10.7. *For any $a\ b \in G$, $\phi(a) = \phi(b) \iff a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$.*

Proof. ($\Longrightarrow$) $\phi(a)^{-1}\phi(b) = \phi(a^{-1})\phi(b) = \phi(a^{-1}b) = e \to a^{-1}b \in \operatorname{Ker}\phi$ then $a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$.

($\Longleftarrow$) $a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$ imples $a^{-1}b \in \operatorname{Ker}\phi$ imples $\phi(a^{-1}b) = e$ imlpes $\phi(a^{-1})\phi(b) = e$ imples $\phi(a)^{-1}\phi(b) = e$ imples $\phi(a) = \phi(b)$ $\square$

Lemma 10.8 (Inverse Image of Homomorphism). *For any $g \in G$, if $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\operatorname{Ker}\phi$.*

Proof. Let $x \in \phi^{-1}(g')$, then $\phi(x) = g'$, by $\phi(g) = g'$ we have $\phi(x) = \phi(g)$ and $x\operatorname{Ker}\phi = g\operatorname{Ker}\phi$, thus $x \in g\operatorname{Ker}\phi$.

Let $gx \in \operatorname{Ker}\phi$ where $\phi(x) = e$. $\phi(gx) = \phi(g)\phi(x) = g'e = g'$, thus $gx \in \phi^{-1}(g')$. $\square$

Theorem 10.1 (Properties of Homomorphism). *The propositions above are true.*

Proof. Trivial. $\square$

The following lemmas assume H is a subgroup of G.

Theorem 10.2 (Properties of Subgroups Under Homomorphisms). *The following propositions are true.*

Lemma 10.9 (Homomorphism Preserves Subgroup). *$\phi(H)$ is a subgroup of $\phi(\overline{G})$.*

Proof. By three-steps:

- $\phi(e) \in \phi(H)$.
- For any $\phi(a)$ $\phi(b) \in \phi(H)$, $\phi(a)\phi(b) = \phi(ab) \in \phi(H)$.
- For any $\phi(a) \in \phi(H)$, $\phi(a)^{-1} = \phi(a^{-1}) \in \phi(H)$.

$\square$

Lemma 10.10 (Homomorphism Preserves Cyclic). *If H is cyclic, then $\phi(H)$ is cyclic.*

Proof. Let $H = \langle h \rangle$. For any $\phi(h^n) \in \phi(H)$, $\phi(h^n) = \phi(h)^n$, thus $\phi(H) = \langle \phi(h) \rangle$. $\square$

Lemma 10.11 (Homomorphism Preserves Abelian). *If H is Abelian, then $\phi(H)$ is Abelian.*

Proof. For any $\phi(a)$ $\phi(b) \in \phi(H)$. $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$. $\square$

Lemma 10.12 (Homomorphism Preserves Normality). *If $H \triangleleft G$, then $\phi(H) \triangleleft \phi(G)$.*

Proof. For any $\phi(g) \in \phi(G)$ and $\phi(h) \in \phi(H)$.

$$\begin{aligned}
&\phi(g)\phi(h)\phi(g)^{-1} \\
=&\phi(ghg^{-1}) \\
=&\phi(h') \in \phi(H) && \text{(By } H \triangleleft G\text{)}
\end{aligned}$$

$\square$

Lemma 10.13. *If* $|\operatorname{Ker}\phi| = n$*, then* ϕ *is an* n*-to-*1 *mapping from* G *onto* $\phi(G)$*.*

Proof. It is trivial that ϕ is G onto $\phi(G)$.

Let $g \in G$, and for any $x \in \operatorname{Ker}\phi$, $\phi(xg) = \phi(x)\phi(g) = \phi(g)$. In other words, $\phi(g \operatorname{Ker}\phi) = \{\phi(g)\}$. □

Lemma 10.14. *If* H *is finite, then* $|\phi(H)|$ *divides* $|H|$*.*

Proof. Let $K = H \cap \operatorname{Ker}\phi$, since both H and $\operatorname{Ker}\phi$ are subgroups of G, so is K.

We will show that K is normal in H. For any $h \in H$ and $k \in K$, since h, h^{-1} and k are in H, so is hkh^{-1}. $\phi(hkh^{-1}) = \phi(h)\phi(k)\phi(h^{-1}) = \phi(h)e\phi(h^{-1}) = e$ so $hkh^{-1} \in \operatorname{Ker}\phi$. So $hkh^{-1} \in K$.

Then we show $H/K \approx \phi(H)$. We claim the following function is an isomorphism:

$$\boxed{\psi(hK) = \phi(h)}$$

But first of all, we need to show it **is** a function. For any hK and kK in H/K, and $hK = kK$. We have $h^{-1}k \in K$ which implies $h^{-1}k \in \operatorname{Ker}\phi$ and then $h \operatorname{Ker}\phi = k \operatorname{Ker}\phi \to \phi(h) = \phi(k)$.

- One-to-one: If $\psi(hK) = \psi(kK)$, then $\phi(h) = \phi(k)$ and $h \operatorname{Ker}\phi = k \operatorname{Ker}\phi$. Since h and k are in H, $hH = kH = H$. So:

$$\begin{aligned}
hK &= h(H \cap \operatorname{Ker}\phi) \\
&= hH \cap h \operatorname{Ker}\phi && \text{(Since } \lambda x.hx \text{ is injective)} \\
&= kH \cap k \operatorname{Ker}\phi \\
&= k(H \cap \operatorname{Ker}\phi) \\
&= kK
\end{aligned}$$

- Onto: For any $\phi(h) \in \phi(H)$ for some h, $\psi(hK) = \phi(h)$.

- Structure-Preserve:

$$\begin{aligned}
\psi(hKkK) &= \psi(hkK) \\
&= \phi(hk) \\
&= \phi(h)\phi(k) \\
&= \psi(hK)\psi(kK)
\end{aligned}$$

Thus, $|\phi(H)| = \dfrac{|H|}{|K|}$. $\square$

Lemma 10.15 (Kernel is Normal)**.** $\operatorname{Ker}\phi$ *is normal in* G

Proof. We need to show: $\forall g \in G, g(\operatorname{Ker}\phi)g^{-1} \subseteq \operatorname{Ker}\phi$. For any $g \in G$ and $k \in \operatorname{Ker}\phi$, $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e\phi(g^{-1}) = e$. So $gkg^{-1} \in \operatorname{Ker}\phi$. $\square$

Lemma 10.16. $\phi(Z(G))$ *is a subgroup of* $Z(\phi(G))$.

Proof. For any $\phi(g) \in \phi(Z(G))$ for some $g \in Z(G)$. For any $\phi(a) \in \phi(G)$, $\phi(a)\phi(g) = \phi(ag) = \phi(ga) = \phi(g)\phi(a)$, so $\phi(g) \in Z(\phi(G))$. Thus $\phi(Z(G)) \subseteq Z(\phi(G))$.

Then by three-steps:

- $\phi(e) \in \phi(Z(G))$.
- For any $\phi(a)$ $\phi(b) \in \phi(Z(G))$ where a $b \in Z(G)$, $\phi(a)\phi(b) = \phi(ab) \in \phi(Z(G))$.
- For any $\phi(a) \in \phi(Z(G))$ where $a \in Z(G)$, $\phi(a)^{-1} = \phi(a^{-1}) \in \phi(Z(G))$.

$\square$

Lemma 10.17 (Inverse Image of Subgroup is Subgroup)**.** *If* $\overline{K}$ *is a subgroup of* $\overline{G}$*, then* $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ *is a subgroup of* G.

Proof. It is clearly a subset of G.

We will prove it is a subgroup by three-steps:

- $\phi(e) \in \overline{K}$
- For any a $b \in \phi^{-1}(\overline{K})$, $\phi(ab) = \phi(a)\phi(b)$ where $\phi(a)$ $\phi(b) \in \overline{K}$, so is $\phi(ab)$.
- For any $a \in \phi^{-1}(\overline{K})$, $\phi(a^{-1}) = \phi(a)^{-1}$ where $\phi(a) \in \overline{K}$, so is $\phi(a)^{-1}$.

$\square$

Lemma 10.18 (Inverse Image of Normal is Normal)**.** *If* $\overline{K}$ *is a normal subgroup of* G*, then* $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ *is a normal subgroup of* G.

Proof. We proved that $\phi^{-1}(\overline{K})$ is a subgroup of G.

For any $g \in G$ and $k \in \phi^{-1}(\overline{K})$, $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \overline{k}' \in \overline{K}$ since $\overline{K}$ is normal, thus $gkg^{-1} \in \phi^{-1}(\overline{K})$. □

Lemma 10.19. *If $\phi : G \to \overline{G}$ is onto and $\operatorname{Ker}\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$*

Proof. We need to show ϕ is one-to-one.

For any $\phi(a)$ and $\phi(b)$ such that $\phi(a) = \phi(b)$. We know $a \operatorname{Ker}\phi = b \operatorname{Ker}\phi$, but $\operatorname{Ker}\phi = \{e\}$. So $\{a\} = \{b\}$ implies $a = b$. □

Theorem 10.3 (First Isomorphism Theorem). *Let $\phi : G \to \overline{G}$, then the mapping from $G/\operatorname{Ker}\phi$ to $\phi(G)$, given by $g \operatorname{Ker}\phi \mapsto \phi(g)$ is an isomorphism.*

Proof. We denote that isomorphism as ψ. First, we need to show ψ **is** a function. That is, for any $g \operatorname{Ker}\phi$ and $h \operatorname{Ker}\phi$, if $g \operatorname{Ker}\phi = h \operatorname{Ker}\phi$, then $\psi(g \operatorname{Ker}\phi) = \psi(h \operatorname{Ker}\phi)$.

If $g \operatorname{Ker}\phi = h \ker\phi$, by Lemma 10.7, we know $\phi(g) = \phi(h)$ and then $\psi(g \operatorname{Ker}\phi) = \psi(h \operatorname{Ker}\phi)$.

Then we need to show it is an isomorphism:

- One-to-one: If $\psi(g \operatorname{Ker}\phi) = \psi(h \operatorname{Ker}\psi)$, $\phi(g) = \phi(h)$ gives $g \operatorname{Ker}\phi = h \operatorname{Ker}\phi$.
- Onto: For any $\phi(g) \in \phi(G)$ for some $g \in G$, we have $\psi(g \operatorname{Ker}\phi) = \phi(g)$.
- Structure-Preserve: For any $g \operatorname{Ker}\phi$ and $h \operatorname{Ker}\phi$:

$$\begin{aligned}
&\psi(g \operatorname{Ker}\phi h \operatorname{Ker}\phi) \\
=&\psi(gh \operatorname{Ker}\phi) \\
=&\phi(gh) \\
=&\phi(g)\phi(h) \\
=&\psi(g \operatorname{Ker}\phi)\psi(h \operatorname{Ker}\phi)
\end{aligned}$$

□

Lemma 10.20 (N/C Theorem). *Suppose H is a subgroup of G, the normalizer $N(H) = \{x \in G \mid xHx^{-1} = H\}$, and the centerlizer $C(H) = \{x \in G \mid \forall h \in H, xh = hx\}$ (or equivalently, $\{C(H) = \{x \in G \mid \forall h \in H, xhx^{-1} = h\}\}$). Consider the homomorphism $\psi(g) = \phi_g : N(H) \to \operatorname{Aut}(H)$. $N(H)/C(H)$ is isomorphic to some subgroup of $\operatorname{Aut}(H)$.*

Proof. It is easy to show that $C(H) = \operatorname{Ker}\psi$. Since for any $g \in N(H)$, $\psi(g) = \phi_e \to \phi_g = \phi_e$, then, g commutes with any $h \in H$, thus $g \in C(H)$. And for any $g \in C(H)$, $\psi(g) = \phi_g$, since g commutes with any $x \in H$, we have $\phi_g(x) = gxg^{-1} = xgg^{-1} = x$. This tell us that $\psi(g) = \phi_g = \phi_e$, thus $\psi(h) \in \operatorname{Ker}\psi$.

Thus $N(H)/C(H) = N(H)/\operatorname{Ker}\psi$, by Theorem 10.3, $N(H)/C(H) \approx \psi(H)$ which is a subgroup of $\operatorname{Aut}(H)$. □

Theorem 10.4 (Normal Subgroups are Kernels)**.** *Let $H \triangleleft G$, H is a kernel of some homomorphism of G. In particular, H is a kernel of the mapping $\gamma(g) = gH$ from G to G/H.*

Proof. First, we need to show γ is a homomorphism. For any $a\ b \in G, \gamma(ab) = abH = aHbH = \gamma(a)\gamma(b)$.

For any $h \in H$, $\gamma(h) = hH = H$ because $h \in H$, since H is the identity of G/H, $H \subseteq \operatorname{Ker}\gamma$.

For any $x \in \operatorname{Ker}\gamma$, we know $\gamma(x) = xH = H$, this implies $x \in H$, thus $\operatorname{Ker}\gamma \subseteq H$. □

Lemma 10.21 (Composition of Homomorphism)**.** *Let $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms. $\psi \circ \phi : G \to K$ is also homomorphism.*

Proof. For any $a\ b \in G$:

$$\begin{aligned}
(\psi \circ \phi)(ab) &= \psi(\phi(ab)) \\
&= \psi(\phi(a)\phi(b)) && \text{(By } \phi \text{ is homomorphism)} \\
&= \psi(\phi(a))\psi(\phi(b)) && \text{(By } \psi \text{ is homomorphism)} \\
&= (\psi \circ \phi)(a)(\psi \circ \phi)(b)
\end{aligned}$$

□

Lemma 10.22 (Restricted Homomorphism)**.** *Let $\phi : G \to \overline{G}$ and H a subgroup of G. If $\operatorname{Ker}\phi \subseteq H$, prove that $\psi : H \to \overline{G}$ given by $\psi(h) = \phi(h)$ is also a homomorphism with kernel $\operatorname{Ker}\phi$.*

Proof. ψ preserve structure by directly calls ϕ. For any $k \in \operatorname{Ker}\phi$, since $\operatorname{Ker}\phi \subseteq H$, $\psi(k) = \phi(k) = e$. And for any $h \in H$ such that $\psi(h) == e$, $h \in \operatorname{Ker}\phi$ since $\psi(h) = \phi(h) = e$. □

Lemma 10.23 (Homomorphism on Internal Direct Product is False)**.** *The following proposition is False: Let ϕ a homomorphism from G to some group and $G = H \times K$. Show that $\phi(H \times K) = \phi(H) \times \phi(K)$.*

Proof. Consider $G = Z_2 \oplus Z_2$ and homomorphism $\phi((a,b)) = a+b$. Obviously $\langle(1,1)\rangle$ is the kernel, and $Z_2 \oplus Z_2 = (Z_2 \oplus \{e\}) \times (\{e\} \oplus Z_2)$. If the hypothesis is true, then the intersection of $\phi(Z_2 \oplus \{e\}) = Z_2$ and $\phi(\{e\} \oplus Z_2) = Z_2$ should be $\{e\}$ but it is not. $\square$