Module 5: Group Homomorphisms & The Fundamental Theorem of Finite Abelian Groups

§ Group Homomorphisms

Definition 5.1. A *homomorphism* ϕ from a group $(G, *)$ to a group $(\overline{G}, \star)$ is a mapping from G to $\overline{G}$ that preserves the group operation, that is, $\phi(a * b) = \phi(a) \star \phi(b)$ for all $a, b \in G$.

Definition 5.2. The *kernel* of a homomorphism ϕ from a group G to a group $\overline{G}$ with identity $\overline{e}$ is the set

$$\ker(\phi) = \{x \in G \mid \phi(x) = \overline{e}\}.$$

Remark 5.3. Group homomorphisms, get the picture.

♦ **Exercise 5.4.** Determine which of the following maps are homomorphisms.

1. $\phi\colon \mathbb{R}^* \to \mathbb{R}^*$, $x \mapsto x^2$

2. $\phi\colon (\mathbb{R}, +) \to (\mathbb{R}, +)$, $x \mapsto x^2$

3. $\phi\colon (\mathbb{R}, +) \to \mathbb{R}^*$, $x \mapsto 2^x$

4. $\phi\colon (\mathbb{Z}, +) \to \mathbb{Z}_n$, $x \mapsto x \pmod{n}$ for any $n \in \mathbb{Z}^+$

Remark 5.5. Reference Theorem 3.9 from Module 3 to compare the properties of isomorphisms to the properties of homomorphisms.

Proposition 5.6 (Properties of Elements Under Homomorphisms)**.** Let ϕ be a group homomorphism from G to $\overline{G}$. Let $a \in G$.

1. $\phi(e) = \overline{e}$
2. $\phi(a^n) = \phi(a)^n$ for every $n \in \mathbb{Z}$
3. If $|a|$ is finite, then $|\phi(a)|$ divides $|a|$.

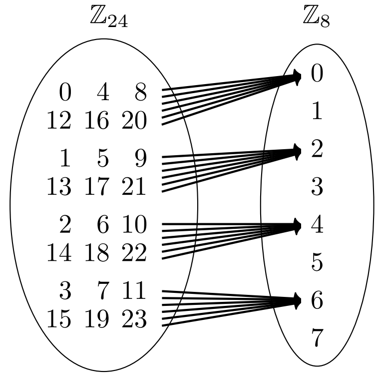
Proof. (1) and (2) follow the same argument as in the proof of Theorem 3.9.

Proposition 5.7 (Properties of Kernels)**.** Let ϕ be a group homomorphism from G to $\overline{G}$. Let $a, b \in G$.

1. $\phi(a) = \phi(b)$ if and only if $a \ker(\phi) = b \ker(\phi)$.
2. If $\phi(a) = \overline{a}$, then $\phi^{-1}(\overline{a}) = a \ker(\phi)$.
3. If $|\ker(\phi)| = n$, then ϕ is an n-to-one map from G onto $\phi(G)$.
4. If ϕ is onto and $\ker(\phi) = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.

Proof.

♦ **Exercise 5.8.** Let $\phi\colon \mathbb{Z}_{24} \to \mathbb{Z}_8$ be defined by $\phi(x) = 2x \pmod 8$.



1. Show that ϕ is a homomorphism.

2. Find $\ker(\phi)$.

3. Show that $|10|$ and $|\phi(10)|$ satisfies property 3 of Proposition 5.6

4. Show that $\phi^{-1}(4)$ satisfies property 2 of Proposition 5.7.

5. Find $\phi(\langle 6\rangle)$. How is this related to $\mathbb{Z}_8$?

6. Find $\phi^{-1}(\langle 4\rangle)$. How is this related to $\mathbb{Z}_{24}$?

Proposition 5.9 (Push Forward Properties)**.** Let ϕ be a group homomorphism from G to $\overline{G}$. Let $H \leq G$.

1. $\phi(H)$ is a subgroup of $\overline{G}$.
2. If H is cyclic, then $\phi(H)$ is cyclic.
3. If H is abelian, then $\phi(H)$ is abelian.
4. If $H \triangleleft G$, then $\phi(H) \triangleleft \phi(G)$.
5. If $|H| = n$, then $|\phi(H)|$ divides n.

Proof. (1)-(3) follow the same argument as in the proof of Theorem 3.9.

Proposition 5.10 (Pull Back Properties)**.** Let ϕ be a group homomorphism from G to $\overline{G}$.

1. If $\overline{K} \leq \overline{G}$, then $\phi^{-1}(\overline{K}) \leq G$.
2. If $\overline{K} \lhd \overline{G}$, then $\phi^{-1}(\overline{K}) \lhd G$.

Proof.

Corollary 5.11. Let ϕ be a group homomorphism from G to $\overline{G}$. Then $\ker(\phi)$ is a normal subgroup of G.

Proof.

§ The First Isomorphism Theorem

Theorem 5.12 (First Isomorphism Theorem)**.** Let ϕ be a group homomorphism from G to $\overline{G}$. Then the following map

$$\begin{aligned} \psi \colon G/\ker(\phi) &\to \overline{G} \\ g\ker(\phi) &\mapsto \phi(g) \end{aligned}$$

is an isomorphism. Hence $G/\ker(\phi) \cong \phi(G)$.

Proof.

Example 5.13. Apply the First Isomorphism Theorem to the homomorphism from Exercise 5.4 defined by $\phi\colon \mathbb{Z}_{24} \to \mathbb{Z}_8$, $\phi(x) = 2x \pmod 8$.

Corollary 5.14. If ϕ is a group homomorphism from G to $\overline{G}$, then $|G|/|\ker(\phi)| = |\phi(G)|$.

Corollary 5.15. If ϕ is a group homomorphism from G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

⧫ **Exercise 5.16.** Use the First Isomorphism Theorem to show the following.

1. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

2. Let $n = dk$. Then $\mathbb{Z}_n/\langle k\rangle \cong \mathbb{Z}_k$.

Theorem 5.17. Every normal subgroup of a group G is the kernel of some homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping from G to G/N defined by $g \mapsto gN$.

Proof.

§ The Fundamental Theorem of Finite Abelian Groups

Theorem 5.18 (The Fundamental Theorem of Finite Abelian Groups)**.** Every finite abelian group G is isomorphic to a group of the form

$$\mathbb{Z}_{{p_1}^{n_1}} \oplus \mathbb{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{n_k}}$$

where the p_i's are not necessarily distinct primes and the prime powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G.

Remark 5.19. It is often convenient to combine the cyclic factors of relatively prime order and to list the factors from smallest to largest.

Example 5.20. There are 2 isomorphism classes for an abelian group of order 12.

⧫ **Exercise 5.21.**

1. List the 3 isomorphism classes for an abelian group of order 24.

2. List the 4 isomorphism classes for an abelian group of order 36.

⧫ **Exercise 5.22.** Let G be an abelian group of order 24. Suppose that G has exactly three elements of order 2. Determine the isomorphism class of G.

Corollary 5.23. If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof.

Example 5.24. Let G be an abelian group of order 72. Produce a subgroup of order 12.

⧫ **Exercise 5.25.** Show that there are two abelian groups of order 108 that have exactly one subgroup of order 3.

End of Module 5