CHAPTER 10

Group Homomorphisms

Definitions and Examples

DEFINITION (Group Homomorphism). A homomorphism from a group G to a group $\overline{G}$ is a mapping $\phi : G \to \overline{G}$ that preserves the group operation:

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G.$$

DEFINITION (Kernal of a Homomorphism). The kernel of a homomorphism $\phi : G \to \overline{G}$ is the set $\operatorname{Ker}\phi = \{x \in G | \phi(x) = e\}$

EXAMPLE.

(1) Every isomorphism is a homomorphism with $\operatorname{Ker}\phi = \{e\}$.

(2) Let $G = \mathbb{Z}$ under addition and $\overline{G} = \{1, -1\}$ under multiplication. Define $\phi : G \to \overline{G}$ by

$$\phi(n) = \begin{cases} 1, & n \text{ is even} \\ -1, & n \text{ is odd} \end{cases}$$

is a homomorphism. For m and n odd:

(even–even)

$$\phi(2n + 2m) = \phi(2(n + m)) = 1 = \phi(2n)\phi(2m)$$

(even–odd)

$$\phi(2n + m) = -1 = 1(-1) = \phi(2n)\phi(m)$$

(odd–odd)

$$\phi(n + m) = 1 = (-1)(-1) = \phi(n)\phi(m)$$

$\operatorname{Ker}\phi = \{\text{even integers}\}$.

(3) $\phi : \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}^*$ (nonzero reals under multiplication) defined by $\phi(A) = \det A$ is a homomorphism.

$$\phi(AB) = \det AB = (\det A)(\det B) = \phi(A)\phi(B).$$

$\operatorname{Ker} \phi = \mathrm{SL}(2, \mathbb{R})$.

(4) Let $\mathbb{R}[x]$ denote the group of all polynomials with real coefficients under addition. Let $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ be defined by $\phi(f) = f'$. The group operation preservation is simply "the derivative of a sum is the sum of the derivatives."

$$\phi(f + g) = (f + g)' = f' + g' = \phi(f) + \phi(g).$$

$\operatorname{Ker} \phi$ is the set of all constant polynomials.

(5) The <u>natural homomorphism</u> from $\mathbb{Z}$ to $\mathbb{Z}_n$ is defined by $\phi(m) = m \bmod n$. $\operatorname{Ker} \phi = \langle n \rangle$.

(6) Consider $\phi : \mathbb{R} \to \mathbb{R}$ under addition defined by $\phi(x) = x^2$. Since

$$\phi(x + y) = (x + y)^2 = x^2 + 2xy + y^2$$

and

$$\phi(x + \phi(y) = x^2 + y^2,$$

this is not a homomorphism.

(7) Every vector space linear transformation is a group homomorphism and the nullspace is the kernel.

Properties of Homomorphisms

THEOREM (10.1 – Properties of Elements Under Homomorphisms). *Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let $g \in G$. Then:*

(1) $\phi(e) = \overline{e}$.

(2) $\phi(g^n) = \big[\phi(g)\big]^n$.

PROOF. (For (1) and (2)) Same as in Theorem 6.2. □

(3) If $|g|$ is finite, then $|\phi(g)|\,\big|\,|g|$.

PROOF.

Suppose $|g| = n \Longrightarrow g^n = e$. Then

$$\overline{e} = \phi(e) = \phi(g^n) = \big[\phi(g)\big]^n \Longrightarrow \text{(Corollary 2 to Theorem 4.1)}\,|\phi(g)|\,\big|\,n.$$

□

(4) $\operatorname{Ker}\phi \le G$.

PROOF.

By (1), $\operatorname{Ker}\phi \neq \emptyset$. Suppose $a, b \in \operatorname{Ker}\phi$. Then

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\big[\phi(b)\big]^{-1} = \overline{e}\cdot\overline{e}^{-1} = \overline{e}\cdot\overline{e} = \overline{e},$$

so $ab^{-1} \in \operatorname{Ker}\phi$. Thus $\operatorname{Ker}\phi \le G$ by the one-step test. □

(5) $\phi(a) = \phi(b) \iff a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$.

PROOF.

$$\phi(a) = \phi(b) \iff$$
$$\overline{e} = (\phi(b))^{-1}\phi(a) = \phi(b^{-1})\phi(a) = \phi(b^{-1}a) \iff b^{-1}a \in \operatorname{Ker}\phi \iff$$
$$b\operatorname{Ker}\phi = a\operatorname{Ker}\phi \text{ (by property 6 of the lemma in Chapter 7)}$$

□

(6) If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \big| \phi(x) = g'\} = g \operatorname{Ker} \phi$.

PROOF.

[We prove by mutual set inclusion.] Suppose $x \in \phi^{-1}(g')$. Then

$\phi(x) = g' = \phi(g) \Longrightarrow x \operatorname{Ker} \phi = g \operatorname{Ker} \phi$ by property (5)$\Longrightarrow$

$x \in g \operatorname{Ker} \phi$ (by property 4 of the lemma in Chapter 7).

Thus $\phi^{-1}(g') \subseteq g \operatorname{Ker} \phi$.

Now suppose $k \in \operatorname{Ker} \phi$, so that $\phi(gk) = \phi(g)\phi(k) = g'\overline{e} = g'$. Thus, by definition, $gk \in \phi^{-1}(g') \Longrightarrow g \operatorname{Ker} \phi \subseteq \phi^{-1}(g')$, and so by mutual set inclusion,

$g \operatorname{Ker} \phi = \phi^{-1}(g')$. □

Since homomorphisms preserve the group operation, they also preserve many other group properties.

THEOREM (10.2 – Properties of Subgroups Under Homomorphisms).

Let $\phi : G \to \overline{G}$ be a homomorphism and let $H \leq G$. Then

(1) $\phi(H) = \{\phi(h) | h \in H\} \leq \overline{G}$.

(2) H cyclic $\Longrightarrow \phi(H)$ cyclic.

(3) H Abelian $\Longrightarrow \phi(H)$ Abelian.

PROOF. (For (1), (2), and (3)) Same as in Theorem 6.3. □

(4) $H \triangleleft G \Longrightarrow \phi(H) \triangleleft \phi(G)$.

PROOF.

Let $\phi(h) \in \phi(H)$ and $\phi(g) \in \phi(G)$. Then

$$\phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$$

since $ghg^{-1} \in H$ because $H \triangleleft G$. □

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

PROOF. Follows directly from property 6 of Theorem 10.1 and the fact that all cosets of $\operatorname{Ker}\phi = \phi^{-1}(e)$. □

(6) If $|H| = n$*, then* $|\phi(H)|\big|n$*.*

PROOF.

Let ϕ_H denote the restriction of ϕ to H. Then ϕ_H is a homomorphism from H onto $\phi(H)$. Suppose $|\operatorname{Ker}\phi_H| = t$. Then, from (5), ϕ_H is a t-to-1 mapping, so $|\phi(H)|t = |H|$. □

(7) If $\overline{K} \leq \overline{G}$*, then* $\phi^{-1}(\overline{K}) = \{k \in G | \phi(k) \in \overline{K}\} \leq G$*.*

PROOF.

Clearly $e \in \phi^{-1}(\overline{K})$, so $\phi^{-1}(\overline{K}) \neq \emptyset$. Let $k_1, k_2 \in \phi^{-1}(\overline{K})$. Then

$$\phi(k_1), \phi(k_2) \in \overline{K} \Longrightarrow \phi(k_2)^{-1} \in \overline{K}.$$

Thus

$$\phi(k_1k_2^{-1}) = \phi(k_1)\phi(k_2^{-1}) = \phi(k_1)\phi(k_2)^{-1} \in \overline{K}.$$

By definition, $k_1k_2^{-1} \in \phi^{-1}(\overline{K})$ and so $\phi^{-1}(\overline{K}) \leq G$ by the one-step test. □

(8) If $\overline{K} \lhd \overline{G}$*, then* $\phi^{-1}(\overline{K}) = \{k \in G | \phi(k) \in \overline{K}\} \lhd G$*.*

PROOF.

Every element of $x\phi^{-1}(\overline{K})x^{-1}$ has the form xkx^{-1} where $\phi(k) \in \overline{K}$. Since $\overline{K} \lhd \overline{G}$,

$$\phi(xkx^{-1}) = \phi(x)\phi(k)\phi(x)^{-1} \in \overline{K},$$

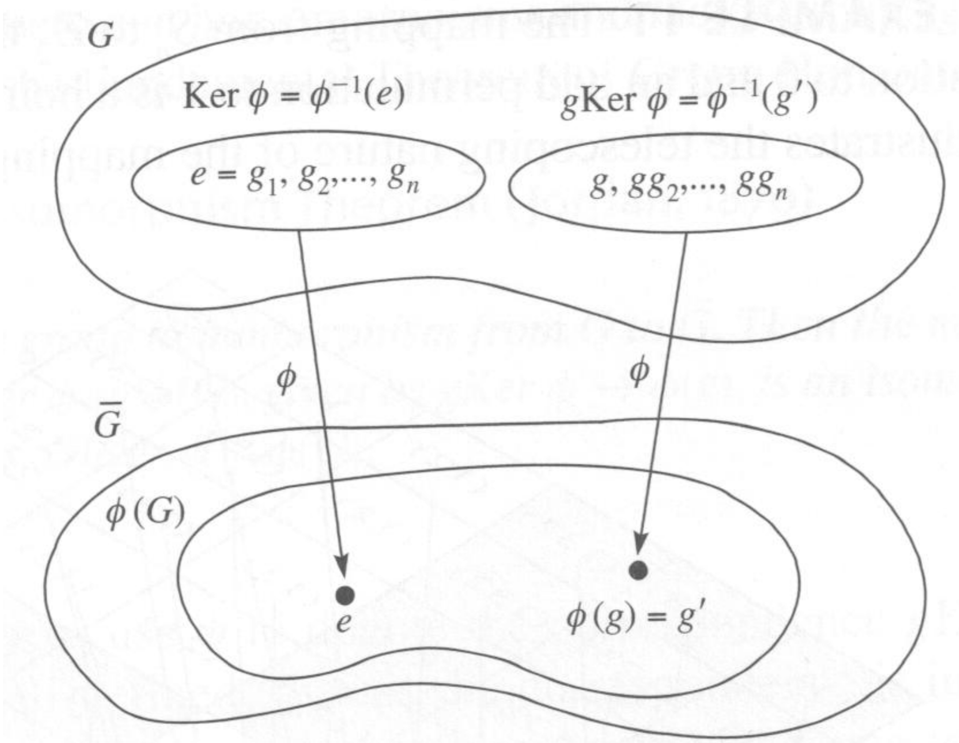
and so $xkx^{-1} \in \phi^{-1}(\overline{K})$. Thus $x\phi^{-1}(\overline{K})x^{-1} \subseteq \phi^{-1}(\overline{K})$ and $\phi^{-1}(\overline{K}) \lhd G$ by Theorem 9.1. □

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

PROOF. Follows directly from (5). □

COROLLARY (To (8)). $\operatorname{Ker}\phi \lhd G$.

PROOF. Let $\overline{K} = \{e\}$ in (8). $\square$



EXAMPLE. Consider $\phi : \mathbb{C}^\star \to \mathbb{C}^\star$ defined by $\phi(x) = x^4$. ϕ is a homomorphism since

$$\phi(xy) = (xy)^4 = x^4y^4 = \phi(x)\phi(y).$$

$\operatorname{Ker}\phi = \{1, -1, i, -i\}$. Thus ϕ is a 4-to-1 mapping by property (5) of Theorem 10.2. Since $\phi(3^{1/4}) = 3$, again by property (5) of Theorem 10.2,

$$\phi^{-1}(3) = 3^{1/4}\operatorname{Ker}\phi = \{3^{1/4}, -3^{1/4}, 3^{1/4}i, -3^{1/4}i\}$$

Now let $H = \langle \cos 60^\circ + i \sin 60^\circ \rangle$. Since

$$(\cos 60^\circ + i \sin 60^\circ)^6 = \cos 360^\circ + i \sin 360^\circ = 1,$$

$|H| = 6$.

$$\phi(H) = \langle (\cos 60^\circ + i \sin 60^\circ)^4 \rangle = \langle \cos 240^\circ + i \sin 240^\circ \rangle \Longrightarrow |\phi(H)| = 3,$$

so $|\phi(H)| \big| |H|$.

Example. Define $\phi : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ by $\phi(x) = 4x$. ϕ is a homomorphism since, for $x, y \in \mathbb{Z}_{16}$,

$$\phi(x+y) = 4(x+y) = 4x + 4y = \phi(x) + \phi(y).$$

$\operatorname{Ker}\phi = \{0, 4, 8, 12\}$. Thus ϕ is 4-to-1. Since $\phi(3) = 12$, by property (5) of Theorem 10.2,

$$\phi^{-1}(12) = 3 + \operatorname{Ker}\phi = \{3, 7, 11, 15\}.$$

Since $\langle 3 \rangle$ is cyclic, so is $\phi(\langle 3 \rangle)$.

$$\langle 3 \rangle = \{3, 6, 9, 12, 15, 2, 5, 8, 11, 14, 1, 4, 7, 10, 13, 0\}.$$

$$\phi(\langle 3 \rangle) = \{12, 8, 4, 0\} = \langle 4 \rangle = \langle 12 \rangle.$$

Also, $|\phi(3)| = 4$ and $|3| = 16$, so $|\phi(3)| \big| |3|$.

With $\overline{K} = \{0, 4, 8, 12\} \le \mathbb{Z}_{16}$, $\phi^{-1}(\overline{K}) = \langle 3 \rangle \le \mathbb{Z}_{16}$.

Problem (Page 221 # 25). Hom many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_{10}$? How many are there to $\mathbb{Z}_{10}$?

Solution.

$\mathbb{Z}_{20}$ and $\mathbb{Z}_{10}$ are both cyclic and additive. By property (2) of Theorem 10.1, written additively, $\phi(ng) = n\phi(g)$. Such homomorphisms are completely determined by $\phi(1)$, i.e., if $\phi(1) = a$, $\phi(x) = \phi(x \cdot 1) = x\phi(1) = xa$. By Lagrange, $|a| \big| 10$, and by property (3) of Theorem 10.1, $|a| \big| |1|$ or $|a| \big| 20$.

Thus $|a| = 1, 5, 10$, or 2.

$|a| = 10 : 1, 3, 7, 9$ have order 10 in $\mathbb{Z}_{10}$, so 4 homomorphisms are onto.

$|a| = 5 : 2, 4, 6, 8$.

$|a| = 2 : 5$.

$|a| = 1 : 0$.

In all cases,

$$\phi(x+y) = (x+y)a = xa + ya = \phi(x + \phi(y).$$

$\square$

The First Isomorphism Theorem

THEOREM (10.3 — First Isomorphism Theorem). *Let $\phi : G \to \overline{G}$ be a group homomorphism. Then $\psi : G/\operatorname{Ker}\phi \to \phi(G)$ defined by $\psi(g\operatorname{Ker}\phi) = \phi(g)$ is an isomorphism, i.e., $G\operatorname{Ker}\phi \approx \phi(G)$.*

PROOF.

That ψ is well-defined, i.e., the correspondence is independent of the particular coset representation chosen, and is 1–1 follows directly from property (5) of Theorem 10.1. ψ is clearly onto.

[To show ψ is operation-preserving.] For all $x\operatorname{Ker}\phi, y\operatorname{Ker}\phi \in G/\operatorname{Ker}\phi$,

$$\psi(x\operatorname{Ker}\phi\; y\operatorname{Ker}\phi) = \psi(xy\operatorname{Ker}\phi) = \phi(xy) = \phi(x)\phi(y) = \psi(x\operatorname{Ker}\phi)\psi(y\operatorname{Ker}\phi),$$

so ψ is operation-preserving and this is an isomorphism. $\square$

COROLLARY. *If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides both $|G|$ and $|\overline{G}|$.*

EXAMPLE. The natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$ is defined by $\phi(m) = m \bmod n$ has $\operatorname{Ker}\phi = \langle n\rangle$. Thus, by the first isomorphism theorem,

$$\mathbb{Z}/\langle n\rangle \approx \mathbb{Z}_n.$$

THEOREM (10.4 — Normal Subgroups are Kernels). *Every normal subgroup of a group G is the kernel of a homomorphism of G.In particular, a normal subgroup N is a kernel of the mapping $g \to gN$ from G to G/N.*

PROOF.

Define $\psi : G \to G/N$ by $\psi(g) = gN$ (the natural homomorphism from G to G/N). Then $\psi(xy) = (xy)N = xNyN = \psi(x)\psi(y)$. Moreover,

$$g \in \operatorname{Ker}\psi \iff gN = \psi(g) = N \iff g \in N$$

by property (2) of the lemma in Chapter 7. $\square$

Example. Consider $G = \overline{G} = A_4$ as given by the Cayley table below, where i represents the permutation α_i (from page 111):

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	10	9	12	11
3	3	4	1	2	7	8	5	6	11	12	9	10
4	4	3	2	1	8	7	6	5	12	11	10	9
5	5	8	6	7	9	12	10	11	1	4	2	3
6	6	7	5	8	10	11	9	12	2	3	1	4
7	7	6	8	5	11	10	12	9	3	2	4	1
8	8	5	7	6	12	9	11	10	4	1	3	2
9	9	11	12	10	1	3	4	2	5	7	8	6
10	10	12	11	9	2	4	3	1	6	8	7	5
11	11	9	10	12	3	1	2	4	7	5	6	8
12	12	10	9	11	4	2	1	3	8	6	5	7

Define $\phi : A_4 \to A_4$ by $\{1, 2, 3, 4\} \to 1$, $\{5, 6, 7, 8\} \to 5$, $\{9, 10, 11, 12\} \to 9$. Then $\operatorname{Ker} \phi = \{1, 2, 3, 4\}$. Then $\psi : A_4/\operatorname{Ker} \phi \to \phi(A_4) = \{1, 5, 9\}$ is an isomorphism by Theorem 10.3.

The following table shows $A_4/\operatorname{Ker} \phi$ where $H = \operatorname{Ker} \phi$:

.	$1H$	$5H$	$9H$
$1H$	$1H$	$5H$	$9H$
$5H$	$5H$	$9H$	$1H$
$9H$	$9H$	$1H$	$5H$

Note.

Consider the natural mapping $\gamma : G \to G/\operatorname{Ker}\phi$ given by $\psi(g) = g\operatorname{Ker}\phi$. Then the proof of Theorem 10.3 shows $\phi = \psi\gamma$. The diagram below illustrating this is called a <u>commutative diagram</u>:

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \phi(G) \\ & G/\operatorname{Ker}\phi \arrow[ur, "\psi"'] & \end{tikzcd}$$

All homomorphic images of G can be determined (up to isomorphism) by using G. These must be expressible in the form G/K where $K \lhd G$ since there is a 1–1 correspondence between homomorphic images of G and normal subgroups of G (given by ψ in the commutative diagram — each $K \lhd G$ can be a kernel for a ϕ).

To find all homomorphic images of G, find all normal subgroups K of G, and construct G/K. Wikth $\gamma_K : G \to G/K$ the natural map and $\psi_K : G/K \to \overline{G}$ as in Theorem 10.3, $\phi_K = \psi_K\gamma_K$.

Also, since a factor group of an Abelian group is Abelian, so is its homomorphic image.

If G is cyclic of order n, the number of factor groups and thus homomorphic images of G is the number of divisors of n, since there is exactly one subgroup of G (and therefore one factor group of G) for each divisor of n. But keep in mind that there may be more than one homomorphism to a given homomorphic image.