§3.7 Homomorphisms

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

Review (Brief Version of Exam II Review)

- A group isomorphism $\phi : (G_1, *) \to (G_2, \cdot)$ **Find/Verify ϕ**
- **Lagrange's Theorem** If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \mid n$.
- Cayley's Theorem Every group is isomorphic to a permutation group.
  - **Cyclic group:** Infinite: $\cong \mathbf{Z}$ & Finite: $\cong \mathbf{Z}_n$ $\rightsquigarrow$ multiplicative G
  - **Dihedral group** D_n of order $2n$
  - **Alternating group** A_n of order $n!/2$
- Product of two subgroups is not always a subgroup.

  If $h^{-1}kh \in K$ for all $h \in H, k \in K$, then HK is a subgroup. $\rightsquigarrow$ G abelian
- Direct product of (two $\rightsquigarrow$ n) groups: e.g., $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \cdots \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n)$

  The order of an element is the **lcm** of the orders of each component.

Group Homomorphism

A function $\phi : (G_1, *) \to (G_2, \cdot)$ is a **group homomorphism** if
$$\phi(a * b) = \phi(a) \cdot \phi(b) \qquad \text{for all } a, b \in G_1.$$

Every isomorphism is a homomorphism, but conversely not true.

Example 1 (Determinant of an invertible matrix, $n > 1$)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.

ϕ is a group homomorphism. [Why?] However, ϕ is not an isomorphism.

ϕ is not one-to-one since different matrices could have the same det.

ϕ is onto. e.g., consider a diagonal matrix $\mathrm{diag}(a, 1, \ldots, 1)$ for any $a \in \mathbf{R}^\times$.

Example 2 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. [Why?]

But ϕ is not an isomorphism since it is not one-to-one. [Why?] ϕ is onto.

Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$

Properties of Group Homomorphisms

Let $\phi : (G_1, *, e_1) \to (G_2, \cdot, e_2)$ be a group homomorphism.

i) $\phi(e_1) = e_2$.

ii) $\phi(a^{-1}) = \big(\phi(a)\big)^{-1}$ for all $a \in G_1$.

iii) $\phi(a^n) = \big(\phi(a)\big)^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.

iv) If $o(a) = n$ in G_1, then $o\big(\phi(a)\big)$ in G_2 is a divisor of n.

Proof: Proofs of i)-iii) are the same as in the case of a group isomorphism.

i) $\phi(e_1) \cdot \phi(e_1) = \phi(e_1 * e_1) = \phi(e_1) \quad \rightsquigarrow \phi(e_1) = e_2$.

ii) $\phi(a) \cdot \phi(a^{-1}) = \phi(a * a^{-1}) = \phi(e_1) \overset{\text{i)}}{=} e_2 \quad \rightsquigarrow \phi(a^{-1}) = \big(\phi(a)\big)^{-1}$.

iii) Just as in the case of an isomorphism, use an *induction* argument.

iv) $\big(\phi(a)\big)^n \overset{\text{iii)}}{=} \phi(a^n) = \phi(e_1) \overset{\text{i)}}{=} e_2$. Thus $o(\phi(a))|n$. □

Example 3 (Exponential functions for groups)

Let G be a group and $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$ for all $n \in \mathbf{Z}$.

ϕ is a homomorphism since $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$.

ϕ is onto if and only if $G = \langle a \rangle$.

ϕ is one-to-one if and only if $o(a) = \infty$.

Example 4 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$ for all $[x] \in \mathbf{Z}_n$.

ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.

ϕ is a homomorphism since $\phi([x]+[y]) = \cdots = \phi([x]) + \phi([y])$.

ϕ is one-to-one and onto if and only if $(m, n) = 1$: $\cdots\cdots(\star)$

Recall: $mx \equiv y \pmod{n}$ has a solution if and only if $d|y$ with $d = (m, n)$.

Moreover, if $d|y$, then there are d distinct solutions modulo n.

$\rightsquigarrow$ Consider a general argument, i.e., homomorphisms defined on cyclic gps

In particular, we can give a group-theoretic proof for the above result $(\star)$!

Homomorphisms Defined on Cyclic Groups

Let $C = \langle a \rangle$. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. $\rightsquigarrow \phi(a^m) = g^m$

It follows that ϕ is completely determined by its value on a.

If $o(a) = n < \infty$, then $o(g)|n$ since $g = \phi(a)$ and ϕ is a homomorphism.

$\rightsquigarrow$ Any homomorphism $\phi\colon \mathbf{Z}_n \to \mathbf{Z}_k$ is completely determined by $\phi([1]_n)$.

Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. So $n \cdot [m]_k = [nm]_k = [0]_k \rightsquigarrow k|mn$.

- $\phi([x]_n) = [xm]_k$ defines a homomorphism if and only if $k|mn$.
- Every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.
- $\phi(\mathbf{Z}_n)$ is the cyclic subgroup generated by $[m]_k$ since $\phi([1]_n) = [m]_k$.
  $\rightsquigarrow \phi$ is onto if and only if $[m]_k$ is a generator of $\mathbf{Z}_k$, i.e., $(m, k) = 1$.

$\phi\colon \mathbf{Z}_{10} \to \mathbf{Z}_5$, $\phi([1]_{10}) = [2]_5$ is an onto homomorphism since $(2, 5) = 1$.

However, ϕ is not one-to-one. For example, $\phi([1]_{10}) = \phi([6]_{10}) = [2]_5$.

If $\phi([x]_{10}) = \phi([y]_{10})$, then $[2x]_5 = [2y]_5 \Leftrightarrow [2(x - y)]_5 = [0]_5 \Leftrightarrow 5|(x - y)$

Kernel and Image of a Homomorphism

Let $\phi : G_1 \to G_2$ be a group homomorphism. The **kernel** of ϕ is the set

$$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1.$$

The **image** of ϕ is the set $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$.

Recall that ϕ: $\mathbf{Z}_{10} \to \mathbf{Z}_5$ with $\phi([1]_{10}) = [2]_5$ is an onto homomorphism.
$\rightsquigarrow \mathrm{im}(\phi) = \mathbf{Z}_5$ and $\ker(\phi) = \{[0]_{10}, [5]_{10}\}$.

Revisit Example 3: Exponential functions for groups

Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$ for all $n \in \mathbf{Z}$. Then ϕ is a homomorphism.
By definition, $\ker(\phi) = \{n \mid a^n = e\}$.

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$.
- If $o(a) = \infty$, then $\ker(\phi) = \{0\}$. $\rightsquigarrow \phi$ is 1-to-1 in this case.

In either case,ker(ϕ) is a subgroup of $\mathbf{Z}$.
By definition, $\mathrm{im}(\phi) = \{a^n \mid n \in \mathbf{Z}\} =: \langle a \rangle$, which is a subgroup of G.
$\rightsquigarrow \phi$ is onto if and only if $G = \langle a \rangle$.

More Properties of Group Homomorphisms

Let $\phi : G_1 \to G_2$ be a group homomorphism.

i) $\ker(\phi)$ is a subgroup of G_1.

ii) $\mathrm{im}(\phi)$ is a subgroup of G_2.

iii) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.

iv) ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$.

Proof: i) $\ker(\phi)$ is nonempty since $e_1 \in \ker(\phi)$. For $a, b \in \ker(\phi)$, to show $ab^{-1} \in \ker(\phi)$: $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2$.

ii) $\mathrm{im}(\phi)$ is nonempty since $e_2 \in \mathrm{im}(\phi)$. For $x, y \in \mathrm{im}(\phi)$, to show $xy^{-1} \in \mathrm{im}(\phi)$ Say $\phi(a) = x$ and $\phi(b) = y$ for some $a, b \in G_1$. So $xy^{-1} = \cdots = \phi(ab^{-1})$.

iii) ϕ is one-to-one $\overset{\S 3.4}{\Longleftrightarrow}$ $\phi(x) = e_2$ implies $x = e_1$, i.e., $\ker(\phi) = \{e_1\}$.

iv) It is clear that ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$. □

Let $\phi : G_1 \to G_2$ be a group homomorphism. Assume that ϕ is onto.

If G_1 is abelian (resp. cyclic), then G_2 is also abelian (resp. cyclic).

Let $\phi : G_1 \to G_2$ be a group homomorphism. Assume that ϕ is onto.

i) If G_1 is abelian, then G_2 is also abelian.

ii) If G_1 is cyclic, then G_2 is also cyclic.

i) For $x, y \in G_2$, $\exists$ $a, b \in G_1$ s.t. $\phi(a) = x, \phi(b) = y$ since ϕ is onto.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

ii) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. To show $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: ✓ [Why?]
- $G_2 \subseteq \langle \phi(a) \rangle$: To show every element y of G_2 is a power of $\phi(a)$.

  We can write $y = \phi(b)$ for some $b \in G_1$ since ϕ is onto.

  We can also write $b = a^m$ for some $m \in \mathbf{Z}$. [Why?] This implies that

$$y = \phi(b) = \phi(a^m) = (\phi(a))^m. \qquad \square$$

One comment: i) and ii) are not necessarily true if ϕ is not onto.

Homorphisms Between Cyclic Groups

In slide # 6, define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$

ϕ well-defined $\Leftrightarrow k|mn$. Every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ is of this form.

Next, find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$.
Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof: ϕ is a homomorphism since $\phi(x + y) = \cdots = \phi(x) + \phi(y)$.
ϕ is completely determined by its value on 1. [Why?] Say $\phi(1) = m \in \mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \cdots = mx$. For $x \in \mathbf{Z}^-, x = -|x| : \phi(x) = \cdots = mx$.

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$.
Then ϕ is a homomorphism. Every homomorphism must be of this form.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$.

The **only** homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ is defined by $\phi([x]_n) = 0$ for $[x]_n \in \mathbf{Z}_n$.

Say $o([x]_n) = d|n \quad \rightsquigarrow o(\phi([x]_n))|d$. But in $\mathbf{Z}$, only 0 has a finite order.

Normal Subgroup

Let $\phi : G_1 \to G_2$ be a homomorphism.

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Proof: $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = e_2$ □

A subgroup H of the group G is called a **normal** subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

1) For a homomorphism $\phi : G_1 \to G_2$, $\ker(\phi)$ is a normal subgroup of G_1.

2) If $H = G$ or $H = \{e\}$, then H is normal.

3) Any subgroup of an abelian group is normal.

Let $\phi : G_1 \to G_2$ be a homomorphism.

i) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.

ii) If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

iii) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.

iv) If H_2 is normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

Proof: i) Nonempty: $e_2 \in \phi(H_1)$. For $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and $xy^{-1} = \cdots = \phi(ab^{-1}) \in \phi(H_1)$.

ii) Let $x \in G_2$ and $y \in \phi(H_1)$. To show $xyx^{-1} \in \phi(H_1)$.

There exist $g \in G_1$ s.t. $\phi(g) = x$ [Why?] and $y = \phi(h)$ for some $h \in H_1$.

$$xyx^{-1} = \cdots = \phi(ghg^{-1}) \in \phi(H_1) \text{ [Why?]}$$

iii) Note that $\phi^{-1}(H_2) := \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. For any $a, b \in \phi^{-1}(H_2)$, $ab^{-1} \in \phi^{-1}(H_2)$ since $\phi(ab^{-1}) \in H_2$ [Why?].

iv) Let $g \in G_1$ and $h \in \phi^{-1}(H_2)$. To show $ghg^{-1} \in \phi^{-1}(H_2)$.

This is true since $\phi(ghg^{-1}) = \cdots = \phi(g)\phi(h)(\phi(g))^{-1} \in H_2$ [Why?]. □

Equivalence Relation on G_1 Associated with $\phi\colon G_1 \to G_2$

Natural equivalent relation on G_1: For $a, b \in G_1$, $a \sim_\phi b$ if $\phi(a) = \phi(b)$, and write $[a]_\phi$ as the equivalence class of $a \in G_1$. Set $G_1/\phi := \{[a]_\phi\}$.

The multiplication of equivalence classes in the set G_1/ϕ is well-defined, and G_1/ϕ is a group under this multiplication. The natural projection

$$\pi\colon G_1 \to G_1/\phi$$

defined by $\pi(a) = [a]_\phi$ is a group homomorphism.

Proof: Multiplication is well-defined: to show $ac \sim_\phi bd$ if $a \sim_\phi b, c \sim_\phi d$.
$\phi(ac) = \phi(a)\phi(c) \overset{!}{=} \phi(b)\phi(d) = \phi(bd)$. $\rightsquigarrow ac \sim_\phi bd$
Associativity: For all $a, b, c \in G_1$, $[a]_\phi([b]_\phi[c]_\phi) = \cdots = ([a]_\phi[b]_\phi)[c]_\phi$.
Identity $[e]_\phi$: $[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi$ & $[a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$
Inverses $[a^{-1}]_\phi$: $[a^{-1}]_\phi[a]_\phi = [a^{-1}a]_\phi = [e]_\phi$ & $[a]_\phi[a^{-1}]_\phi = [aa^{-1}]_\phi = [e]_\phi$
Thus, G_1/ϕ is a group under the multiplication of equivalence classes.
π is a homomorphism: For all $a, b \in G_1$, $\pi(ab) = \cdots = \pi(a)\pi(b)$. $\square$

The set of equivalence classes $G_1/\phi = \{[a]_\phi\}$, $[a]_\phi = \{b \in G_1 \mid \phi(b) = \phi(a)\}$.

We know $\pi\colon G_1 \to G_1/\phi$ defined by $\pi(a) = [a]_\phi$ is a group homomorphism.

Theorem

Let $\phi : G_1 \to G_2$ be a homomorphism. There exists a group **isomorphism**

$$\overline{\phi} : G_1/\phi \to \phi(G_1) \quad \text{defined by } \overline{\phi}([a]_\phi) = \phi(a) \text{ for all } [a]_\phi \in G_1/\phi.$$

$G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$ gives $\phi = \iota \circ \overline{\phi} \circ \pi$, ι is the inclusion mapping

Proof: well-defined: If $[a]_\phi = [b]_\phi$, then $\overline{\phi}([a]_\phi) = \phi(a) = \phi(b) = \overline{\phi}([b]_\phi)$.

one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. Thus $[a]_\phi = [b]_\phi$.

onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} = \mathrm{im}(\phi) = \phi(G_1)$

$\overline{\phi}$ is a group homomorphism: For any $[a]_\phi, [b]_\phi \in G_1/\phi$,

$$\overline{\phi}([a]_\phi[b]_\phi) = \overline{\phi}([ab]_\phi) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}([a]_\phi)\overline{\phi}([b]_\phi). \qquad \square$$

Look ahead: Fundamental Homomorphism Theorem $G_1/\ker(\phi) \cong \mathrm{im}(\phi)$

Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$. TFAE:

(1) $\phi(a) = \phi(b) \quad \Leftrightarrow \quad a \sim_\phi b \quad \Leftrightarrow \quad [a]_\phi = [b]_\phi$;

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

Proof: (1) $\Rightarrow$ (2) $\phi(ab^{-1}) = \cdots = e_2 \quad \rightsquigarrow ab^{-1} \in \ker(\phi)$

(2) $\Rightarrow$ (3) $ab^{-1} = k \in \ker(\phi) \quad \rightsquigarrow a = kb \qquad$ (3) $\Rightarrow$ (1) $\phi(a) = \cdots = \phi(b)$

Similarly, we can show that (1) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (1). □

In proof of Lagrange's theorem: Let H be a subgroup of the group G.

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

$\rightsquigarrow$ Let $H = \ker(\phi)$. Write $G/\ker(\phi)$ for G/ϕ. So $G_1/\phi \cong \phi(G_1)$ becomes

Fundamental Homomorphism Theorem: $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$

Reprove 2nd Theorem in §3.5

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$ for some $n \in \mathbf{Z}^+$.

Use Fundamental Homomorphism Theorem $G_1/\ker(\phi) \cong \mathrm{im}(\phi)$):

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. By Example 3, ϕ is onto.

- If $o(a) = \infty$, then ϕ is one-to-one. So the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements.
  Thus $\mathbf{Z}/\ker(\phi) = \mathbf{Z}/\phi = \mathbf{Z} \cong \mathrm{im}(\phi) = G$.
- If $o(a) = n < \infty$, then $a^m = a^k \Leftrightarrow m \equiv k \pmod{n}$, i.e., $\phi(m) = \phi(k)$ if and only if $m \equiv k \pmod{n}$. This implies that $\mathbf{Z}/\ker(\phi) = \mathbf{Z}/\phi$ is the additive group of congruence classes modulo n. Thus $\mathbf{Z}_n \cong G$.

e.g., Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [x]_n$. So ϕ is an onto homomorphism.
$\rightsquigarrow \ker(\phi) = n\mathbf{Z}$. By Fundamental Homomorphism Theorem, $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$.

We just use $G_1/\ker(\phi)$ to replace G_1/ϕ without its formal definition right now.
Looking ahead: We will give a formal proof of $G_1/\ker(\phi) \cong \mathrm{im}(\phi)$ in §3.8.