MTH 339

Group Homomorphisms

Def A homomorphism ϕ from a group G to a group $\overline{G}$ is a mapping from $G \to \overline{G}$ that preserves the group operation; that is

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

Def Kernel of a Homomorphism

The kernel of ϕ is defined as

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

Example: Let $\mathbb{R}^*$ be the group of nonzero real numbers under multiplication

$\phi : A \to \det(A)$ is a homomorphism

$GL(2, \mathbb{R}) \to \mathbb{R}^*$. $\ker \phi = SL(2, \mathbb{R})$

MTH 339

<u>Example:</u> Express $\mathcal{U}(40) = \mathcal{U}_5(40) \times \mathcal{U}_8(40)$

as $\mathcal{U}_5(40)\,\mathcal{U}_8(40) = \{ab \mid a \in \mathcal{U}_5(40),\ b \in \mathcal{U}_8(40)\}$.

Then $\phi(ab) = a$ is a homomorphism

$\mathcal{U}(40) \to \mathcal{U}(40)$ with kernel $\mathcal{U}_8(40)$.

$\tilde{\phi}(ab) = b$ is a homomorphism with kernel

$\mathcal{U}_5(40)$.

<u>Example:</u> $\phi : \mathbb{R} \to \mathbb{R}$ (with $\mathbb{R}$ under addition)

$\phi(x) = x^2$ is not a homomorphism since

$\phi(a+b) = (a+b)^2 = a^2 + 2ab + b^2$ whereas

$\phi(a) + \phi(b) = a^2 + b^2$.

<u>Example:</u> Linear transformations are group homomorphisms, where the kernel is the nullspace.

MTH 339

Thm Properties of Elements Under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and $g \in G$.

(1) $\phi(e) = \bar{e}$ (e is the identity of G and $\bar{e}$ is the identity of $\overline{G}$)

(2) $\phi(g^n) = (\phi(g))^n$

(3) If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$ and if $|G|$ is finite, then $|\phi(g)|$ also divides $|\phi(G)|$.

(4) $\operatorname{Ker} \phi$ is a subgroup of G.

(5) $\phi(a) = \phi(b)$ if and only if $a \ker \phi = b \ker \phi$.

(6) If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \ker \phi$.

Proof:

(1), (2): ($\to$ Do now)

(3): If $g^n = e$, $\bar{e} = \phi(e) = \phi(g^n) = (\phi(g))^n$

So $|\phi(g)|$ divides n. That $|\phi(g)|$ divides $|\phi(G)|$ follows from Lagrange's theorem if $|G|$ is finite.

(Corollary 4, p. 155)

(4): ($\to$ Do now)

(5): First assume $\phi(a) = \phi(b)$. Then

$e = (\phi(b))^{-1}\phi(a) = \phi(b^{-1}a)$, so $b^{-1}a \in \ker\phi$.

Therefore, $b\ker\phi = a\ker\phi$ (Lemma p. 151 (6)).

(6): We need to show that $\phi^{-1}(g') \subseteq g\ker\phi$ and $g\ker\phi \subseteq \phi^{-1}(g')$.

"$\subseteq$": $x \in \phi^{-1}(g')$, so $\phi(x) = g'$. Then,
$\phi(g) = \phi(x)$ and therefore
$g \ker\phi = x \ker\phi$ and thus $x \in g\ker\phi$.

"$\supseteq$": To prove $g\ker\phi \subseteq \phi^{-1}(g')$, let $k \in \ker\phi$.
$\phi(gk) = \phi(g)\phi(k) = g'e = g'$, so
$gk \in \phi^{-1}(g')$

$\square$

Thm Properties of Subgroups under Homomorphisms

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

(1) $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup.

(2) If H is cyclic, then $\phi(H)$ is cyclic.

(3) If H is Abelian, then $\phi(H)$ is Abelian

(4) If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.

MTH 339

(5) If $|\ker \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.

(6) If H is finite, then $|\phi(H)|$ divides $|H|$.

(7) $\phi(Z(G))$ is a subgroup of $Z(\phi(G))$.

(8) 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.

(9) If K is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K})$ is a normal subgroup of G.

(10) If ϕ is onto and $\ker \phi = \{e\}$, then ϕ is an isomorphism $G \to \overline{G}$.

<u>Proof:</u> (1), (2), (3): proofs identical to proofs about isomorphisms.

(4): 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 H is normal in G.

(5): $\ker\phi = \phi^{-1}(e)$ and all cosets of $\ker\phi$ have the same number of elements.

(6): Let ϕ_H be the restriction of ϕ to elements of H. Then ϕ_H is a homomorphism from H onto $\phi(H)$. Suppose $|\ker\phi_H| = t$.
Then, ϕ_H is a t-to-1 mapping.
So, $|\phi(H)|\,t = |H|$.

(7): (Do now)

(8): one-step subgroup test:
$e \in \phi^{-1}(\overline{K})$, so $\phi^{-1}(\overline{K})$ is not empty.
Let $k_1, k_2 \in \phi^{-1}(\overline{K})$, then $\phi(k_1), \phi(k_2) \in \overline{K}$

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

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

(9): Every element in $x\phi^{-1}(\overline{K})x^{-1}$ has the form xkx^{-1} with $\phi(k) \in \overline{K}$. Since $\overline{K}$ is normal in $\overline{G}$, $\phi(xkx^{-1}) = \phi(x)\phi(k)(\phi(x))^{-1} \in \overline{K}$ and, therefore, $xkx^{-1} \in \phi^{-1}(\overline{K})$.

(10): Follows from (5).

<u>Example</u>: Consider $\phi: C^* \to C^*$ $\phi(x) = x^4$

Note that $\phi(xy) = (xy)^4 = x^4 y^4 = \phi(x)\phi(y)$

is a homomorphism. $\ker\phi = \{1, -1, i, -i\}$

So ϕ is a 4-to-1 mapping.

Let's find all the elements that map to 2. We have $\phi(\sqrt[4]{2}) = 2$.

MTH 339

9/10

So, the set of all elements that map to 2 is $\sqrt[4]{2}\ \mathrm{Ker}\,\phi = \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}$.

The First Isomorphism Theorem

Let ϕ be a group homomorphism from $G \to \overline{G}$. Then the mapping $\psi : G/\ker\phi \to \phi(G)$ defined by $\psi(g\ker\phi) = \phi(g)$ is an isomorphism: $G/\ker\phi \approx \phi(G)$

Proof: ψ is operation-preserving

$\psi(x\ker\phi)\,\psi(y\ker\phi) = \phi(x)\,\phi(y)$
$= \phi(xy) = \psi(xy\ker\phi) = \psi(x\ker\phi\, y\ker\phi)$

The fact that ψ is one-to-one follows from (5) of the first theorem

$\square$

MTH 339 10/10

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

<u>Corollary</u>: If ϕ is a homomorphism from a finite group $G \to \overline{G}$, then
$|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

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

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

MTH 339 Do Now

1./ Prove $\phi(e) = \bar{e}$ and $\phi(g^n) = (\phi(g))^n$

2./ Prove that $\ker \phi$ is a subgroup.

3./ Prove that $\phi(Z(G))$ is a subgroup of $Z(\phi(G))$.

MTH 339 - HW

1./ If ϕ is a homomorphism $G \to H$ and σ is a homomorphism $H \to K$, show that $\sigma \circ \phi$ is a homomorphism $G \to K$. How are $\ker \phi$ and $\ker \sigma \circ \phi$ related? If ϕ and σ are onto and G is finite, describe $[\ker \sigma \circ \phi : \ker \phi]$ in terms of $|H|$ and $|K|$.

2./ Prove that $\varphi : G \oplus H \to G$ given by $\varphi(g,h) = g$ is a homomorphism. What is the kernel?

3./ Suppose $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ is a homomorphism and $\ker \phi = \{0, 10, 20\}$. If $\phi(23) = 9$, determine all elements that map to 9.

4./ Suppose $\phi : U(30) \to U(30)$ is a homomorphism and $\ker \phi = \{1, 11\}$. If $\phi(7) = 7$, find all elements that map to 7.