Lecture 14  Homomorphisms, Kernels.

Definition Let G and H be groups. Let \( \varphi : G \to H \) be a function. \( \varphi \) is a **homomorphism** if for all \( g_1, g_2 \in G \),

\[
\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)
\]

An isomorphism is the same thing as a bijective homomorphism, but a homomorphism is not required to be injective or surjective, and it may be neither.

Examples 1) \( G = \mathbb{Z}, H = \mathbb{Z}, d \in \mathbb{Z} : \varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(k) = kd \).

This is a homomorphism since \( \varphi(k_1 + k_2) = (k_1 + k_2)d = k_1d + k_2d = \varphi(k_1) + \varphi(k_2) \).

If \( d = \pm 1 \), \( \varphi \) is bijective, so it is an isomorphism.

If \( d = 0 \), \( \varphi(k) = 0 \) for all \( k \), so neither injective nor surjective.

If \( d \in \{ -1, 0, 1 \} \), \( \varphi \) is injective, not surjective, image = \( \langle d \rangle \).

2) \( \varphi : \mathbb{Z} \to \mathbb{Z}/_d, \varphi(k) = [k] : \)

\[
\varphi(k_1 + k_2) = [k_1 + k_2] = [k_1] + [k_2] = \varphi(k_1) + \varphi(k_2)
\]

surjective, not injective.

3) \( G = GL(n, \mathbb{R}) = \{ A \mid A \text{ is an } n \times n \text{ matrix with determinant } 1 \} \)

\( H = \mathbb{R}^* = \mathbb{R} \setminus \{ 0 \} \) with multiplication (General linear group)

\( \varphi : GL(n, \mathbb{R}) \to \mathbb{R}^* \varphi(A) = \det(A) \)

homomorphism because \( \det(AB) = \det(A) \det(B) \).

4) \( S_n = \text{Sym}(\{1, 2, \ldots, n\}) \) symmetric group. Define \( T : S_n \to GL(n, \mathbb{R}) \)

as follows: let \( \vec{e}_i \) be the standard basis vectors in \( \mathbb{R}^n \).

For \( \sigma \in S_n \), let \( T(\sigma) = [ \vec{e}_{\sigma(1)}, \vec{e}_{\sigma(2)}, \ldots, \vec{e}_{\sigma(n)} ] \).
E.g. $n=3$  $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$  $T(\sigma) = [\vec{e}_3 \ | \ \vec{e}_1 \ | \ \vec{e}_2] = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Thus $T(\sigma)$ is the matrix of the unique linear transformation such that $T(\sigma) \vec{e}_i = \vec{e}_{\sigma(i)}$ for all basis vectors $\vec{e}_i$.

$T$ is a homomorphism: $T(\sigma \tau) \vec{e}_i = \vec{e}_{\sigma \tau(i)} = T(\sigma)T(\tau) \vec{e}_i$ so $T(\sigma \tau) = T(\sigma)T(\tau)$.

**Proposition (2.4.10)** If $\varphi : G \to H$ and $\psi : H \to K$ are homomorphisms, so is $\psi \circ \varphi : G \to K$.

**Proof:** Exercise.

**Example** $T : S_n \to GL(n, \mathbb{R})$  $\varepsilon : = \det \circ T : S_n \to \mathbb{R}^*$. Every matrix $T(\sigma)$ has a single 1 on the diagonal, so $\det (T(\sigma)) = \pm 1$. Thus $\varepsilon : S_n \to \{\pm 1\}$ is a homomorphism; called the **sign homomorphism**.

$\sigma$ is called **even** if $\varepsilon(\sigma) = +1$.

$\sigma$ is called **odd** if $\varepsilon(\sigma) = -1$.

Any transposition (2-cycle) $(ij)$ is odd.

If $\sigma$ is the product of $k$ 2-cycles, $E(\sigma) = (-1)^k$.

Even permutations are precisely those that can be written as a composition of an even number of 2-cycles.

**Proposition (2.4.11)** Let $\varphi : G \to H$ be a homomorphism.

Then (1) $\varphi(e_g) = e_H$  (2) $\varphi(g^{-1}) = (\varphi(g))^{-1}$

**Proof:** (1) $e_H = \varphi(e_g) = \varphi(e_g e_g) = \varphi(e_g) \varphi(e_g) = e_H$ by cancellation law.

(2) $e_H = \varphi(e_g) = \varphi(gg^{-1}) = \varphi(g)(\varphi(g)^{-1})$ so $\varphi(g)^{-1} = \varphi(g^{-1})$ by Prop. 2.1.2.
Proposition (2.4.12) \( \phi: G \to H \) a homomorphism.

1. For any subgroup \( A \leq G \), \( \phi(A) \leq H \) is a subgroup.
2. For any subgroup \( B \leq H \), \( \phi^{-1}(B) = \{ g \in G \mid \phi(g) \in B \} \leq G \) is a subgroup.

Proof: See Text for (1). For (2) let \( g_1, g_2 \in \phi^{-1}(B) \). Then \( \phi(g_1), \phi(g_2) \in B \). Since \( B \) is subgroup, \( \phi(g_1) \cdot \phi(g_2) \in B \) since \( \phi \) is homomorphism, \( \phi(g_1) \phi(g_2) = \phi(g_1g_2) \), and thus is in \( B \), so \( g_1g_2 \in \phi^{-1}(B) \). So \( \phi^{-1}(B) \) is closed under mult.

Also, if \( g \in \phi^{-1}(B) \), \( \phi(g) \in B \), so \( \phi(g^{-1}) = \phi(g)^{-1} \in B \), so \( g^{-1} \in \phi^{-1}(B) \), and \( \phi^{-1}(B) \) is closed under inversions.

Special case when \( B = \{ \epsilon \} \leq H \). Then \( \phi^{-1}(B) = \phi^{-1}(\{ \epsilon \}) = \{ g \in G \mid \phi(g) = \{ \epsilon \} \} \).

This is called the kernel of \( \phi \) and denoted \( \ker(\phi) \).

Example (i) \( \phi: \mathbb{Z} \to \mathbb{Z}_n \) \( \phi(k) = [k] \), \( \ker(\phi) = \{ x \mid [x] = [0] \} \) \( = \phi_n, -\phi_n, 0, \phi_n, 2\phi_n, \ldots \phi = \langle n \rangle \).

(ii) \( \varepsilon: S_n \to \{ \pm 1 \} \). \( \ker(\varepsilon) = \) even permutations.
\( A_n := \ker(\varepsilon) \) is called the alternating group on \( n \) elements.

(iii) \( \det: GL(n, \mathbb{R}) \to \mathbb{R}^* \). \( \ker(\det) = \{ A \mid \det(A) = 1 \} \) \( SL(n, \mathbb{R}) := \ker(\det) \) is the special linear group.

The kernel of a homomorphism has a special property.

Def: A subgroup \( N \leq G \) is called normal if for all \( n \in N \) and all \( g \in G \), \( gng^{-1} \in N \).

Not every subgroup has this property!
**Proposition (2.4.15)** Let \( \varphi : G \to H \) be a homomorphism.

Then \( \ker(\varphi) \) is a normal subgroup of \( G \).

**Proof:** Suppose \( n \in \ker(\varphi) \) and \( g \in G \).

Thus \( \varphi(gng^{-1}) = \varphi(g) \varphi(n) \varphi(g^{-1}) = \varphi(g) e_H \varphi(g)^{-1} \)

\[ = \varphi(g) \varphi(g)^{-1} = e_H. \]

So \( gng^{-1} \in \ker(\varphi) \) \( \Box \)

One use of the concept of kernel is that it makes it a bit easier to tell if a homomorphism is injective.

**Proposition (2.4.16)** Let \( \varphi : G \to H \) be a homomorphism.

Then \( \varphi \) is injective if and only if \( \ker(\varphi) = \{ e_G \} \).

**Proof:** Suppose \( \ker(\varphi) = \{ e_G \} \). Let \( g_1, g_2 \in G \) with \( \varphi(g_1) = \varphi(g_2) \).

Then \( e_H = \varphi(g_1) \varphi(g_2)^{-1} = \varphi(g_1) \varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1}) \).

Thus \( g_1 g_2^{-1} \in \ker(\varphi) \). So \( g_1 g_2^{-1} = e_G \) and \( g_1 = g_2 \).

Since \( \varphi(g_1) = \varphi(g_2) \) implies \( g_1 = g_2 \), \( \varphi \) is injective.

Now suppose \( \varphi \) is injective. Since \( \varphi(e_G) = e_H \), if \( g \in \ker(\varphi) \)

then \( \varphi(g) = e_H = \varphi(e_G) \). By injectivity, \( g = e_G \).

So \( \ker(\varphi) = \{ e_G \} \). \( \Box \)