Homomorphisms

Let $G$ and $H$ be groups. A function $\varphi : G \rightarrow H$ is called a homomorphism if for all $g_1, g_2 \in G$ we have $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$.

If $\varphi$ is also bijective, then $\varphi$ is an isomorphism, but a homomorphism is not necessarily bijective.

Examples:

1. Pick $d \in \mathbb{Z}$, and define $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ by $\varphi(k) = kd$.
   Check $\varphi(k_1+k_2) = (k_1+k_2)d = k_1d + k_2d = \varphi(k_1) + \varphi(k_2)$
   so $\varphi$ is a homomorphism.
   - If $d = \pm 1$, $\varphi$ is an isomorphism.
   - If $d = 0$, $\varphi(k) = 0$ for all $k$ (\(\varphi\) constant).
   - If $d \neq 0, 1, -1$, then $\varphi$ is injective but not surjective.

2. $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $\varphi(k) = [k] : \varphi(k_1+k_2) = [k_1+k_2] = [k_1] + [k_2] = \varphi(k_1) + \varphi(k_2)$
   This function is surjective but not injective.
   Related: For a cyclic group $G = \langle a \rangle$, we define $\varphi : \mathbb{Z} \rightarrow G$ by $\varphi(k) = a^k$.

3. General linear group = invertible $n \times n$ matrices
   $GL(n, \mathbb{R}) = \{ A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0 \text{ (or } \exists \text{ } A^{-1} \text{ exists)} \}$
   real entries

   Affine transformations:
   $Aff(\mathbb{R}^n) = \{ T : \mathbb{R}^n \rightarrow \mathbb{R}^n \mid T(x) = Ax + b \text{ for some } A \in GL(n, \mathbb{R}), b \in \mathbb{R}^n \}$

   $\varphi : Aff(\mathbb{R}^n) \rightarrow GL(n, \mathbb{R}) \quad \varphi(T) = A \quad \text{where } T(x) = Ax + b$
   surjective, not injective. [Check it is homomorphism].
4. \( \mathbb{R}^\times = \mathbb{R} \setminus \{0\} \) is a group under multiplication. Determinant function

\[
\text{det} : \text{GL}(n, \mathbb{R}) \to \mathbb{R}^\times
\]

is a homomorphism since \( \text{det}(AB) = \text{det}(A) \text{det}(B) \)

5. Let \( \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\} \). It is a group under multiplication.

The rules \( e^{x+y} = e^x e^y \) and \( \ln(xy) = \ln(x) + \ln(y) \)

mean that \( \exp : (\mathbb{R}_+, \cdot) \to (\mathbb{R}_+, \ast) \) are homomorphisms

\( \ln : (\mathbb{R}_+, \ast) \to (\mathbb{R}_+, \cdot) \)

Since \( \exp \) and \( \ln \) are inverses, these are bijective functions, hence isomorphisms. Thus \( (\mathbb{R}_+, \cdot) \) is isomorphic to \( (\mathbb{R}_+, \ast) \).

6. \( S_n = \) permutations of \( 1, 2, \ldots, n \).

\( T : S_n \to \text{GL}(n, \mathbb{R}) \)

\( T(\sigma) = (e_{\sigma(1)} | e_{\sigma(2)} | \cdots | e_{\sigma(n)}) \)

where \( e_j = (0, \ldots, 0, 1, 0, \ldots) \) \( j \)-th spot is the standard basis of \( \mathbb{R}^n \).

This is the matrix of the linear transformation that maps \( e_i \to e_{\sigma(i)} \) "permutate the basis by \( \sigma \)."

\[
T(\sigma_1 \sigma_2) e_j = e_{\sigma_1 \sigma_2(j)} = T(\sigma_1) T(\sigma_2) e_j
\]

is true for every \( j \), so \( T(\sigma_1 \sigma_2) = T(\sigma_1) T(\sigma_2) \).

Proposition: Let \( \phi : G \to H \) and \( \psi : H \to K \) be homomorphisms. Then \( \psi \circ \phi : G \to K \) is a homomorphism.

**Exercise.

Example: \( T : S_n \to \text{GL}(n, \mathbb{R}) \), \( \text{det} : \text{GL}(n, \mathbb{R}) \to \mathbb{R}^\times \).

\[ E = \text{det} \circ T : S_n \to \mathbb{R}^\times \] is a homomorphism.

Fact: \( \text{det}(T(\sigma)) = \pm 1 \) for each \( \sigma \in S_n \).

\( E : S_n \to \{ \pm 1 \} \) is called the sign homomorphism.
Proposition. Let $\varphi: G \to H$ be a homomorphism. Then
(i) $\varphi(e_G) = e_H$
(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.

Proof: Let $g \in G$. Then $\varphi(g) = \varphi(ge_G) = \varphi(g) \varphi(e_G)$
$\implies \varphi(e_G) = e_H$ by exercise 2.1.3.

$\varphi(g^{-1}) \varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_H$
$\implies \varphi(g^{-1}) = \varphi(g)^{-1}$ by Prop. 2.1.2.

Proposition: Let $\varphi: G \to H$ be a homomorphism.
(i) If $A$ is a subgroup of $G$, then $\varphi(A)$ is a subgroup of $H$.
(Direct image of a subgroup is a subgroup)
(ii) If $B$ is a subgroup of $H$, then $\varphi^{-1}(B) = \{ g \in G | \varphi(g) \in B \}$
is a subgroup of $G$. (Inverse image of a subgroup is a subgroup).

Proof: See text for (a). For (b): Let $B \leq H$ be a subgroup.
Since $\varphi(e_G) = e_H$ and $e_H \in B$, we have $e_G \in \varphi^{-1}(B)$.
so $\varphi^{-1}(B) \neq \emptyset$.

$\varphi^{-1}(B)$ is closed under multiplication: Suppose $g_1, g_2 \in \varphi^{-1}(B)$; this means
$\varphi(g_1), \varphi(g_2) \in B$. Then
$\varphi(g_1g_2) = \varphi(g_1) \varphi(g_2) \in B$ since $B$ is a subgroup.
so $g_1g_2 \in \varphi^{-1}(B)$.

$\varphi^{-1}(B)$ is closed under inverses: Suppose $g \in \varphi^{-1}(B)$ so $\varphi(g) \in B$
then $\varphi(g^{-1}) = \varphi(g)^{-1} \in B$ since $\varphi(g) \in B$ and $B$ is a subgroup.
Thus $g^{-1} \in \varphi^{-1}(B)$. 

}$
Back to the homomorphism \( \varepsilon : S_n \to \{ \pm 1 \} \)

\[ \varepsilon(\sigma) = \text{det}(T(\sigma)) = \text{"permutation matrix"} = (e_{\sigma(1)} \ldots e_{\sigma(n)}) \]

**Definition**

- If \( \varepsilon(\sigma) = 1 \), we call \( \sigma \) an **even permutation**.
- If \( \varepsilon(\sigma) = -1 \), we call \( \sigma \) an **odd permutation**.

Identity is even: \( T(\varepsilon) = (e_1 \ldots e_n) = \text{identity matrix} = I \)

\[ \varepsilon(\varepsilon) = \text{det}(I) = 1 \]

A transposition is odd: \( T((i \ j)) = (\ldots e_i \ e_j \ e_i \ e_j \ e_i \ e_j \ e_i \ e_j) \)

\[ \varepsilon((i \ j)) = \text{det}(T((i \ j))) = -1 \text{ since swapping columns changes sign of det.} \]

Now every permutation can be written as a product of transpositions.

**Proposition**

A permutation is even iff it can be written as a product of an even number of transpositions.

**Proof**

For \( \sigma \in S_n \), write \( \sigma = \tau_1 \tau_2 \cdots \tau_k \), \( \tau_i \) a transposition.

Then \( \varepsilon(\sigma) = \varepsilon(\tau_1 \tau_2 \cdots \tau_k) = \varepsilon(\tau_1) \varepsilon(\tau_2) \cdots \varepsilon(\tau_k) \)

\[ = (-1)(-1) \cdots (-1) = (-1)^k \]

So \( \sigma \) even \( (\iff) \) \( \varepsilon(\sigma) = 1 \iff k \) is even

\( \sigma \) odd \( (\iff) \) \( \varepsilon(\sigma) = -1 \iff k \) is odd.

**Corollary** A \( k \)-cycle is even as a permutation iff \( k \) is odd.

**Proof**: A \( k \)-cycle can be written as a product of \( k-1 \) transpositions.

**Exercise** \( (125)(389)(410) \) is even.
Kernel of a homomorphism: \( \varphi: G \to H \) a homomorphism.

Now \( B = \{ e_H \}^3 \leq H \) is a subgroup. Therefore \( \varphi^{-1}(\{ e_H \}) = \{ g \in G \mid \varphi(g) = e_H \}^3 \) is a subgroup of \( G \).

We write
\[
\ker(\varphi) = \varphi^{-1}(\{ e_H \})
\]
and we call this the kernel of \( \varphi \).

**Example:**
1. \( \varphi: \mathbb{Z} \to \mathbb{Z}_n \), \( \varphi(k) = [k] \).
   \[
   \ker(\varphi) = \{ k \mid [k] = [0] \}^3 = \{ k \mid k \equiv 0 \mod n \} = \langle n \rangle = n\mathbb{Z}.
   \]
2. \( \varepsilon: S_n \to \{ \pm 1 \} \), \( \ker(\varepsilon) \) = set of even permutations.
   Notation: \( A_n = \ker(\varepsilon) \) is the alternating group on \( \{1, 2, \ldots, n\} \).
3. \( \det: GL(n, \mathbb{R}) \to \mathbb{R}^\times \), \( \ker(\det) = \{ A \mid \det(A) = 1 \} = \text{SL}(n, \mathbb{R}) \).

The kernel is always a subgroup, and it has a special property.

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

**Proposition:** Let \( \varphi: G \to H \) be a homomorphism.
Then \( \ker(\varphi) \) is a normal subgroup of \( G \).

**Proof:** We know \( \ker(\varphi) \) is a subgroup; just need to show it is normal.

Let \( g \in G \) and \( n \in \ker(\varphi) \), so \( \varphi(n) = e \).

Need to show \( gng^{-1} \in \ker(\varphi) \), so need to show \( \varphi(gng^{-1}) = e \).

Indeed
\[
\varphi(gng^{-1}) = \varphi(g) \varphi(n) \varphi(g^{-1}) = \varphi(g) e \varphi(g^{-1}) = \varphi(g) \varphi(g^{-1}) = \varphi(g) \varphi(g^{-1}) = e.
\]
So we are done.
For a group $G$, a subset $N \subseteq G$, and $g \in G$, define

$$gN g^{-1} = \{gn g^{-1} \mid n \in N\}.$$  

**Proposition** Given a subgroup $N \subseteq G$, $N$ is normal iff for all $g \in G$, we have $gNg^{-1} = N$.

**Proof:** The definition of being normal is that for all $g \in G$,

$$gN g^{-1} \subseteq N,$$

so it is clearly implied by the condition $gNg^{-1} = N$.

On the other hand, suppose $\forall g \in G$, $gNg^{-1} \subseteq N$.

Then take $h = g^{-1}$, and we have $hNh^{-1} \subseteq N$.

So $g^{-1}Ng \subseteq N$.

Thus $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$, so $N = gNg^{-1}$. \qed