Homomorphisms

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

If φ is also bijective, then φ is an isomorphism, but a homomorphism is not necessarily bijective.

Examples: ① Pick $d \in \mathbb{Z}$, and define $\varphi: \mathbb{Z} \to \mathbb{Z}$ by $\varphi(k) = kd$

Check $\varphi(k_1 + k_2) = (k_1 + k_2)d = k_1 d + k_2 d = \varphi(k_1) + \varphi(k_2)$

so φ is a homomorphism.

→ If $d = \pm 1$, φ is an isomorphism

→ If $d = 0$, $\varphi(k) = 0$ for all k (φ constant)

→ If $d \neq 0, 1, \text{or} -1$, then φ is injective but not surjective.

② $\varphi: \mathbb{Z} \to \mathbb{Z}_n$ 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 $G = \langle a \rangle$, can define

$\varphi: \mathbb{Z} \to G \qquad \varphi(k) = a^k$.

③ General linear group = invertible $n \times n$ matrices

$$GL(n, \mathbb{R}) = \{ A \ \underset{\text{real entries}}{n \times n \text{ matrix}} \mid \det(A) \neq 0 \ (\text{or } A^{-1} \text{ exists}) \}$$

Affine transformations:

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

$\varphi: \mathrm{Aff}(\mathbb{R}^n) \to GL(n, \mathbb{R}) \qquad \varphi(T) = A \qquad$ 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
$$\det : GL(n,\mathbb{R}) \longrightarrow \mathbb{R}^\times$$
is a homomorphism since $\det(AB) = \det(A)\det(B)$

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

(6) S_n = permutations of $\{1,2,\dots,n\}$.
$T : S_n \to GL(n,\mathbb{R}) \quad T(\sigma) = \left(e_{\sigma(1)} \mid e_{\sigma(2)} \mid \cdots \mid e_{\sigma(n)} \right)$
where $e_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ ← j-th spot is the standard basis of $\mathbb{R}^n$.
This is the matrix of the linear transformation that maps
$e_i \mapsto e_{\sigma(i)}$ "permute the basis by σ."

$T(\sigma_1\sigma_2)e_j = e_{\sigma_1\sigma_2(j)} = T(\sigma_1)e_{\sigma_2(j)} = T(\sigma_1)T(\sigma_2)e_j$
is true for every j, so $T(\sigma_1\sigma_2) = T(\sigma_1)T(\sigma_2)$. ✓

Proposition: Let $\varphi : G \to H$ and $\psi : H \to K$ be homomorphisms.
Then $\psi \circ \varphi : G \to K$ is a homomorphism.
Pf. exercise.

Example $T : S_n \to GL(n,\mathbb{R})$, $\det : GL(n,\mathbb{R}) \to \mathbb{R}^\times$.
$\varepsilon = \det \circ T : S_n \to \mathbb{R}^\times$ is a homomorphism.
Fact: $\det(T(\sigma)) = \pm 1$ for each $\sigma \in S_n$.
$\varepsilon : S_n \to \{\pm 1\}$ is called the sign homomorphism.

<u>Proposition</u> Let $\varphi: G \to H$ be a homomorphism, then
(i) $\varphi(e_G) = e_H$ (ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.

<u>Proof</u> Let $g \in G$. Then $\varphi(g) = \varphi(g e_G) = \varphi(g)\varphi(e_G)$
$\Rightarrow \varphi(e_G) = e_H$ by exercise 2.1.3.

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

<u>Proposition</u> 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 $\varphi^{-1}(B) = \{g \in G \mid \varphi(g) \in B\}$
is a subgroup of H. (Inverse image of a subgroup is a subgroup).

<u>Proof</u>: 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
$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \in B$ since B is a subgrp.
so $g_1 g_2 \in \varphi^{-1}(B)$.

* $\varphi^{-1}(B)$ 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 subgroup.
Thus $g^{-1} \in \varphi^{-1}(B)$. ▨

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

$\varepsilon(\sigma) = \det(T(\sigma))$ $\quad T(\sigma) =$ "permutation matrix"

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

<u>Definition</u> If $\varepsilon(\sigma) = 1$, we call σ an <u>even permutation</u>

If $\varepsilon(\sigma) = -1$, we call σ an <u>odd permutation</u>.

Identity is even: $T(\sigma) = (e_1 | \cdots | e_n) =$ identity matrix $= I$

$$\varepsilon(\sigma) = \det(I) = 1$$

A transposition is odd: $T((ij)) = (\cdots | e_{i-1} | e_j | e_{i+1} | \cdots | e_{j-1} | e_i | e_{j+1} \cdots)$

$\varepsilon((ij)) = \det(T((ij))) = -1$ since swapping columns changes sign of det.

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

<u>Proposition</u> A permutation is even iff it can be written as a product of an even number of transpositions.

<u>Proof</u> for $\sigma \in S_n$, write $\sigma = \tau_1 \tau_2 \cdots \tau_k$, τ_i a transposition.

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

$$= \underbrace{(-1)(-1)\cdots(-1)}_{k \text{ times}} = (-1)^k$$

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

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

<u>Corollary</u> A k-cycle is even as a permutation iff k is odd.

<u>Proof</u>: A k-cycle can be written as a product of $k-1$ transpositions.

<u>Exercise</u> $(125)(3789)(4\ 10)$ is even.

<u>Kernel of a homomorphism</u>: $\varphi: G \to H$ a homomorphism.
Now $B = \{e_H\} \leq H$ is a subgroup. Therefore
$\varphi^{-1}(\{e_H\}) = \{g \in G \mid \varphi(g) = e_H\}$ is a subgroup of G.
We write

$$\ker(\varphi) = \varphi^{-1}(\{e_H\})$$

and we call this the <u>kernel</u> of φ.

<u>Example</u>: ⓐ $\varphi: \mathbb{Z} \to \mathbb{Z}_n$ $\varphi(k) = [k]$.
$\ker(\varphi) = \{k \mid [k] = [0]\} = \{k \mid k = nq \text{ for } q \in \mathbb{Z}\} = \langle n \rangle = n\mathbb{Z}$.

ⓑ $\varepsilon: S_n \to \{\pm 1\}$, $\ker(\varepsilon) =$ set of even permutations.
Notation: $A_n = \ker(\varepsilon)$ is the <u>alternating group</u> on $\{1, 2, ..., n\}$.

ⓒ $\det: GL(n, \mathbb{R}) \to \mathbb{R}^\times$ $\ker(\det) = \{A \mid \det(A) = 1\} = SL(n, \mathbb{R})$.

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

<u>Definition</u>: A subgroup $N \leq G$ is called <u>normal</u> if
for all $g \in G$ and all $n \in N$, we have $gng^{-1} \in N$

<u>Proposition</u>: Let $\varphi: G \to H$ be a homomorphism.
Then $\ker(\varphi)$ is a normal subgroup of G.

<u>Proof</u>: 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
$gNg^{-1} = \{ gng^{-1} \mid n \in N \}$.

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

Proof: The definition of being normal is that for all $g \in G$, $gNg^{-1} \subseteq N$, 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 $g^{-1}Ng \subseteq N$.
Then $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$! so $N = gNg^{-1}$! ∎