MAT3004 Lecture 6 Notes: Group Homomorphisms

Recall

$$\begin{aligned}
\phi : D_4 &\to S_4 \\
r &\mapsto (1\,2\,3\,4) \\
s &\mapsto (2\,4) \\
rs &\mapsto (1\,2)(3\,4) \\
&\vdots
\end{aligned}$$

[Diagram: A square with vertices labeled 1, 2, 3, 4 undergoing rotation/reflection symmetries]

---

1 Group Homomorphisms

Definition 1. Let $(G, *_G)$ and $(H, *_H)$ be groups. A map $\phi : G \to H$ is a **homomorphism** if:

$$\phi(g *_G g') = \phi(g) *_H \phi(g')$$

[Diagram: Visual representation of mapping from domain G to codomain H, showing preservation of structure]

1.1 Examples

1. $\phi : D_4 \to S_4$ is an **injective** homomorphism.

$$\text{e.g., } \phi(rs) = \phi(r)\phi(s)$$

2. $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ (positive numbers with multiplication).

$$\exp(a) := e^a$$

is a **bijective** homomorphism.

Proof. Since $\exp(a + b) := e^{a+b} = e^a \times e^b = \exp(a) \times \exp(b)$. □

3. $\det : (GL(n, \mathbb{R}), \times) \to (\mathbb{R}^*, \times)$ is a homomorphism.

$$\det(A \times B) = \det(A) \cdot \det(B)$$

4. Let $T : V \to W$ be a linear transformation between vector spaces, then
$$T : (V, +_V) \to (W, +_W)$$
is a homomorphism.
$$T(v +_V v') = T(v) +_W T(v')$$

5. $\pi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\pi(a) = [a]_n$ is a homomorphism.

Proof.
$$\begin{aligned} \pi(a+b) &:= [a+b]_n \\ &= [a]_n + [b]_n \quad \text{(definition of modular arithmetic)} \\ &= \pi(a) + \pi(b) \end{aligned}$$
□

6. $\psi : (\mathbb{Z}_n, +) \to (S_n, \times)$
$$\begin{aligned} &\psi([0]) := e \\ &\psi([1]) := (1\,2\,4\,5) \quad \textit{(Note: Specific example values)} \\ &\psi([2]) = (1\,4)(2\,5) \\ &\psi([3]) = (1\,5\,4\,2) \end{aligned}$$
is an injective homomorphism. (Exercise)

(6b) **Question:** Can I define a homomorphism $\psi' : \mathbb{Z}_4 \to S_8$ (or $S_?$) with $\psi'([1]) = (1\,2\,3)$?

Ans: No, since:
$$\begin{aligned} \psi'([0]) &= \psi'([1] + [1] + [1] + [1]) \\ &= \psi'([1]) \cdots \psi'([1]) \\ &= (1\,2\,3)^4 \\ &= (1\,2\,3)^3 \cdot (1\,2\,3) = e \cdot (1\,2\,3) = (1\,3\,2) \quad \text{(*calculation note)} \end{aligned}$$
But $\psi'([0])$ must map to identity e.
$$\implies (1\,3\,2) = e \quad \text{(Contradiction)}$$

(7) Another non-example of homomorphism:
$$\phi : (\mathbb{Z}_8^{\times}, \times) \to (\mathbb{Z}_8, +)$$
$$\phi([k]) := [k]$$

(8) (Exercise) $\phi : (S_n, \times) \to (\mathbb{Z}_2, +)$
$$\phi(\sigma) := \begin{cases} [0]_2 & \text{if } \sigma \text{ is even} \\ [1]_2 & \text{if } \sigma \text{ is odd} \end{cases}$$
is a surjective homomorphism. E.g.:

- $\phi(\sigma \cdot \tau) = [1]$ (even $\cdot$ odd = odd) $= [0] + [1] = \phi(\sigma) + \phi(\tau)$
- $\phi(\sigma \cdot \tau) = [0]$ (odd $\cdot$ odd = even) $= [1] + [1] = \phi(\sigma) + \phi(\tau)$

(9) If $H \leq G$ is a subgroup, then inclusion map $i : (H, \times) \to (G, \times)$, $i(h) = h$ is an injective homomorphism.

(10) For any $(G, \times), (H, \cdot)$, the trivial map:

$$t : (G, \times) \to (H, \cdot)$$

$$t(g) := e_H, \quad \forall g \in G$$

is a homomorphism.

$$t(g \times g') = e_H = e_H \cdot e_H = t(g) \cdot t(g')$$

---

2 Properties

Proposition 1.

1. *If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $\psi \circ \phi : G \to K$ is also a homomorphism.*
2. *If $\phi : G \to H$ is a homomorphism, then $\phi(e_G) = e_H$ and $\phi(g^{-1}) = (\phi(g))^{-1}$.*

Proof

(1) Consider $(\psi \circ \phi)(a \times_G b)$. Since ϕ is homom:

$$= \psi(\phi(a) *_H \phi(b))$$

Since ψ is homom:

$$= \psi(\phi(a)) *_K \psi(\phi(b))$$
$$= (\psi \circ \phi)(a) *_K (\psi \circ \phi)(b)$$

(2) First, for the identity:

$$\phi(e_G) = \phi(e_G \times_G e_G)$$
$$\phi(e_G) = \phi(e_G) *_H \phi(e_G)$$

By cancellation in group H (multiply by $\phi(e_G)^{-1}$), we get $e_H = \phi(e_G)$.

Second, for inverses:

$$\begin{aligned} \phi(g)\phi(g^{-1}) &= \phi(g \times g^{-1}) \\ &= \phi(e_G) \\ &= e_H \end{aligned}$$

Similarly $\phi(g^{-1})\phi(g) = e_H$. Thus $\phi(g^{-1}) = (\phi(g))^{-1}$.

---

3 Isomorphisms

Definition 2. A **bijective** group homomorphism $\phi : G \to H$ is called a group **isomorphism**.

Proposition 2. *If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is also a group homomorphism.*

Proof. For any $h = \phi(g), h' = \phi(g') \in H$:

$$\begin{aligned}
\phi^{-1}(h *_H h') &= \phi^{-1}(\phi(g) *_H \phi(g')) \\
\text{(since } \phi \text{ is homom)} &= \phi^{-1}(\phi(g \times g')) \\
&= g \times g' \\
&= \phi^{-1}(h) \times_G \phi^{-1}(h')
\end{aligned}$$

□

Remark 1. If $\phi : G \xrightarrow{\cong} H$ are isomorphic, then all information on H can be "obtained" from G (and vice versa). E.g., to compute $h *_H h' \in H$:

$$h *_H h' = \phi(g) *_H \phi(g') = \phi(g \times g')$$

If I know $g \times g'$, then I know $h *_H h'$ by ϕ.

Theorem 1. *Let $\phi : G \to H$ be an isomorphism. Then:*

(a) G is abelian $\iff$ H is abelian

(b) G is cyclic $\iff$ H is cyclic

Proof. By Proposition 2 (inverse is homom), it is enough to show " $\implies$ " in both (a) & (b).

(a) If G is abelian, then for any $h = \phi(g), h' = \phi(g') \in H$:

$$\begin{aligned}
h *_H h' &= \phi(g) *_H \phi(g') \\
&= \phi(g \times g') \\
\text{(G is abelian)} &= \phi(g' \times g) \\
&= \phi(g') *_H \phi(g) \\
&= h' *_H h
\end{aligned}$$

(b) If $G = \langle g \rangle$ is cyclic, then (Exercise) $H = \langle \phi(g) \rangle$ and hence it is cyclic as well. □

Examples of distinguishing groups

1. S_3 and $\mathbb{Z}_6$ both have 6 elements. But $S_3 \ncong \mathbb{Z}_6$ because S_3 is **not abelian** while $\mathbb{Z}_6$ is abelian.

2. $|\mathbb{Z}_9| = |\mathbb{Z}_3 \times \mathbb{Z}_3| = 9$. But $\mathbb{Z}_9 \ncong \mathbb{Z}_3 \times \mathbb{Z}_3$. $\mathbb{Z}_9$ is cyclic, while $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not cyclic. (Ex: $\langle ([a], [b]) \rangle$ has at most 3 elements).

Remark 2. We will classify groups up to isomorphisms. e.g., $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$ are "the same" group. But $\mathbb{Z}_9 \ncong \mathbb{Z}_3 \times \mathbb{Z}_3$ are "different" groups.

---

4 Kernel and Image

Definition 3. Let $\phi : G \to H$ be a homomorphism. Then:

- $\ker(\phi) := \{g \in G \mid \phi(g) = e_H\}$
- $\mathrm{im}(\phi) := \{\phi(g) \in H \mid g \in G\}$ $(:= \phi(G))$

Proposition 3. *1.* $\ker(\phi) \leq G$ *(is a subgroup)*

2. $\mathrm{im}(\phi) \leq H$ *(is a subgroup)*

3. ϕ *is injective* $\iff \ker(\phi) = \{e_G\}$ *(the trivial subgroup)*

4. ϕ *is surjective* $\iff \mathrm{im}(\phi) = H$

Proof of (1). Take $a, b \in \ker(\phi)$. Then

$$\phi(a) = e_H, \quad \phi(b) = e_H$$

$$\phi(ab) = \phi(a)\phi(b) = e_H \times e_H = e_H$$

$\therefore ab \in \ker(\phi)$.

Also $\phi(a^{-1}) = (\phi(a))^{-1} = (e_H)^{-1} = e_H$. $\therefore a^{-1} \in \ker(\phi)$. Thus $\ker(\phi) \leq G$. $\square$