§1 Tutorial 11-08

§1.1 Homomorphisms

$\varphi : G \to H$. Then $\varphi(xy) = \varphi(x) \cdot \varphi(y)$. Intuitively thing of a homomorphism as recovering some of the structure of one group in another group.

Theorem 1.1 (1st Isomorphism Theorem)
Let $\varphi : G \to H$ be a homomorphism. Then

$$N = \ker(\varphi) = \{x \in G | \varphi(x) = e_H\}$$

Note that N is normal in G, that $\varphi(G)$ is a subgroup of H and that $G/N \cong \varphi(G)$.

Example 1.2

$$\varphi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$

where $\varphi(a) = (a, 0)$. Therefore $\ker(\varphi) = \{0\}$, the trivial subgroup.

Example 1.3

$$\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

where $\varphi(a, b) = a$. $\ker(\varphi) = \{(0, b) : b \in \mathbb{Z}\}$. This is a non trivial kernel.

Thus $\mathbb{Z} \cong \mathbb{Z}^2 / \ker(\varphi)$ by the 1st Isomorphism Theorem.

Exercise 1.4. Let A be an $n \times m$ matrix. Then the map $\varphi(x) = Ax$ defines a homomorphism from $\mathbb{R}^n \to \mathbb{R}^m$.

Let $x, y \in \mathbb{R}^n$. Then $\varphi(x + y) = A(x + y) = Ax + Ay = \varphi(x) + \varphi(y)$

<u>Intution</u>: Multiplying by a matrix corresponds to applying a linear map (we could be scaling, rotating, projecting, etc).

Example 1.5

$$A = \begin{pmatrix} 4/5 & 2/5 \\ 2/5 & 1/5 \end{pmatrix}$$

Exercise 1.6.

$$\epsilon : S_n \to \{\pm 1\}$$

$$\epsilon(\sigma) = \begin{cases} 1, & \sigma \text{ composed of an even number of transpositions} \\ -1, & \sigma \text{ composed of an even number of transpositions} \end{cases}$$

Homomorphism: $\sigma, \tau \in S_n$,

$$\epsilon(\sigma\tau) = \begin{cases} 1, & \sigma\tau \text{ composed of an even number of transpositions} \\ -1, & \sigma\tau \text{ composed of an even number of transpositions} \end{cases}$$

$$\epsilon(\sigma\tau) = \begin{cases} 1, & \sigma \text{ \& } \tau \text{ both even or odd} \\ -1, & \text{Either } \sigma \text{ even and } \tau \text{ odd or } \sigma \text{ odd and } \tau \text{ even} \end{cases}$$

Therefore it works out that $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$.

Example computation:

$$\sigma = (1\,2)$$
$$\tau = (1\,4)(3\,5)(1\,6)$$
$$\sigma\tau = (1\,2)(1\,4)(3\,5)(1\,6)$$
$$\epsilon(\sigma) \cdot \epsilon(\tau) = -1 \cdot -1 = 1 = \epsilon(\sigma\tau)$$

What is the kernel of ϵ? $\ker(\epsilon) = A_n$ (all the even permutations)

Therefore, by the 1st Isomorphism Theorem, $S_n/A_n \cong \{\pm 1\}$.

Exercise 1.7. Let $\varphi : G \to H$. Prove that φ is injective if and only if $\ker(\varphi) = \{e\}$.

Proof.

($\Rightarrow$) Let $g \in \ker(\varphi)$.

$$\varphi(g) = e = \varphi(e)$$

So therefore $g = e$ because φ is injective. Therefore the only element that maps to $\{e\}$ is e itself.

($\Leftarrow$) Assume that $\ker(\varphi) = \{e\}$ and let $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$. We want to show that $g_1 = g_2$.

$$\begin{aligned} \varphi(g_1) = \varphi(g_2) &\Rightarrow \varphi(g_1)(\varphi(g_2))^{-1} = e_H \\ &\Rightarrow \varphi(g_1)\varphi(g_2^{-1}) = e_H \\ &\Rightarrow \varphi(g_1 g_2^{-1}) = e_H \\ &\Rightarrow g_1 g_2^{-1} = e_G \\ &\Rightarrow g_1 = g_2 \end{aligned}$$

$\square$

Intuitively this makes sense. If and only if φ is injective than we can recover everything from G. If and only if $\ker(\varphi) = \{e\}$ then we can recover everything from G. Therefore φ is injective if and only if $\ker(\varphi) = \{e\}$.

Exercise 1.8. Let $\phi : G \to H$, $N = \ker(\phi)$, $K \subseteq G$ is a subgroup. Show that $\phi^{-1}(\phi(K)) = KN$ where $KN = \{kn : k \in K, n \in N\}$.

Proof.

$$\begin{gathered}\text{Let } g \in \phi^{-1}(\phi(K)) \\ \Leftrightarrow \phi(g) = \phi(k) \text{ for some } k \in K \\ \Leftrightarrow \phi(g) \cdot \phi(k)^{-1} = \phi(gk^{-1}) = e \\ \Leftrightarrow gk^{-1} \in N \Rightarrow g \in kN \\ \Leftrightarrow g \in KN\end{gathered}$$

$\square$

Exercise 1.9. Let $\varphi : G \to H$ where $G = \langle g \rangle$ i.e. G is cyclic. Show that φ is determined by $\varphi(g)$.

Proof. Let $g' \in G$. Then $g' = g^k$ for some k (we know this because of the properties of a generator).

$$\begin{gathered}\text{Fix } \varphi(g) = h. \text{ Then} \\ \varphi(g') = \varphi(g^k) = \varphi(g)^k = h^k.\end{gathered}$$

$\square$

Remark 1.10. We can generalize this statement to groups that have finitely many generators.

Example 1.11

Try to find an Isomorphism between $U(20)$ and $U(16)$.

$$\begin{gathered}U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\} \\ \langle 3 \rangle = \{3, 9, 7, 1\} \\ \langle 19 \rangle = \{19, 1\} \\ \langle 3 \rangle \times \langle 19 \rangle = U(20) \\ \\ U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\} \\ \langle 3 \rangle = \{3, 9, 11, 1\} \\ \langle 15 \rangle = \{15, 1\} \\ \langle 3 \rangle \times \langle 15 \rangle = U(16)\end{gathered}$$

So fixing $\varphi(3) = 3, \varphi(19) = 15$ is a valid isomorphism.