Homomorphism and Isomorphisms

Let $(G, *_G)$ and $(H, *_H)$ be groups. A group homomorphism is a map $\varphi : G \to H$ that satisfies:

$$\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$$

For every $g_1, g_2 \in G$. If in addition φ is bijective, we say φ is an isomorphism. If there is an isomorphism, we say they are isomorphic and write $G \cong H$. We also indicate this as $\varphi : G \xrightarrow{\cong} H$.

Example: Let $G = \langle a \rangle$ be a cyclic group of order n, i.e. $G = \{a, a^2, \dots, a^{n-1}, e\}$. Define $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$, $[j]_n \mapsto a^j$. Show this is an isomorphism.

We first want to show that $[j]_n \mapsto a^j$ is well defined.
Let $[i]_n = [j]_n$. We can write $i = j + nk$, $k \in \mathbb{Z}$.
So:

$$\begin{aligned}\varphi([i]_n) &= a^i \\ &= a^{j+nk} \\ &= a^j (a^n)^k \\ &= a^j e_G \\ &= \varphi([j]_n)\end{aligned}$$

Thus φ is well-defined.

We now would like to show that φ is a homomorphism.
Let $[j]_n, [m]_n \in \mathbb{Z}/n\mathbb{Z}$. We have

$$\begin{aligned}\varphi([j]_n + [m]_n) &= \varphi([j+m]_n) \\ &= a^{j+m} \\ &= a^j a^m \\ &= \varphi([j]_n)\varphi([m]^n).\end{aligned}$$

Thus φ is a homomorphism.

Trick: Two finite sets of same size, injectivity $\Rightarrow$ surjectivity.

We now want to show injectivity and surjectivity.
Suppose $\varphi([j]_n) = \varphi([m]_n)$ for some $[j]_n, [m]_n \in \mathbb{Z}/n\mathbb{Z}$.
This means $a^j = a^m$.
We said before that this means $j \equiv m \pmod{n}$, i.e. $[j]_n = [m]_n$. Thus φ is injective.

Let $g \in G$. We can write a^j for some $0 \leq j \leq n-1$ because G is cyclic. Note now that $\varphi([j]_n) = a^j = g$. Hence φ is surjective.

Surjectivity
- Start with general element in codomain
- Show something maps to it

Thus $G \cong H$.

Proposition: Let $\varphi: G \to H$ be a homomorphism. $\forall g \in G$:

1) $\varphi(e_G) = e_H$
2) $\varphi(g^n) = \varphi(g)^n$
3) $|\varphi(g)| \mid |g|$
4) $\varphi(g^{-1}) = \varphi(g)^{-1}$

proof: (1)

$$\varphi(e_G) = \varphi(e_G *_G e_G)$$
$$= \varphi(e_G) *_H \varphi(e_G)$$
$$\Rightarrow \varphi(e_G) *_H \varphi(e_G)^{-1} = \varphi(e_G) *_H \varphi(e_G) *_H \varphi(e_G)^{-1}$$
$$e_H = \varphi(e_G) *_H e_H$$
$$e_H = \varphi(e_G)$$

(2) Base case: Let $n=2$. Then $\varphi(g^2) = \varphi(g *_G g) = \varphi(g) *_H \varphi(g)$
$$= \varphi(g)^2$$

Inductive Hypothesis: Suppose our statement holds true for $n=k$. For $n=k+1$:

$$\varphi(g^{k+1}) = \varphi(g^k *_G g) = \varphi(g^k) *_H \varphi(g)$$
$$= \varphi(g)^k *_H \varphi(g)$$
$$= \varphi(g)^{k+1}$$

(3) Let $|g| = m$. We have:

$$\varphi(g)^m = \varphi(g^m) \quad \text{From (2)}$$
$$= \varphi(e_G)$$
$$= e_H \quad \text{From (1)}$$

Since $\varphi(g)^m = e_H$, we have $|\varphi(g)| \mid m = |\varphi(g)| \mid |g|$.

(4) Note $\varphi(g) *_H \varphi(g^{-1}) = \varphi(g *_G g^{-1})$
$$= \varphi(e_G)$$
$$= e_H.$$

Since inverses are unique, it must be the case that $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Definition: Let $\varphi: G \to H$ be a homomorphism.
The *kernel* of φ is defined as $\operatorname{Ker}\varphi = \{g \in G : \varphi(g) = e_H\}$.

Example: Define $\varphi: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by $\varphi(m) = [m]_2$.
Let $m,n \in \mathbb{Z}$. We have $\varphi(m+n) = [m+n]_2 = [m]_2 + [n]_2 = \varphi(m) + \varphi(n)$.
So

$$\begin{aligned}
\operatorname{Ker}\varphi &= \{m \in \mathbb{Z} : \varphi(m) = [0]_2\} \\
&= \{m \in \mathbb{Z} : [m]_2 = [0]_2\} \\
&= \{m \in \mathbb{Z} : m \text{ is even}\} \\
&= 2\mathbb{Z}
\end{aligned}$$

Review what this explicitly means

Proposition: Let $\varphi: G \to H$ be a homomorphism.
We have $\operatorname{Ker}\varphi$ is a subgroup of G.

proof: Note $\operatorname{Ker}\varphi \neq \emptyset$ b/c $e_G \in \operatorname{Ker}\varphi$.
Let $g_1, g_2 \in \operatorname{Ker}\varphi$. We have:

$$\begin{aligned}
\varphi(g_1 *_G g_2^{-1}) &= \varphi(g_1) *_H \varphi(g_2^{-1}) \\
&= \varphi(g_1) *_H \varphi(g_2)^{-1} \\
&= e_H *_H e_H^{-1} \\
&= e_H
\end{aligned}$$

Thus $g_1 * g_2^{-1} \in \operatorname{Ker}\varphi$.

Proposition: Let $\varphi: G \to H$ be a homomorphism.
The function φ is injective if and only if $\operatorname{Ker}\varphi = \{e_G\}$.

proof: $(\Rightarrow)$ Assume φ is injective. Let $g \in \operatorname{Ker}\varphi$.
This means $\varphi(g) = e_H = \varphi(e_G)$. Since φ is injective, $g = e_G$. Thus $\operatorname{Ker}\varphi = \{e_G\}$.
$(\Leftarrow)$ Assume $\operatorname{Ker}\varphi = \{e_G\}$. Let $g_1, g_2 \in G$ so that $\varphi(g_1) = \varphi(g_2)$. Multiply both sides by $\varphi(g_2)^{-1}$:

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

Observe

$$\begin{aligned}
e_H &= \varphi(g_2)^{-1} * \varphi(g_1) \\
&= \varphi(g_2^{-1}) * \varphi(g_1) \\
&= \varphi(g_2^{-1} * g')
\end{aligned}$$

So $g_2^{-1} * g_1 \in \operatorname{Ker}\varphi = \{e_G\}$
So $g_2^{-1} * g_1 = e_G$

So $\underline{g_1 = g_2}$

Exercise: Define $\varphi : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by $\varphi([a]_{10}) = [a]_2$

1) Show well-defined
2) Show φ is a homomorphism
3) Find $\operatorname{Ker}\varphi$

1) Let $[i]_{10} = [j]_{10}$

So $i = j + 10k$, $k \in \mathbb{Z}$

$$\begin{aligned}\varphi([i]_{10}) &= [i]_2 \\ &= [j+10k]_2 \\ &= [j]_2 + [10k]_2 \\ &= [j]_2 \\ &= \varphi([j]_{10})\end{aligned}$$

2) Let $[i]_{10}, [j]_{10} \in \mathbb{Z}/10\mathbb{Z}$

$$\begin{aligned}\varphi([i]_{10} + [j]_{10}) &= \varphi([i+j]_{10}) \\ &= [i+j]_2 \\ &= [i]_2 + [j]_2 \\ &= \varphi([i]_{10}) + \varphi([j]_{10})\end{aligned}$$

3)
$$\begin{aligned}\operatorname{Ker}\varphi &= \{[m]_{10} \in \mathbb{Z}/10\mathbb{Z} : \varphi([m]_{10}) = [0]_2\} \\ &= \{\text{''} \qquad \text{''} : [m]_2 = [0]_2\} \\ &= 2\mathbb{Z}/10\mathbb{Z}\end{aligned}$$