Discuss in your group:

Let g be a group element with $\text{ord}(g) = 6$. Consider the cyclic group $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Elizabeth says,

> "The operations of $\mathbb{Z}_6$ and $\langle g \rangle$ match up."

What might she mean?

$+$ $\quad$ $*$ $\quad$ $\theta(3) = g^3$

Key property: Consider $\theta : \mathbb{Z}_6 \to \langle g \rangle$ where $\theta(a) = g^a$ for all $a \in \mathbb{Z}_6$.

θ is *operation preserving*, i.e., $\boxed{\theta(a+b) = \theta(a) * \theta(b)}$ for all $a, b \in \mathbb{Z}_6$.

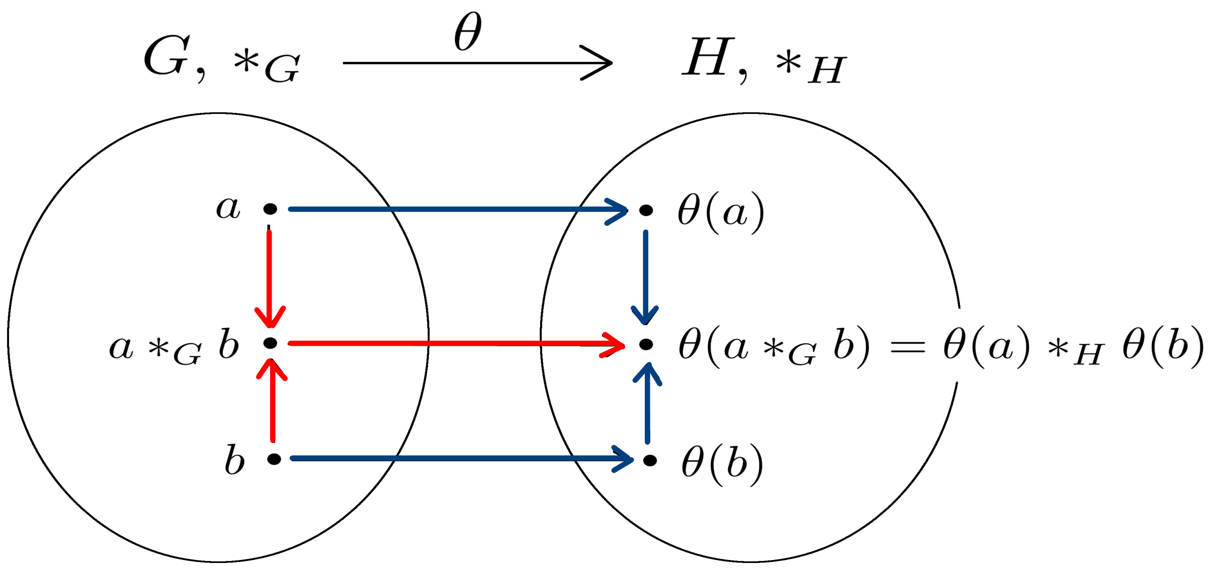
$$g^{a+b} = g^a * g^b$$

(i.e., addition in $\mathbb{Z}_6$ *feels like* multiplication in $\langle g \rangle$.)

Definition. Let G and H be groups w/ operations $*_G$ and $*_H$.

A function $\theta : G \to H$ is a ~~isomorphism~~ homomorphism if

- ~~θ is a bijection (i.e., one-to-one and onto), and~~
- θ is *operation preserving*, i.e., $\theta(a *_G b) = \theta(a) *_H \theta(b)$ for all $a, b \in G$.



Note: An isomorphism is a special type of a homomorphism.

Important example:

$\varphi(43) = 3$

Define $\varphi : \mathbb{Z} \to \mathbb{Z}_5$ where $\varphi(a) = a \pmod 5$ for all $a \in \mathbb{Z}$.

- $\varphi(26 +_{\mathbb{Z}} 17) = \varphi(43) = 43 \pmod 5 = 3 \pmod 5$.
- $\varphi(26) +_{\mathbb{Z}_5} \varphi(17) = 26 \pmod 5 + 17 \pmod 5 = 1 \pmod 5 + 2 \pmod 5 = 3 \pmod 5$.

$$\Longrightarrow \varphi(26 +_{\mathbb{Z}} 17) \quad = \quad \varphi(26) +_{\mathbb{Z}_5} \varphi(17)$$

add, then reduce. | reduce each, then add.

$\Longrightarrow \varphi$ is a homomorphism.

Key: Homomorphisms provide a *unifying language* to describe familiar algebraic properties.

$$g^{a+b} = g^a * g^b \quad \Longrightarrow \quad \theta(a+b) = \theta(a) * \theta(b)$$

$$a + b \pmod 5 = a\ (5) + b\ (5) \quad \Longrightarrow \quad \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$6(a+b) = 6a + 6b \quad \Longrightarrow \quad \gamma(a+b) = \gamma(a) + \gamma(b)$$

$$(ab)^3 = a^3 b^3 \quad \Longrightarrow \quad \lambda(a * b) = \lambda(a) * \lambda(b)$$

$$\det(\alpha\beta) = \det\alpha \cdot \det\beta \quad \Longrightarrow \quad \delta(\alpha * \beta) = \delta(\alpha) * \delta(\beta)$$

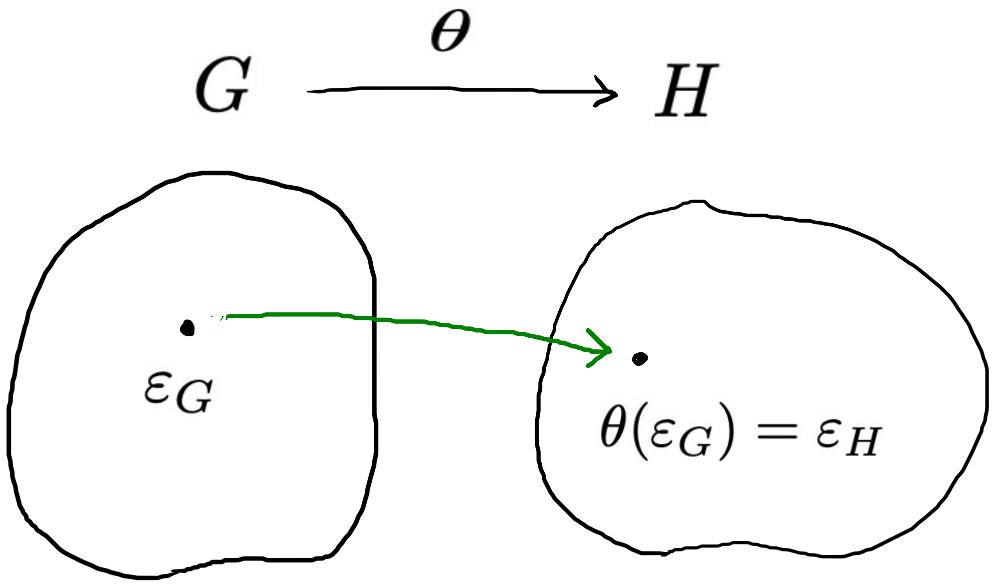
Theorem. Let $\theta : G \to H$ be a group homomorphism.

Then θ maps the identity of G to the identity of H, i.e., $\theta(\varepsilon_G) = \varepsilon_H$.

(See Chapter 17 reading for the proof.)

Problem #5: We have...

- $\varphi : \mathbb{Z} \to \mathbb{Z}_5$ with $\varphi(0) = 0 \pmod 5$.
- $\gamma : \mathbb{Z}_{12} \to \mathbb{Z}_{18}$ with $\gamma(0) = 0$.
- $\lambda : U_{13} \to U_{13}$ with $\lambda(1) = 1$.
- $\delta : G(\mathbb{Z}_{10}) \to U_{10}$ with $\delta(\varepsilon) = 1$.



Problem #7: We have $\alpha = \left[\begin{smallmatrix} 2 & 1 \\ 5 & 4 \end{smallmatrix}\right]$ and $\alpha^{-1} = \left[\begin{smallmatrix} 8 & 3 \\ 5 & 4 \end{smallmatrix}\right]$. ($\beta$)

In $G(\mathbb{Z}_{10})$		In U_{10}
$\alpha \cdot \alpha^{-1} = \varepsilon$	$\Longrightarrow$	$\delta(\alpha \cdot \alpha^{-1}) = \delta(\varepsilon)$
	$\Longrightarrow$	$\delta(\alpha) \cdot \delta(\alpha^{-1}) = 1$
	$\Longrightarrow$	$\delta(\alpha^{-1})$ is the inverse of $\delta(\alpha)$
	$\Longrightarrow$	$\delta(\alpha^{-1}) = \delta(\alpha)^{-1}$ ← "inverse of"

Theorem: Let $\theta : G \to H$ be a group homomorphism.
Then $\theta(g^{-1}) = \theta(g)^{-1}$ for all $g \in G$.

Proof: Let $g \in G$. Then $g *_G g^{-1} = \varepsilon_G$.

Applying θ to both sides, $\theta(g *_G g^{-1}) = \theta(\varepsilon_G)$.

Since θ is operation preserving, $\theta(g *_G g^{-1}) = \theta(g) *_H \theta(g^{-1})$.

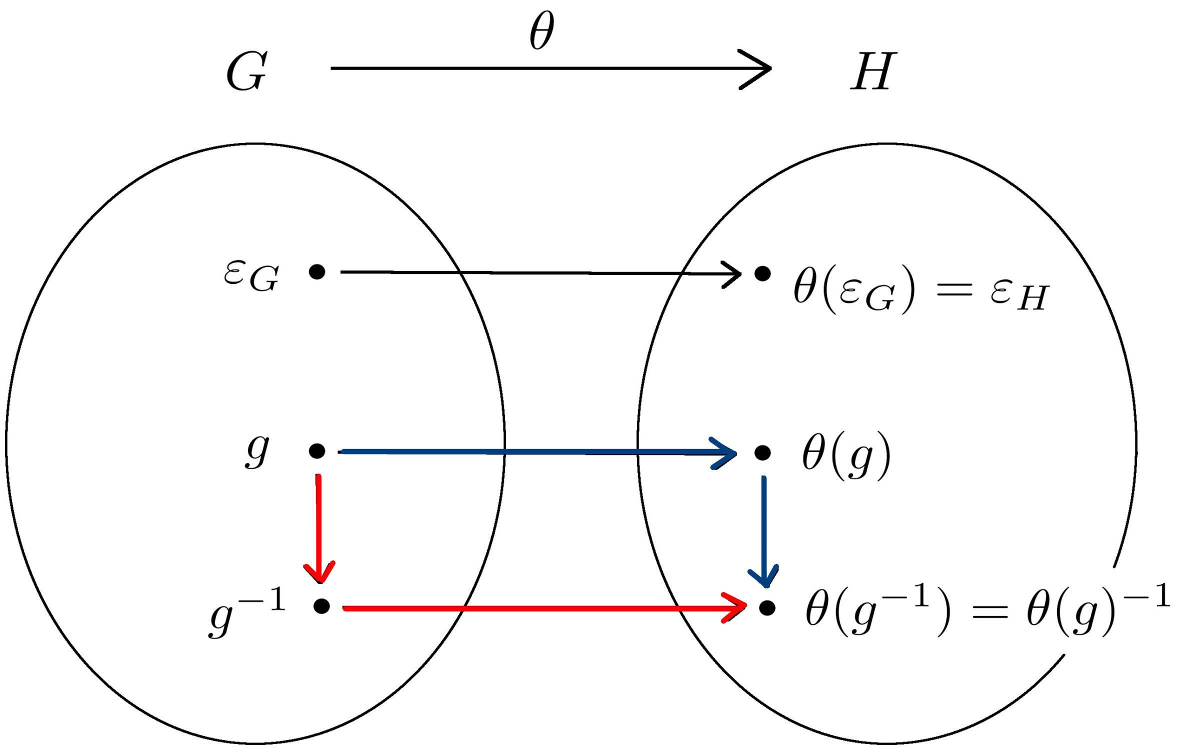
Since θ preserves the identity, $\theta(\varepsilon_G) = \varepsilon_H$.

Thus, we have $\theta(g) *_H \theta(g^{-1}) = \varepsilon_H$.

Hence, $\theta(g^{-1})$ is the inverse of $\theta(g)$ in H.

In other words, $\theta(g^{-1}) = \theta(g)^{-1}$. ← "inverse of"

Summary: Let $\theta : G \to H$ be a group homomorphism.



Note that $\theta(g^{-1}) = \theta(g)^{-1}$ means it doesn't matter whether we...

- first invert in G, then apply θ or
- first apply θ, then invert in H.