Let g be a group element with $\operatorname{ord}(g) = 6$. Consider the cyclic group

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$

ε

$$= \{\ldots, g^{-4}, g^{-3}, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, g^4, \ldots\}$$

Discuss in your group:

(a) Find the smallest positive integer k such that $g^{45} = g^k$. $(k = 3)$

(b) Same as above, but with: $g^{-2} = g^k$. $(k = 4)$

ε

(c) Find the *distinct* elements of $\langle g \rangle$. $\{g^0, g^1, g^2, g^3, g^4, g^5\}$

With $\text{ord}(g) = 6$, consider the cyclic group $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

For the groups $\mathbb{Z}_6$ and $\langle g \rangle$, we've seen that:

1. The elements in $\mathbb{Z}_6$ and $\langle g \rangle$ "match up."

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \quad \text{and} \quad \langle g \rangle = \{g^0, g^1, g^2, g^3, g^4, g^5\}.$$

ε

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

In $\mathbb{Z}_6$: $3 + 5 = 2$ In $\langle g \rangle$: $g^3 \cdot g^5 = g^2$

Conclusion: The groups $\mathbb{Z}_6$ and $\langle g \rangle$ are *isomorphic*.

(In other words, they're essentially the same group.)

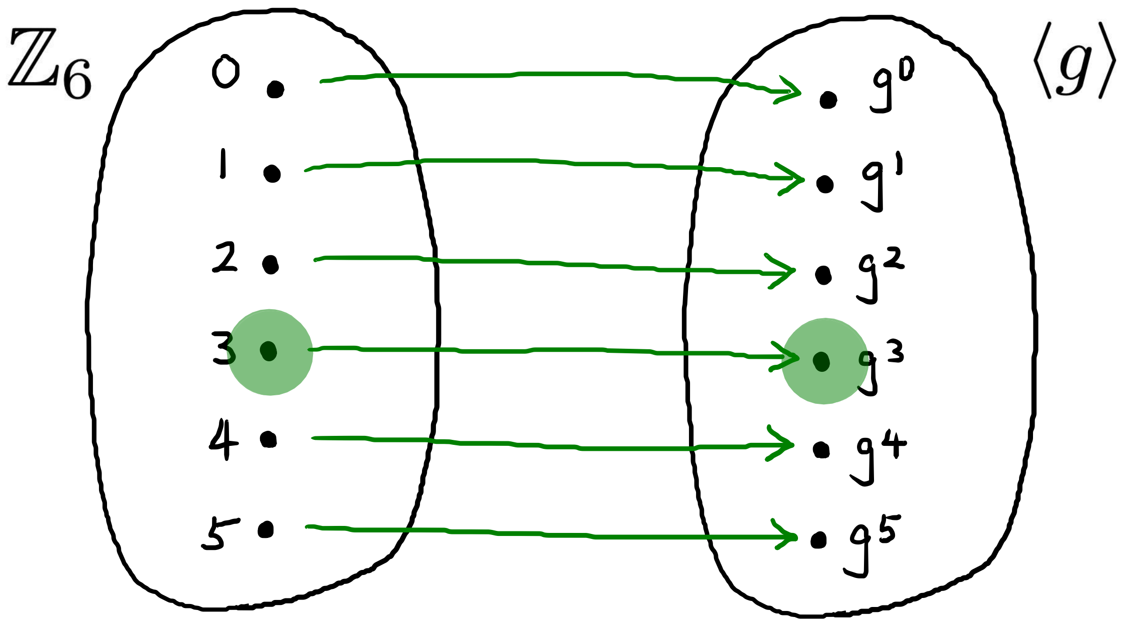
Consider the function $\theta : \mathbb{Z}_6 \to \langle g \rangle$ where $\theta(a) = g^a$ for all $a \in \mathbb{Z}_6$.

$\theta(3) = g^3$

Note: We still have $\mathrm{ord}(g) = 6$.

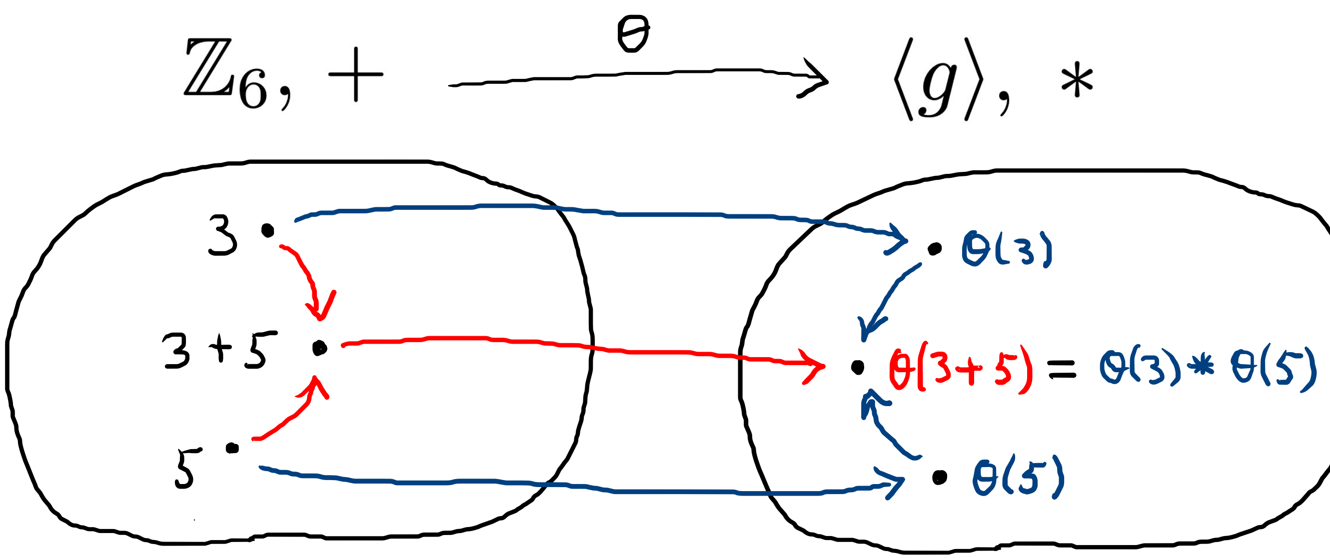
1. ~~The elements in $\mathbb{Z}_6$ and $\langle g \rangle$ "match up."~~

1. θ is a bijection (i.e., one-to-one and onto).



Note: θ specifies *how* these elements "match up."

~~2. The operations of $\mathbb{Z}_6$ and $\langle g \rangle$ also "match up."~~



Given $3,\ 5 \in \mathbb{Z}_6$, we can...

- Add them first in $\mathbb{Z}_6$, then apply θ to the sum: $\theta(3+5)$ or g^{3+5}
- Apply θ to each, then multiply in $\langle g \rangle$: $\theta(3) * \theta(5)$ or $g^3 * g^5$

Since $g^{3+5} = g^3 * g^5$, we have: $\theta(3+5) = \theta(3) * \theta(5)$

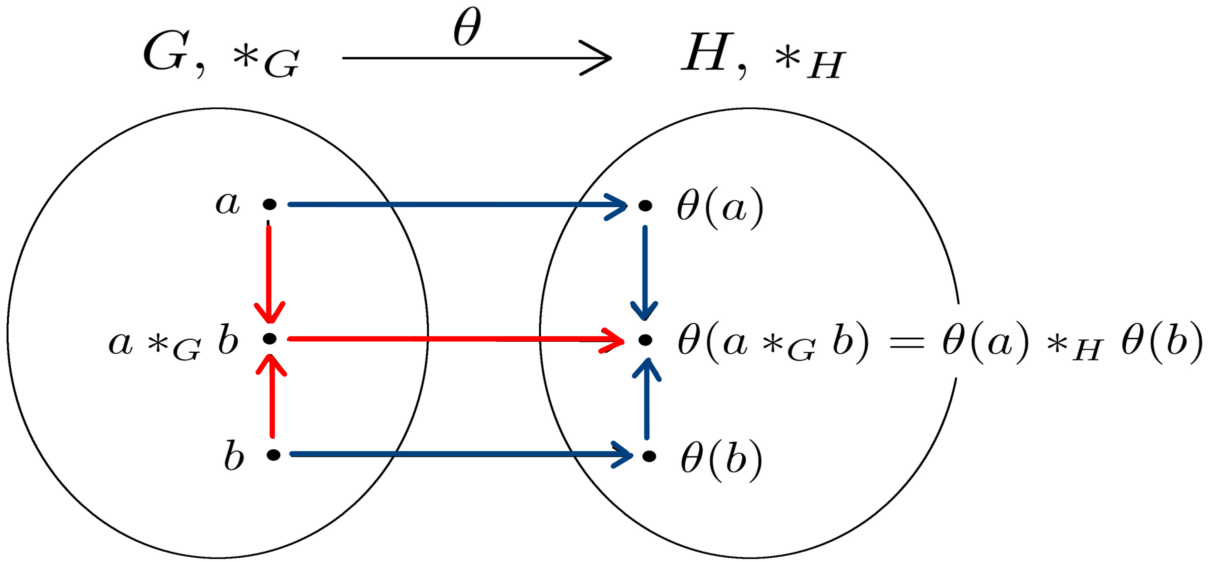
Definition. Let G and H be groups w/ operations $*_G$ and $*_H$.
A function $\theta : G \to H$ is an isomorphism if...

1. θ is a bijection (i.e., one-to-one and onto), and

2. θ is *operation preserving*, i.e.,

$$\theta(a *_G b) = \theta(a) *_H \theta(b)$$

for all $a, b \in G$.



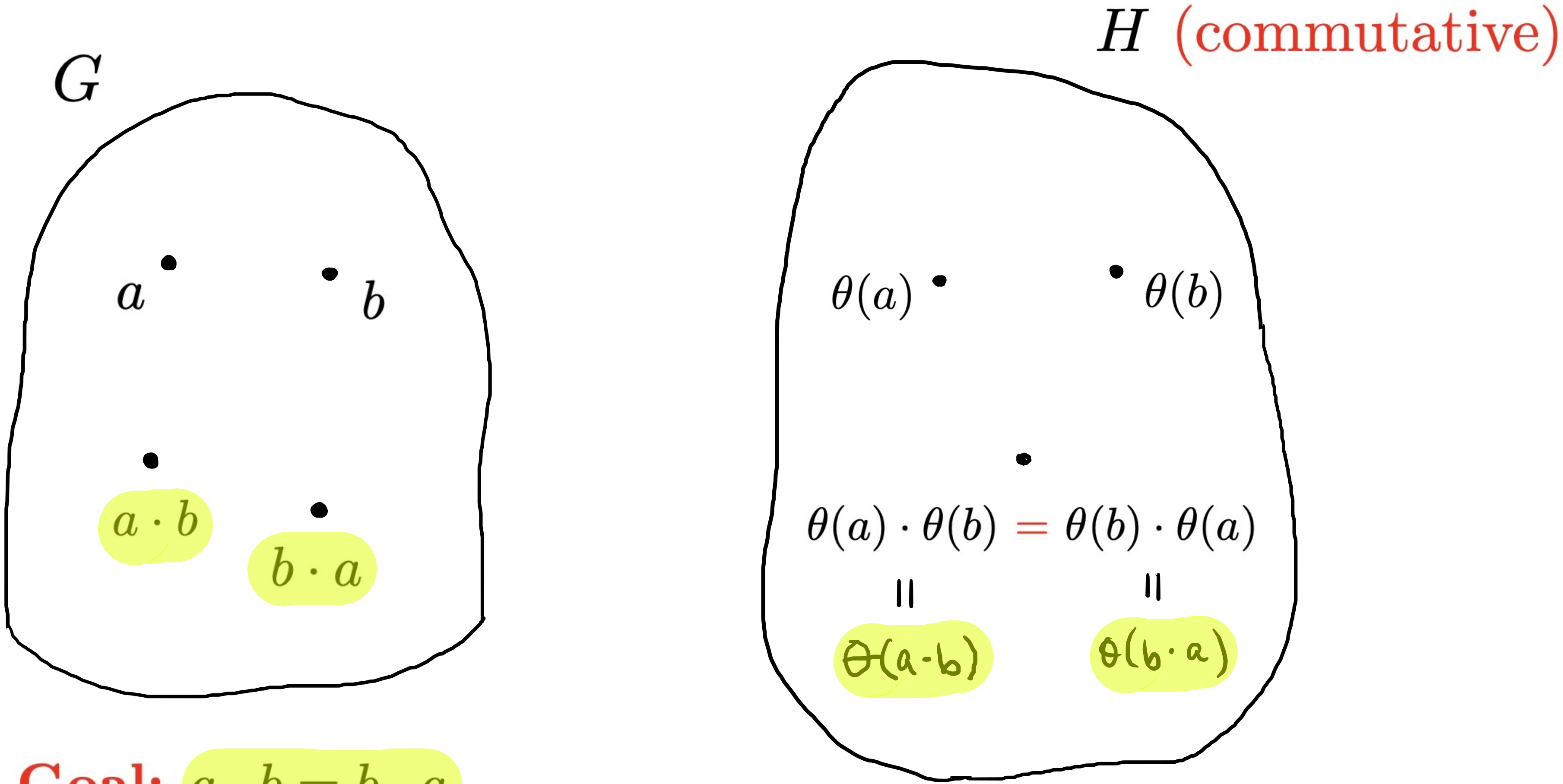
And we say that G is isomorphic to H and write $G \cong H$.

Key: $G \cong H$ means they're essentially the same group.

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

If H is commutative, then G is commutative.

Picture:



Goal: $a \cdot b = b \cdot a$

Theorem. Let $\theta : G \to H$ be a group isomorphism.
If H is commutative, then G is commutative.

Proof: Assume H is commutative. We must show that G is commutative.

Let $a, b \in G$.

We have $\theta(a *_G b) = \theta(a) *_H \theta(b)$, since θ is operation preserving.

Similarly, $\theta(b *_G a) = \theta(b) *_H \theta(a)$.

Since H is commutative, $\theta(a) *_H \theta(b) = \theta(b) *_H \theta(a)$.

Therefore, $\theta(a *_G b) = \theta(b *_G a)$.

Thus, since θ is one-to-one, $a *_G b = b *_G a$.