Warm-Up: Let G, H, K be groups.
Prove

1. If $\varphi: G \to H$ and $\psi: H \to K$ are isomorphisms, then
$$\psi \circ \varphi: G \to K$$
are isomorphisms.

2. If $\varphi: G \to H$ is an isomorphism, then
$$\varphi^{-1}: H \to G$$
is an isomorphism.

Note: Only need to prove they are homomorphisms.

Remark: The above properties show that $\cong$ is an equivalence relation on groups.

They also show that the **automorphisms** of a group G, "self isomorphisms"

$$\mathrm{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ is an isomorphism}\}$$

is a group under $\circ$.

Ex: $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$.

Idea: Any isomorphism $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ is determined by $\varphi(1)$, so the range is $\langle \varphi(1) \rangle$.

Thus, $\varphi(1)$ must be relatively prime to n, i.e., $\varphi(1) \in U(n)$.

Classification of finite groups - some history

1854 - Def. of abstract groups (Cayley)

1870s-80s - <u>Simple groups</u> identified as basic "building blocks" (Jordan-Hölder)

2008 - Finite simple groups completely classified

n	# of groups of order n, up to $\cong$
1	1
2	1
3	1
4	2 - $\mathbb{Z}_4$ and V_4
5	1
6	2 - $\mathbb{Z}_6$ and S_3
7	1
8	5 - $\mathbb{Z}_8$, two other abelian groups, D_4, and Q_8
9	2
10	2
$\vdots$	
15	1 - first non-prime for which $\mathbb{Z}_n$ is only iso. class
16	14
17	1
$\vdots$	
62	2
63	4
64	267 !
65	1
$\vdots$	

Lemma: Let $\varphi : G \to H$ be a group homomorphism. Then

① $\varphi(e_G) = e_H$, where e_G is the identity of G and e_H is the identity of H.

② For all $g \in G$, $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

③ For all $g \in G$ and $n \in \mathbb{Z}$,

$$\varphi(g^n) = (\varphi(g))^n.$$

④ If $K \leq G$ is a subgroup of G, then $\varphi(K) = \{\varphi(k) \mid k \in K\}$ is a subgroup of H.

In particular, the range $\varphi(G) \leq H$.

Proof: ① Since $e_G = e_G \cdot e_G$, we have

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G).$$

By cancellation, $\varphi(e_G) = e_H$.

② Since $gg^{-1} = e_G = g^{-1}g$, we have

$$\varphi(gg^{-1}) = \varphi(e_G) = \varphi(g^{-1}g),$$

so

$$\varphi(g)\varphi(g^{-1}) = e_H = \varphi(g^{-1})\varphi(g).$$

By uniqueness of inverses, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

③ For $n=0$, this is ①.
For $n \geq 1$, use induction.
For $n \leq -1$, use induction (② is base case).

④ Since $e_G \in K$, $\varphi(e_G) = e_H \in \varphi(K)$.

For $k_1, k_2 \in K$, we have $k_1 k_2^{-1} \in K$, so

$$\varphi(k_1 k_2^{-1}) = \varphi(k_1)\varphi(k_2^{-1})$$
$$= \varphi(k_1)\varphi(k_2)^{-1} \in \varphi(K).$$

So $\varphi(K) \leq H$ by the subgroup criterion.

$\blacksquare$

<u>Cor</u>: If $\varphi: G \to H$ is an injective group homomorphism, then $G \cong \varphi(G)$.