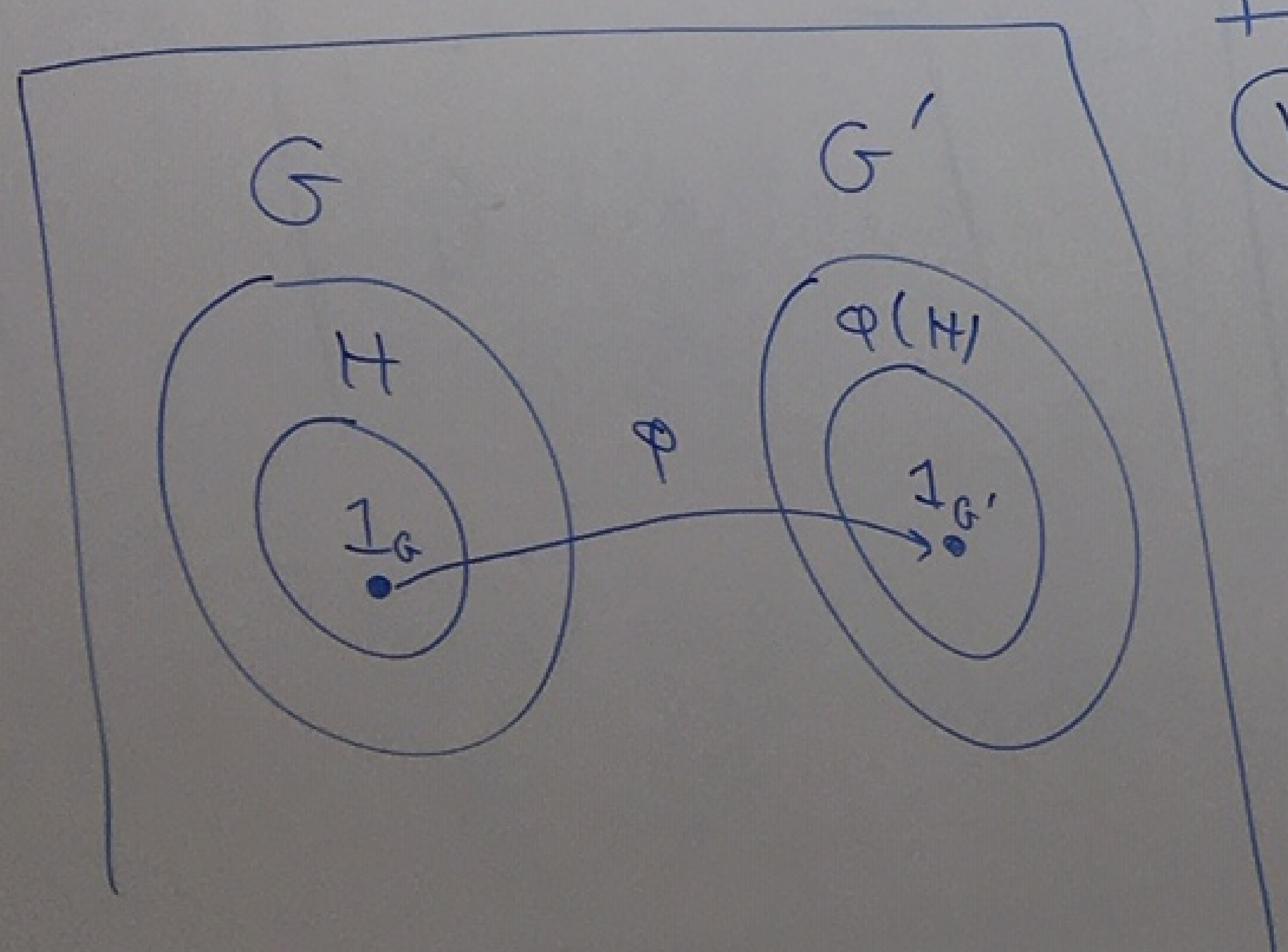
From lecture but never proved.

Lemma: Let $\varphi : G \to G'$ be a homomorphism. Let $H \leq G$. Then $\varphi(H) \leq G'$.

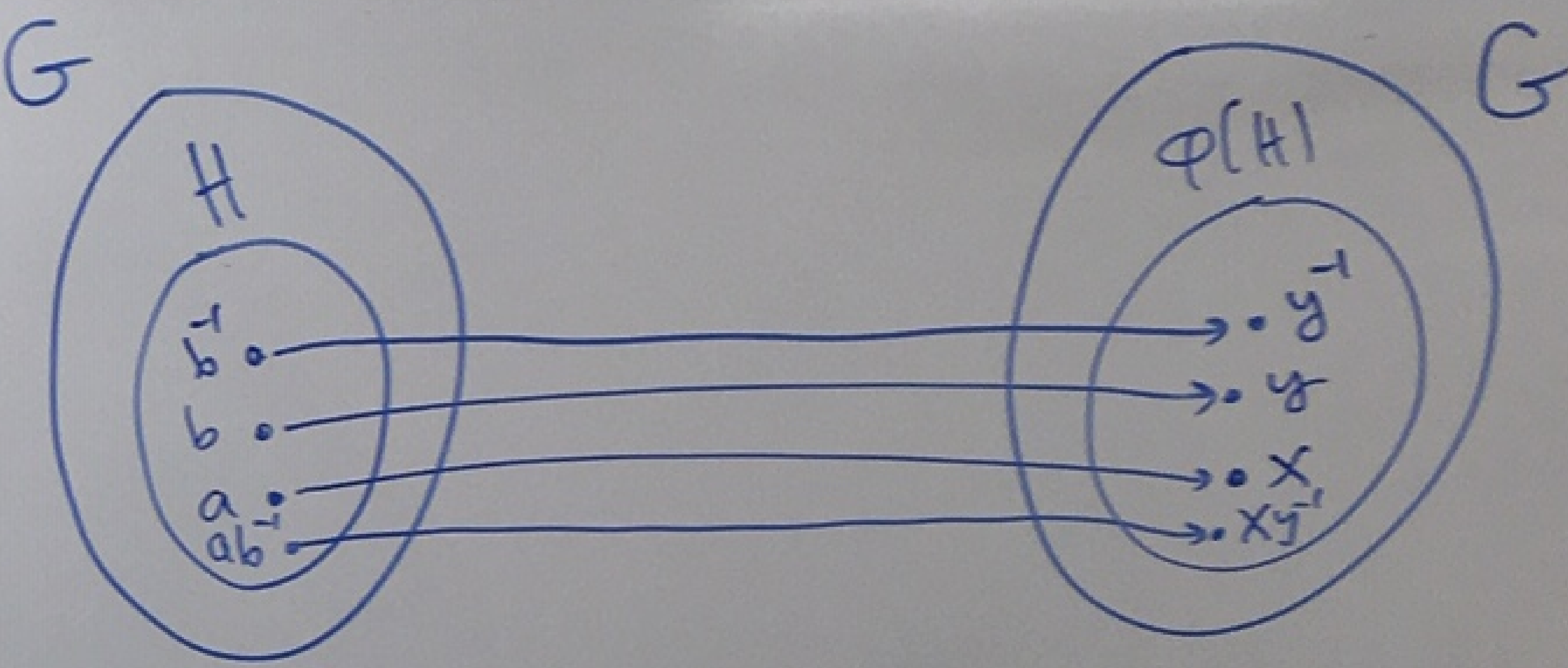
proof:



① Let 1_G and $1_{G'}$ be the identities of G and G'.

Since $H \leq G$ we have $1_G \in H$.

Then, $1_{G'} = \varphi(\underbrace{1_G}_{\text{in } H}) \in \varphi(H)$.



② Pick $x, y \in \varphi(H)$.

There exist $a, b \in H$ with

$\varphi(a) = x$ and $\varphi(b) = y$.

Since $H \leq G$, we have $b^{-1} \in H$.

Since φ is a homomorphism, $\varphi(b^{-1}) = (\varphi(b))^{-1} = y^{-1}$.

Since $H \leq G$, $ab^{-1} \in H$.

So, $xy^{-1} = \varphi(a)\varphi(b^{-1})$

$= \varphi(\underbrace{ab^{-1}}_{\text{in } H}) \in \varphi(H)$.

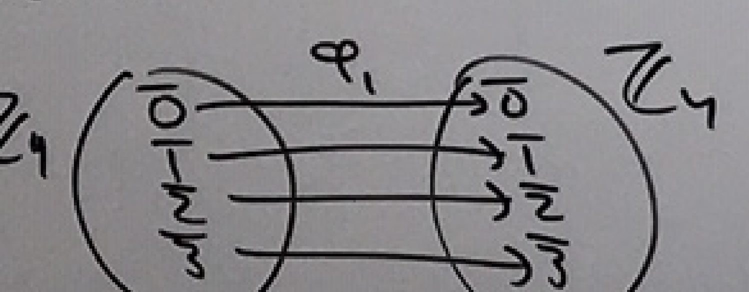
By ① and ②, $\varphi(H) \leq G'$. ☺

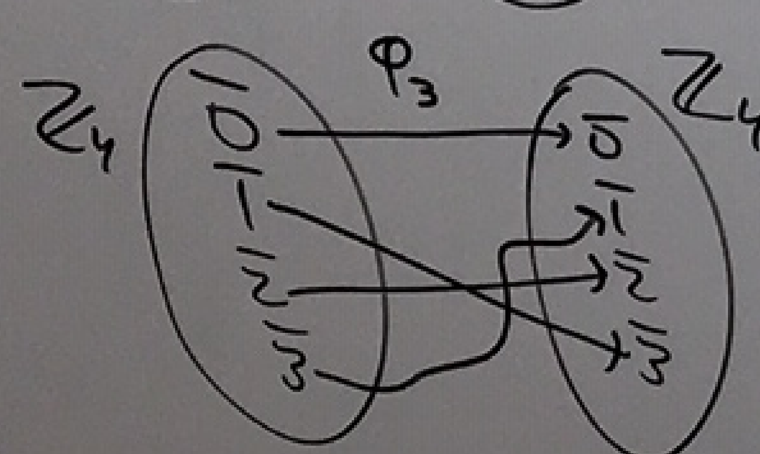
Ex:

$\mathrm{Aut}(\mathbb{Z}_4) = \{\varphi_1, \varphi_3\}$

$\varphi_1(\overline{x}) = \overline{x}$

$\varphi_3(\overline{x}) = \overline{3x}$





Theorem: Let G be a cyclic group of size n.
For each $a \in \mathbb{Z}$, define $\varphi_a : G \to G$ where $\varphi(x) = x^a$.
Then, $\mathrm{Aut}(G) = \left\{ \varphi_a \;\middle|\; \begin{array}{l} 1 \le a \le n \\ \gcd(a,n) = 1 \end{array} \right\}$.

Proof: Let $S = \left\{ \varphi_a \;\middle|\; \begin{array}{l} 1 \le a \le n \\ \gcd(a,n) = 1 \end{array} \right\}$

We will prove that $\mathrm{Aut}(G) = S$.

① $S \subseteq \mathrm{Aut}(G)$

Let $\varphi_a \in S$ where $1 \le a \le n$ and $\gcd(a,n) = 1$.

Fact: Let $f : X \to Y$ where X and Y are finite of the same size. Then f is 1-1 iff f is onto.

φ

Th

1-

Si

im

S

Then,

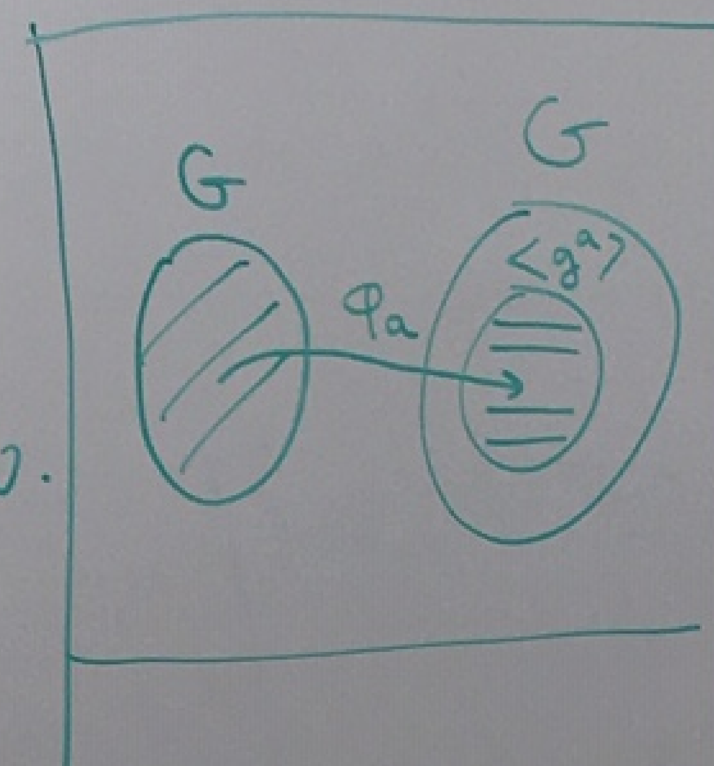
of the same size

φ_a is a homomorphism : Let $x, y \in G$.

Then, $\varphi_a(xy) = (xy)^a = \underbrace{(xy)(xy)\cdots(xy)}_{a \text{ times}} = xx\cdots x\,yy\cdots y =$

$= x^a y^a = \varphi_a(x)\varphi_a(y)$

↑ G is abelian



1-1 and onto : Let's show φ_a is onto.

Since $\varphi_a : G \to G$ and G is finite, this will imply φ_a is 1-1.

Since G is cyclic, $G = \langle g \rangle$ where $g \in G$.

Then, $\varphi_a(G) = \varphi_a(\langle g \rangle) = \{\varphi_a(g^k) \mid k \in \mathbb{Z}\} = \{(g^k)^a \mid k \in \mathbb{Z}\}$

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

What's the order of g^a ?

$$|g^a| = \frac{|g|}{\gcd(|g|, a)} = \frac{n}{\gcd(n, a)} = \frac{n}{1} = n.$$

So, g^a generates G.

Thus, $\varphi_a(G) = \langle g^a \rangle = G$.

Ergo, φ_a is onto.

② $\underline{\mathrm{Aut}(G) \subseteq S}$

Let $\varphi \in \mathrm{Aut}(G)$.

So $\varphi : G \to G$ is an isomorphism.

Since G is cyclic, $G = \langle g \rangle$ for some $g \in G$.

Since $\varphi(g) \in G = \{\underset{\boxed{g^n}}{1}, g, g^2, \dots, g^{n-1}\}$ we know $\varphi(g) = g^a$ where $1 \leq a \leq n$.

Let $x \in G$.

Then $x = g^k$ where $k \in \mathbb{Z}$.

So, $\varphi(x) = \varphi(g^k) = \varphi(g)^k = (g^a)^k = (g^k)^a = x^a = \varphi_a(x)$.

That is, $\varphi = \varphi_a$.

n.

Since φ is an isomorphism, φ is onto.

So, $\varphi(G) = G$.

Thus,

$$G = \varphi(G) = \varphi(\langle g \rangle) = \{\varphi(g^k) \mid k \in \mathbb{Z}\}$$
$$= \{(g^k)^a \mid k \in \mathbb{Z}\}$$
$$= \{(g^a)^k \mid k \in \mathbb{Z}\} = \langle g^a \rangle$$

So, g^a generates G.

Thus, $|g^a| = n$.

So, $n = |g^a| = \dfrac{|g|}{\gcd(|g|, a)} = \dfrac{n}{\gcd(n,a)}$.

Thus, $\gcd(n,a) = 1$.

Therefore,

$\varphi = \varphi_a$ with $1 \leq a \leq n$ and $\gcd(a,n) = 1$.

So, $\varphi \in S$. $\blacksquare$

Ex:

$\mathbb{Z}_6 = \{\cancel{\bar{0}}, \bar{1}, \cancel{\bar{2}}, \cancel{\bar{3}}, \cancel{\bar{4}}, \bar{5}\}$

$\gcd(1,6)=1$, $\gcd(2,6)=2$, $\gcd(4,6)=2$, $\gcd(5,6)=1$, $\gcd(3,6)=3$

$\mathbb{Z}_6^\times = \{\bar{1}, \bar{5}\}$

Theorem: Let G be a cyclic group of size n. Then $\operatorname{Aut}(G) \cong \mathbb{Z}_n^\times$.

proof: We know $\operatorname{Aut}(G) = \left\{ \varphi_a \;\middle|\; \begin{array}{l} 1 \le a \le n \\ \gcd(a,n)=1 \end{array} \right\}$ ← group operation is composition of functions

And $\mathbb{Z}_n^\times = \left\{ \bar{a} \;\middle|\; \begin{array}{l} 1 \le a \le n \\ \gcd(a,n)=1 \end{array} \right\}$ ← group under multiplication

Define $\Psi : \mathbb{Z}_n^\times \to \operatorname{Aut}(G)$ by $\Psi(\bar{a}) = \varphi_a$.

Ψ is well-defined:

Suppose $\bar{a}_1 = \bar{a}_2$ in $\mathbb{Z}_n^\times$. Goal: Show $\Psi(\bar{a}_1) = \Psi(\bar{a}_2)$.

Then $a_1 \equiv a_2 \pmod{n}$.

S

Th

(*

Ψ is

Ψ is

Let

Then,

group operation is composition of functions

So, $a_1 - a_2 = nk$ where $k \in \mathbb{Z}$.

Then, $\psi(\overline{a_1}) = \varphi_{a_1} \overset{(*)}{=} \varphi_{a_2} = \psi(\overline{a_2})$

(*) because given $x \in G$ we have

$$\varphi_{a_1}(x) = x^{a_1} = x^{nk+a_2} = (x^n)^k x^{a_2} = x^{a_2} = \varphi_{a_2}(x).$$

$x^n = x^{|G|} = 1$

ψ is 1-1 and onto by def.

ψ is homomorphism

Let $\overline{a_1}, \overline{a_2} \in \mathbb{Z}_n^\times$.

Then, $\psi(\overline{a_1} \cdot \overline{a_2}) = \psi(\overline{a_1 a_2}) = \varphi_{a_1 a_2} = \varphi_{a_1} \circ \varphi_{a_2} = \psi(a_1) \circ \psi(a_2)$ $\blacksquare$

$$\varphi_{a_1 a_2}(x) = x^{a_1 a_2} = (x^{a_2})^{a_1} = \varphi_{a_1}(x^{a_2}) = \varphi_{a_1}(\varphi_{a_2}(x)) = \varphi_{a_1} \circ \varphi_{a_2}(x)$$