10/24
Thursday

HW 3.2

#4 Suppose $|G| = pq$ where p and q are Primes (not necessarily distinct)
Then either $\underbrace{G \text{ is abelian}}_{Z(G) = G}$ or $Z(G) = \{1\}$.

proof: Since $Z(G) \leq G$ we know
by Lagrange, $|Z(G)|$ divides $|G|$.
So, $|Z(G)| = 1, p, q,$ or pq.
We will rule out $|Z(G)| = p$ or $|Z(G)| = q$ and we are done.

So
Th
So
By
Th
So
Sam
So e

es [not necessarily distinct]

.

Suppose $|Z(G)| = p$.

Then, $|G/Z(G)| = |G| / |Z(G)| = pq/p = q$.

So, $G/Z(G)$ is cyclic since q is prime. [$Z(G) \trianglelefteq G$ so $G/Z(G)$ is a group.]

By HW 3.1 #36, G is abelian.

This would imply $Z(G) = G$, which contradicts $|Z(G)| = p$.

So this case can't happen.

Same idea if $|Z(G)| = q$.

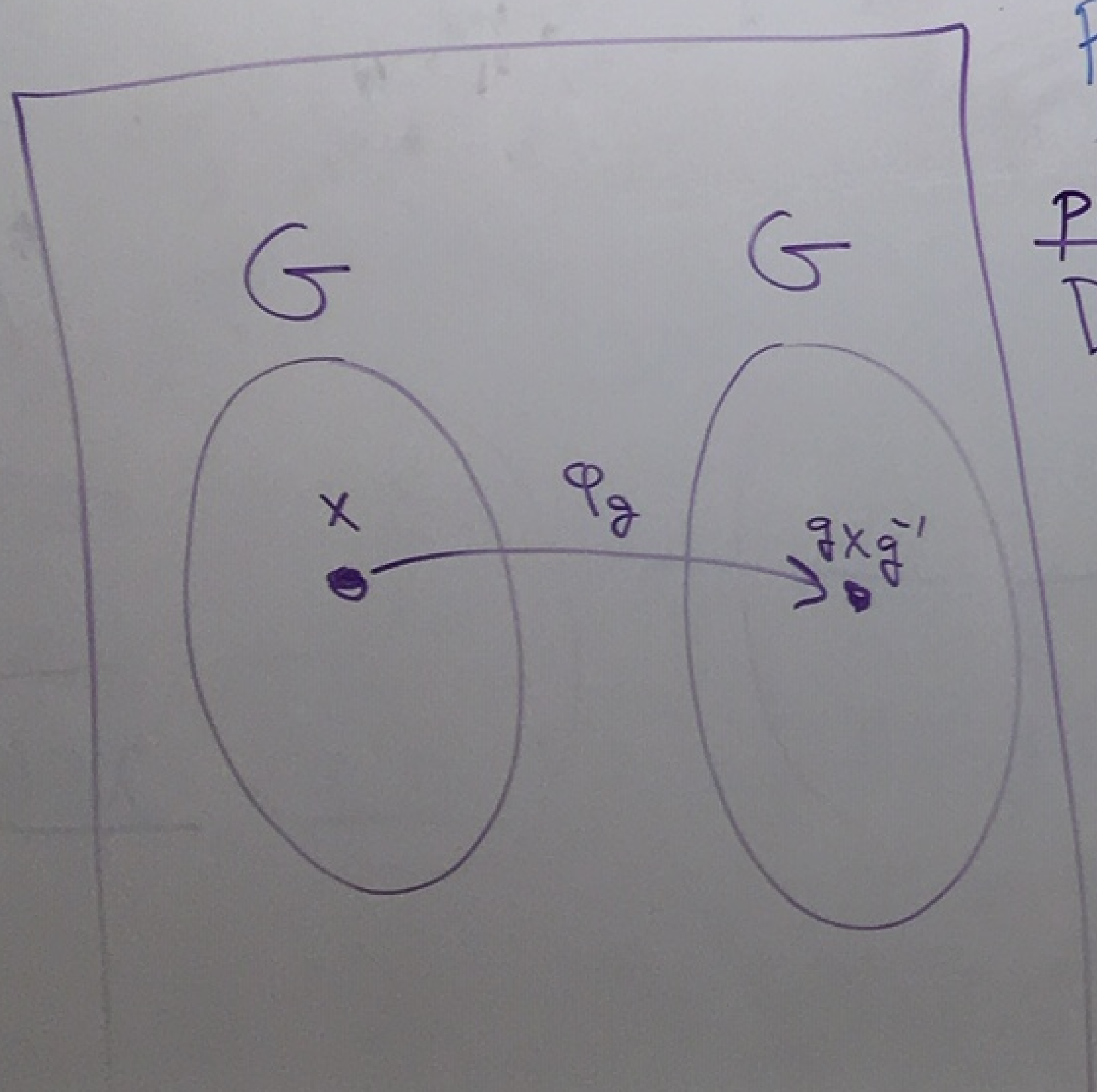
So either $|Z(G)| = 1$, or $|Z(G)| = pq$ which implies $G = Z(G)$ so G is abelian. ▥

and we are done.

3.2 Let G be a finite group.

5(a) Let $H \leq G$. Let $g \in G$.

Prove that $gHg^{-1} \leq G$ and $|gHg^{-1}| = |H|$.



proof: Let $H \leq G$ and $g \in G$.

Define $\varphi_g : G \to G$ by $\varphi_g(x) = gxg^{-1}$.

Step 1: φ_g is an isomorphism.

(i) Let $x, y \in G$. Then, $\varphi_g(x)\varphi_g(y) = (gxg^{-1})(gyg^{-1}) = gxyg^{-1} = \varphi_g(xy)$.

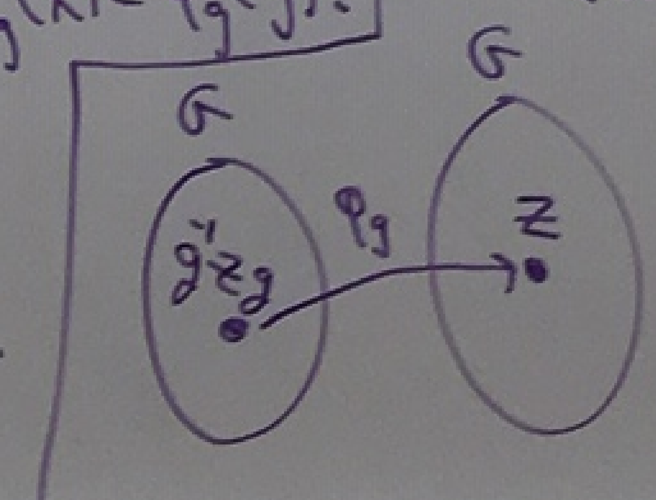
So, φ_g is a homomorphism.

(ii) Let $x, y \in G$ and suppose $\varphi_g(x) = \varphi_g(y)$.

Then, $gxg^{-1} = gyg^{-1}$.

So, $g^{-1}(gxg^{-1})g = g^{-1}(gyg^{-1})g$.

Thus, $x = y$. So, φ_g is 1-1.

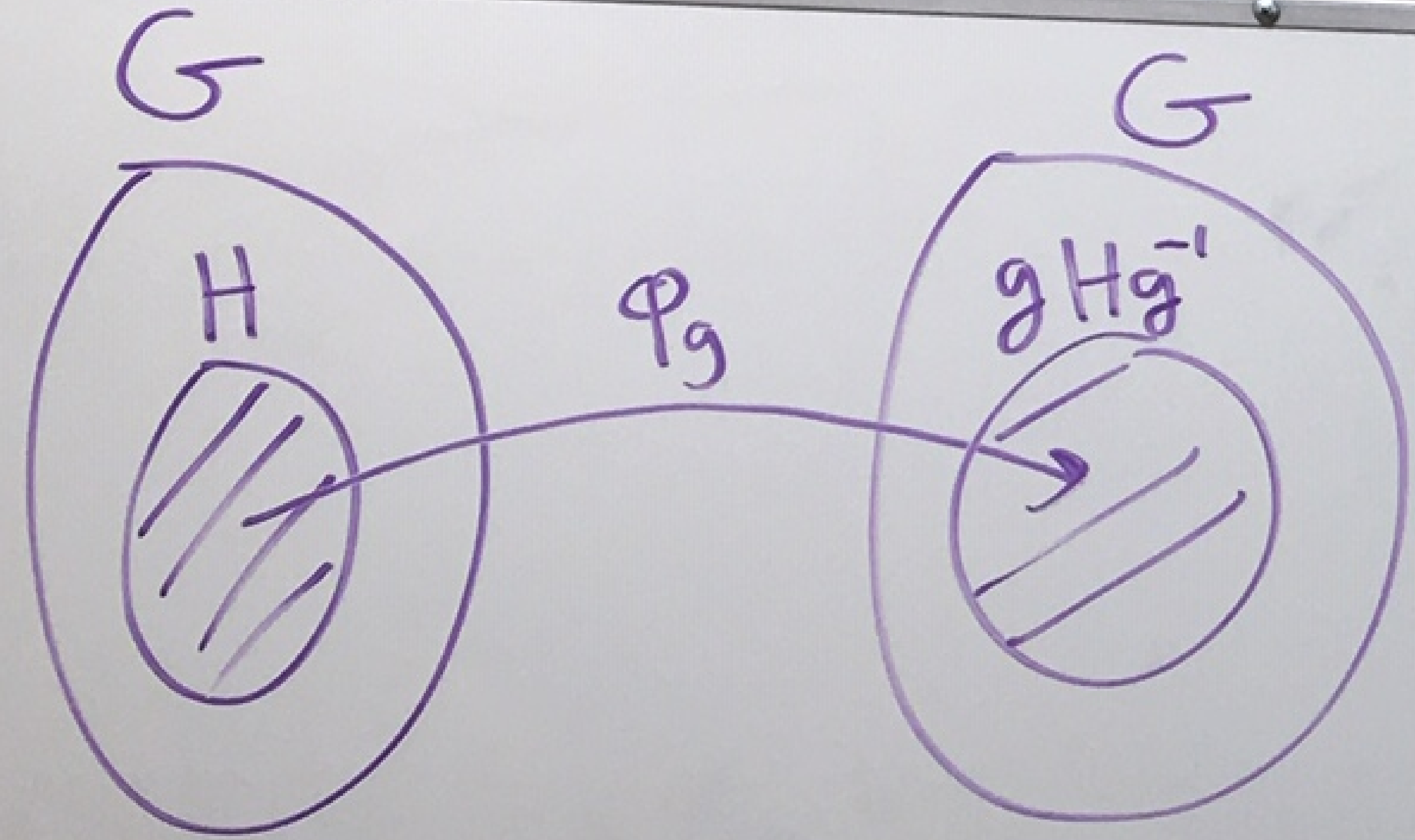


(iii) Let $z \in G$.

Then $g^{-1}zg \in G$ and

$\varphi_g(g^{-1}zg) = g(g^{-1}zg)g^{-1} = z$.

Thus, φ_g is onto. $\boxed{\text{Step 1}}$



Fact: Let $\varphi : G \to G'$ where G and G' are groups. Let φ be a homomorphism. If $H \leq G$, then $\varphi(H) \leq G'$.

Step 2:

Note that

$$\varphi_g(H) = \{\varphi_g(h) \mid h \in H\}$$
$$= \{ghg^{-1} \mid h \in H\}$$
$$= gHg^{-1}.$$

So by the fact above, $gHg^{-1} = \varphi(H) \leq G$.

Since φ_g is 1-1 and onto and $\varphi_g(H) = gHg^{-1}$ we must have that $|H| = |gHg^{-1}|$. $\blacksquare$

Two sets have the same size iff there exists a bijection between the two sets.

4.4 – Automorphisms

Def: Let G be a group.
An <u>automorphism</u> of G is an isomorphism $\varphi : G \to G$.
The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

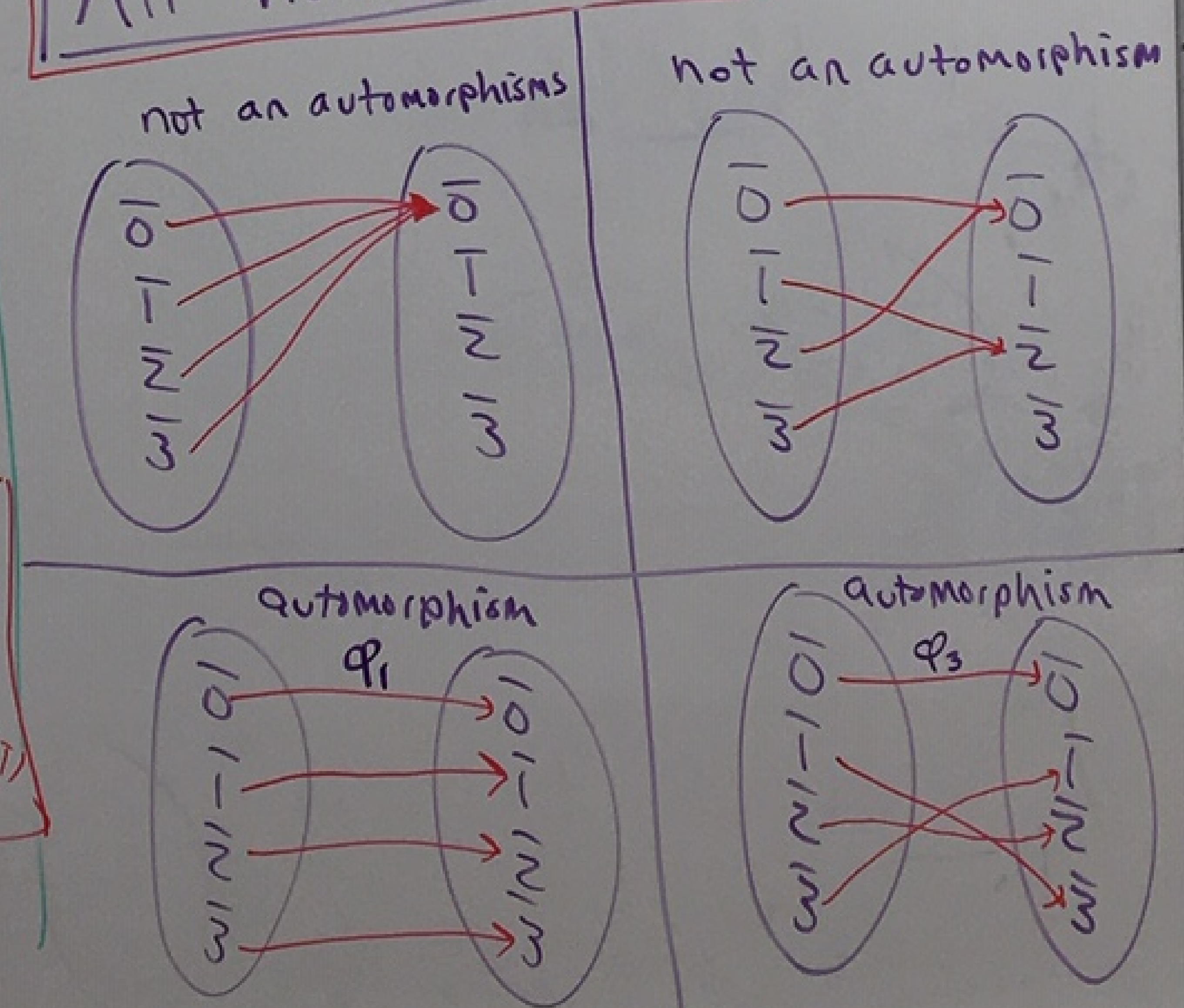
If $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4$ is a homomorphism then the generator $\bar{1}$ of $\mathbb{Z}_4$ must satisfy $|\varphi(\bar{1})|$ divides $|\bar{1}| = 4$.

$\varphi(\bar{2}) = \varphi(\bar{1}+\bar{1}) = \varphi(\bar{1}) + \varphi(\bar{1})$
$\varphi(\bar{3}) = \varphi(\bar{1}+\bar{1}+\bar{1}) = \varphi(\bar{1}) + \varphi(\bar{1}) + \varphi(\bar{1})$

Ex: Find all automorphisms of $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

orders: 1, 4, 2, 4

$\boxed{\text{All homomorphisms}}$



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

$\varphi_1(\bar{x}) = \bar{x}$
$\varphi_3(\bar{x}) = \overline{3x} = \bar{x} + \bar{x} + \bar{x}$

$\mathrm{Aut}(\mathbb{Z}_4)$ is a group under composition.

$\varphi_1 \circ \varphi_3 = \varphi_3$
$\varphi_3 \circ \varphi_3 = \varphi_1 \leftarrow (\varphi_3 \circ \varphi_3)(\bar{x}) = \varphi_3(\varphi_3($
$= \varphi_3(\overline{3x}) = \overline{9}$
$= \bar{x}$

his ms of $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

orders: $1 \quad 4 \quad 2 \quad 4$

phism

ism

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

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

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

$\mathrm{Aut}(\mathbb{Z}_4)$ is a group under composition.

$\varphi_1 \circ \varphi_3 = \varphi_3$

$\varphi_3 \circ \varphi_3 = \varphi_1 \leftarrow (\varphi_3 \circ \varphi_3)(\bar{x}) = \varphi_3(\varphi_3(\bar{x})) = \varphi_3(\overline{3x}) = \overline{9x} = \bar{x} = \varphi_1(\bar{x})$

$\mathrm{Aut}(\mathbb{Z}_4)$	φ_1	φ_3
φ_1	φ_1	φ_3
φ_3	φ_3	φ_1

$\boxed{\text{In general, if } G \text{ is a group then } \mathrm{Aut}(G) \text{ is a group under composition of functions.}}$

- identity is $i : G \to G$, $i(x) = x$ for all $x \in G$
- Given $\varphi \in \mathrm{Aut}(G)$, then φ^{-1} is the inverse function of φ.