Math 4550

Topic 5 - Cyclic groups

<u>Theorem:</u> Let G be a cyclic group. If $H \leq G$, then H is cyclic.

<u>proof:</u> Suppose $G = \langle x \rangle$ is cyclic.

Let $H \leq G$.

If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic.

Suppose $H \neq \{e\}$.

Then there must exist $a \in H$ with $a \neq e$.

Since $H \leq G$ we know $a \in G$.

Thus, $a = x^k$ for some $k \in \mathbb{Z}$, $k \neq 0$.

If $k < 0$, then $a^{-1} = x^{-k}$ is also in H since H is a subgroup.

We can conclude that H contains

some x^n where n is a positive integer.

Let m be the smallest positive integer where $x^m \in H$.

<u>Claim:</u> $H = \langle x^m \rangle$

We know $\langle x^m \rangle \subseteq H$ because $x^m \in H$ and H is a subgroup so $(x^m)^l \in H$ for any $l \in \mathbb{Z}$.

Let's show that $H \subseteq \langle x^m \rangle$.

Let $y \in H$.

Then $y = x^a$ for some $a \in \mathbb{Z}$ since $H \leq G$ and $G = \langle x \rangle$.

By the division algorithm $a = mq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$.

Then, $y = x^a = x^{mq} x^r$

So, $x^r = (x^{mq})^{-1} y = \underbrace{(x^m)^{-q}}_{\text{in } H \text{ since } x^m \in H} \underbrace{y}_{\text{in } H}$

Thus, $x^r \in H$.

Since $x^r \in H$ and $0 \le r < m$ and m is the smallest positive integer with $x^m \in H$ we must have that $r = 0$.

Thus, $y = x^a = x^{mq} x^r = (x^m)^q x^0$
$= (x^m)^q e$
$= (x^m)^q$

So, $y \in \langle x^m \rangle$.

Thus, $H \subseteq \langle x^m \rangle$.

So, $H = \langle x^m \rangle$ and H is cyclic. ∎

<u>Ex:</u> Find all subgroups of $\mathbb{Z}_{12}$.

Since $\mathbb{Z}_{12}$ is cyclic all its subgroups must be cyclic.

<u>Lemma:</u> If G is a group and $x \in G$, then $\langle x^{-1} \rangle = \langle x \rangle$.

<u>proof:</u> HW.

<u>all subgroups of $\mathbb{Z}_{12}$:</u>

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \mathbb{Z}_{12} = \langle \overline{11} \rangle$ ← $\boxed{\bar{1}^{-1} = \overline{11}}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\} = \langle \overline{10} \rangle$ ← $\boxed{\bar{2}^{-1} = \overline{10}}$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = \langle \bar{9} \rangle$ ← $\boxed{\bar{3}^{-1} = \bar{9}}$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\} = \langle \bar{8} \rangle$ ← $\boxed{\bar{4}^{-1} = \bar{8}}$

$\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \overline{10}, \bar{3}, \bar{8}, \bar{1}, \bar{6}, \overline{11}, \bar{4}, \bar{9}, \bar{2}, \bar{7}\}$

$= \mathbb{Z}_{12} = \langle \bar{7} \rangle \leftarrow \boxed{\bar{5}^{-1} = \bar{7}}$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$

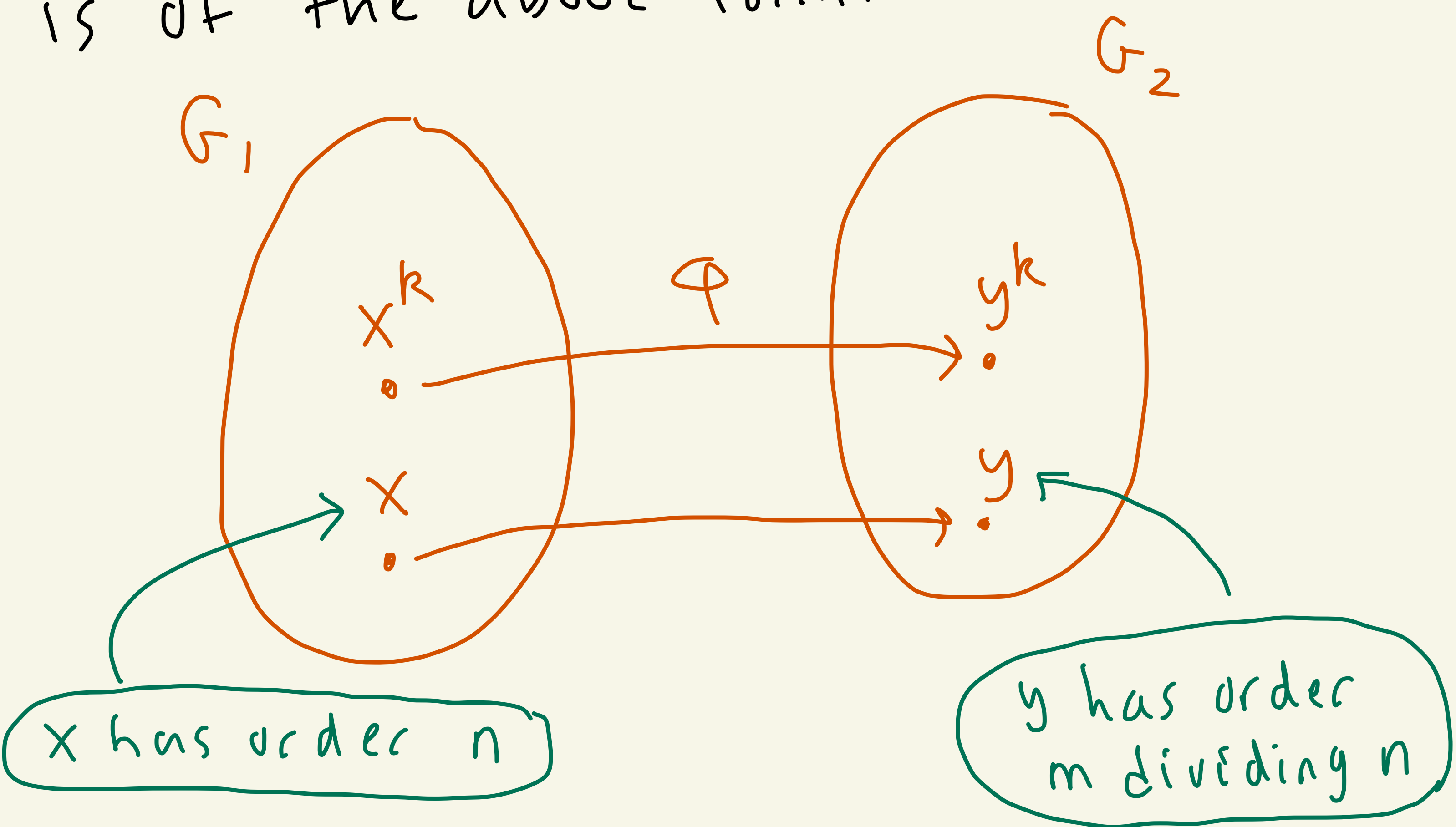
<u>subgroup diagram</u>

$$
\begin{tikzcd}
 & \mathbb{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & \\
\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\} \arrow[d, dash] & & \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \arrow[d, dash] \\
\{\bar{0}, \bar{4}, \bar{8}\} \arrow[dr, dash] & & \{\bar{0}, \bar{6}\} \arrow[dl, dash] \\
 & \{\bar{0}\} &
\end{tikzcd}
$$

<u>Theorem:</u> (Homomorphisms out of cyclic groups) Let $G_1 = \langle x \rangle$ be a cyclic group. Let G_2 be a group.

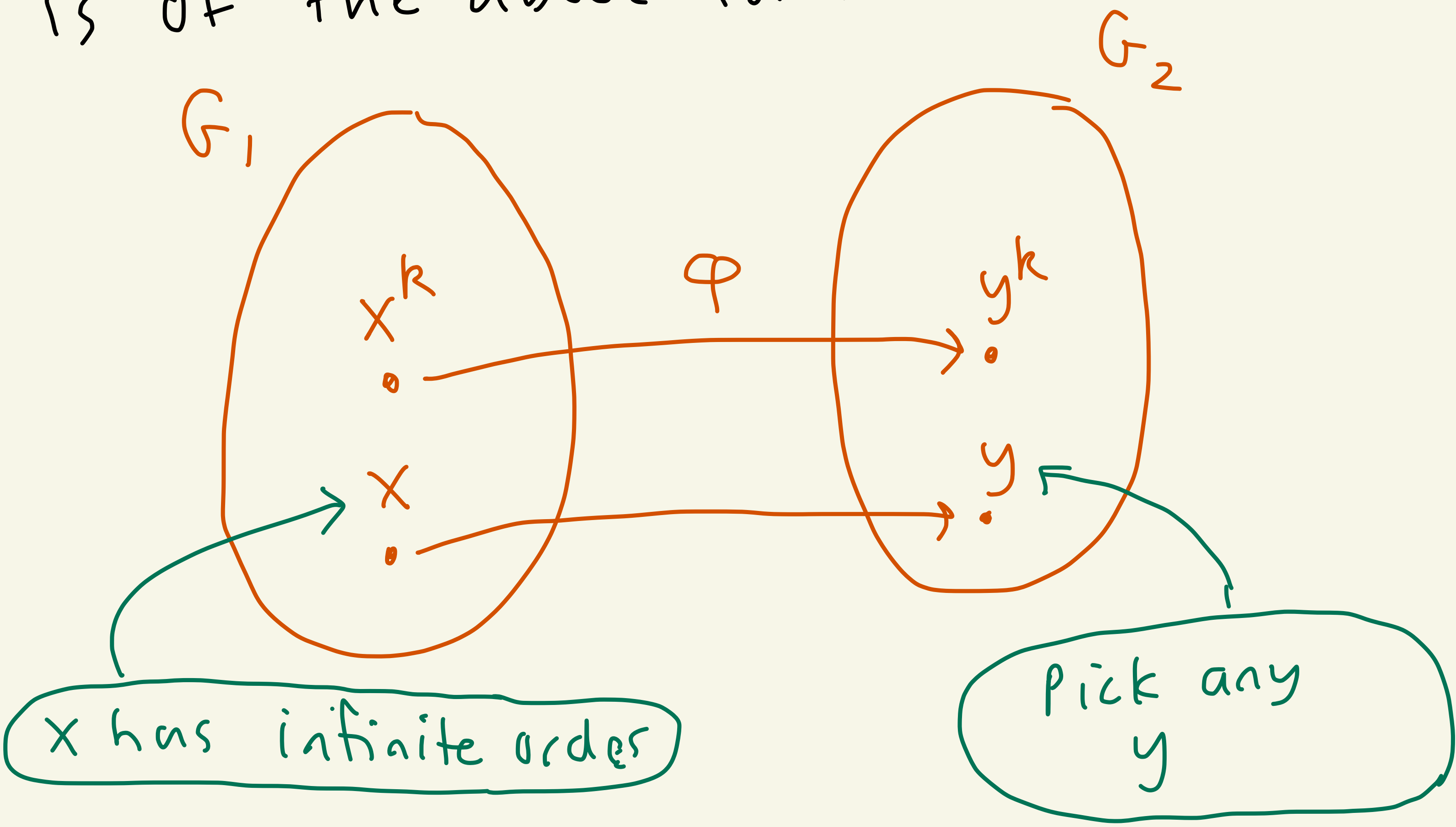
<u>Case 1: Suppose x has finite order n</u>

Pick $y \in G_2$ with order m dividing n. Then, $\varphi : G_1 \to G_2$ given by $\varphi(x^k) = y^k$ is a homomorphism. Furthermore, every homomorphism from G_1 to G_2 is of the above form.



Case 2: Suppose x has infinite order

Pick any $y \in G_2$.
Then $\varphi : G_1 \to G_2$ given by $\varphi(x^k) = y^k$ is a homomorphism. Furthermore, every homomorphism from G_1 to G_2 is of the above form.



---

proof: At end of these notes. $\blacksquare$

Ex: Let's find all homomorphisms

$\varphi : U_6 \to U_4$.

We have

$U_6 = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$ where $\rho = e^{\frac{2\pi}{6}i}$ has order 6.

and

$U_4 = \{1, \gamma, \gamma^2, \gamma^3\}$ where $\gamma = e^{\frac{2\pi}{4}i}$ has order 4.

elements of U_4	order
1	1
γ	4
γ^2	2
γ^3	4

To construct $\varphi : U_6 \to U_4$ first we pick a generator for U_6. We have

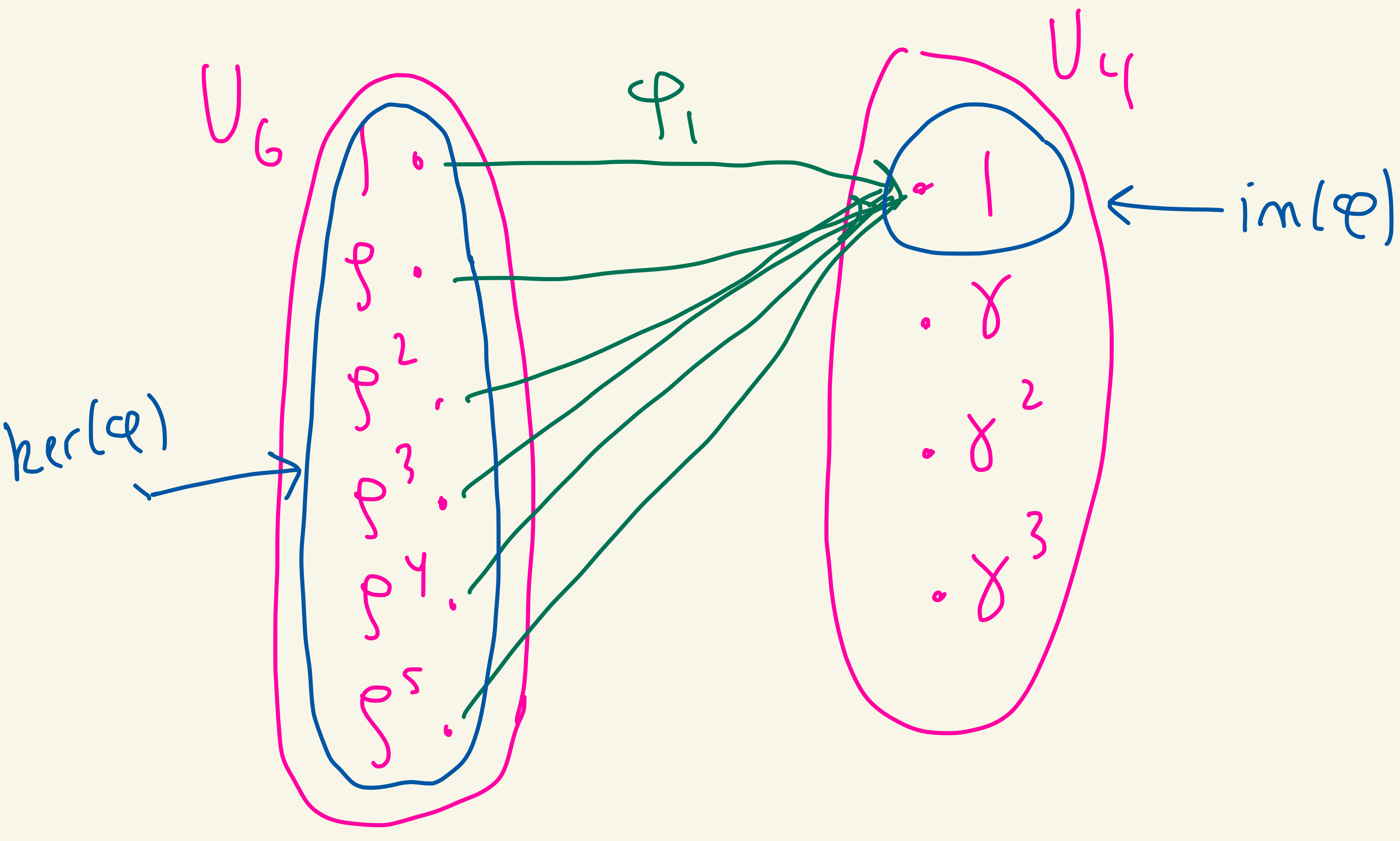
$U_6 = \langle \rho \rangle$ with ρ having order 6.

To build φ we pick an element of U_4 having order dividing 6.
We can pick 1 or γ^2.

<u>case 1: Pick 1 from U_4.</u>

Define $\varphi : U_6 \to U_4$ where $\varphi(\rho^k) = 1^k$

Thus, $\varphi(\rho^k) = 1$ for all k.



Here $\ker(\varphi_1) = U_6$ and $\text{im}(\varphi_1) = \{1\}$.

Case 2: Pick γ^2 from U_6.

Define $\varphi_2 : U_6 \to U_4$ where $\varphi_2(\rho^k) = (\gamma^2)^k$

So,

$$\varphi_2(1) = \varphi_2(\rho^0) = (\gamma^2)^0 = 1$$

$$\varphi_2(\rho) = (\gamma^2)^1 = \gamma^2$$

$$\varphi_2(\rho^2) = (\gamma^2)^2 = \gamma^4 = 1$$

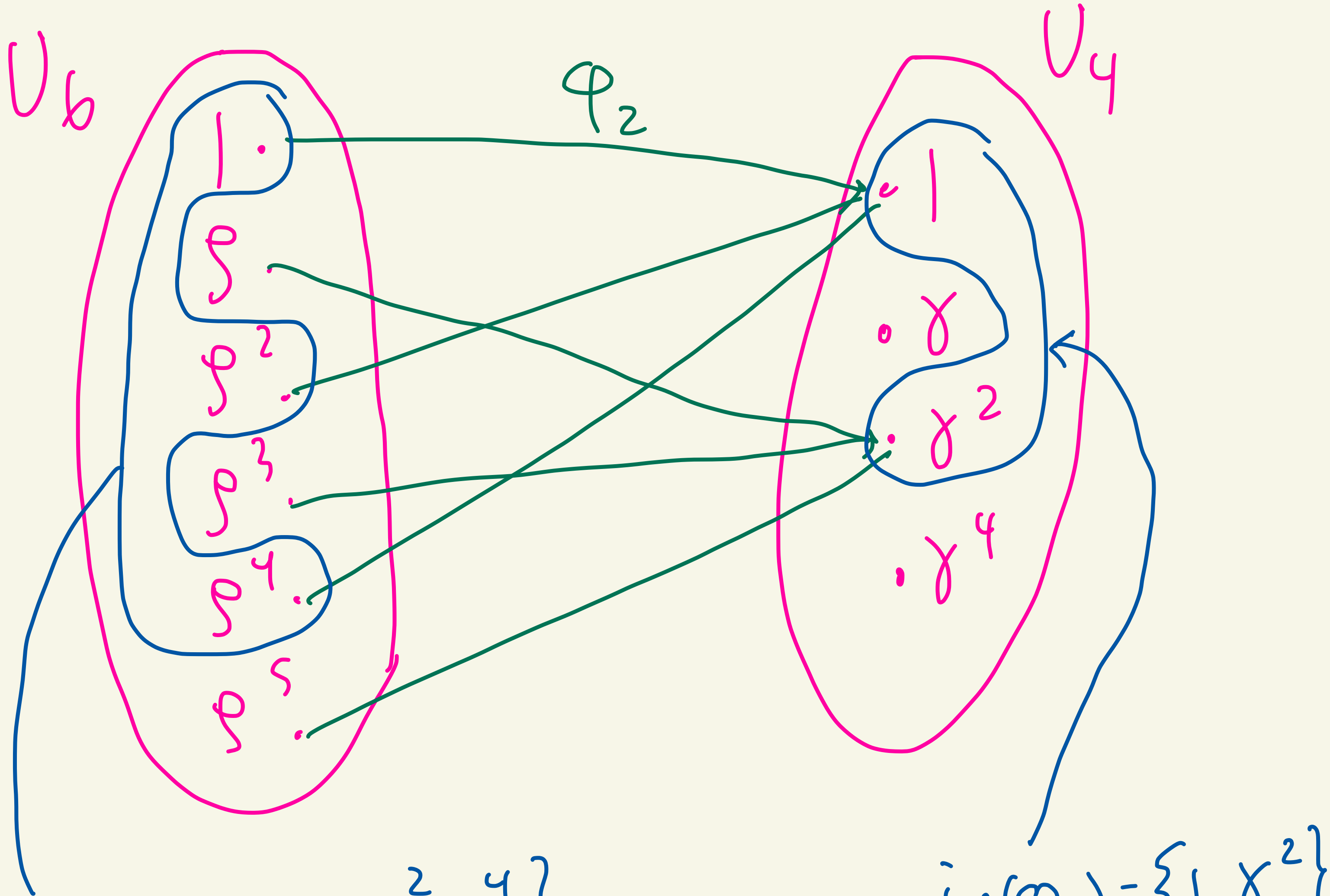
$$\varphi_2(\rho^3) = (\gamma^2)^3 = \gamma^6 = \gamma^4\gamma^2 = \gamma^2$$

$$\varphi_2(\rho^4) = (\gamma^2)^4 = \gamma^8 = \gamma^4\gamma^4 = 1$$

$$\varphi_2(\rho^5) = (\gamma^2)^5 = \gamma^{10} = \gamma^4\gamma^4\gamma^2 = \gamma^2$$

$\boxed{\text{Use } \gamma^4 = 1}$

Here is the picture



$\ker(\varphi_2) = \{1, \rho^2, \rho^4\}$

$\mathrm{im}(\varphi_2) = \{1, \gamma^2\}$

So, there are two homomorphisms from U_6 to U_4.

Let me discuss why the above is constructed this way.

Let's say we wanted

$$\varphi(\rho) = \gamma^2$$

Then for φ to be a homomorphism we need

$$\varphi(\rho^2) = \varphi(\rho)\varphi(\rho) = \gamma^2\gamma^2 = (\gamma^2)^2$$

and

$$\varphi(\rho^3) = \varphi(\rho)\varphi(\rho)\varphi(\rho) = \gamma^2\gamma^2\gamma^2 = (\gamma^2)^3$$

and so on.

This is why one you decide where ρ goes it forces where $\varphi(\rho^k)$ goes.

Ex: Let's construct a homomorphism $\varphi : \mathbb{Z} \to \mathbb{R}$.

We know $\mathbb{Z}$ is cyclic with $\mathbb{Z} = \langle 1 \rangle$.

Since 1 has infinite order we can pick any element of $\mathbb{R}$ to make φ.

Let's pick π.

Then, by the theorem we define

$$\varphi(n) = n\pi$$

$\mathbb{Z}$ and $\mathbb{R}$ are groups under addition so "powers" of elements are sums

Let's explain where this comes from.

Let's say we want $\varphi(1) = \pi$.

Then for φ to be a homomorphism we need

$$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = \pi + \pi = 2\pi$$

and

$$\varphi(3) = \varphi(1+1+1) = \varphi(1)+\varphi(1)+\varphi(1)$$
$$= \pi + \pi + \pi$$
$$= 3\pi$$

inverse here is under adding

and

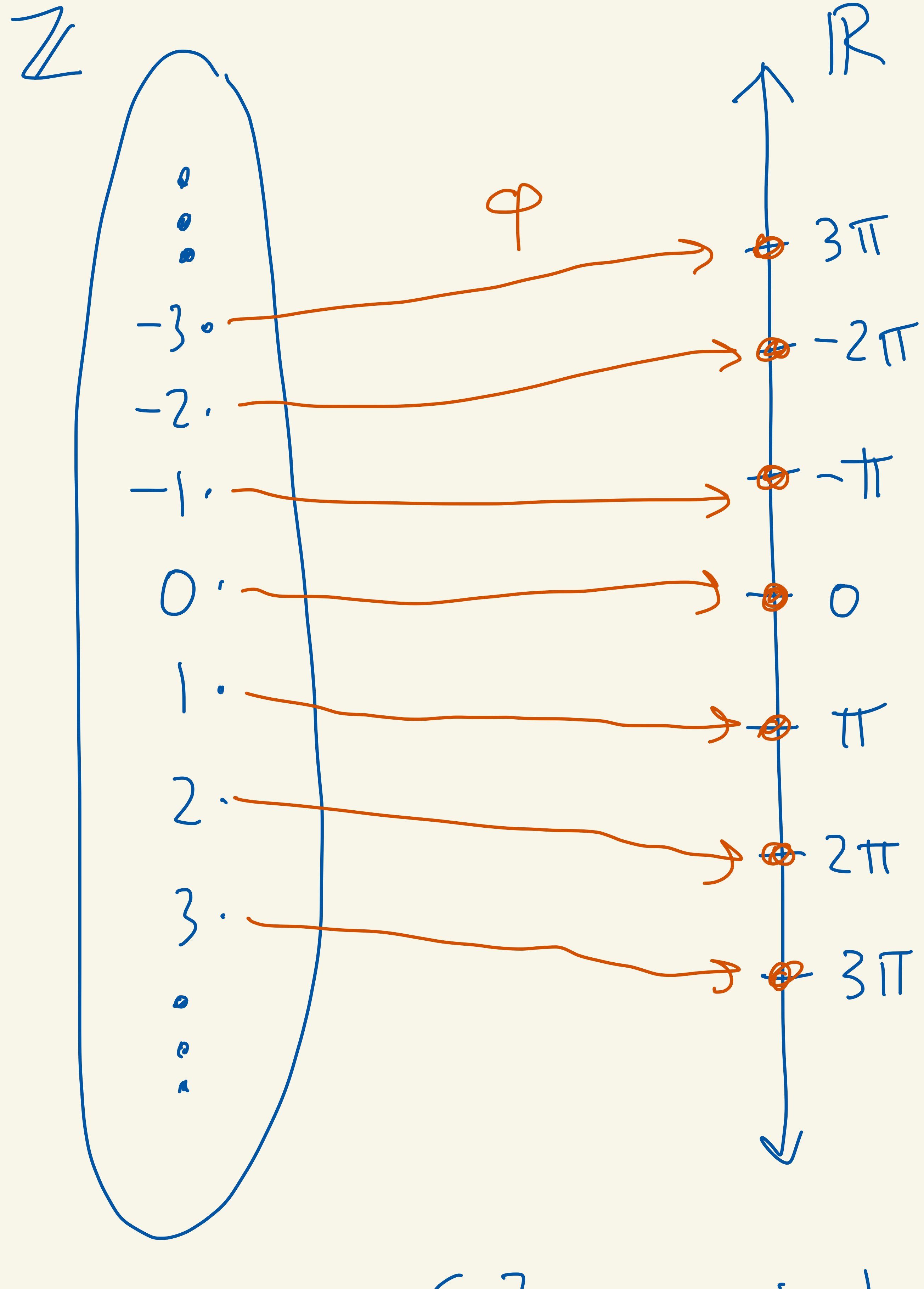
$$\varphi(-1) = [\varphi(1)]^{-1} = [\pi]^{-1} = -\pi$$

$$\varphi(-2) = \varphi(-1-1) = \varphi(-1)+\varphi(-1)$$
$$= -\pi - \pi$$
$$= -2\pi$$

and so on.

This is why once you pick $\varphi(1) = \pi$ you must then have $\varphi(n) = n\pi$.

So we get this picture:



Here $\ker(\varphi) = \{0\}$ so φ is 1-1.

$\operatorname{im}(\varphi) = \{k\pi \mid k \in \mathbb{Z}\}$

Theorem: (Classification of cyclic groups)

Let G be a cyclic group.

- If $|G| = n$, then $G \cong \mathbb{Z}_n$
- If $|G| = \infty$, then $G \cong \mathbb{Z}$.

---

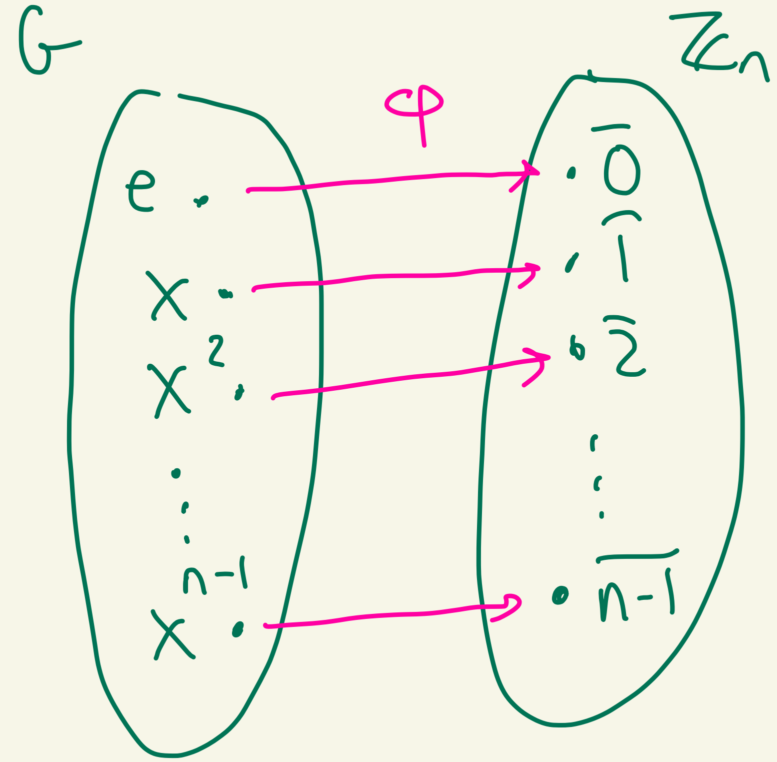
proof:

case 1: Let $G = \langle x \rangle$ where x has order n. Then, $G = \{1, x, x^2, \ldots, x^{n-1}\}$.

Define $\varphi: G \to \mathbb{Z}_n$ by $\varphi(x^k) = \overline{k}$

[We picked $\overline{1}$ in $\mathbb{Z}_n$ of order n and $\overline{k}$ is the "k-th power" of $\overline{1}$]

By the previous theorem, φ is a homomomomorphism.

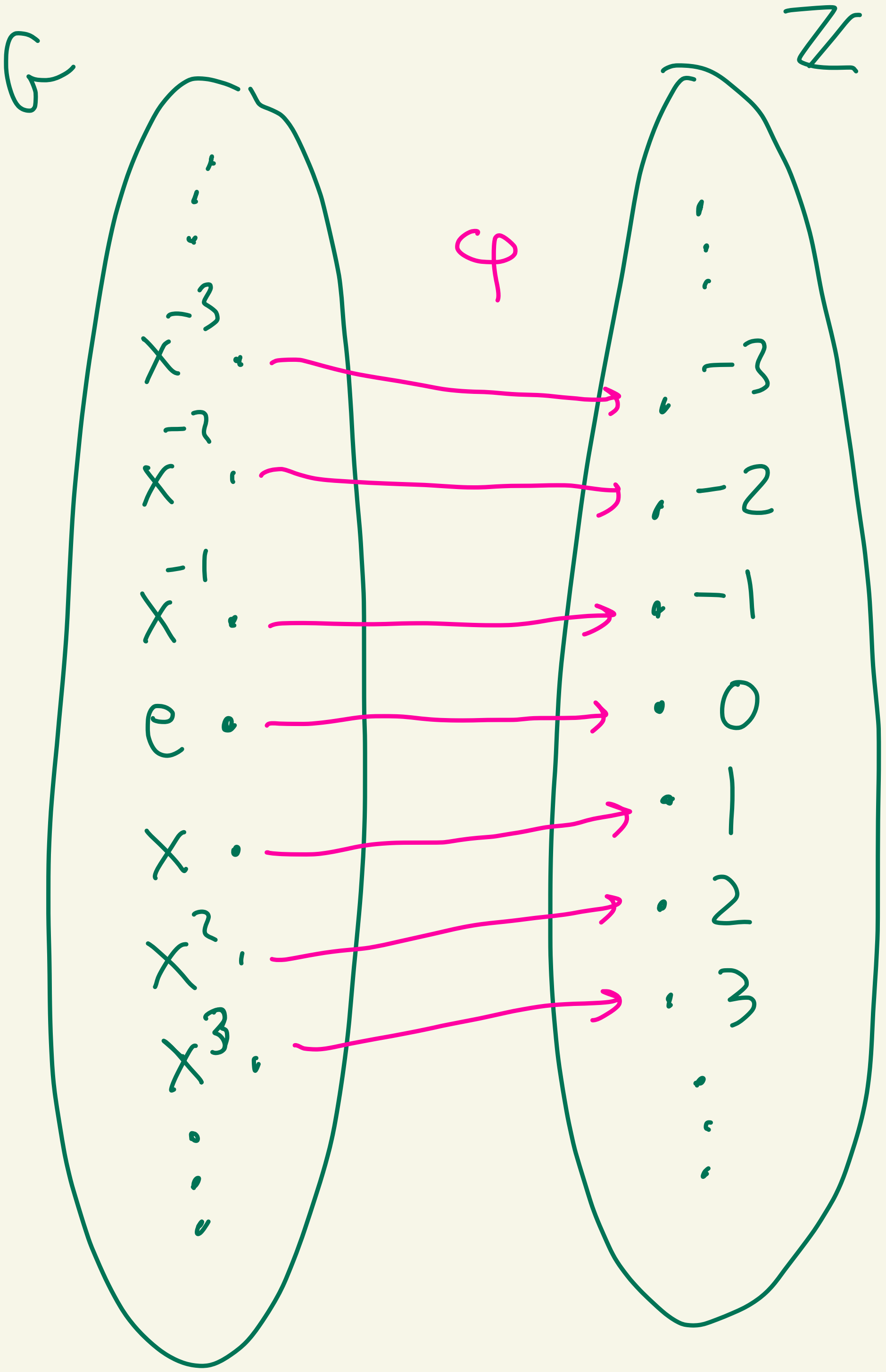


We see that φ is 1-1 and onto so φ is an isomorphism. Thus, $G \cong \mathbb{Z}_n$.

<u>Case 2:</u> Let $G = \langle x \rangle$ where x has infinite order. Define $\varphi : G \to \mathbb{Z}$ where $\varphi(x^k) = k$.

[We picked 1 in $\mathbb{Z}$ and k is the "k-th power" of 1]

By the previous theorem, φ is a homomorphism.

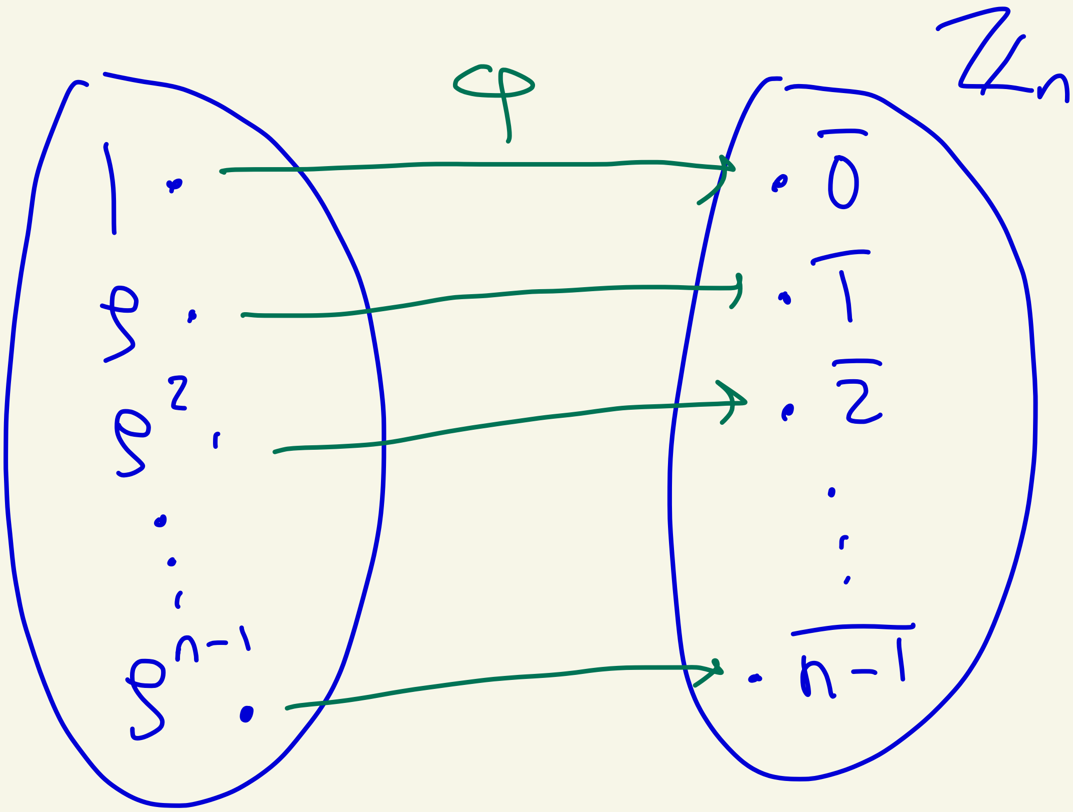


We see that φ is 1-1 and onto.

Thus, φ is an isomorphism

And $G \cong \mathbb{Z}$

Ex: $U_n \cong \mathbb{Z}_n$ since both are cyclic of size n.



φ is an isomorphism.

Below is the proof of the theorem about homomorphisms from the notes

First a lemma.

<u>Lemma:</u> Let G be a group. Let $x \in G$ where x has order n. If $x^k = e$ for some integer k, then n divides k.

<u>proof:</u> By the division algorithm

$$k = qn + r$$

where $0 \leq r < n$.

Then

$$e = x^k = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r$$

Since n is the order of x and $0 \leq r < n$ we must have $r = 0$.

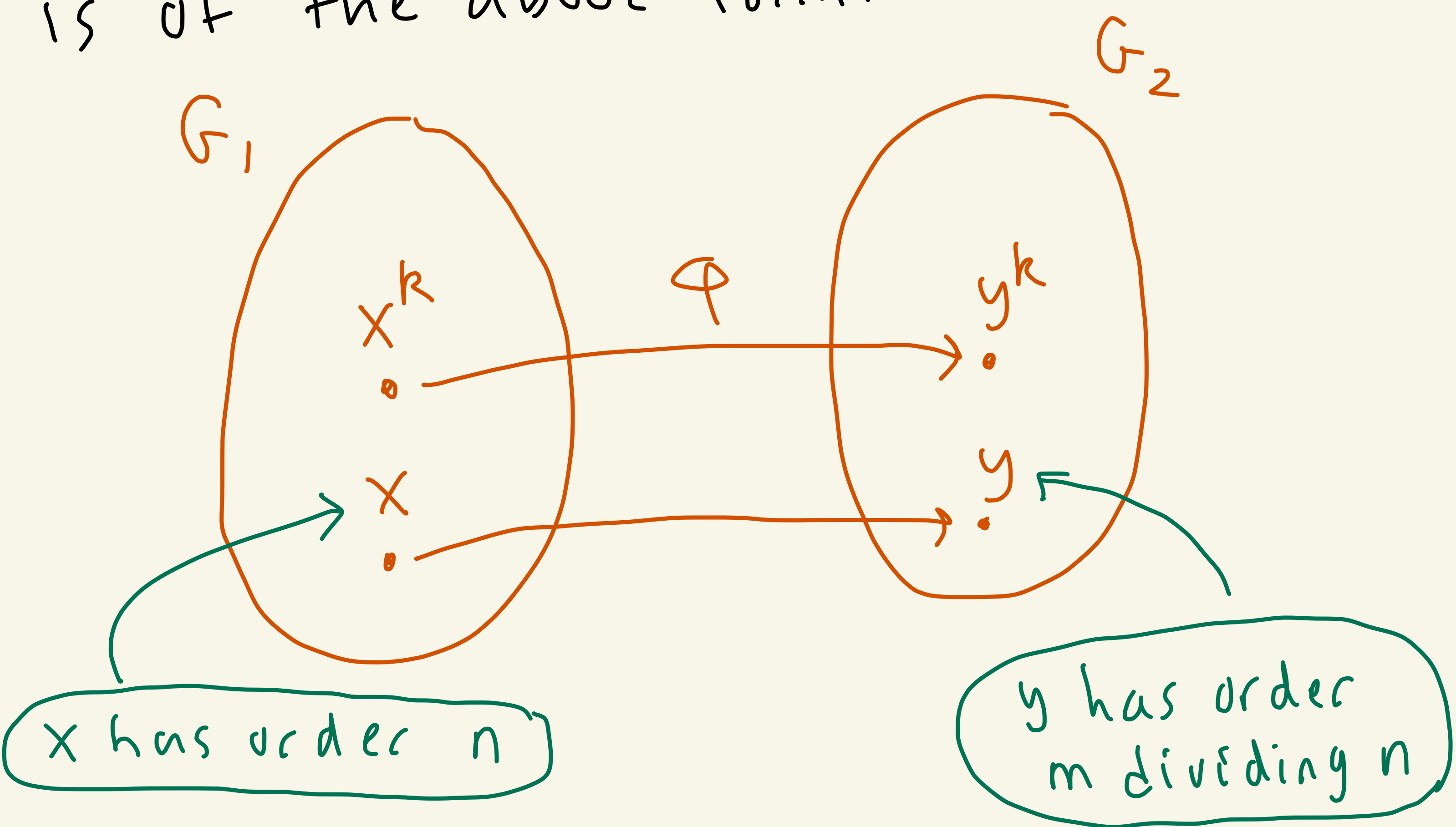
Thus, $k = qn$.

So, n divides k. $\blacksquare$

Theorem: (Homomorphisms out of cyclic groups) Let $G_1 = \langle x \rangle$ be a cyclic group. Let G_2 be a group.

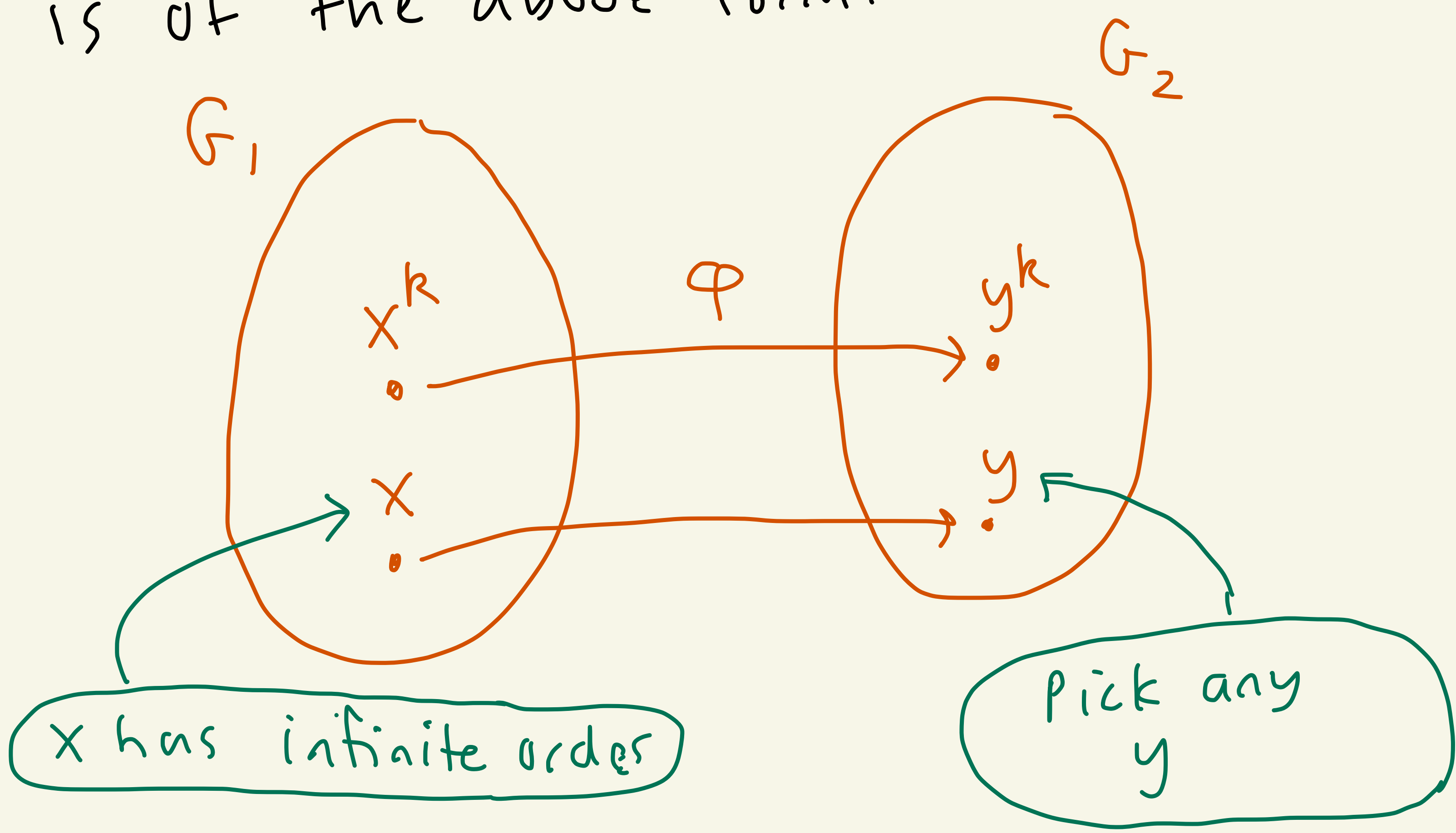
Case 1: Suppose x has finite order n

Pick $y \in G_2$ with order m dividing n. Then, $\varphi : G_1 \to G_2$ given by $\varphi(x^k) = y^k$ is a homomorphism. Furthermore, every homomorphism from G_1 to G_2 is of the above form.



Case 2: Suppose x has infinite order

Pick any $y \in G_2$.
Then $\varphi : G_1 \to G_2$ given by $\varphi(x^k) = y^k$
is a homomorphism. Furthermore,
every homomorphism from G_1 to G_2
is of the above form.



proof:
Let $G = \langle x \rangle$ where $x \in G$.

Case 1: Suppose x has order n.

Let $y \in G_2$ have order m.
Suppose m divides n.
Then $n = ml$ where $l \in \mathbb{Z}$.
Let $\varphi : G_1 \to G_2$ be defined as $\varphi(x^k) = y^k$
First we show that φ is well-defined.
Suppose $x^a = x^b$ where $a \geq b$.
Then $x^{a-b} = e_1$ where e_1 is the identity of G_1
By the lemma $a-b = nq$ for some $q \in \mathbb{Z}$.
Note that

$$y^{a-b} = \varphi(x^{a-b}) = \varphi(x^{nq}) = \varphi(x^{mlq})$$
$$= y^{mlq} = (y^m)^{lq} = e_2^{lq} = e_2$$

So, $y^{a-b} = e_2$ where e_2 is the identity of G_2.
By the lemma $a-b = mj$ where $j \in \mathbb{Z}$.
So, $\varphi(x^a) = y^a = y^{b+mj} = y^b y^{mj}$

$$= y^b (y^m)^j = y^b e_2^j = y^b = \varphi(x^b)$$

Thus if $x^a = x^b$ then $\varphi(x^a) = \varphi(x^b)$

and φ is well-defined.

Now we show that φ is a homomorphism.

Let $w, z \in G_1$.

Then $w = x^c$ and $z = x^d$ where $c, d \in \mathbb{Z}$.

So,

$$\varphi(wz) = \varphi(x^c x^d) = \varphi(x^{c+d}) = y^{c+d}$$

$$= y^c y^d = \varphi(x^c)\varphi(x^d) = \varphi(w)\varphi(z)$$

Thus φ is a homomorphism.

Now we show the furthermore part of the theorem.

Suppose that $\psi: G_1 \to G_2$ is a homomorphism.

Let $y = \psi(x)$.

By induction and the fact that ψ is a homomorphism we get that $\psi(x^k) = y^k$.

Let y have order m.

By the division algorithm
$n = mq + r$ for some $q, r \in \mathbb{Z}$
with $0 \leq r < m$.

Then,

$$e_2 = \varphi(e_1) = \varphi(x^n) = \varphi(x^{mq+r})$$
$$= y^{mq+r} = (y^m)^q y^r = e_2^q y^r$$
$$= y^r$$

Thus, $y^r = e_2$.

Since y has order m and $0 \leq r < m$
we must have $r = 0$.

Thus, $n = mq$.

So m divides n.

This finishes case 1.

<u>case 2:</u> Exercise. (This is easier than case 1 because there's no well-defined part, the rest is similar) $\boxtimes$