Math 4550

Topic 4 - Homomorphisms

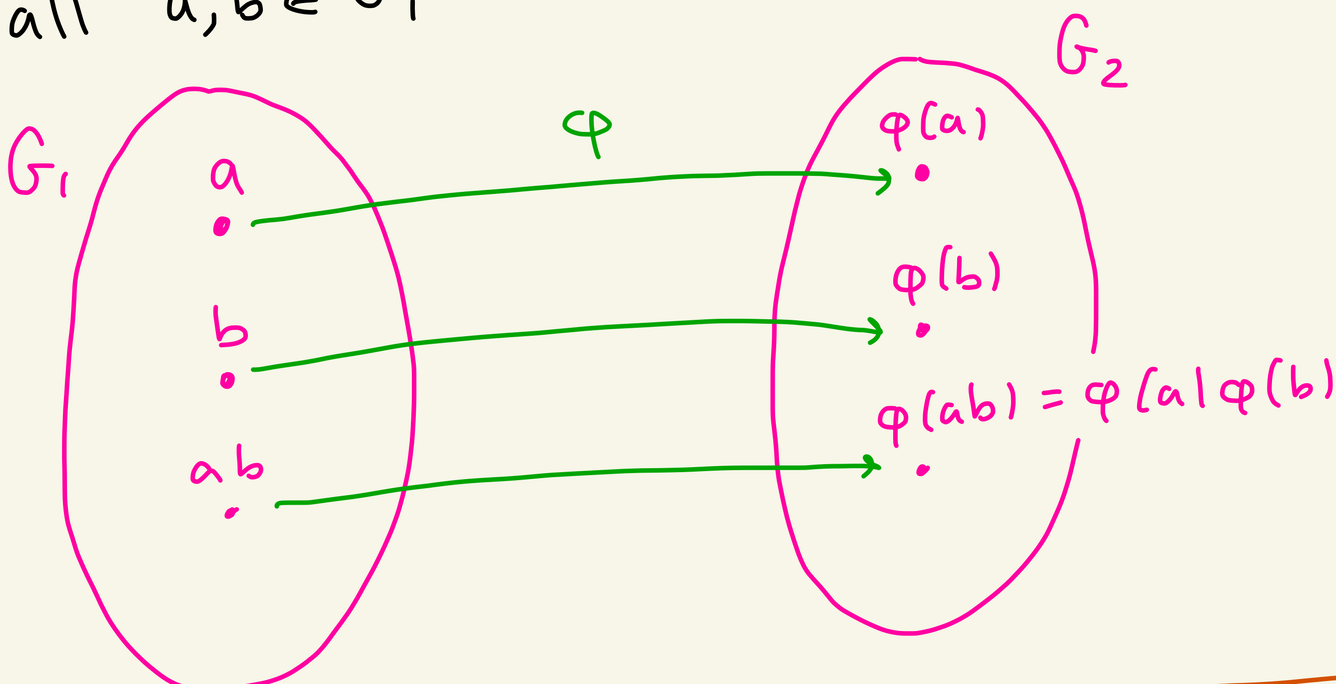
The way we compare two groups is with a function that respects their group properties

---

<u>Def:</u> Let G_1 and G_2 be groups.
A function $\varphi : G_1 \to G_2$ is called a <u>homomorphism</u> if

$$\varphi(ab) = \varphi(a)\varphi(b)$$

for all $a, b \in G_1$



<u>Note:</u> If G_1 and G_2 have operations $*_1$ and $*_2$ respectively than the equation above is

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$$

but we just write

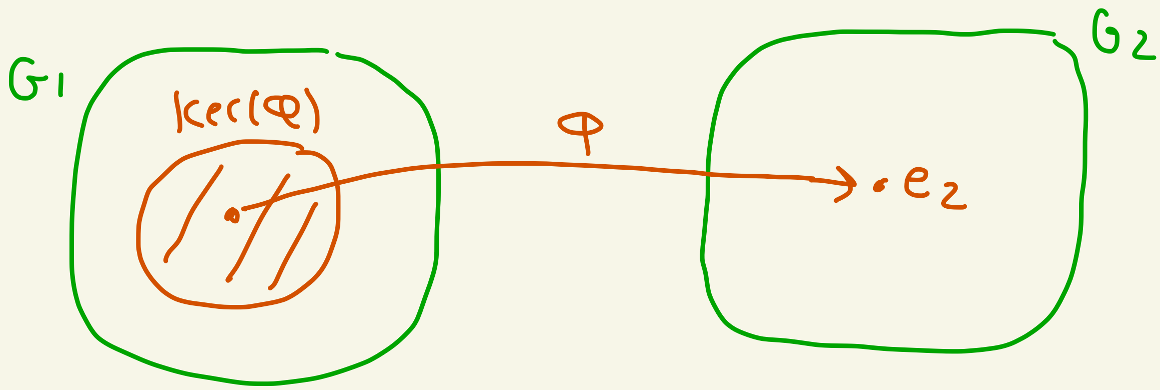
$$\varphi(ab) = \varphi(a)\varphi(b)$$

for simplicity

The <u>kernel</u> of φ is

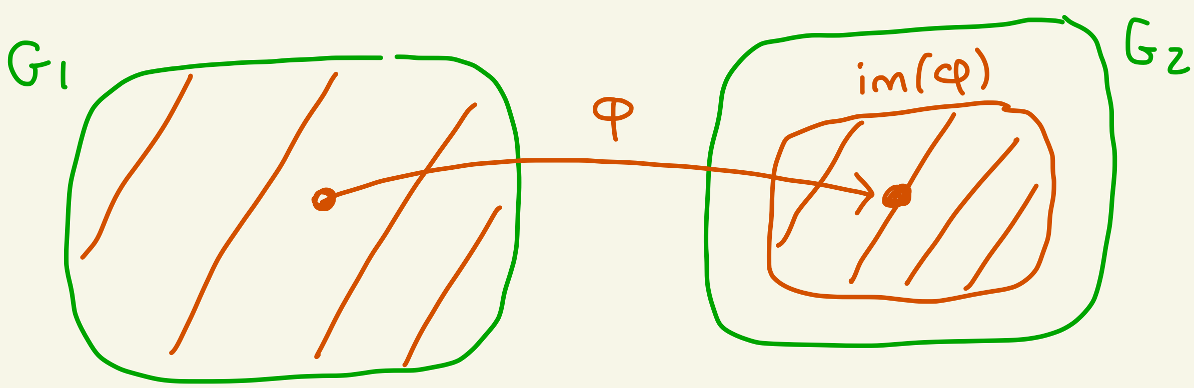
$$\ker(\varphi) = \{ x \in G_1 \mid \varphi(x) = e_2 \}$$

where e_2 is the identity of G_2.



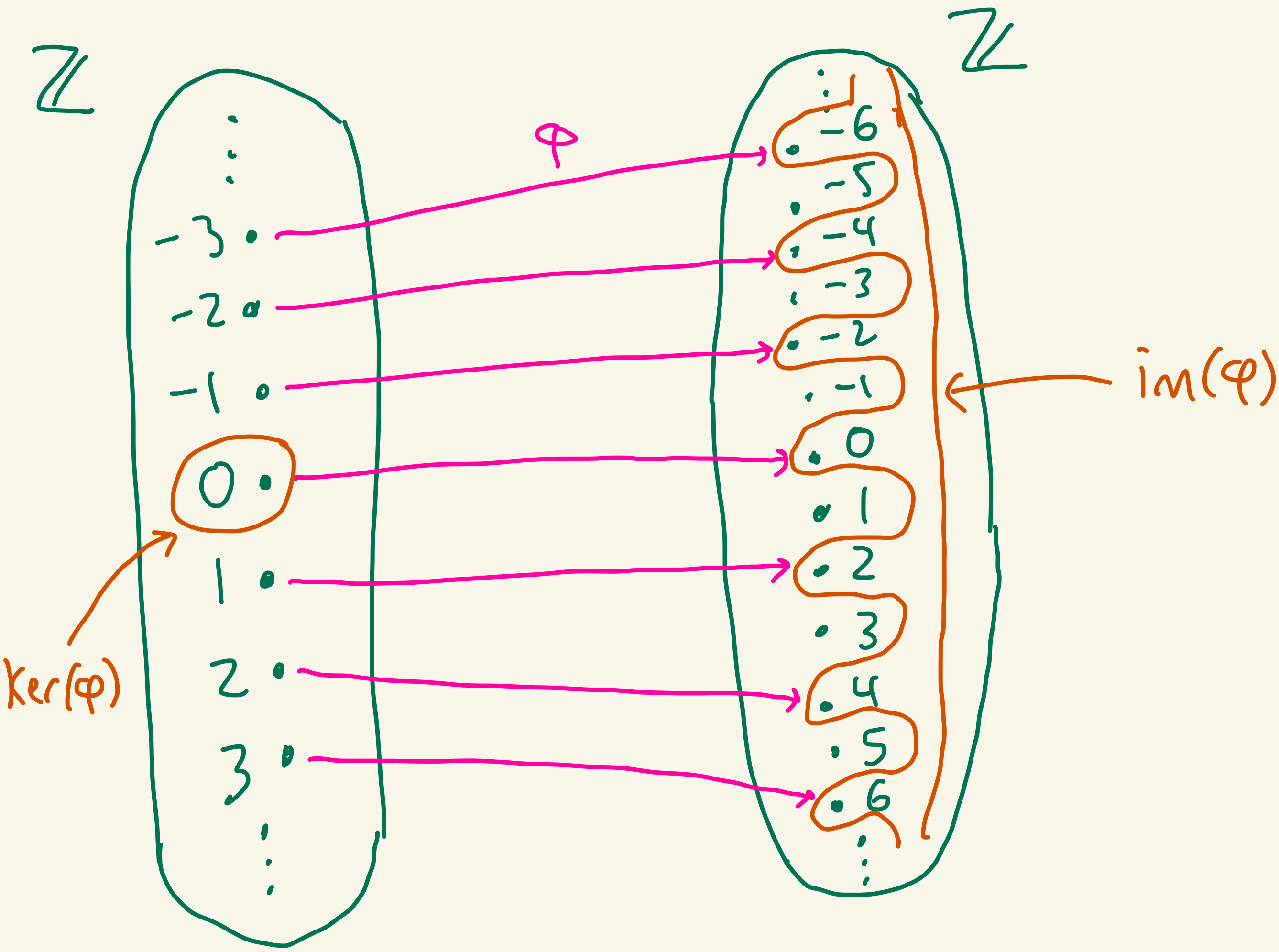
The <u>image</u> of φ is

$$\operatorname{im}(\varphi) = \{ \varphi(x) \mid x \in G_1 \}$$



If $\varphi: G_1 \to G_2$ is a homomorphism that is one-to-one and onto then we call φ an <u>isomorphism</u> and say that G_1 and G_2 are isomorphic and write $G_1 \cong G_2$.

Ex: $\varphi : \mathbb{Z} \to \mathbb{Z}$
$\varphi(x) = 2x$



Let's show that φ is a homomorphism.
Given $x, y \in \mathbb{Z}$ we have that

$$\varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y).$$

Thus, φ is a homomorphism.

Note that
$\ker(\varphi) = \{0\}$

and

$$\operatorname{im}(\varphi) = \{\varphi(x) \mid x \in \mathbb{Z}\}$$
$$= \{2x \mid x \in \mathbb{Z}\}$$
$$= 2\mathbb{Z}$$

Later we will see that a homomorphism $\varphi: G_1 \to G_2$ is one-to-one iff $\ker(\varphi) = \{e_1\}$

Here $\varphi: \mathbb{Z} \to \mathbb{Z}$ and $\ker(\varphi) = \{0\}$.

Thus, φ is one-to-one.

Recall that φ is onto iff $\operatorname{im}(\varphi) = \mathbb{Z}$.

Here $\operatorname{im}(\varphi) = 2\mathbb{Z} \neq \mathbb{Z}$.

Thus, φ is not onto

Summarizing the above,

$\varphi: \mathbb{Z} \to \mathbb{Z}$ given by $\varphi(x) = 2x$

is a homomorphism.

$\ker(\varphi) = \{0\}$ and $\operatorname{im}(\varphi) = 2\mathbb{Z}$.

φ is one-to-one but not onto.

So, φ is not an isomorphism.

Ex: Consider the two groups $\mathbb{Z}_3$ and U_3.

$\langle \mathbb{Z}_3, + \rangle$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\langle U_3, \cdot \rangle$	1	ρ	ρ^2
1	1	ρ	ρ^2
ρ	ρ	ρ^2	1
ρ^2	ρ^2	1	ρ

Do you see how these tables are the same under the correspondence

$\bar{0} \longleftrightarrow 1 \qquad \bar{1} \longleftrightarrow \rho \qquad \bar{2} \longleftrightarrow \rho^2$

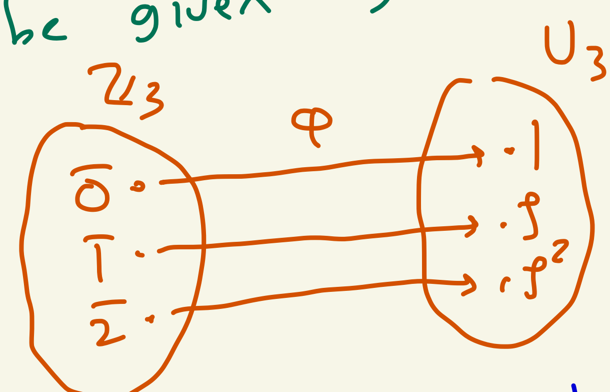
identity elements

The groups are essentially the same. The elements are just called different things and the operations are different.

We can describe this with an isomorphism.

Let $\varphi : \mathbb{Z}_3 \to U_3$ be given by

$$\varphi(\bar{0}) = 1$$
$$\varphi(\bar{1}) = \rho$$
$$\varphi(\bar{2}) = \rho^2$$



$\ker(\varphi) = \{\bar{0}\}$ $\quad$ $\mathrm{im}(\varphi) = U_3$

φ is 1-1 and onto.

Why is φ a homomorphism?

We need to check that

$$\varphi(x+y) = \varphi(x)\varphi(y)$$

operation in $\mathbb{Z}_3$

operation in U_3

for all $x, y \in \mathbb{Z}_3$.

But the tables show this!

For example,

$$\varphi(\bar{1}+\bar{2}) = \varphi(\bar{3}) = \varphi(\bar{0}) = 1$$

$$\varphi(\bar{1})\varphi(\bar{2}) = \rho \cdot \rho^2 = 1$$

$\mathbb{Z}_3$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$			
$\bar{1}$			$\bar{0}$
$\bar{2}$			

U_3	1	ρ	ρ^2
1			
ρ			1
ρ^2			

Or instead of seeing that the tables verify that φ is a homomorphism you can do all 9 checks:

$$\varphi(\bar{0}+\bar{0}) = \varphi(\bar{0}) = 1 = 1\cdot 1 = \varphi(\bar{0})\varphi(\bar{0})$$
$$\varphi(\bar{0}+\bar{1}) = \varphi(\bar{1}) = \rho = 1\cdot\rho = \varphi(\bar{0})\varphi(\bar{1})$$
$$\varphi(\bar{0}+\bar{2}) = \varphi(\bar{2}) = \rho^2 = 1\cdot\rho^2 = \varphi(\bar{0})\varphi(\bar{2})$$
$$\varphi(\bar{1}+\bar{0}) = \varphi(\bar{1}) = \rho = \rho\cdot 1 = \varphi(\bar{1})\varphi(\bar{0})$$
$$\varphi(\bar{1}+\bar{1}) = \varphi(\bar{2}) = \rho^2 = \rho\cdot\rho = \varphi(\bar{1})\varphi(\bar{1})$$
$$\varphi(\bar{1}+\bar{2}) = \varphi(\bar{0}) = 1 = \rho\cdot\rho^2 = \varphi(\bar{1})\varphi(\bar{2})$$
$$\varphi(\bar{2}+\bar{0}) = \varphi(\bar{2}) = \rho^2 = \rho^2\cdot 1 = \varphi(\bar{2})\varphi(\bar{0})$$
$$\varphi(\bar{2}+\bar{1}) = \varphi(\bar{0}) = 1 = \rho^2\cdot\rho = \varphi(\bar{2})\varphi(\bar{1})$$
$$\varphi(\bar{2}+\bar{2}) = \varphi(\bar{1}) = \rho = \rho^2\rho^2 = \varphi(\bar{2})\varphi(\bar{2})$$

use $\rho^3 = 1$

Thus, φ is an isomorphism and $\mathbb{Z}_3 \cong U_3$.

Theorem: Let $\varphi: G_1 \to G_2$ be a homomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively.

Then:

1. $\varphi(e_1) = e_2$
2. If $x \in G_1$, then $\varphi(x^{-1}) = [\varphi(x)]^{-1}$
3. If $x \in G$ and $k \in \mathbb{Z}$, then $\varphi(x^k) = [\varphi(x)]^k$
4. $\ker(\varphi) \leq G_1$
5. $\operatorname{im}(\varphi) \leq G_2$
6. φ is one-to-one iff $\ker(\varphi) = \{e_1\}$
7. φ is onto iff $\operatorname{im}(\varphi) = G_2$.

proof.

1. We have that

φ is a homomorphism

$$\varphi(e_1) = \varphi(e_1 e_1) = \varphi(e_1)\varphi(e_1)$$

Thus,

$$\varphi(e_1)^{-1}\varphi(e_1) = \varphi(e_1)^{-1}\varphi(e_1)\varphi(e_1)$$

So, $e_2 = \varphi(e_1)$.

(2) We have

$$\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e_1) \overset{\text{part (1)}}{=} e_2$$

Thus, $\varphi(x^{-1}) = [\varphi(x)]^{-1}$

---

(3) If $k=0$, then

$$\varphi(x^k) = \varphi(x^0) = \varphi(e_1) \overset{\text{part (1)}}{=} e_2 = [\varphi(x)]^0 = [\varphi(x)]^k$$

If $k>0$, then

$$\varphi(x^k) = \varphi(\underbrace{x\,x\cdots x}_{k \text{ times}}) \underset{\varphi \text{ is a homomorphism}}{=} \varphi(x)\varphi(x)\cdots\varphi(x) = [\varphi(x)]^k$$

and

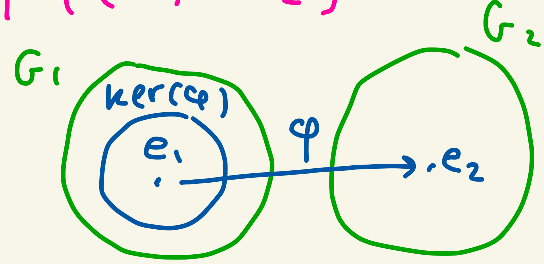
$$\varphi(x^{-k}) = \varphi((x^k)^{-1}) \underset{\text{part (2)}}{=} [\varphi(x^k)]^{-1} = [\varphi(x)\varphi(x)\cdots\varphi(x)]^{-1}$$

$$= \varphi(x)^{-1}\varphi(x)^{-1}\cdots\varphi(x)^{-1}$$

$$= [\varphi(x)]^{-k}$$

---

(4) Recall that $\ker(\varphi) = \{x \in G_1 \mid \varphi(x) = e_2\}$



(i) By part (1) we know $\varphi(e_1) = e_2$.

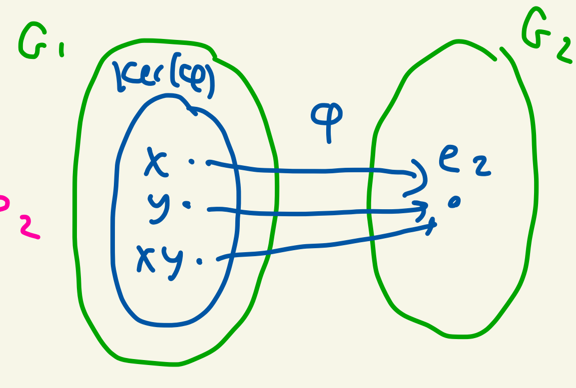
Thus, $e_1 \in \ker(\varphi)$

(ii) Suppose $x, y \in \ker(\varphi)$.

Then $\varphi(x) = e_2$ and $\varphi(y) = e_2$.

Thus, $\varphi(xy) = \varphi(x)\varphi(y) = e_2 e_2 = e_2$

So, $xy \in \ker(\varphi)$



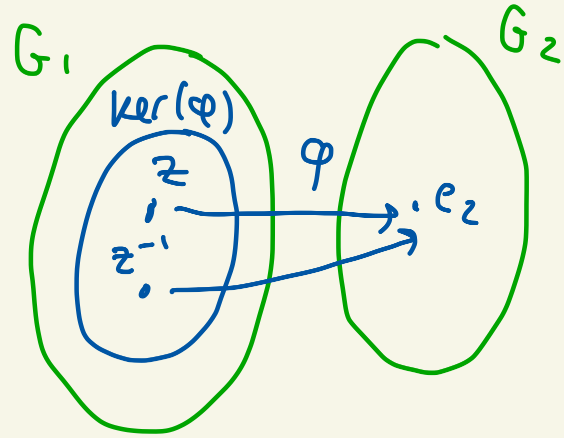
(iii) Suppose $z \in \ker(\varphi)$.

Then $\varphi(z) = e_2$.

Thus, $\varphi(z^{-1}) = [\varphi(z)]^{-1} = e_2^{-1} = e_2$

part ②

So, $z^{-1} \in \ker(\varphi)$.



By (i), (ii), (iii) we get $\ker(\varphi) \leq G_1$

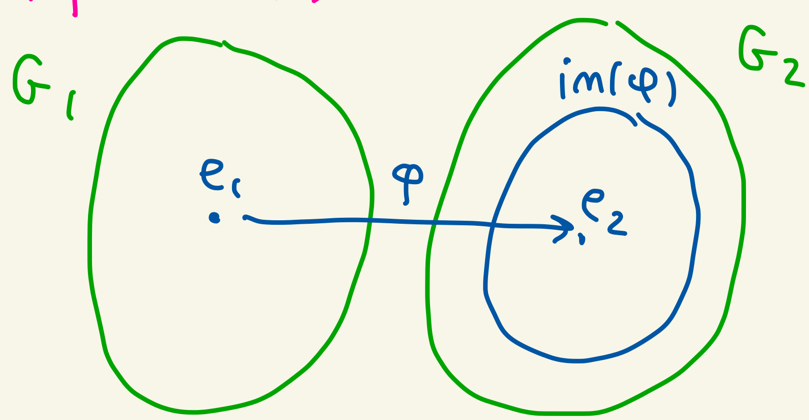
---

⑤ Recall $\mathrm{im}(\varphi) = \{\varphi(x) \mid x \in G_1\}$

(i) Since $e_1 \in G_1$

and $e_2 = \varphi(e_1)$

we know $e_2 \in \mathrm{im}(\varphi)$



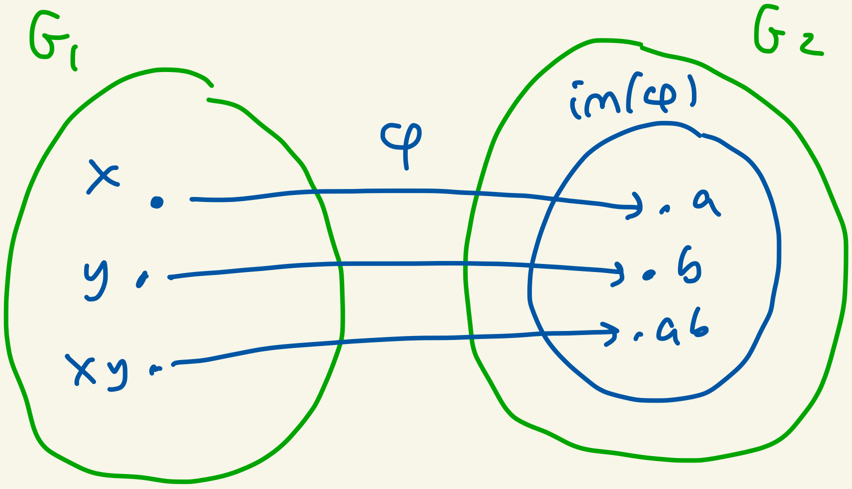
(ii) Let $a, b \in \mathrm{im}(\varphi)$.

Then there exist

$x, y \in G_1$ where

$\varphi(x) = a$ and

$\varphi(y) = b$.

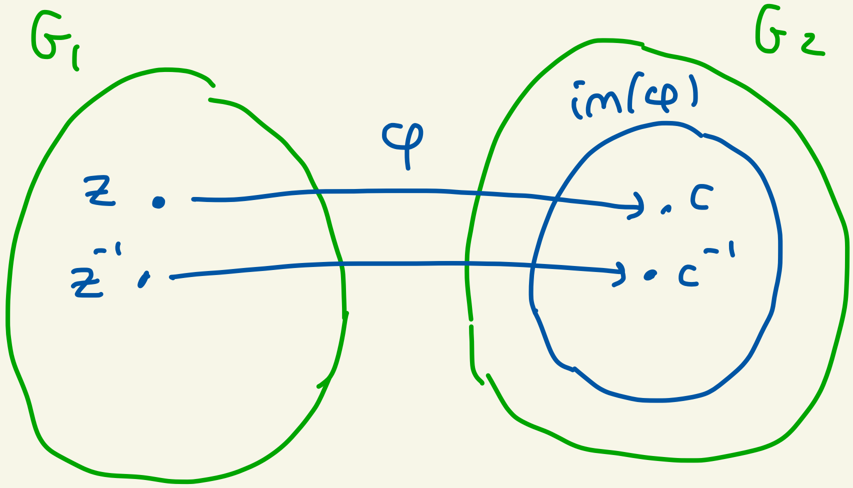


Then, $ab = \varphi(x)\varphi(y) = \varphi(xy)$

Since $xy \in G_1$ we get

that $ab \in \mathrm{im}(\varphi)$.

(iii) Let $c \in \text{im}(\varphi)$.
Then there exists
$z \in G_1$ where
$\varphi(z) = c$.
Then, $c^{-1} = [\varphi(z)]^{-1} = \varphi(z^{-1})$
and $z^{-1} \in G_1$.
Thus, $c^{-1} \in \text{im}(\varphi)$.



By (i), (ii), (iii) we have that $\text{im}(\varphi) \leq G_2$

6

($\Leftarrow$) Suppose φ is one-to-one.
Let's show that $\ker(\varphi) = \{e_1\}$
We know from part 1 that $e_1 \in \ker(\varphi)$ since $\varphi(e_1) = e_2$.
Suppose $x \in \ker(\varphi)$.
Then $\varphi(x) = e_2 = \varphi(e_1)$
But φ is one-to-one with $\varphi(x) = \varphi(e_1)$.
This implies $x = e_1$.
Thus, $\ker(\varphi) = \{e_1\}$

($\Rightarrow$) Suppose $\ker(\varphi) = \{e_1\}$
Let's show that φ is one-to-one.
Suppose $\varphi(x) = \varphi(y)$ where $x, y \in G_1$.

Then $\varphi(x)[\varphi(y)]^{-1} = \underbrace{\varphi(y)[\varphi(y)]^{-1}}_{e_2}$

So, $\varphi(x)\varphi(y^{-1}) = e_2$

Thus, $\varphi(xy^{-1}) = e_2$

Thus, $xy^{-1} \in \ker(\varphi)$.

So, $xy^{-1} = e_1$ because $\ker(\varphi) = \{e_1\}$.

Thus, $xy^{-1}y = e_1 y$.

So, $x = y$.

Thus φ is one-to-one.

---

7 φ is onto iff $\text{im}(\varphi) = G_2$.

This is the definition of onto.
