Monday Week 6 Sept. 26, 2016

Example: $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ ← group using +

$U_3 = \{1, \rho, \rho^2\}$, $\rho = e^{2\pi i/3}$ ← group using mult.

$\langle \mathbb{Z}_3, + \rangle$	$\bar{0}$	$\bar{1}$	$\bar{2}$ ($=\bar{y}$)
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{x} = \bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

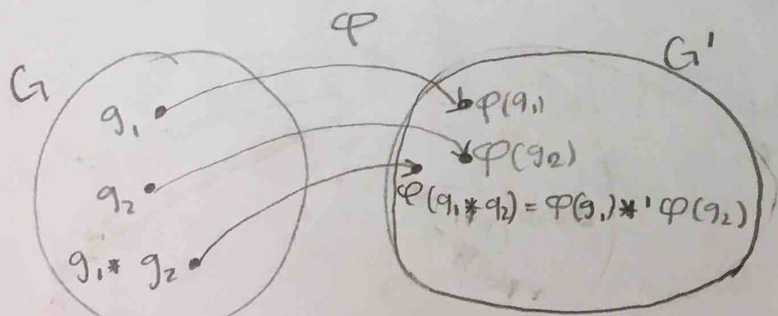
$\varphi(\bar{x}) \cdot \varphi(\bar{y}) = \varphi(\bar{x} + \bar{y})$

$\langle U_3, \cdot \rangle$	1	ρ	ρ^2 ($\varphi(\bar{y})$)
1	1	ρ	ρ^2
$\varphi(\bar{x}) \to \rho$	ρ	ρ^2	1 ($= \bar{x} + \bar{y}$)
ρ^2	ρ^2	1	ρ

$\bar{0} \longleftrightarrow 1$
$\bar{1} \longleftrightarrow \rho$
$\bar{2} \longleftrightarrow \rho^2$
} tables are the same

$\rho^3 = 1$
$\rho^3 = (e^{2\pi i/3})^3$
$= e^{2\pi i} = 1$
In general
$U_n = \{1, \rho, \rho^2, \dots \rho^{n}\}$
$\rho = e^{2\pi i/n}$ and $\rho^n = 1$

Def: Let G and G' be groups with operations $*$ and $*'$.
We say that a function $\varphi: G \to G'$ is a group homomorphism if $\varphi(g_1 * g_2) = \varphi(g_1) *' \varphi(g_2)$ for all $g_1, g_2 \in G$



Isomorphism is
1. 1-1
2. onto
3. homomorphism

If in addition φ is one-to-one and onto then we call φ an a group isomorphism.

When there exists an isomorphism between two groups G_1 and G_2 then we say that G_1 and G_2 are isomorphic and we write:

$$G_1 \simeq G_2$$

Example:

$\varphi : \mathbb{Z}_3 \to U_3$ where $\boxed{\varphi(\bar{0}) = 1, \varphi(\bar{1}) = \rho, \varphi(\bar{2}) = \rho^2}$

For φ to be a group homomorphism we need to have $\varphi(\overline{x+y}) = \varphi(\bar{x}) \cdot \varphi(\bar{y})$

for all $\bar{x}, \bar{y} \in \mathbb{Z}_3$, the table shows this is true.

equal $\begin{cases} \varphi(\bar{1}+\bar{2}) = \varphi(\bar{3}) = \varphi(\bar{0}) = 1 \\ \varphi(1) \cdot \varphi(\bar{2}) = \rho \cdot \rho^2 = \rho^3 = 1 \end{cases}$ ← check for $\bar{x} = \bar{1}, \bar{y} = \bar{2}$

φ is a homomorphism (from the table) ✓

φ is 1-1 and onto

φ is isomorphic

so $\mathbb{Z}_3 \simeq U_3$ ($\mathbb{Z}_3$ is isomorphic to U_3)

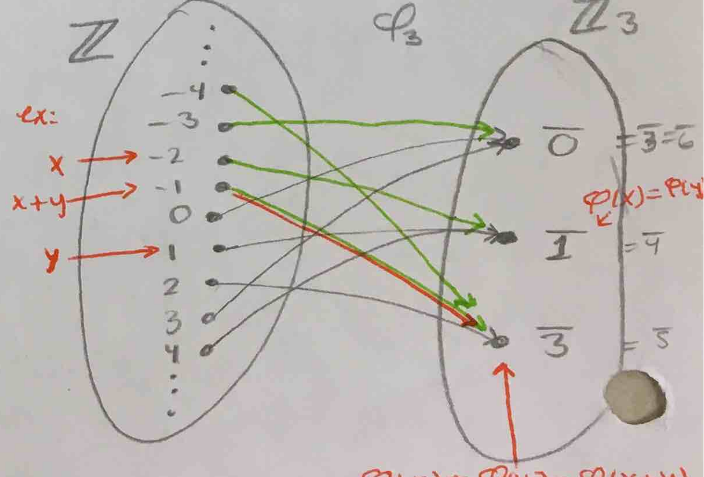
Example: Let $\varphi_n : \mathbb{Z} \to \mathbb{Z}_n$ where $n \geq 2$ be defined by $\varphi(x) = \bar{x}$ (call φ the reduction mod n map)

φ_n is a homomorphism

Proof let $\bar{x}, \bar{y} \in \mathbb{Z}$ then

$$\varphi(x+y) \underset{\substack{\uparrow \\ \text{def of } \varphi_n}}{=} \overline{x+y} \underset{\substack{\uparrow \\ \text{def of} \\ + \text{ in } \mathbb{Z}_n}}{=} \bar{x} + \bar{y} \underset{\substack{\uparrow \\ \text{def of } \varphi_n}}{=} \varphi_n(x) + \varphi_n(y)$$

Ex $(n=3)$



φ is a homomorphism

φ is onto

φ is not 1-1

Wednesday Week 6 Sept. 28, 2016

- Recall: $\varphi: G \to G'$ is homomorphism if

  $\varphi(g * h) = \varphi(g) *' \varphi(h)$ for all $g, h \in G$

  $*$ is G operation

  $*'$ is G' operation

From now on

we write this equation as

$\varphi(gh) = \varphi(g)\varphi(h)$

$*$ is here but we don't write it

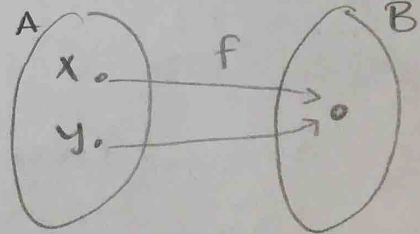
same thing here for $*'$

unless we have specific groups like $\mathbb{Z}$ or something in that case we write $+$ or $\circ$

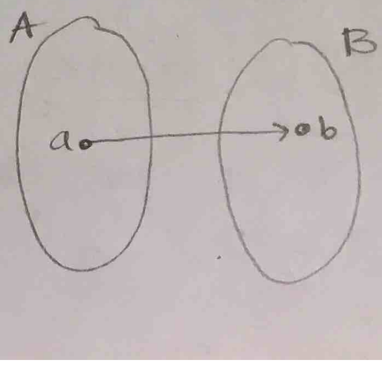
- Def: Let $f: A \to B$ be a function between two sets A and B

(1) f is $(1-1)$ one to one if whenever $x, y \in A$ and $x \neq y$ then we have $f(x) \neq f(y)$, or equivalently whenever $x, y \in A$ and $f(x) = f(y)$ then $x = y$

f is one to one if this picture never happens



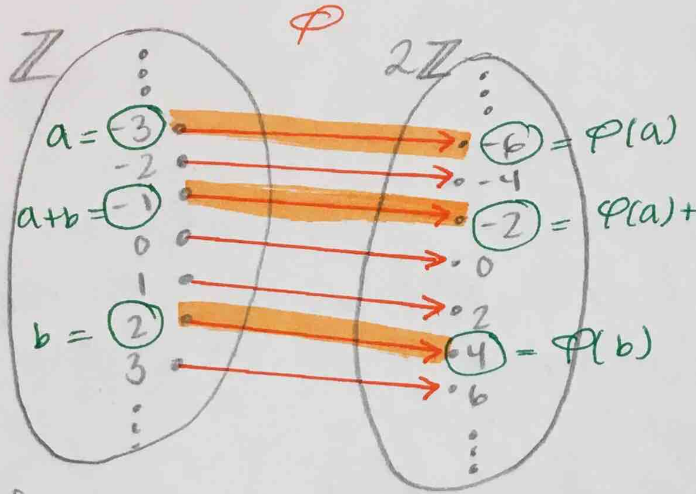
(2) f is onto the set B if for every $b \in B$ $\exists\, a \in A$ with $f(a) = b$



Example : $\mathbb{Z} \simeq 2\mathbb{Z}$ even #s

where $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\} = \{\ldots \underset{2(-2)}{-4}, \underset{2(-1)}{-2}, \underset{2(0)}{0}, \underset{2(1)}{2}, \underset{2(2)}{4}, \ldots\}$

Both $\mathbb{Z}$ and $2\mathbb{Z}$ are groups under addition



Define

$\varphi : \mathbb{Z} \to 2\mathbb{Z}$

where $\varphi(n) = 2n$

• I claim that φ is an isomorphism

(1) homomorphism
(2) 1-1
(3) onto

Proof

(1) Let $a, b \in \mathbb{Z}$

Then $\varphi(a+b) \overset{\text{def of } \varphi}{=} 2(a+b) = 2a+2b = \varphi(a) + \varphi b$

operation in $\mathbb{Z}$ operation in $2\mathbb{Z}$

so φ is a hormomophism

$\varphi : G \to G'$
$\varphi(gh) = \varphi(g)\varphi(h)$
G operation G' operation

(2) Suppose $a, b \in \mathbb{Z}$ and $\varphi(a) = \varphi(b)$

Then $2a = 2b$

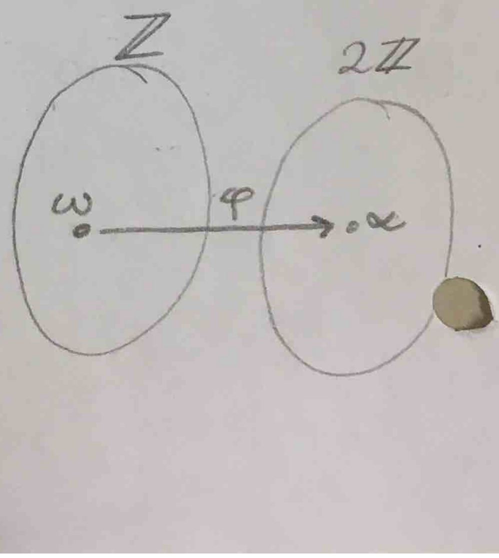
So $a = b$, Thus φ is one-to-one

(3) Let $\alpha \in 2\mathbb{Z}$

Then $\alpha = 2\omega$ where $\omega \in \mathbb{Z}$

then $\varphi(\omega) = \alpha$

Thus φ is onto



Therefore φ is an isomorphism

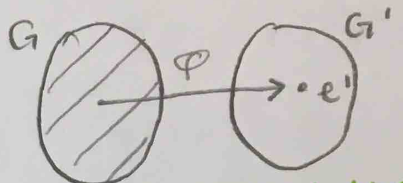
Thus $\mathbb{Z} \simeq 2\mathbb{Z}$ ☒

9/28 P. 2

Example: Let G and G' be groups and e' be the identity of G'

Let $\varphi : G \to G'$ where $\varphi(g) = e' \ \forall g \in G$

Then φ is a homomorphism



This is called the trivial homomorphism

Proof

Let $g, h \in G$

then $\varphi(gh) = e' = e'e' = \varphi(g)\varphi(h)$ ☒

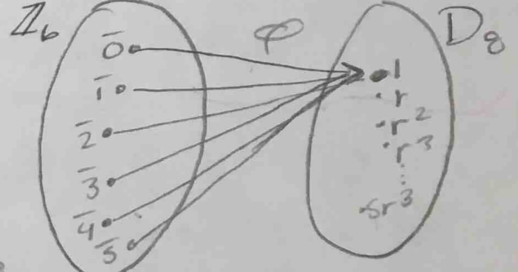
def of φ

Example:

Ex $G = \mathbb{Z}_6$ $G' = D_8$

- everything in $\mathbb{Z}_6$ is mapped onto the identity which is $1 \in D_8$

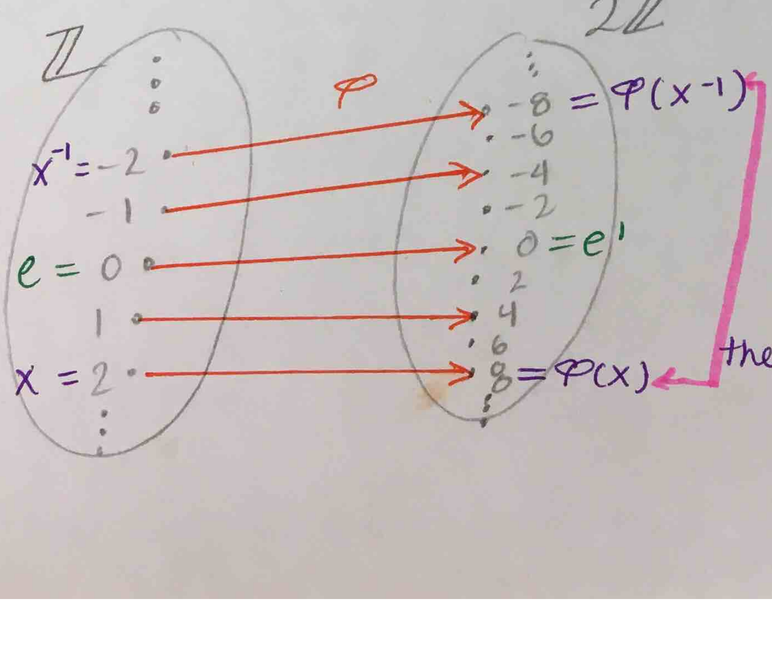
Picture of trivial homomorphism



Example: $\varphi : \mathbb{Z} \to 2\mathbb{Z}$

$\varphi(n) = 4(n)$

φ is a homomorphism



they are inverses

note: not onto so this is not isomorphism

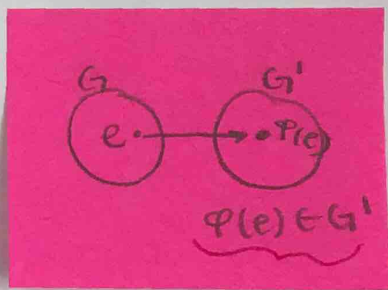
Theorem: Let G and G' be groups with identity elements e and e'.
Let $\varphi: G \to G'$ be a homomorphism. Then
(1) $\varphi(e) = e'$
(2) For every $x \in G$, we have $\varphi(x^{-1}) = [\varphi(x)]^{-1}$
(3) for every $x \in G$ we have $\varphi(x^n) = [\varphi(x)]^n$ for any $n \in \mathbb{Z}$ (prove by induction)

Proof:

(1) we have that $\varphi(e) = \varphi(ee) \underset{\uparrow}{=} \varphi(e)\varphi(e)$
φ is homomorphism

put a $[\varphi(e)]^{-1}$ on both sides

$$\underbrace{[\varphi(e)]^{-1}\varphi(e)}_{e'} = \underbrace{[\varphi(e)]^{-1}\varphi(e)}_{e'}\varphi(e)$$



so $e' = \varphi(e)$

(2) Let $x \in G$ φ is homomorphism
Then $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e'$
and $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e'$
So $\varphi(x)$ and $\varphi(x^{-1})$ are inverses in G'
Thus, $[\varphi(x)]^{-1} = \varphi(x^{-1})$

③ Use induction

Idea: Let $x \in G$

$$\varphi(x^4) = \varphi(xxxx)$$
$$= \varphi(x)\varphi(x)\varphi(x)\varphi(x)$$
$$= [\varphi(x)]^4$$

↑
need to generalize this with induction