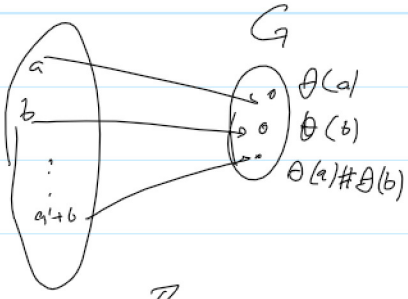
Review

Monday, March 15, 2021 8:48 AM

LNGT §2. Ex. 8. $G = \{0, 2, 4, 6, 8\}$, $\#$

a) $\theta : \mathbb{Z} \to G$

$\forall a, b \in \mathbb{Z}, \ \theta(a+b) = \theta(a) \# \theta(b)$



$a = 6$

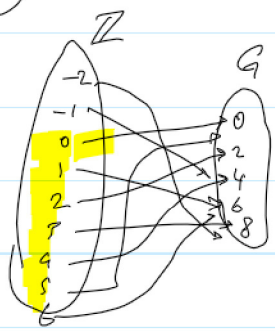
$\forall n \in \mathbb{Z}, \ \theta(n) = n(6) = 6n \mod 10$

$\forall i, j \in \mathbb{Z}$

$\theta(i+j) = 6(i+j)$

$= 6i + 6j \mod 10$

$= \theta(i) \# \theta(j)$



b)

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$\mathbb{Z}_5$ and G are isomorphic for $\theta : \mathbb{Z}_5 \to G$ is a bijection defined by $\theta(n) = 2n$ $\forall n \in \mathbb{Z}_5$

$\mathbb{Z}_5$: n	0	1	2	3	4
G: $\theta(n)$	0	2	4	6	8

Here we have $\forall i, j \in \mathbb{Z}_5$,

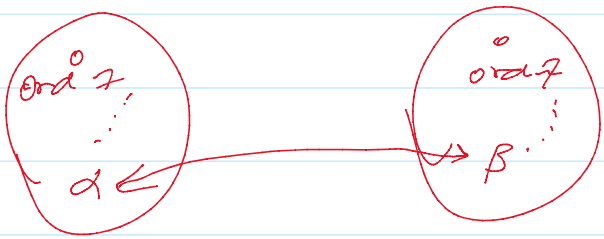
$\theta(i+j) = \theta(i) \# \theta(j)$ □

To show $G_1 \ncong G_2$

① $|G_1| \neq |G_2|$

② one is cyclic the other isn't. ←→

③ if $\exists a \in G_1$, $\forall b \in G_1$, $\text{ord}(a) \neq \text{ord}(b)$



The easy way:

if G_1 and G_2 are cyclic, with $|G_1| = |G_2|$

Let $\langle \alpha \rangle = G_1$

$\langle \beta \rangle = G_2$

We construct $\theta : G_1 \longrightarrow G_2$ as an isomorphism defined by $\theta(\alpha^i) = \beta^i \quad \forall\, i = 1, 2, \dots, |G_1|$

Ex. 9

$$\mathbb{Z}_{125}^* \Longrightarrow |\mathbb{Z}_{125}^*| = \phi(125) = 100$$

$$|\mathbb{Z}_{250}^*| = \phi(250) = 100$$

$\mathbb{Z}_{125}^*$ is cyclic for $125 = 5^3 = p^3$

$\mathbb{Z}_{250}^*$ is cyclic for $250 = 2 \cdot 5^3 = 2 \cdot p^3$

Let $\langle \alpha \rangle = \mathbb{Z}_{125}^*$

$\langle \beta \rangle = \mathbb{Z}_{250}^*$

① Bijection → we construct $\theta : \mathbb{Z}_{125}^* \longrightarrow \mathbb{Z}_{250}^*$ defined by

$\theta(\alpha^i) = \beta^i, \ \forall i = 1, 2, \dots, 100$ □

or

a	α	α^2	α^3	α^4	...	$\alpha^{100} = 1$
b	β	β^2	β^3	β^4	....	$\beta^{100} = 1$

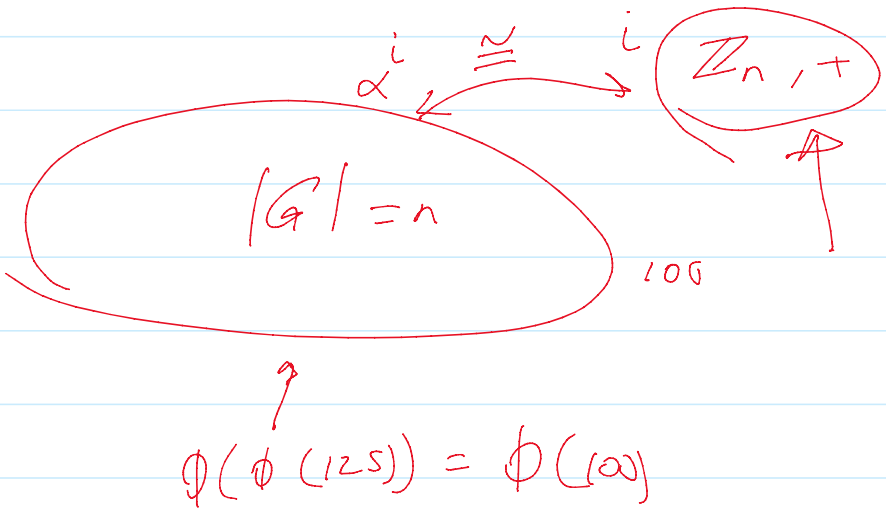
② To show θ is homomorphic

$$\theta(\alpha^i \cdot \alpha^j) = \theta(\alpha^{i+j})$$

$i+j$

$$\theta(\alpha \cdot \alpha) = \theta(\alpha^{\,}) = p^{i+j} = p^i \cdot p^j = \theta(\alpha^i) \cdot \theta(\alpha^j)$$

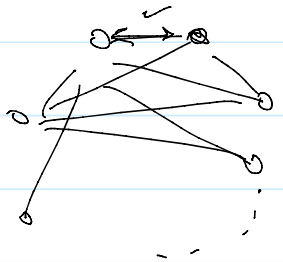
H/W □



HW 2

Exer 11. Forouzan's §3.

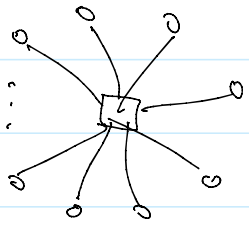
a) 100 members



$\frac{100(99)}{2} = 4950$

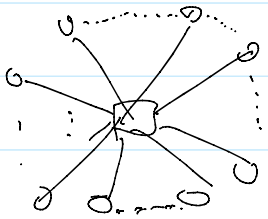
handshake theorem

b)



100 keys

c)



100 secret keys