Monday Week 8, October 10, 2016

continued from last time....

- theorem: Let G be a cyclic group and $H \leq G$, then H is cyclic.

proof: If $H = \{e\}$, then $H = \langle e \rangle$, so H is cyclic in this case

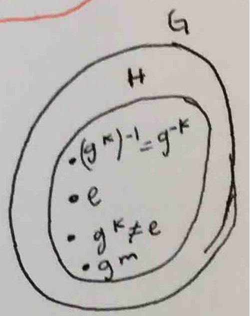
· Suppose $H \neq \{e\}$

since G is cyclic then $\exists\, g \in G$ s.t. $G = \langle g \rangle$

since $H \neq \{e\}$ then there must exist some $g^k \in H$ for some $k \in \mathbb{Z} \setminus \{0\}$
$\neq e$

if $k < 0$ then $(g^k)^{-1} = g^{-k} \in H$ since H is a subgroup.

so there must exist a positive power of g in H.



let $m > 0$ be the smallest positive integer w/ $g^m \in H$

claim: $H = \langle g^m \rangle$

Lets first show $\langle g^m \rangle \subseteq H$

since $g^m \in H$ and H is a subgroup we must have that

- $(g^m)^\ell \in H \;\; \forall\, \ell \in \mathbb{Z}$ (Because H is closed under the group operation and taking inverses.)

Now lets show $H \subseteq \langle g^m \rangle$

Let $h \in H$, then since $H \subseteq G$ and $G = \langle g \rangle$

we know that $h = g^w$ where $w \in \mathbb{Z}$.

By the division alorithm $\exists$ q and r where $w = qm + r$ and $0 \leq r < m$

Note that: $g^w = g^{qm+r} = (g^m)^q (g^r)$ so, $g^r = \underbrace{(g^m)^{-q}}_{\text{is in } H \text{ since } g^m \in H} \underbrace{(g^w)}_{\text{in } H} \in H$, since H is a subgroup of G

so $g^r \in H$ and $0 \leq r < m$

since m is the smallest positive integer with $g^m \in H$

we must have that $r = 0$.

- Thus $w = qm$ and $h = g^w = (g^m)^q \in \langle g^m \rangle$

so, $H \subseteq \langle g^m \rangle$

Example: Consider the cyclic group $\mathbb{Z}$

all the subgroups of $\mathbb{Z}$ are of the form

$$n\mathbb{Z} = \langle n \rangle = \{nk \mid k \in \mathbb{Z}\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

where $n \geq 0$ [this is because $\langle n \rangle = \langle -n \rangle$]

subgroups of $\mathbb{Z}$:

$n=0 \rightarrow \{0\}$

$n=1 \rightarrow \mathbb{Z}$

$n=2 \rightarrow 2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$n=3 \rightarrow 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$\vdots \qquad \vdots \qquad \vdots$ (forever and ever and ever and ever)

Lemma from homework: Let G be a group and $x \in G$, then $\langle x \rangle = \langle x^{-1} \rangle$

Example: Find all the subgroups of $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\rangle$

since $\mathbb{Z}_{12} = \langle \bar{1} \rangle$ we know that $\mathbb{Z}_{12}$ is cyclic.

so all its subgroups are cyclic.

All subgroups

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

$\langle \bar{1} \rangle = \mathbb{Z}_{12} = \langle \bar{11} \rangle$ since $\bar{1}$ and $\bar{11}$ are inverses.

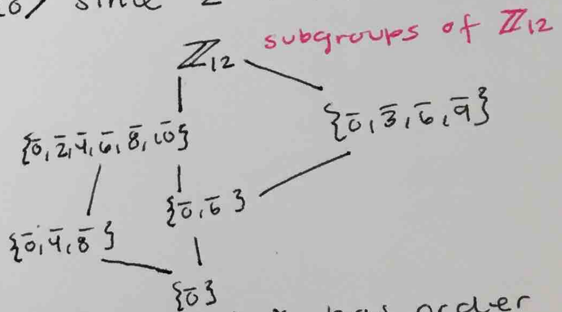
$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} = \langle \bar{10} \rangle$ since $\bar{2}$ and $\bar{10}$ are inverses

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = \langle \bar{9} \rangle$

$\langle \bar{4} \rangle = \langle \bar{8} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$

$\langle \bar{5} \rangle = \mathbb{Z}_{12} = \langle \bar{7} \rangle$

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



Lemma: Let G be a group. Suppose $x \in G$ and x has order n.
If $x^k = e$ for some $k \in \mathbb{Z}$ then n divides k

proof: x has order n means that n is the smallest positive integer with $x^n = e$. By the division algorithm $\exists\, q, r \in \mathbb{Z}$ s.t $k = nq + r$ and $0 \leq r < n$. Then

$$e = x^k = x^{nq+r} = \underbrace{(x^n)^q}_{e^q = e}(x^r) = x^r$$

so $x^r = e$ and $0 \leq r < n$ with n being the order of x.

so $r = 0$, so $k = nq$

Thus n divides k ∎

10/12 P.1 Wednesday Week 8, October 12, 2016

Ψ : psi

Proposition: (Homomorphism out of cyclic groups)

Let $G = \langle x \rangle$ be a cyclic group where $x \in G$

Let H be any other group

case 1 Suppose x has finite order n

Let $y \in H$ with order m. If m divides n, then $\varphi: G \to H$ defined by $\varphi(x^k) = y^k$ is a homomorphism.

Furthermore, any homomorphism $\Psi: G \to H$ must be of this form. [That is, there is a $y \in H$ with order dividing n and $\Psi(x^k) = y^k \ \forall k$]

case 2 Suppose x has infinite order

Let $y \in H$. Then $\varphi: G \to H$ defined by $\varphi(x^k) = y^k$ is a homomorphism. All homomorphism from G to H are of this form

[That is, if $\Psi: G \to H$ is a homomorphism then there exists $y \in H$ where $\Psi(x^k) = y^k$ for all k]

Example: $G = \mathbb{Z}_9 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$

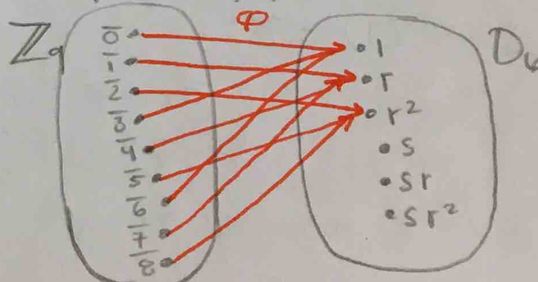
$H = D_6 = \{1, r, r^2, s, sr, sr^2\}$

Find all homomorphisms from $\mathbb{Z}_9$ to D_6

Possible y's

D_6	1	r	r^2	s	sr	sr^2
order	1	3	3	2	2	2

divide 9 — Do not divide 9



Case 1: Let $y = r$ (case 1)

- Send $\bar{1}$ to r
- Everything else is forced.

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

$\varphi(\bar{3}) = \varphi(\bar{1}+\bar{1}+\bar{1}) = \varphi(\bar{1})\varphi(\bar{1})\varphi(\bar{1}) = r \cdot r \cdot r = r^3 = 1$

$\mathbb{Z}_9 = \langle \bar{1} \rangle$

$x = \bar{1}$ has order 9

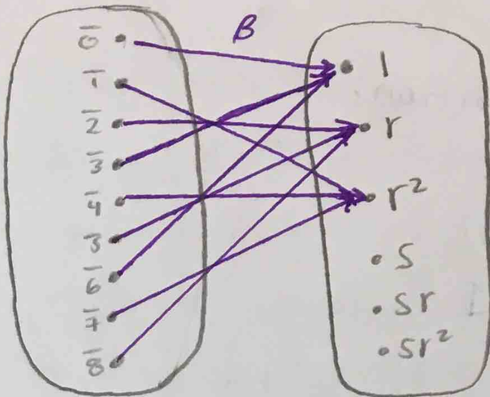
Case 2: let $y = r^2$

$\cdot\ \beta(\bar{1}) = r^2$

$\beta(\bar{2}) = \beta(\bar{1}+\bar{1}) = \beta(\bar{1})\beta(\bar{1}) = r^2r^2 = r^4 = r^3r = r$

$\beta(\bar{3}) = \beta(\bar{1}+\bar{1}+\bar{1}) = \beta(\bar{1})\beta(\bar{1})\beta(\bar{1}) = r^2r^2r^2 = r^3r^3 = 1$

$\beta(\bar{4}) = \beta(\bar{3}+\bar{1}) = \beta(\bar{3})\beta(\bar{1}) = 1 \cdot r^2 = r^2$

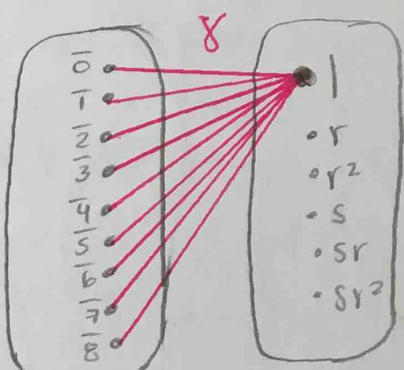


Case 3: The trivial Homomorphism

Let $y = 1$

$\gamma(\bar{1}) = 1$

$\gamma(\bar{2}) = \gamma(\bar{1}+\bar{1}) = \gamma(\bar{1})\gamma(\bar{1}) = 1 \cdot 1 = 1$



Example:

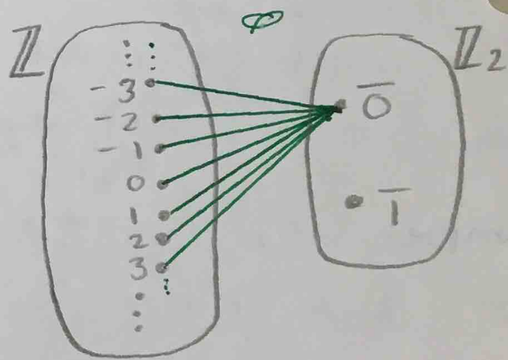
Find all homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_2$

$G = \mathbb{Z}, \quad H = \mathbb{Z}_2$

$\mathbb{Z} = \langle 1 \rangle$ and 1 has infinite order

$x = 1$

Since 1 has infinite order we can send it anywhere in $\mathbb{Z}_2$ to create a homomorphism.



Suppose $\varphi(1) = \bar{0}$

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

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

$\varphi(0) = \bar{0}$ ← identity

$\varphi(-1) = \bar{0}$

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

↑

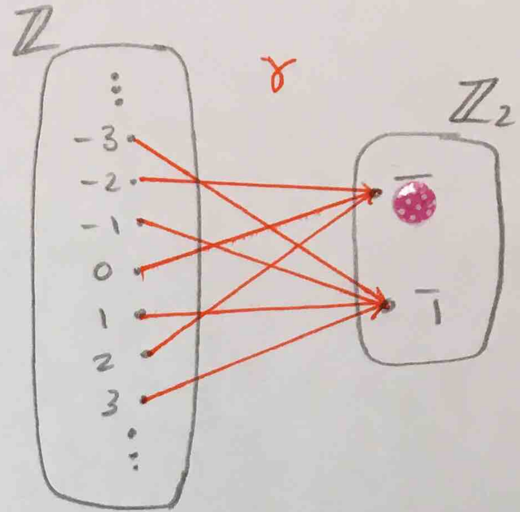
$\boxed{\varphi(a^{-1}) = [\varphi(a)]^{-1}}$

$a^{-1} = -1 \qquad \varphi(1) = \bar{0}$

$a = 1 \qquad \bar{0}^{-1} = \bar{0}$

10/12 P.2

Suppose $\gamma(1) = \bar{1}$



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

$\gamma(3) = \bar{1} + \bar{1} + \bar{1} = \bar{1}$

$\gamma(-1) = \gamma(1)^{-1} = \bar{1}^{-1} = \bar{1}$

$\gamma(-2) = \gamma(-1) + \gamma(-1) = \bar{1} + \bar{1} = \bar{0}$

- φ and γ are the only two homomorphisms

Example: $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

D_8 is not cyclic (no element has order 8) and not abelian

$H = \{1, r^2, sr^2, s\}$

$H \leq D_8$ and H is not cyclic but H is abelian (all elements of H have order 2, none have order 4)