Quiz

1) $(\mathbb{Z}_4, +_4) = G$ which are subgroups?

a) $\{0,1\}$

$1 +_4 1 = 2 \notin \{0,1\}$

$\{0,1\}$ not closed

$\Rightarrow$ not a subgp.

b) $\{0,2\}$.

1) $2 +_4 2 = 0$

$0 +_4 0 = 0$

$0 +_4 2 = 2$

closed.

2) $e = 0$

3) $2 +_4 2 = 0$

$\exists$ inverses in $\{0,2\}$.

$\boxed{\text{GROUP.}}$

c) $\{0,3\}$

not closed

d) $\{0,1,2\}$

not closed.

2) $G = \langle a \rangle$ $\quad |G| = 9$ $\quad H \leq G$ $\quad H = \langle a^3 \rangle = a * a * a$

$$\boxed{a^9 = e \in G}$$

$|H| = ?$

$$H = \{ (a^3)^0, a^3, (a^3)^2, \cancel{(a^3)^3} \} \quad |H| = 3.$$

$(a^3)^0 = e$, $\quad (a^3)^3 = a^9$

or apply Thm 6.14

3) $G = \langle a \rangle$ $\quad |G| = 7$ $\quad a^7 = e.$

$$a^{12} = a^{7 \cdot 1 + 5} = a^{7 \cdot 1} a^5 = e \cdot a^5 = a^5.$$

Native $a^{12} = a^{14-2} = \cancel{(a^7)^2}\, a^{-2} = a^{-2}.$ $\quad (a^7)^2 = e$

$\cancel{H}$

a^0, a^{-6}, a^7 $\quad a^7 = a^0.$

4) a) Cyclic groups only have trivial groups

FALSE $G = (\mathbb{Z}_4, +_4)$ cyclic $\{0,2\} \leq G$

non-trivial

b) Subgroups of cyclic groups are cyclic

Thm 6.6

<u>TRUE</u>

c) An infinite cyclic grp isomorphic to $(\mathbb{Z}, +)$

structure Thm. TRUE

d) Cyclic groups have unique generators FALSE

$(\mathbb{Z}, +)$ $\langle 1 \rangle = \{ n(1) \ n \in \mathbb{Z} \}$

$\langle -1 \rangle = \{ n(-1) \ n \in \mathbb{Z} \}$

Let $G = \langle a \rangle$ be a cyclic group of order

n. Cyclic $\Rightarrow$ $G = \{ a^n \mid n \in \mathbb{Z} \}$.

$|G| = n$.

$$G = \{ a^0, a^1, a^2, \dots, a^{n-1}, \overset{a^0}{\overset{\shortparallel}{a^n}}, \overset{a^1}{a^{n+1}}, \overset{a^2}{\dots} $$

No repeats. $a^i \neq a^j$ for $i \neq j$ and $0 \le i, j \le n-1$

So $a^n = e$.

Why is $a^{(n+m)} = a^{(m+n)}$?

(we used this fact in Thm 6.6

<u>Answer</u>. Here $n, m \in \mathbb{Z}$ and $n+m = m+n$ addition of integers is commutation.

$$a^{(n+m)} := (\underbrace{a * a * \cdots * a}_{n \text{ times}}) * (\underbrace{a * \cdots * a}_{m \text{ times}})$$

$$= (\underbrace{a * \cdots * a}_{m \text{ times}}) * (\underbrace{a * \cdots * a}_{n \text{ times}})$$

$$= a^{(m+n)}$$

This is really using associativity

(G1
$a * (a * a)$
$= (a * a) * a$.

Recap

Subgroups: **Thm** $H \leq G$ if
- H is closed
- $e \in H$ where e identity in G
- $\forall\, a \in H$ $a^{-1} \in H$ where a^{-1} inverse of $a \in G$.

- order of G is $|G|$.
- cyclic subgroups of G are $H = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ $a \in G$.

<u>Cyclic groups</u> : G is cyclic if $G = \{ a^n \mid n \in \mathbb{Z} \}$ for some $a \in G$.
Section 6.

Thm Structure thm G cyclic then

- if $|G| = \infty$ $G \cong (\mathbb{Z}, +)$
- if $|G| = n$ $G \cong (\mathbb{Z}_n, +_n)$.

- Thm subgroups of cyclic groups are cyclic

- Thm size of a subgroup $\langle a^s \rangle$ of a cyclic group $G = \langle a \rangle$ is $\dfrac{n}{\gcd(n,s)}$
$|G| = n$.

Exercise Fix r, s.

Show that $H = \{ nr + ms \mid n, m \in \mathbb{Z} \}$ is a subgroup of $(\mathbb{Z}, +)$.

Thm $H \leq G$ if
- H is closed $\boxed{0}$
- $e \in H$ where e identity in G. $\boxed{1}$
- $\forall a \in H$ $a^{-1} \in H$ where a^{-1} inverse of $a \in G$. $\boxed{2}$

Breakout room # n works on showing condition r where $n = 3q + r$.

Exercise Draw the subgroup diagram for

$(\mathbb{Z}_{24}, +_{24})$.