Recall

$(G, *)$ - group & $H \subseteq G$

$H \leq G$ iff

1) H is closed under $*$
2) Identity of G is in H, $e_G \in H$
3) Inverses of elems of H are in H

$\forall h \in H \quad h^{-1} \in H$

Multiplicative notation - Use $\cdot$ instead of $*$
or just write xy
instead of $x*y$

Theorem

Let G be a group

Let $H = \{a^n \mid n \in \mathbb{Z}\}$ where $a \in G$

Then H is a subgroup of G called **cyclic subgroup** of G denoted

$\langle a \rangle$

where a is called the **generator** of H

H is the smallest subgroup of G

containing a.

In additive groups,
$H = \langle a \rangle = \{ na \mid n \in \mathbb{Z} \}$

Proof

Notice $H = \{ a^n \mid n \in \mathbb{Z} \} \subseteq G$ by closure property bcs $a \in G$

$$\forall \underset{a^{n_1}}{n_1}, \underset{a^{n_2}}{n_2} \in H \quad n_1 \cdot n_2 = a^{n_1} \cdot a^{n_2}$$

$$= a^{n_1 + n_2}$$

$$= a^n \in H$$

bcs $n_1 + n_2 \in \mathbb{Z}$

hence H is closed under op induced from G

$\forall h \in H$, $h^{-1} = (a^n)^{-1} = a^{-n} \in H$

bcs $-n \in \mathbb{Z}$

$\therefore H \leq G$

Moreover, H is smallest subgroup of G

containing a bcs

if H' is a subgroup of G containg a, then H' has to contain H as a subgroup bcs H' contains all finite integral products of a by closure property.

__Example__

$$
\begin{tikzcd}
(\mathbb{Z}_4, +_4) = \langle 1 \rangle = \langle 3 \rangle \arrow[d, dash] \\
\{0, 2\} \arrow[d, dash] \\
\{0\} = \langle 0 \rangle
\end{tikzcd}
\qquad
\begin{tikzcd}
 & (\mathbb{Z}_2 \times \mathbb{Z}_2, +_2) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{(0,0),(0,1)\} = \langle (0,1) \rangle \arrow[dr, dash] & \{(0,0),(1,0)\} = \langle (1,0) \rangle \arrow[d, dash] & \{(0,0),(1,1)\} = \langle (1,0) \rangle \arrow[dl, dash] \\
 & \{(0,0)\} = \langle (0,0) \rangle &
\end{tikzcd}
$$

In general, the trivial subgroup of any group is cyclic bcs

$$\langle e \rangle = \{e\}$$

Definition

A group G is **cyclic** iff $\exists a \in G$, $\langle a \rangle = G$

(generated by a)

Notice:

For $(\mathbb{Z}_n, +_n)$, the generator a is

for $n=2$, $a=1$
for $n=3$, $a=1$, $a=2$
for $n=4$, $a=1$, $a=3$
for $n=5$, $a=1$, $a=2$, $a=3$, $a=4$
for $n=6$, $a=1$, $a=5$

In general,
a non-trivial (non-identity) element m of $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff
m is relatively prime to the order of the group, n, that is
$\gcd(m,n)=1$

If $n = p$ - prime #, then any nontrivial element of $\mathbb{Z}_n$ is a generator

$(\mathbb{Z}, +)$ is an example of an infinite cyclic group

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$$

Example

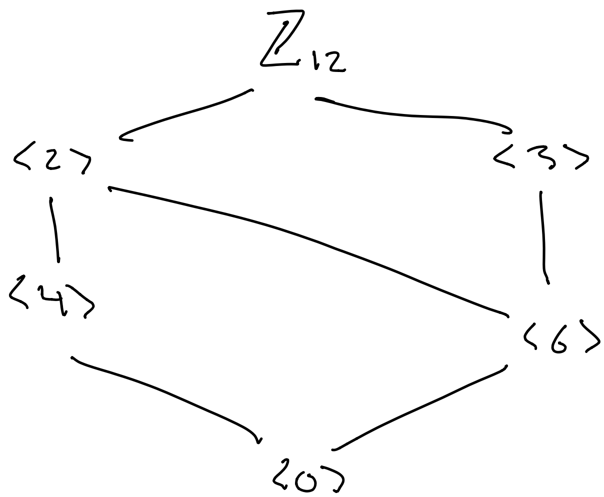
Find all subgroups of cyclic group $(\mathbb{Z}_{12}, +_{12})$

$$\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle, \langle 11 \rangle$$

$$\begin{array}{l} \text{nontrivial} \\ \text{proper} \\ \text{subgroups} \end{array} \left\{ \begin{array}{l} \langle 2 \rangle = \{2, 4, 6, 8, 10, 0\} = \langle 10 \rangle \\ \langle 3 \rangle = \{3, 6, 9, 0\} = \langle 9 \rangle \\ \langle 4 \rangle = \{4, 8, 0\} = \langle 8 \rangle \\ \langle 6 \rangle = \{6, 0\} \\ \langle 0 \rangle = \{0\} \end{array} \right.$$

$$\langle 4 \rangle \subset \langle 2 \rangle \Rightarrow \langle 4 \rangle \leq \langle 2 \rangle$$

$$\langle 6 \rangle \subset \langle 2 \rangle, \langle 3 \rangle \Rightarrow \langle 6 \rangle < \langle 2 \rangle, \langle 3 \rangle$$



Properties

Fact 1

Every cyclic group is abelian
(If G is cyclic group generated by $a \in G$, G is abelian)

Proof:

Since $G = \langle a \rangle$ where $a \in G$

$\forall g_1, g_2 \in G$ $\quad g_1 \cdot g_2 = a^{n_1} \cdot a^{n_2} = a^{n_1+n_2}$

$"a^{n_1}" \quad "a^{n_2}" \quad n_1, n_2 \in \mathbb{Z}$

$$= a^{n_2+n_1}$$

$$= a^{n_2} \cdot a^{n_1}$$

so op $\cdot$ in G is commutative

G is abelian

Note: The converse of fact 1 is not true

Fact 2

Every subgroup of a cyclic group is cyclic

Recall: Division algorithm in $\mathbb{Z}$

let $n \in \mathbb{Z}$ + $m \in \mathbb{Z}^+$

$\exists\, q, r \in \mathbb{Z}$ s.t.

$n = m \cdot q + r$ + $0 \leq r < m$

Proof:

If H is a trivial subgroup, then $H = \langle e \rangle$ is cyclic

let H be a nontrivial subgroup of $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

let m be least pos. int. s.t. $a^m \in H$

$\forall\, b \in H$ $\quad b = a^n \quad n \in \mathbb{Z}$

By Div. Alg.

$\exists q, r \in \mathbb{Z}$ $\quad n = m \cdot q + r$ & $0 \leq r < m$

Thus $b = a^n = a^{m \cdot q + r} = a^{m \cdot q} \cdot a^r$

$\Rightarrow a^r = a^n \cdot ((a^m)^q)^{-1} \in H$

$a^n \in H$ & $a^m \in H$ so by closure

$$(a^m)^q = \underbrace{a^m \cdots a^m}_{q} \in H$$

by inverse property

$(a^{mq})^{-1} \in H$

Since $a^r \in H$ & $0 \leq r < m$ &
m is the least pos. integer s.t.
$a^m \in H$, $r = 0$ hence

$$b = a^n = a^{mq+0} = (a^m)^q$$

which means $H = \langle a^m \rangle$
so H is cyclic

Fact 3

Let G be a cyclic group, then

1) If G is of finite order n

$$G \cong \mathbb{Z}_n \quad \text{for} \quad n \geq 2$$

2) If G is of infinite order

$$G \cong \mathbb{Z}$$

Proof :

Fact 4

Let G be a cyclic group of finite order n, generated by a

Let $b \in G$ s.t. $b = a^s$ for $s \in \mathbb{Z}$
$0 < s < n$

Then a subgroup generated by b ($\langle b \rangle$) is of order n/d where $d = \gcd(n, s)$

$$\overset{a^s}{\overset{\shortparallel}{\langle b \rangle}} = \langle a^t \rangle \text{ iff } \gcd(n,s) = \gcd(n,t)$$

In $\mathbb{Z}_{12}$:

$\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$ bcs

$\gcd(1,12) = \gcd(5,12) = \gcd(7,12) = \gcd(11,12)$

$|\langle 1 \rangle| = |\langle 5 \rangle| = |\langle 7 \rangle| = |\langle 11 \rangle| = \frac{12}{1} = 12$

$\langle 2 \rangle = \langle 10 \rangle$ bcs $\gcd(12,2) = \gcd(12,10) = 2$

$|\langle 2 \rangle| = |\langle 10 \rangle|$ is of order $12/2 = 6$

$\langle 3 \rangle = \langle 9 \rangle$ bcs $\gcd(12,3) = \gcd(12,9) = 3$

$|\langle 3 \rangle| = |\langle 9 \rangle| = 12/3 = 4$

$\langle 4 \rangle = \langle 8 \rangle$ bcs $\gcd(12,4) = \gcd(12,8) = 4$

$|\langle 4 \rangle| = |\langle 8 \rangle| = 12/4 = 3$

$|\langle 6 \rangle| = 12/6 = 2$