Recall: $a \in G$

$$\text{ord}(a) = \begin{cases} \text{smallest positive integer } n \text{ such that } a^n = e \\ \infty \quad \text{if } a^n \neq e \text{ for all } n > 0 \end{cases}$$

$$\langle a \rangle = \text{subgroup generated by } a = \{ a^k \mid k \in \mathbb{Z} \}$$

Lemma

(1) $\text{ord}(a) = |\langle a^k \rangle|$

(2) $b \in \langle a \rangle \Rightarrow \langle b \rangle \subseteq \langle a \rangle$

Proof

(1) Assume $\text{ord}(a) = m < \infty$

$$|\langle a \rangle| = |\{ e, a, \ldots, a^{n-1} \}| = m$$
Theorem
\[ \text{ord}(a) = n, \text{ fix } h \in \mathbb{Z} \]

(a) \[ \langle a^n \rangle = \langle a^{\gcd(h, n)} \rangle \]

(b) \[ \text{ord}(a^k) = \frac{n}{\gcd(k, n)} \]

Proof. Let \( d = \gcd(n, k) \)

(a) "C" \[ d = \gcd(n, k) \mid k \]

\[ \Rightarrow h = md \]

\[ \Rightarrow a^k = (a^d)^m \in \langle a^d \rangle \]

"C" \[ d = sm + tk \] for some integers \( s \) and \( t \)

\[ a^d = a^{sm + tk} = (a^m)^s (a^k)^t \]

\[ = (a^k)^t \in \langle a^k \rangle \Rightarrow \text{claim. (Use Lemma b)} \]
\[ \text{ord}(a^k) = \frac{1}{\langle a^k \rangle} = 1 \quad \langle a^d \rangle = 1 = \text{ord}(a^d) \]

Lemma a

\[ d = \gcd(m, n) | m \Rightarrow m \equiv m \mod d \]

\[ \Rightarrow (a^d)^j = a^{jd} = e \quad \text{if } 0 \leq j < m \]

(because then \( 0 \leq jd < md = n \) and hence \( a^{jd} = e \))

\[ \text{ord}(a) ! \]

and \( (a^d)^m = a^{md} = a^n = e \)

\[ \Rightarrow \text{ord}(a^d) = m = \frac{m}{d} \]

\[ \text{ord} (a^k) \]
Example: What is the order of 20 in \( \mathbb{Z}_{50} \)?

Recall: \( \mathbb{Z}_{50} \) is cyclic with generator 1 \( \equiv a \) (\( \text{ord}(a) = 1, \quad a^k \equiv 1 \) (translating to additive notation).

\[
\begin{align*}
\text{ord}(20) &= \gcd(20, 50) = 10 \\
n &= 50 = \text{ord}(1)
\end{align*}
\]

This was a special case of

**Corollary 1**

The order of \( m \) in \( \mathbb{Z}_n \) is equal to \( \gcd(m, n) \).

**Corollary 2**

Let \( G \) be a cyclic group \( |G| = n \)

\( b \in G \Rightarrow \text{ord}(b) \mid m \)

Proof:

Let \( a \) be a generator of \( G \), i.e., \( G = \langle a \rangle \)

\( \Rightarrow b = a^k \) for some \( k \).

\( \Rightarrow \text{ord}(b) = \gcd(k, n) \mid m \). \( \checkmark \)
Corollary 3: Which elements in \( G \) generate \( \langle a \rangle \)?

\[ \langle a^k \rangle = \langle a \rangle \iff \gcd(k, n) = 1 \]

Example: Assume \( \text{ord}(a) = 12 \), \( G = \langle a \rangle \)
Find all elem. \( b \) in \( G \) s.t. \( G = \langle b \rangle \)?

Solution: by corollary 3, \( b = a^k \) s.t. \( \gcd(k, 12) = 1 \)

Solution: \( k \in \{1, 5, 7, 11\} \)

i.e. \( \langle a \rangle = \langle a^5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle \)
Question: What are the possible subgroups of a cyclic group?

Theorem

Let \( G = \langle a \rangle \) cyclic

Any subgroup \( H \subset G \) is also cyclic, i.e. \( H = \langle a^k \rangle \) for some \( k \)

Proof

Let \( H \subset G \) be a subgroup

Let \( t \) be smallest positive integer such that \( a^t \in H \)
(assume \( H \neq \{e_3\} \))

Claim: any elem. in \( H \) is of the form \( a^m = (a^k)^n \) for some integer \( m \).

Proof

Let \( a^k \in H \)

Let \( k = tq + r \), \( 0 \leq r < t \)
$a^k = (a^t)^q a^r$

can solve for $a^r$, as $[(a^t)^q]^{-1} \in H$

$\Rightarrow a^r = (a^{tq})^{-1} a^k \in H$

If $r > 0$ \text{ contradicts } t \text{ smallest pos. integer } s.t. \ a^t \in H \ (as \ r < t !)\\
\Rightarrow r = 0$ \ i.e. \ $1 = tq$

$\Rightarrow b = a^k = (a^t)^q \in \langle a^t \rangle$ \ $\Rightarrow H \text{ cyclic.}$
Theorem: Let \( G \) be a finite cyclic group of order \( n \).

Then, there exists exactly one subgroup \( H \) for each divisor \( d \mid n \), and these are all subgroups of \( G \).

Proof: Follow from previous theorem and its proof.

We have seen that a cyclic group \( G \) contains a subgroup \( H \) generated by an element \( a \) such that

\[ H = \langle a \rangle = \langle \text{g.c.d.}(b, n) \rangle \]

where \( b \) is any divisor of \( n \). This subgroup is the first theorem today.

Example: Write down all subgroups of \( \mathbb{Z}_{12} \).

Answer: The subgroups are given by divisors of 12:

- Subgroups are
  - \( \langle 1 \rangle = \mathbb{Z}_{12} \)
  - \( \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle \)
  - \( \{0, 1, 2, 4, 6, 8, 10\} \)
  - \( \{0, 1, 4, 8\} \)