Fundamental Theorem of Cyclic Groups: Let $G = \langle x \rangle$ be a cyclic group.

1. If $H \leq G$, then $H = \{1\}$ or $H = \langle x^k \rangle$ where $k \in \mathbb{Z}^+$ is the smallest such that $x^k \in H$.

2. If $|G| = n$, then for each positive divisor $a$ of $n$, there is a unique subgroup of $G$ of order $a$. This subgroup is $\langle x^d \rangle$ where $d := n/a$.

   Furthermore, $\forall m \in \mathbb{Z}$, $\langle x^m \rangle = \langle x^{gcd(m,m)} \rangle$.

3. If $|G| = \infty$, then for any $a, b \in \mathbb{Z}^+$, $a \neq b$, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, $\forall m \in \mathbb{Z}$, $\langle x^m \rangle = \langle x^{\text{abs}(m)} \rangle$ where $\text{abs}(m)$ is the absolute value of $m$. 
Proof:
(1) Suppose \( G = \langle x \rangle \) and let \( H \leq G \).

If \( H = \{ e \} \), then \( H = \langle e \rangle \).

Let \( H \neq \{ e \} \) and let \( S := \{ n \in \mathbb{Z}^+ \mid x^n \in H \} \).

Since \( H \) is a nontrivial subgroup, \( \exists x \in H \) s.t. \( i \neq 0 \) and \( x^{-i} \in H \). Observe that either \( i \) or \( -i \) is positive, then \( S \neq \emptyset \). By the WOP, \( S \) has a smallest element, namely \( k \in \mathbb{Z}^+ \).

Claim: \( H = \langle x^k \rangle \)

(2) \( \triangleright \)

(\( \subseteq \)) Let \( h \in H \), then \( h = x^l \) for some \( l \in \mathbb{Z} \) because \( h \in G \).
By the Division Algorithm, \( l = kq + r \) s.t. \( 0 \leq r < k \). Consequently,

\[
 x^r = x^{l-kq} = x^l (x^{-k})^q = h (x^{-k})^q \in H \quad \text{because} \quad H \text{ is a subgroup, then} \quad r = 0.
\]

Since \( k \) is the smallest in \( S \) and \( 0 \leq r < k \), then \( r = 0 \). Therefore

\[
 h = x^l = (x^k)^q, \quad \text{i.e.} \quad h \in \langle x^k \rangle.
\]

(2)

Existence: Let \( a \mid n \) and \( a \in \mathbb{Z}^+ \), then \( \exists d \in \mathbb{Z}^+, n = da \).

Consider the subgroup \( \langle x^d \rangle \). Then \( |\langle x^d \rangle| = |x^d| = \frac{n}{\gcd(n,d)} = \frac{n}{d} = a \).

Uniqueness: Let \( H \leq G \) s.t. \( |H| = a \). By part (1), \( H = \langle x^b \rangle \) where \( b \in \mathbb{Z}^+ \) is the smallest s.t. \( x^b \in H \). Observe that

\[
 \frac{n}{d} = a = |H| = |x^b| = \frac{n}{\gcd(n,b)}.
\]
so \( d = \gcd(n, b) \). In particular, \( d \mid b \), i.e., \( b \) is a multiple of \( d \). Thus, \( H = \langle x^b \rangle \leq \langle x^d \rangle \). Since \( |H| = a = |\langle x^d \rangle| \), then \( H = \langle x^d \rangle \).

* Let \( m \in \mathbb{Z} \) and \( d = \gcd(m, n) \). Observe that \( \langle x^m \rangle \leq \langle x^d \rangle \). Moreover, 
\[
|x^m| = \frac{n}{d} \quad \text{and} \quad |x^d| = \frac{n}{\gcd(d, n)} = \frac{n}{d}.
\]
Therefore, \( \langle x^m \rangle = \langle x^d \rangle \).

(3) Exercise.
Summary: Let $G = \langle x \rangle$

1. $G$ is abelian
2. $|\langle x \rangle| = |x|$

$|\langle x \rangle| = n$

- $|x| = n$
- $x^i = x^j \iff i \equiv j \pmod{n}$
- $\langle x^a \rangle = \langle x \rangle \iff \text{gcd}(a,n) = 1$
- $a \mid n \Rightarrow \langle x^{na} \rangle$ is the only subgroup of order $a$
- $\forall m \in \mathbb{Z}, \quad \langle x^m \rangle = \langle x^{\text{gcd}(m,n)} \rangle$

Exercise: Write this summary in additive notation.

$|\langle x \rangle| = \infty$

- $|x| = \infty$
- $x^i = x^j \iff i = j$
- Only $x$ and $x^{-1}$ generate $\langle x \rangle$.
- Each $\langle x^a \rangle$, $a \in \mathbb{Z}^+$ is a different subgroup.
- $\forall m \in \mathbb{Z}, \quad \langle x^m \rangle = \langle x^{\text{abs}(m)} \rangle$
Examples:

1. Let $G = \langle a \rangle$ with $|a| = 30$. Find $\langle a^{26} \rangle$ and $\langle a^{17} \rangle$

   $\langle a^{26} \rangle = \langle a^{\gcd(30,26)} \rangle = \langle a^2 \rangle = \{ e, a^2, a^4, a^6, \ldots, a^{26}, a^{28} \}$

   $|\langle a^{26} \rangle| = |a^{26}| = \frac{30}{2} = 15$

   $\langle a^{17} \rangle = \langle a^{\gcd(30,17)} \rangle = \langle a \rangle = \{ e, a, a^2, \ldots, a^{29} \}$

2. Find all the generators of $\text{Rot} = \{ 1, r, r^2, \ldots, r^{11} \} \leq D_{24}$

   Since $|r| = 12$ then we have a generator $r^a$ if $\gcd(a,12) = 1$.

   Thus, $r^5$, $r^7$ and $r^{11}$ are generators of $\text{Rot}$. 
Let $G = \langle b \rangle$ and $|b| = 20$. Find all the subgroups of $G$.

We have a subgroup per each divisor of 20.

$1 | 20 \implies H_1 = \langle b^{20/1} \rangle = \{e\}$ \hspace{1cm} order 1

$2 | 20 \implies H_2 = \langle b^{20/2} \rangle = \langle b^{10} \rangle = \{e, b^{10}\}$ \hspace{1cm} order 2

$4 | 20 \implies H_4 = \langle b^{20/4} \rangle = \langle b^{5} \rangle = \{e, b^{5}, b^{10}, b^{15}\}$ \hspace{1cm} order 4

$5 | 20 \implies H_5 = \langle b^{20/5} \rangle = \{e, b^{4}, b^{8}, b^{12}, b^{16}\}$ \hspace{1cm} order 5

$10 | 20 \implies H_{10} = \langle b^{20/10} \rangle = \{e, b^{2}, b^{4}, b^{6}, b^{8}, b^{10}, b^{12}, b^{14}, b^{16}, b^{18}\}$ \hspace{1cm} order 10

$20 | 20 \implies H_{20} = \langle b \rangle = G$ \hspace{1cm} order 20
Lattice of subgroups of a group

- Order 20
  - \langle b \rangle
- Order 10
  - \langle b^2 \rangle
    - \langle b^4 \rangle
- Order 5
  - \langle b^5 \rangle
    - \langle b^{10} \rangle
- Order 2
  - \{e\}

\langle b^4 \rangle \text{ is a subgroup of } \langle b^2 \rangle
\langle b^5 \rangle \text{ is a subgroup of } \langle b \rangle
\langle b^{10} \rangle \text{ is a subgroup of } \langle b^4 \rangle \text{ and } \langle b^5 \rangle
Find all the subgroups of $\mathbb{Z}/12$ and draw the lattice diagram.

\(\mathbb{Z}/12\) is an additive group. Watch out!!!

\[
\begin{align*}
2|12 & \implies H_2 = \langle \left(\frac{12}{2}\right) [1] \rangle = \langle 6[1] \rangle = \langle [6] \rangle = \{ [0], [6] \} \\
3|12 & \implies H_3 = \langle \left(\frac{12}{3}\right) [1] \rangle = \langle 4[1] \rangle = \{ [0], [4], [8] \} \\
4|12 & \implies H_4 = \langle \left(\frac{12}{4}\right) [1] \rangle = \langle 3[1] \rangle = \{ [0], [3], [6], [9] \} \\
6|12 & \implies H_6 = \langle [2] \rangle = \{ [0], [2], [4], [6], [8], [10] \}
\end{align*}
\]
Find all subgroups of \( \mathbb{Z} \).

All subgroups of \((\mathbb{Z}, +)\) are of the form \( n\mathbb{Z} = \langle n \rangle = \langle -n \rangle \) with \( n \in \mathbb{Z}^+ \).

Also, \( n\mathbb{Z} \leq m\mathbb{Z} \iff m \mid n \). For instance, \( 1 \mathbb{Z} \leq 2 \mathbb{Z} \leq \cdots \leq 8 \mathbb{Z} \leq 4 \mathbb{Z} \leq 2 \mathbb{Z} \).
Group Homomorphisms and Isomorphisms

**Def:** A map of sets \( f: A \to B \) is well-defined if \( \forall a, a' \in A \) \( a = a' \Rightarrow f(a) = f(a') \).

**Def:** Let \((G, \ast)\) and \((H, \cdot)\) be groups. A well-defined map \( \phi: G \to H \) is called a homomorphism if

\[ \phi(a \ast b) = \phi(a) \cdot \phi(b) \quad \forall a, b \in G. \]

**Def:** A homomorphism \( \phi: G \to H \) is called

(1) a monomorphism if \( \phi \) is injective, i.e., the following condition is satisfied:

\[ \forall a, b \in G, \quad \phi(a) = \phi(b) \Rightarrow a = b \]
(2) an epimorphism if \( \varphi \) is surjective, i.e. the following condition is satisfied:

\[
\forall b \in H \exists a \in G \quad \varphi(a) = b.
\]

(3) an isomorphism if \( \varphi \) is injective and surjective. We say \( G \) and \( H \) are isomorphic.

**Notation:**

\( \varphi: G \hookrightarrow H \) monomorphism

\( \varphi: G \rightarrow H \) epimorphism

\( \varphi: G \xrightarrow{\cong} H \) isomorphism or \( G \cong H \)