Theorem. If \( G = \langle x \rangle \) is a cyclic group, then every subgroup of \( G \) is a cyclic subgroup.

Proof. Let \( H \) be a subgroup of \( G = \langle x \rangle \), such that \( H \neq \{e\} \). Let \( m = \min \{ k \in \mathbb{N} \setminus \{0\} \mid x^k \in H \} \).

Claim: \( H = \{ x^{lm} \in G \mid l \in \mathbb{Z} \} \).

First, \( \forall l \in \mathbb{Z}, \ x^{lm} = (x^m)^l \in H \) since \( x^m \in H \).

Second, suppose \( x^s \in H \), we will show \( m \mid s \):

Suppose \( m \nmid s \), then \( \exists q, r \in \mathbb{Z} \) such that 
\[
   s = qm + r, \quad 0 < r < m.
\]

This implies \( x^s = x^{qm \cdot r} \Rightarrow x^r \in H \).

Contradict to \( m = \min \{ k \in \mathbb{N} \setminus \{0\} \mid x^k \in H \} \).

So we conclude \( H = \{ x^{lm} \in G \mid l \in \mathbb{Z} \} = \langle x^m \rangle \).

Remark. A cyclic group may have more than one generators, as we have seen for the case of \( \mathbb{Z}^+ \).

In general, \( G = \langle x \rangle \) can be generated by \( x^k \) if and only if \( |x| \) and \( k \) are relatively prime.
**Homomorphism and Isomorphism**

**Definition.** $G$ and $G'$ are groups. A homomorphism $\varphi : G \rightarrow G'$ is a map satisfying $\forall a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$.

That is, the function is compatible with the group structures.

**Example.** Determinant function:

\[
\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*
\]

\[
A \mapsto \det(A)
\]

**Example.** $G$ is a group and $x \in G$.

Define $\varphi : \mathbb{Z}^+ \rightarrow G$

\[
k \mapsto x^k
\]

This is a homomorphism.

**Proposition.** A homomorphism $\varphi : G \rightarrow G'$ maps identity to identity and inverse to inverse:

1. $\varphi(1_G) = 1_{G'}$
2. $\forall g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$

**Proof.**

1. $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \cdot \varphi(1_G) \Rightarrow \varphi(1_G) = 1_{G'}$
2. $\varphi(g) \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(1_G) = 1_{G'} \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$

**Definition.** $\varphi : G \rightarrow G'$ is a homomorphism. Define:

\[
\ker \varphi = \{ g \in G \mid \varphi(g) = 1_{G'} \}, \text{ call the kernel of } \varphi
\]

\[
\text{Im } \varphi = \{ \varphi(g) \in G' \mid g \in G \}, \text{ call the image of } \varphi
\]
Proposition. \( \Psi: G \rightarrow G' \) is a homomorphism, then:
ker \( \Psi \) is a subgroup of \( G \) and \( \text{Im} \Psi \) is a subgroup of \( G' \).

Proof. If \( a, b \in \text{ker} \Psi \), \( \Psi(a) = \Psi(b) = 1_{G'} \).
\( \Psi(a \cdot b) = \Psi(a) \cdot \Psi(b) = 1_{G'} \cdot 1_{G'} = 1_{G'} \)
so \( a \cdot b \in \text{ker} \Psi \), hence \( \text{ker} \Psi \) is a subgroup of \( G \).

If \( x, y \in \text{Im} \Psi \), then there exists \( a, b \in G \) such that
\( x = \Psi(a) \), \( y = \Psi(b) \).
\( x \cdot y = \Psi(a) \cdot \Psi(b) = \Psi(a \cdot b) = \Psi(1_{G'}) \)
so \( x \cdot y \in \text{Im} \Psi \), hence \( \text{Im} \Psi \) is a subgroup of \( G' \).

Proposition. \( \Psi: G \rightarrow G' \) is a homomorphism, then:
\( \Psi \) is injective if and only if \( \text{ker} \Psi = \{1_G\} \).

Proof. If \( \Psi \) is injective, then it's obvious \( \text{ker} \Psi = \{1_G\} \), since
\( \text{ker} \Psi = \Psi^{-1}(1_{G'}) \) contains at most one element when
\( \Psi \) is injective, and \( \Psi(1_G) = 1_{G'} \).
If \( \text{ker} \Psi = \{1_G\} \), \( \Psi(a) = \Psi(b) \), then:
\( \Psi(a) \cdot \Psi(b)^{-1} = 1_{G'} \Rightarrow \Psi(ab^{-1}) = 1_{G'} \)
\( \Rightarrow a \cdot b^{-1} \in \text{ker} \Psi = \{1_G\} \)
\( \Rightarrow a \cdot b^{-1} = 1_G \)
\( \Rightarrow a = b. \)

So \( \Psi \) is injective.

Example. \( \text{det}: \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^* \) is a homomorphism.
\( \text{ker}(\text{det}) = \{A \in \text{GL}_n(\mathbb{R}) \mid \text{det}(A) = 1\} = \text{SL}_n(\mathbb{R}). \)