Section 6  Cyclic Groups.

Let's begin by looking at some special kinds of subgroups.

\[
\begin{align*}
\langle \sqrt{2} \rangle &= H = \{ \ldots, -\sqrt{2}, 0, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots \} = \{ n\sqrt{2} \mid n \in \mathbb{Z} \} \leq \mathbb{R} \\
\langle 3 \rangle &= H = \{ \ldots, -3, 0, 3, 6, 9, 12, \ldots \} = \{ n \cdot 3 \mid n \in \mathbb{Z} \} \leq \mathbb{R} \\
\langle 2 \rangle &= H = \{ 0, 2, 4, 6, 8, 10 \ldots \} = \{ n \cdot 2 \mid n \in \mathbb{Z} \} \leq \mathbb{Z}_4 \\
\langle 3 \rangle &= H = \{ 0, 1 \frac{1}{3}, 2 \frac{1}{3}, 1, 3, 9, 27, 81, \ldots \} = \{ 3^n \mid n \in \mathbb{Z} \} \leq \mathbb{R}^* \\
\langle i \rangle &= H = \{ 1, i, -1, -i \} = \{ i^n \mid n \in \mathbb{Z} \} \leq \mathbb{U} \\
\langle -1 \rangle &= H = \{ 1, -1 \} \leq \mathbb{U}
\end{align*}
\]

---

**Definition.** Given an element \( a \in G \), the following subgroup can be formed.

\[
H = \{ n \cdot a \mid a \in \mathbb{Z} \} \quad \text{(if operator is \( + \))}
\]

\[
H = \{ a^n \mid n \in \mathbb{Z} \} \quad \text{(if operator is \( \cdot \))}
\]

H is called the cyclic subgroup generated by \( a \).

**Notation:** \( H = \langle a \rangle \). \( a \) is a generator of \( H \).

---

**Example.** \( G = \mathbb{Z}_{12} \)

\[
\begin{align*}
\langle 1 \rangle &= \mathbb{Z}_{12} \\
\langle 2 \rangle &= \{ 0, 2, 4, 6, 8, 10 \} \\
\langle 3 \rangle &= \{ 0, 3, 6, 9 \} \\
\langle 4 \rangle &= \{ 0, 4, 8 \} \\
\langle 5 \rangle &= \{ 0, 5, 10, 3, 8, 11 \} \\
\langle 6 \rangle &= \{ 0, 6 \} \\
\langle 7 \rangle &= \{ 0, 7 \} = \langle 4 \rangle
\end{align*}
\]
Not every subgroup of $G$ is cyclic.

Examples:

\[
\langle U_n, \cdot \rangle = \{ e^0, e^1, e^2, \ldots \} = \{ e^n \mid n \in \mathbb{Z} \} = \langle e \rangle \\
\langle \mathbb{Z}_n^+, \cdot \rangle = \{ 0, 1, 2, \ldots, n-1 \} = \{ n \cdot 1 \mid n \in \mathbb{Z} \} = \langle 1 \rangle \\
\langle \mathbb{Z}, + \rangle = \{ n \mid n \in \mathbb{Z} \} = \langle 1 \rangle = \langle -1 \rangle \quad (1 \text{ and } -1 \text{ are generators}) \\
\langle 5\mathbb{Z}, + \rangle = \{ 5n \mid n \in \mathbb{Z} \} = \langle 5 \rangle = \langle -5 \rangle \quad (5 \text{ and } -5 \text{ are generators})
\]

Some groups are not cyclic.

\[
V = \{ 00, 10, 01, 11 \} \\
\langle 00 \rangle = \{ 00 \} \\
\langle 10 \rangle = \{ 00, 10 \} \\
\langle 01 \rangle = \{ 00, 01 \} \\
\langle 11 \rangle = \{ 00, 11 \}
\]

Definition. Group $G$ is cyclic if $\exists a \in G$ with $G = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$. (or $G = \langle a \rangle = \{ na \mid n \in \mathbb{Z} \}$)

Element $a$ is called the generator.
Properties of Cyclic Groups

Theorem  Every cyclic group is abelian.

Proof  Suppose \( G \) is cyclic, so \( G = \langle a \rangle \). For some \( a \in G \). If \( x, y \in G \), Then \( x = a^m \), \( y = a^n \) for integers \( m, n \). Then \( xy = a^m a^n = a^{m+n} = a^n a^m = yx \).

Theorem  Every subgroup of a cyclic group is cyclic.

Proof: Read the proof in text. Read it carefully.
Understand it.

Consequence  Every subgroup of \( \mathbb{Z} \) is of form \( \langle n \rangle = n\mathbb{Z} \).

Theorem  Suppose \( G \) is cyclic. Then either \( G \cong \mathbb{Z} \) or \( G \cong \mathbb{Z}_n \) for some \( n \in \mathbb{Z}^+ \).

Proof  Let \( G = \langle a \rangle \)
Case 1  Suppose \( G \) is finite. By homework \( a^n = e \) for some \( n \). Then \( G = \{e, a, a^2, a^3, \ldots, a^{n-1}\} \cong \mathbb{Z}_n \cong \mathbb{Z}_n \)

Case 2  Suppose \( G \) is infinite.
Then \( G = \langle a \rangle = \{e, a, a^2, a^3, \ldots\} \)
Define \( \phi : \mathbb{Z} \to G \) as \( \phi(n) = a^n \).
Homomorphism property: \( \phi(mn) = a^{mn} = a^m a^n = \phi(m) \phi(n) \)
Check \( \phi \) is 1-1 and onto. Thus, an isomorphism.