Section 6 Cyclic Groups.

Lets begin by looking at some special kinds of subgroups.

$\langle \sqrt{2} \rangle = H = \{\ldots, -\sqrt{2}, 0, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots\} = \{n\sqrt{2} \mid n \in \mathbb{Z}\} \leq \mathbb{R} \quad +$

$\langle 3 \rangle = H = \{\ldots, -3, 0\ 3, 6, 9, 12 \ldots\} = \{n \cdot 3 \mid n \in \mathbb{Z}\} \leq \mathbb{R} \quad +$

$\langle 2 \rangle = H = \{0, 2, 4, 6, 8, 10\} = \{n \cdot 2 \mid n \in \mathbb{Z}\} \leq \mathbb{Z}_4 \quad +_4$

$\langle 3 \rangle = H = \{\ldots, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, 81, \ldots\} = \{3^n \mid n \in \mathbb{Z}\} \leq \mathbb{R}^*$

$\langle i \rangle = H = \{1, i, -1, i\} = \{i^n \mid n \in \mathbb{Z}\} \leq U, \cdot$

$\langle -1 \rangle = H = \{1, -1\} \leq U$

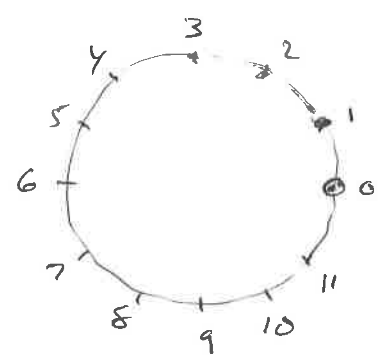
Definition Given an element $a \in G$, the following subgroup can be formed.

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

H is called the cyclic subgroup generated by a.

Notation: $H = \langle a \rangle$. a is a generator of H.

Ex $G = \mathbb{Z}_{12}$



$\langle 1 \rangle = \mathbb{Z}_{12}$

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$

$\langle 3 \rangle = \{0, 3, 6, 9\}$

$\langle 4 \rangle = \{0, 4, 8\}$

$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12}$

$\langle 8 \rangle = \{0, 8, 4\} = \langle 4 \rangle$

Not every subgroup of G is cyclic.

Ex $\mathbb{Q} \leq \mathbb{R}$ $\qquad$ $\mathbb{Q} \leq \mathbb{R}$

$U \leq \mathbb{C}^*$ $\qquad$ $U \leq \mathbb{C}^*$

Sometimes it happens that $\langle a \rangle = G$. Thats what this section is all about.

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

Examples:

$\langle U_n, \cdot \rangle = \{ \zeta^0\ \zeta^1\ \zeta^2 \cdots \} = \{ \zeta^n \mid n \in \mathbb{Z} \} = \langle \zeta \rangle$ $\left(\text{Note } \zeta^{-k} = (\zeta^{-1})^k = (\zeta^{n+1})^k = \zeta^{kn+k} \right)$

$\langle \mathbb{Z}_n\ +_n \rangle = \{ 0, 1, 2, \cdots n-1 \} = \{ n \cdot 1 \mid n \in \mathbb{Z} \} = \langle 1 \rangle$

$\langle \mathbb{Z}, + \rangle = \{ n \cdot 1 \mid n \in \mathbb{Z} \} = \langle 1 \rangle = \langle -1 \rangle$ (1 and -1 are generators)

$\langle 5\mathbb{Z}, + \rangle = \{ 5n \mid n \in \mathbb{Z} \} = \langle 5 \rangle = \langle -5 \rangle$ (5 and -5 are generators)

Some groups are not cyclic

$V = \{ 00, 10, 01\ 11 \}$

$\langle 00 \rangle = \{ 00 \}$

$\langle 10 \rangle = \{ 00, 10 \}$

$\langle 01 \rangle = \{ 00, 01 \}$

$\langle 11 \rangle = \{ 00\ 11 \}$

$\langle \mathbb{R}, + \rangle$

$\langle \mathbb{Q}^* \cdot \rangle$

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 cycli

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 $G = \{e, a, a^2, a^3, \ldots a^{n-1}\} \cong U_n \cong \mathbb{Z}_n$

Case 2 Suppose G is infinite.

Then $G = \langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, a^3, a^4, a^5 \ldots\}$

Define $\varphi : \mathbb{Z} \to G$ as $\varphi(n) = a^n$.

Homomorphism property: $\varphi(m+n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$

Check φ is 1-1 and onto, This is an isomorphism.