Cyclic Groups

Wednesday, March 4, 2026 9:47 PM

Recall: Groups

§ 2. Cyclic Groups

1] Notation: let $a \in G$,

$\langle a \rangle$ is the set of all elements generated by a.

Thus: $\langle a \rangle = \{ x \in G \mid x = a^n, \text{ for } n \in \mathbb{Z} \}$

e.g. $\mathbb{Z}_{11}^*$

$\langle 2 \rangle = \{ 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 \}$

$\langle 4 \rangle = \{ 4, 5, 9, 3, 1 \}$

2] Def^n. Let $\alpha \in G$. Then α is a generator of G if $\langle \alpha \rangle = G$.

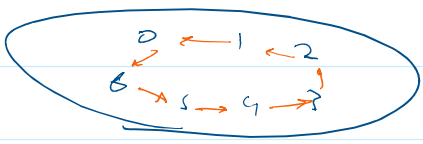
e.g. 2 is a generator (or primitive element) of $\mathbb{Z}_{11}^*$

3] Def^n. The group G is cyclic if it has a generator.

e.g. $\mathbb{Z}_{11}^*$ is cyclic.

4] Prop. Any group of a prime order is cyclic.

e.g. $(\mathbb{Z}_7, +)$



5] Lemma. Let $(G, *)$ be a group, and $a, b \in G$, with $a*b = b*a$, if the orders of a and b are co-prime, then

$$ord(a*b) = ord(a) \cdot ord(b)$$

6] Prop. Let $a \in G$

① if a has an infinite order, and $a^k = a^m$, then $k = m$.

② if $ord(a)$ is finite, and $a^k = e$ iff $ord(a) \mid k$

③ if $ord(a)$ is finite, then $\forall k, m \in \mathbb{Z}$, we have

$$a^k = a^m \quad \text{iff} \quad k \equiv m \pmod{ord(a)}$$