Cyclic Groups

Monday, March 1, 2021 8:43 AM

Recall : Group : $(G, \cdot)$

Subgroup

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

$$\langle a \rangle = \{ x \in G \mid x = a^n \text{ for some } n \}$$

e.g.

$\mathbb{Z}_{11}^*$, $a = 4 \in \mathbb{Z}_{11}^*$

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

$\langle 2 \rangle = \{2, 4, 8, 5, 10, 9, 7, 6, 12, 1\}$

$2 \in \mathbb{Z}_{10}$

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

i	4^i	2^i
1	4	2
2	5	4
3	9	8
4	3	5
5	1	10
6	4	9
7	5	7
8	9	3
9	3	6
10	1	1
11	4	2
12	5	4
⋮	⋮	⋮

Abdullah Eid

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 of $\mathbb{Z}_{11}^*$

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

i.e. $\exists\, \alpha \in G$, $\langle \alpha \rangle = G$

e.g. $\mathbb{Z}_{11}^*$ is cyclic, for $\langle 2 \rangle = G$

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

5] Lemma. Let $(G, *)$ be a group, and $a, b \in G$, with $a * b = b * a$.

if the order of a and b are relatively prime, then

if the order of a and b are relatively prime, then

$$\text{ord}(a*b) = \text{ord}(a) \cdot \text{ord}(b)$$

6] Prop. let $a \in G$,

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

② if a has finite order, then $a^k = e$ iff $\text{ord}(a) \mid k$

③ if a has finite order, and $k, m \in \mathbb{Z}$, then

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

e.g. In $\mathbb{Z}_{11}^*$, $a = 4$; $\text{ord}(a) = 5$

$$4^2 = 4^7 = 4^{12} = 4^{17}$$

7] Prop. let $a \in G$

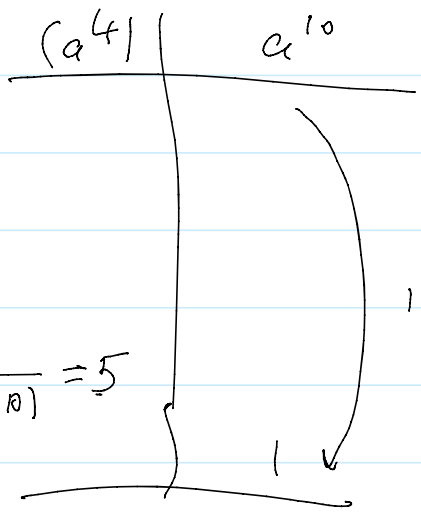
① The set $\langle a \rangle$ is a cyclic subgroup of G.

② $|\langle a \rangle| = \text{ord}(a)$

③ if K is a subgroup of G, with $a \in K$, then $\langle a \rangle \subseteq K$

④ $\forall n \in \mathbb{Z}^+$,

$$\text{ord}(a^n) = \frac{\text{ord}(a)}{\gcd(n, \text{ord}(a))}$$



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

$$\text{ord}(2^4) = \frac{\text{ord}(2)}{\gcd(4, \text{ord}(2))} = \frac{10}{\gcd(4,10)} = 5$$

$$\Rightarrow 2^4 = 5$$

$\Rightarrow 2^4 = 5$

$\Rightarrow 5^5 \equiv 1 \pmod{11}$