Cyclic groups

Wednesday, October 8, 2025 9:14 AM

Missing
100 # 1, 7, 15
200 # 12, 18, 24, 25
500 # Quiz 2

Recall: Group
$(G, \cdot)$

1] Notation: Let $a \in G$, the set of all elements generated by a is denoted $\langle a \rangle$

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

e.g. In $(\mathbb{Z}_9, +)$, $a = 3$

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

In $(\mathbb{Z}_{11}^*, \cdot)$, $a = 2$

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

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

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 of $\mathbb{Z}_{11}^*$ for $\langle 2 \rangle = \mathbb{Z}_{11}^*$

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

Thus $\exists\ \alpha \in G$, s.t. $\langle \alpha \rangle = G$.

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

$\mathbb{Z}_9$ is cyclic for $\langle 1 \rangle = \mathbb{Z}_9 = \langle 8 \rangle$

$$\langle 8 \rangle = \{8, 7, 6, 5, 4, 3, 2, 1, 0\}$$

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

5] Lemma. Let $(G, *)$ be a group, with $a, b \in G$, $a * b = b * a$.
If the orders of a and b are coprime 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 $a^k = a^j$, then $k = j$

② if a has a finite order, and $k \in \mathbb{Z}$, then

$$a^k = e \quad \text{iff} \quad \text{ord}(a) \mid k$$

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

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

7] Prop. Let $a \in G$, then

① $\langle a \rangle$ 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 $\forall n \in \mathbb{Z}^+$, $\text{ord}(a^n) = \dfrac{\text{ord}(a)}{\gcd(\text{ord}(a), n)}$

8] Prop. Let $G = \langle a \rangle$ then

① a^k generates G iff $\gcd(k, |G|) = 1$

② if positive $d \mid |G|$, then G has exactly one subgroup

② if positive $d \mid |G|$, then G has exactly one subgroup of order d.

③ if $d \mid |G|$, then G has exactly $\phi(d)$ elements of order d.

④ G has exactly $\phi(|G|)$ generators

Example:

$$\mathbb{Z}_{19}^* \Rightarrow |\mathbb{Z}_{19}^*| = \phi(19) = 18$$

$$\langle 2 \rangle = \{ \overset{-3}{2}, \overset{-6}{4}, \overset{-12}{8}, \overset{-5}{16}, \overset{-10}{13}, \overset{-1}{7}, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1 \}$$

e.g. [8]

$$\mathbb{Z}_{19}^*, \quad |\mathbb{Z}_{19}^*| = \phi(19) = 18$$

$$\langle 2 \rangle = \{ \overset{1}{2}, \overset{2}{4}, \overset{3}{8}, \overset{4}{16}, \overset{5}{13}, \overset{6}{7}, \overset{7}{14}, \overset{8}{9}, \overset{9}{18}, \overset{10}{17}, \overset{11}{15}, \overset{12}{11}, \overset{13}{3}, \overset{14}{6}, \overset{15}{12}, \overset{16}{5}, \overset{17}{10}, \overset{18}{1} \}$$

①

$2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$

$\Rightarrow$ 2, 13, 14, 15, 3, 10 are the generators

④ We have $\phi(18) = \phi(2 \cdot 3^2) = 1 \cdot 2 \cdot 3^1 = 6$ generators

② $d \mid 18 \Rightarrow q = 18/d$

d	② subgroup of order d	③ elements of order d
6	$q = 18/6 = 3$ $\{2^q, 2^{2q}, 2^9, 2^{12}, 2^{15}, 2^{18}\}$ $= \{8, 11, 12, 7, 18, 1\}$	Exactly $\phi(6) = 2$ elements of order 6 $(2^q)^1 = 8$, $(2^q)^5 = 18$
3	$\{2^6, 2^{12}, 2^{18}\}$ $= \{11, 7, 1\}$	Exactly $\phi(3) = 2$ elements of order 3 $2^6 = 11$, $2^{12} = 7$
2	$\{2^9, 2^{18}\}$ $= \{18, 1\}$	$2^9 = 18$ is of order 2
9	$\{2^2, 2^4, 2^6, 2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18} = 1\}$	$(\alpha = 2^q)^k$ $\gcd(k, 9) = 1$ $2^2, 2^4, 2^8, 2^{10}, 2^{14}, 2^{16}$ $\phi(9) = 6$ elements of order 9