# Primitive Roots

Wednesday, March 3, 2021 8:31 AM

B+1 #3

Recall: cyclic group

$\exists \alpha \in G, \ \langle \alpha \rangle = G$

Prop. 6. $a \in G$, $a^k = a^m$ iff $k \equiv m \pmod{ord(a)}$

Prop. 7. $ord(a^n) = ord(a) / gcd(n, ord(a))$

8] Prop. let $G = \langle \alpha \rangle$

① $\langle \alpha^k \rangle = G$ iff $gcd(k, |G|) = 1$ "relatively prime"

② for every positive divisor $d$ of $|G|$, $G$ has exactly one subgroup of order $d$.

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

④ $G$ has exactly $\Phi(|G|)$ generators.

e.g. $\mathbb{Z}_{11}^*$, $\langle 2 \rangle = \{\check{2}, 4, \check{8}, 5, 10, 9, \check{7}, 3, \check{6}, 1\}$, $|\mathbb{Z}_{11}^*| = 10$

① the generators are: $2^1, 2^3 = 8, 7, 6$

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

② $d = 5 \mid 10$, By consturction:

$q = 10/5 = 2 \implies H = \{(\alpha^q)^i \mid i = 1, 2, 3 \ldots\} = \{4, 5, 9, 3, 1\}$

③ $d = 5 \mid 10$, the elements $4^1, 4^2 = 5, 4^3 = 9, 4^4 = 3$ are of order 5.

9] Thrm: Every subgroup of a cyclic group is cyclic.

10] Def$^n$. The generators of $\mathbb{Z}_n^*$ are called primitive elements of $\mathbb{Z}_n^*$, or primitive roots of $n$.

11] Thrm: (Primitive roots)

11] Thm: (Primitive roots)

$n \geq 1$ has a primitive root iff $n = 2, 4, p^k, 2p^k$

where $p$ is a odd prime, $k \geq 1$

e.g. $\mathbb{Z}_{100}^*$ not cyclic $\longrightarrow$ $n = 100 = 2^2 \cdot 5^2$

$\mathbb{Z}_{17}^*$ cyclic $\longrightarrow$ $n = 17^1$

$\mathbb{Z}_{54}$ cyclic $\longrightarrow$ $n = 2 \cdot 3^3$

12] Def$^n$. Let $G_1, G_2$

$\theta : G_1 \longrightarrow G_2$ be a function

Then $\theta$ is said to be group isomorphism if:

① $\theta$ is a bijection

② $\theta(ab) = \theta(a)\,\theta(b) \quad \forall\, a, b \in G_1$

Here, $G_1$ is isomorphic to $G_2$, $G_1 \cong G_2$

Note: $\theta$ is called group homomorphism if ② holds

13] e.g. $(\mathbb{Z}_4, +) \cong (\mathbb{Z}_5^*, \cdot)$

$\theta : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_5^*$

| $x$ | 0 | 1 | 2 | 3 | $\mathbb{Z}_4$ |
|---|---|---|---|---|---|
| $\theta(x)$ | 1 | 2 | 4 | 3 | $\mathbb{Z}_5^*$ |

14] e.g. (Exponential function for groups)

Let $a \in G$, $(\mathbb{Z}, +)$

We show homomorphism by $\theta$ defined by

$\theta : \mathbb{Z} \longrightarrow G$

$\theta(n) = a^n \in G \quad \forall\, n \in \mathbb{Z}$

$\theta : \mathbb{Z} \to G$

$\theta(n) = a^n \in G \quad \forall\, n \in \mathbb{Z}$

Proof: $\theta(i+j) = a^{i+j} = a^i \cdot a^j = \theta(i)\,\theta(j)$

15]

**[15] Proposition.** If $\theta : G_1 \to G_2$ is a group homomorphism, then

**(a)** $\theta(e_1) = e_2$

**(b)** $(\theta(a))^{-1} = \theta(a^{-1})$ for all $a \in G_1$

**(c)** for any integer $n$ and any $a \in G_1$, we have $\theta(a^n) = (\theta(a))^n$

16]

**[16] Proposition.** Let $\theta : G_1 \to G_2$ be a group isomorphism. Then,

**(a)** $\forall\, a \in G_1$, $\text{ord}(a) = \text{ord}(\theta(a))$

**(b)** If $G_1$ is abelian, then so is $G_2$.

**(c)** If $G_1$ is cyclic, then so is $G_2$.