# Primitive Roots

Monday, March 9, 2026 9:08 PM

Recall: Cyclic groups

↘ $\langle \alpha \rangle = G$

7] Prop. Let $G$ be a group, and $a \in G$. Then

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

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

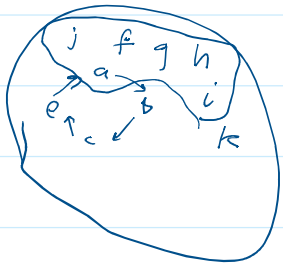
③ if $K$ is any subgroup of $G$, with $a \in K$, then $\langle a \rangle \subseteq K$

④ $\forall n \in \mathbb{Z}^+$, $\text{ord}(a^n) = \dfrac{\text{ord}(a)}{\gcd(n, \text{ord}(a))}$

e.g. $\mathbb{Z}_{13}^*$

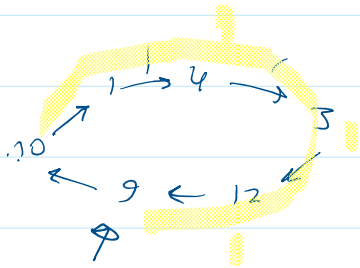
② $\langle 4 \rangle = \{4, 3, 12, 9, 10, 1\}$

③




④ $4^2 = 3$

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




$4^1 - 6$

$4^2 - 3$

$4^3 12 - 2$

$4^4 9 - 3$

$4^5 10 - 6$

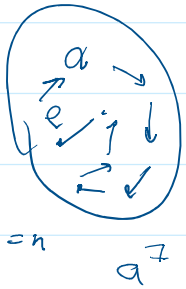
8] Prop. let $G = \langle \alpha \rangle$, then

① the element $\alpha^k$ generator iff $\gcd(k, |G|) = 1$

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 $\varphi(d)$ elements of order $d$.

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



e.g.

$\mathbb{Z}_{19}^*$, $\alpha = 2$

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

(2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18)

(-6 -12 -5 -10 -1)

① the generators $\alpha^k$, $\gcd(k, 18) = 1$

$2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$,

$= 2, 13, 14, 15, 3, 10$.

④ $\varphi(18) = \varphi(2 \cdot 3^2) = 1 \cdot 2(3^1) = 6$ generators

②, ③

| $d$ | Subgroup of order $d$ | elements of order $d$ |
|---|---|---|
| $d = 3$ | $\{ 2^6, 2^{12}, 2^{18} \}$ | We have $\varphi(3) = 2$ |
| $\Rightarrow q = 6$ | $= \{ 7, 11, 1 \}$ | 7, 11 |
| $d = 6$ | $\{ 2^3, 2^6, 2^9, 2^{12}, 2^{15}, 2^{18} \}$ | we have $\varphi(6) = 2$ |
| $\Rightarrow q = 3$ | $= \{ 8, 7, 18, 11, 12, 1 \}$ | 8, 12 |
| $d = 9$ | $\{ 4, 16, 7, 9, 17, 11,$ | $\varphi(9) = 2 \cdot 3^1 = 6$ |
| $\Rightarrow q = 2$ | $6, 5, 1 \}$ | 4, 16, 9, 17, 6, 5 |

9) Thm. 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) Thm. (Primitive Roots Theorem)

$n \in \mathbb{Z}^+$ has a primitive root iff.

$n = 2, 4, p^k$, or $2p^k$

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

e.g.

$100 = 2^2 \cdot 5^2 \implies$ no primitive roots

$125 = 5^3 \implies \mathbb{Z}_{125}^*$ is cyclic

$50 = 2 \cdot 5^2 \implies \mathbb{Z}_{50}^*$ has generators

12] Defn.

**[12] Definition.** Let $G_1$ and $G_2$ be groups, and let $\theta: G_1 \to G_2$ be a function. Then $\theta$ is said to be a ***group isomorphism*** if

**(i)** $\theta$ is a bijection (i.e. a one-to-one and onto function) and
**(ii)** $\theta(ab) = \theta(a)\,\theta(b)$ for all $a, b \in G_1$.

In this case, $G_1$ is said to be ***isomorphic*** to $G_2$, and this is denoted by $G_1 \cong G_2$.
Note: $\theta$ is called a ***group homomorphism*** if (ii) holds.

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

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

| $a$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $\theta(a)$ | 1 | 2 | 4 | 3 |

14] **[14] Example.** (Exponential functions for groups) Let $G$ be any group, and let $a \in G$. Define $\theta: \mathbf{Z} \to G$ by $\theta(n) = a^n$, for all $n \in \mathbf{Z}$. This is a group homomorphism from $\mathbf{Z}$ to $G$. If $G$ is abelian, with its operation denoted additively, then we define $\theta: \mathbf{Z} \to G$ by $\theta(n) = n \cdot a$.

$a \in G$

$\theta(n) = a^n$

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 $G_2$.

$\theta(n+m) = a^{n+m} = a^n \cdot a^m = \theta(n) \cdot \theta(m)$