$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ $\quad (\mathbb{Z}_5, \bar{+})$ ADDITION MODULO 5

$3 \bar{+} 4 = 3+4 \mod 5 = 2$

$4 \bar{+} 1 = 4+1 \mod 5 = 5 \mod 5 = 0$

$\mathbb{Z}_5 = \{\cancel{0}, 1, 2, 3, 4\}$ $\quad (\mathbb{Z}_5, \bar{\cdot})$ $\quad \mathbb{Z}_5^* = \mathbb{Z}_5 \setminus \{0\}$

$\phi(5) = 4$

$3 \bar{\cdot} 2 = 6 \mod 5 = 1$

$4 \bar{\cdot} 4 = 16 \mod 5 = 1$

$1 \bar{\cdot} 3 = 3 \mod 5 = 3$

THIS IS NOT A GROUP

THIS IS A GROUP

$\mathbb{Z}_6 = \{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5\}$ $\quad (\mathbb{Z}_6, \bar{\cdot})$ $\quad \mathbb{Z}_6^* = \{1, 5\}$

$5 \bar{\cdot} 5 = 25 \mod 6 = 1$ $\quad \phi(6) = 2$

$1 \bar{\cdot} 1 = 1$

THIS IS NOT A GROUP

THEOREM

IF $(\mathbb{G}, \cdot)$ IS A FINITE GROUP WHERE $|G| = m$ IS THE ORDER OF THE GROUP, THEN FOR EVERY $g \in \mathbb{G}$, IT HOLDS THAT $g^m = 1_{\mathbb{G}}$

PROOF

- LET'S PROVE THE THEOREM IN THE SPECIAL CASE IN WHICH THE GROUP IS ABELIAN.
- SUPPOSE THAT

$$\mathbb{G} = \{g_1, g_2, \dots, g_m\}$$

AND $g_i \neq g_j$ WHEN $i \neq j$

- LET'S FIX ANY ELEMENT $g \in \mathbb{G}$. WE WANT TO PROVE

$$g_1 \cdot g_2 \cdots g_m = (g g_1) \cdot (g g_2) \cdot \ldots \cdot (g g_m) \qquad (*)$$

ALL THE ELEMENTS ON THE RHS ARE DISTINCT, BECAUSE

$$g g_i = g g_j \Rightarrow g^{-1}(g g_i) = g^{-1}(g g_j)$$
$$\Rightarrow (g^{-1} g) g_i = (g^{-1} g) g_j$$
$$\Rightarrow g_i = g_j$$
$$\Rightarrow i = j$$

- SINCE $(\mathbb{G}, \cdot)$ IS ABELIAN, WE CAN REARRANGE $(*)$, OBTAINING THA

$$g_1 \cdot g_2 \cdot g_3 \ldots g_m = g^m \cdot (g_1 \cdot g_2 \cdot g_3 \cdot \ldots g_m)$$

WE CAN MULTIPLT BOTH SIDES BY $(g_1 \cdot g_2 \cdots g_m)^{-1}$, OBTAINING

$$\underbrace{(g_1 \cdots g_m) \cdot (g_1 \cdots g_m)^{-1}}_{1_{\mathbb{G}}} = g^m \cdot \underbrace{(g_1 \cdots g_m)(g_1 \cdots g_m)^{-1}}_{1_{\mathbb{G}}}$$

$$\Rightarrow 1_{\mathbb{G}} = g^m \cdot 1_{\mathbb{G}} \Rightarrow g^m = 1_{\mathbb{G}}$$