isomorphism
$\varphi : G_1 \to G_2$

- φ 1-1 and onto
- $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G_1$

<u>Ex</u> $G = \langle a \rangle$, $|a| = n$.

$G \approx \mathbb{Z}_n$

"is isomorphic to"

Recall: $G = \{ \underset{a^0}{e}, a, a^2, \ldots, a^{n-1} \}$

Define

$$\varphi : \langle a \rangle \to \mathbb{Z}_n$$

$$\varphi(a^k) = k \qquad (k \in \{0, 1, \ldots, n-1\})$$

1-1?
onto? } yes...direct.

and, if $0 \le k, p < n$

$$\varphi(a^k a^p) = \varphi(a^{(k+p) \bmod n}) = (k+p) \bmod n = \varphi(a^k)\varphi(a^p)$$

group operation in $\langle a \rangle$ — apply φ — group operation in $\mathbb{Z}_n$.

e.g. $|\langle a \rangle| = 8$ $\quad \varphi(a^4 a^6) = \varphi(a^{10}) = \varphi(a^2) = 2.$ $\quad a^{10} = a^2.$

and $\quad \varphi(a^4)\varphi(a^6) = (4+6) \bmod 8 = 10 \bmod 8 = 2.$

addition in $\mathbb{Z}_8$