Proposition: (characterization of order)

If G is a group and $x \in G$, then $o(x)$ is the smallest $n \in \mathbb{N}$ such that $x^n = e$.

proof: If $n \in \mathbb{N}$ is the smallest natural number with $x^n = e$, then $x^{n+1} = x^n \cdot x = e \cdot x = x$.

Similarly, for any positive power of x,

$$x^m = x^{[m]_n}.$$

Observe also that $(n \geq 2)$

$$e = x^n = x^{n-1} \cdot x$$

$$\Rightarrow \quad x^{n-1} = x^{-1}$$ by uniqueness

of the inverse.

Therefore,

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$$

$$\Rightarrow \quad o(x) = n.$$

Other direction next time!

Suppose $o(x) = n \in \mathbb{N}$.

Suppose $\exists\ k \in \mathbb{N}$, $k \leq n$,

$$x^k = e.$$

Then the powers

$$\{e, x, x^2, \ldots, x^{k-1}\}$$

form a subgroup of G by

exactly the same argument

that $\{e, x, x^2, \ldots, x^{n-1}\}$

form a subgroup.

Since $x \in \{e, x, x^2, \ldots, x^{k-1}\}$, We know that

$$\{e, x, x^2, \ldots, x^k\} \subseteq \langle x \rangle$$

We assumed that $o(x) = n$,

So $n = o(x) = |\langle x \rangle| \leq |\underbrace{\{e, x, x^2, \ldots, x^k}_{k}\}|$

We assumed that

$k \leq n$, and we have

proved that $n \leq k$.

Therefore, $n = k$.

$\square$

Theorem: (characterization of cyclic groups)

Let G be a cyclic group.

Then either

1) G is isomorphic to $\mathbb{Z}$

or

2) $\exists\ n \in \mathbb{N}$ with

G isomorphic to $\mathbb{Z}_n$.

proof: Suppose $|G| = \infty$.

Since $\exists\ x \in G$ with

$G = \langle x \rangle$,

then $\forall\ h \in G$, $\exists$

$n \in \mathbb{Z}$ with

$$h = x^n.$$

Define

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

$$\varphi(x^n) = n.$$

φ is surjective by construction.

Now suppose

$$n = \varphi(x^n) = \varphi(x^m) = m$$

We then have

$$x^n = x^m$$

$$\Rightarrow \quad x^{m-n} = e.$$

This shows φ is injective.

Why is φ well-defined?

Suppose $x^m = x^n$.

Then $x^{m-n} = e$

If $m-n \neq 0$, then

$\exists \ k \in \mathbb{N}$ with

$$x^k = e$$

Then by the previous proposition,

$$|G| = |\langle x \rangle| = k.$$

This can't happen since we assumed $|G|$ is infinite.

So φ is well-defined.

Last, we need to check that

$$\varphi(h_1 h_2) = \varphi(h_1) + \varphi(h_2)$$

$\forall\ h_1, h_2 \in G.$

We know $\exists\ n, m \in \mathbb{N}$

with

$$h_1 = x^n, \quad h_2 = x^m.$$

Then

$$h_1 h_2 = x^{n+m} \quad \text{and}$$

$$\varphi(h_1 h_2) = n+m$$

$$= \varphi(h_1) + \varphi(h_2) \checkmark$$

Therefore, φ is an isomorphism,

If $|G| < \infty$, take a generator

$x \in G$, $G = \langle x \rangle$.

Define

$$\varphi : G \to \mathbb{Z}_{|G|}$$

$$\varphi(x^m) = [m] \bmod |G|$$

Reduce

$$\varphi(x^m x^n),$$

$$\varphi(x^m) + \varphi(x^n)$$

mod $|G|$ to get that

$$\varphi(x^m x^n) = \varphi(x^m) + \varphi(x^n)$$

$\square$