Recall: A cyclic group $G = \langle a \rangle$ is one of two "flavors"

Case 1: $|G| = |a| = \infty$. Then we proved

for all $k, l \in \mathbb{Z}$, $k \neq l \Rightarrow a^k \neq a^l$.

Thus,

$$G = \{a^k \mid k \in \mathbb{Z}\} = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, \ldots\},$$

↑ distinct elements

and multiplication in G corresponds to addition of exponents.

Here is an alternative way to say this: The function

$$\begin{aligned} f: \mathbb{Z} &\longrightarrow G = \langle a \rangle \\ k &\longmapsto a^k \end{aligned}$$

is a bijection, and

$$f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) \cdot f(l)$$

for all $k, l \in \mathbb{Z}$.

Such a function is called an <u>isomorphism</u>, and we say that $\mathbb{Z}$ and G are <u>isomorphic</u> groups.

Essentially, this says that $\mathbb{Z}$ and G are "the same group," it's just that we've labeled the elements (and the group operation) differently.

So

$$\boxed{\text{Every infinite cyclic group is isomorphic to — i.e., it "looks the same as" — the group of integers } \mathbb{Z}.}$$

Something similar happens for finite cyclic groups.

Case 2: $|G| = |a| = n \in \mathbb{N}$.

Then we proved that for all $k, l \in \mathbb{Z}$ with $0 \le k, l \le n-1$,

$$k \ne l \implies a^k \ne a^l.$$

Slightly more generally, if $k, l \in \mathbb{Z}$, then

$$a^k = a^l \iff n \mid (l-k)$$

$$\iff k \equiv l \pmod{n}.$$

It follows that

$$G = \{e, a, a^2, \dots, a^{n-1}\}$$

distinct elements

and multiplication in G corresponds to addition of exponents modulo n.

Equivalently, this says that the function

$$\varphi : \mathbb{Z}_n \to G = \langle a \rangle$$
$$k \mapsto a^k$$

<u>Note</u>: This is well-defined!

is an isomorphism.

Thus,

$$\boxed{\text{Every cyclic group of finite order } n \text{ is isomorphic to } \mathbb{Z}_n.}$$

The order of a^k

Lemma: Let G be a group and let $a \in G$ be an element of finite order.

If $a^m = e$ for some $m \in \mathbb{Z}$, then $|a|$ divides m.

Proof: We have already proved this:

$$a^m = e = a^0 \iff n \mid (m-0),$$

where $n = |a|$.

$\blacksquare$

Lemma: Let $x, y, z \in \mathbb{N}$. If $x \mid yz$ and $\gcd(x,y)=1$, then $x \mid z$.

Proof: Math 3345 (look at unique prime factorizations).

$\blacksquare$

Thm: Let G be a group and $x \in G$.

① If $|a| = \infty$, then $|a^k| = \infty$ for all $k \in \mathbb{N}$.

② If $|a| = n \in \mathbb{N}$, then

$$|a^k| = \frac{n}{\gcd(n,k)}$$

for all $k \in \mathbb{N}$.

Note: $|a^{-k}| = |a^k|$, so this tells us the orders of negative powers too (HW 7).

Proof: ① We prove the contrapositive.

Suppose $|a^k| \neq \infty$, so $|a^k| = m \in \mathbb{N}$.

Then

$$(a^k)^m = a^{km} = e,$$

where $km \in \mathbb{N}$. Thus, $|a| \leq km$ is finite. ✓

② Suppose $|a| = n \in \mathbb{N}$, and let $d = \gcd(n,k)$.

Then

$$(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e,$$

Note: $\frac{n}{d}, \frac{k}{d} \in \mathbb{N}$ since $d = \gcd(n,k)$.

so $|a^k|$ is finite. Write $|a^k| = m \in \mathbb{N}$.

By the first lemma, $\boxed{m \mid \frac{n}{d}.}$

On the other hand,

$$(a^k)^m = a^{km} = e,$$

so the lemma also tells us that $n \mid km$.

This means $km = n\ell$ for some $\ell \in \mathbb{N}$. Dividing by d, we have

$$\frac{k}{d} \cdot m = \frac{n}{d} \cdot \ell.$$

So $\frac{n}{d} \mid \left(\frac{k}{d} \cdot m\right)$. But $\gcd\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ (Why?), so the second lemma yields $\boxed{\frac{n}{d} \mid m.}$

Since $\frac{n}{d}$ and m are positive integers dividing each other, we have $m = \frac{n}{d}$, as desired. ✓

■

Corollary: Let $G = \langle a \rangle$ be a cyclic group generated by a.

① If $|a| = \infty$, then a^k generates G if and only if $k = \pm 1$.

② If $|a| = n \in \mathbb{N}$, then a^k generates G if and only if $\gcd(n, k) = 1$.

Proof: ① Let $k \in \mathbb{Z}$ and suppose $\langle a^k \rangle = G$. Then $a \in G = \langle a^k \rangle$, so

$$a = (a^k)^\ell = a^{k\ell}.$$

for some $\ell \in \mathbb{Z}$.

Since $|a| = \infty$, its powers are distinct. Thus, $1 = k\ell$, so either

$$k = \ell = 1 \quad \text{or} \quad k = \ell = -1. \quad \checkmark$$

② If $|a| = n$, then $|G| = n$, so $\langle a^k \rangle = G$ if and only if $|a^k| = n$ also.

By the theorem, this is equivalent to

$$\frac{n}{\gcd(n,k)} = n,$$

i.e., $\gcd(n,k) = 1$. $\blacksquare$