Recall: For $a \in G$, $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is the <u>cyclic subgroup</u> of G generated by a.

Def: Let G be a group. If

$$G = \langle a \rangle$$

for some $a \in G$, then we say that G is a <u>cyclic group</u> and a is a <u>generator</u> of G.

Ex: $\mathbb{Z}$ is cyclic, and 1 is a generator. -1 is also a generator.

Ex: $\mathbb{Z}_{12}$ is cyclic, and 1 is a generator.

What are other generators?

Ex: $U(12)$ is <u>not</u> cyclic, since $\langle a \rangle \neq U(12)$ for all $a \in U(12)$.

Ex: $U(9) = \{1, 2, 4, 5, 7, 8\}$ is cyclic.

One generator is 2. (Check!)

Properties of cyclic groups

Thm: Every cyclic group is abelian.

Proof: Let $G = \langle a \rangle$ be a cyclic group with generator a.

Let $g, h \in G$. Then $g = a^k$ and $h = a^l$ for some $k, l \in \mathbb{Z}$, so

$$gh = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = hg.$$

$\blacksquare$

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

① If $|a| = n \in \mathbb{N}$, then

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

are distinct elements of G (i.e. no two are equal).

② If $|a| = \infty$, then for all $k, l \in \mathbb{Z}$, if $k \neq l$, then $a^k \neq a^l$.

Proof: First, suppose $k, l \in \mathbb{Z}$ with

$$a^k = a^l.$$

Then $e = a^l \cdot (a^k)^{-1} = a^l a^{-k} = a^{l-k}$.

For ①, note that if $0 \leq k \leq l \leq n-1$, then $0 \leq l-k \leq n-1$. Since $|a| = n$, $a^{l-k} = e$ is only possible when $l = k$.

For ②, $a^{l-k} = e$ implies $l-k=0$ when $|a|=\infty$. Hence $a^k = a^l$ implies $l=k$. ∎

Corollary: Let $G = \langle a \rangle$ be a cyclic group with generator a. Then $|G| = |a|$.

Proof: Either $|a| < \infty$ or $|a| = \infty$.

Case 1: $|a| = n \in \mathbb{N}$.

Then $e = a^0, a^1, \dots, a^{n-1} \in G$ are distinct elements by the theorem, so $|G| \geq n$.

On the other hand, let $g \in G$. Then $g = a^k$ for some $k \in \mathbb{Z}$. By the division algorithm,

$$k = nq + r$$

for unique $q, r \in \mathbb{Z}$ with $0 \le r \le n-1$.

Thus,

$$g = a^k = a^{nq+r}$$
$$= (a^n)^q a^r$$
$$= e^q a^r$$
$$= a^r.$$

That is, $g \in \{e, a, \ldots, a^{n-1}\}$, proving $|G| \le n$.

Together, we have $|G| = n$.

<u>Case 2</u>: $|a| = \infty$.

By the theorem, $|G| = |\langle a \rangle| = \infty$, since $a^k \neq a^l$ for integers $k \neq l$.

$\blacksquare$

Corollary: If G is a finite group, then $|a| \leq |G|$ for all $a \in G$, with equality if and only if $G = \langle a \rangle$.

Proof: By the previous corollary, $\langle a \rangle$ is a subset of G of cardinality $|a|$.

The result then follows. $\blacksquare$

Subgroups of a cyclic group

Thm: Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a \rangle$ be a cyclic group with generator a.

Suppose $H \leq G$ is a subgroup.

Case 1: $H = \{e\}$ is the trivial subgroup.

Then $H = \langle e \rangle$ is cyclic.

Case 2: H is nontrivial.

Then, since $G = \langle a \rangle$, H must contain some nonzero power of a.

Let $k \in \mathbb{N}$ be the smallest positive integer such that $a^k \in H$.

Note: Since H is closed under inverses, and $H \neq \{e\}$, H must contain some positive power of a.

Claim: $H = \langle a^k \rangle$, so H is cyclic.

Since $a^k \in H$, we have $\langle a^k \rangle \leq H$. So we only need to prove the reverse containment.

Let $h \in H$. Then, since $h \in G = \langle a \rangle$, we have $h = a^m$ for some $m \in \mathbb{Z}$.

By the division algorithm,

$$m = kq + r$$

for $q, r \in \mathbb{Z}$ with $0 \leq r \leq k-1$.

Thus,

$$\underbrace{h}_{\in H} = a^m = \underbrace{(a^k)^q}_{\in H} \cdot a^r,$$

so by closure we have

$$a^r = h(a^k)^{-q} \in H.$$

Since $0 \leq r < k$, we must have $r = 0$ by minimality of k.

Hence, $h = (a^k)^q \in \langle a^k \rangle$, proving $H \leq \langle a^k \rangle$, as desired.

$\blacksquare$