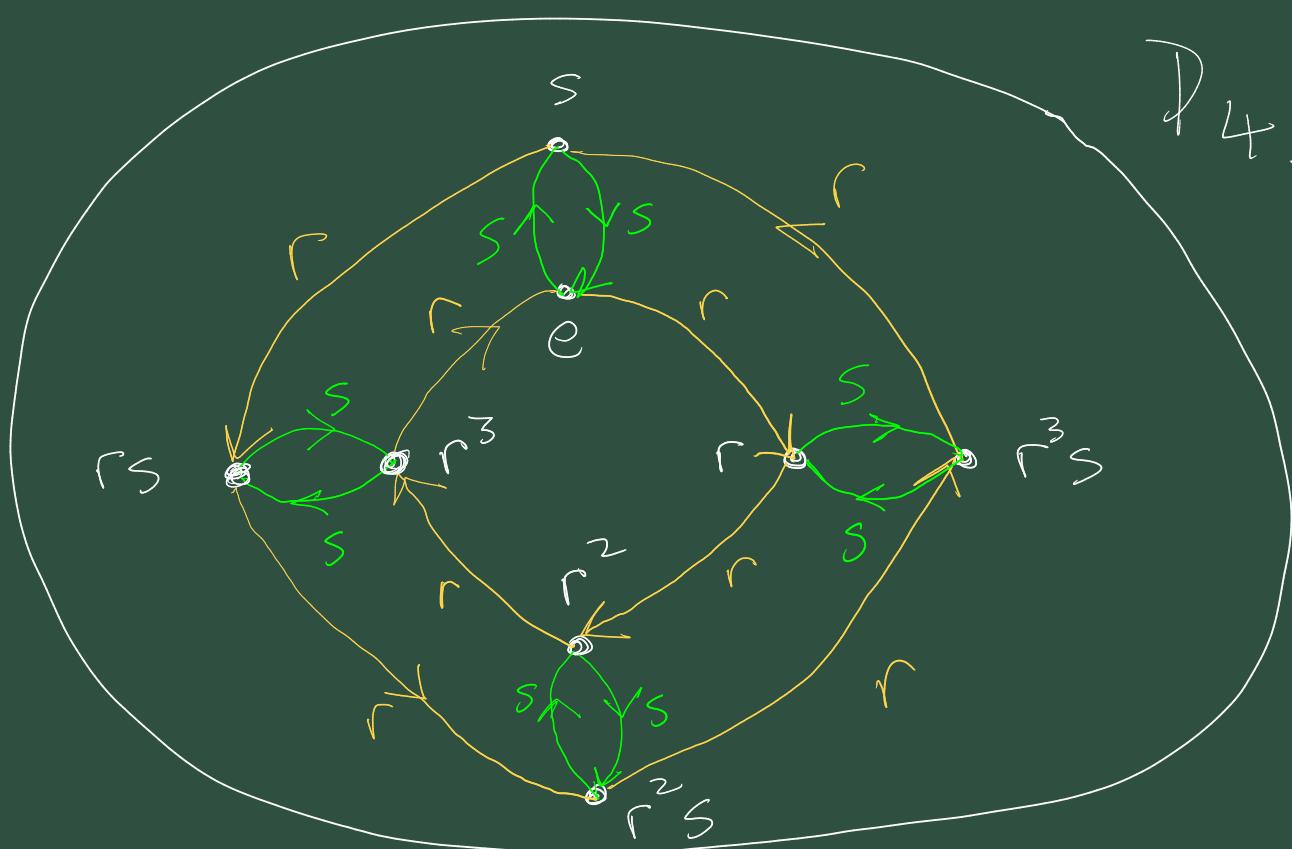


Can also represent the reflections as the products $\{s, rs, r^2s, r^3s\}$

where s is one of the reflections.

Remember products in D_4 are compositions of the transformations.

Let's draw a Cayley diagram to "show" this group.



$$sr^3 = r^{-1}sr^2 = r^{-2}sr = r^{-3}s = r s$$

We can see here two "cyclic subgroups" of D_4 .

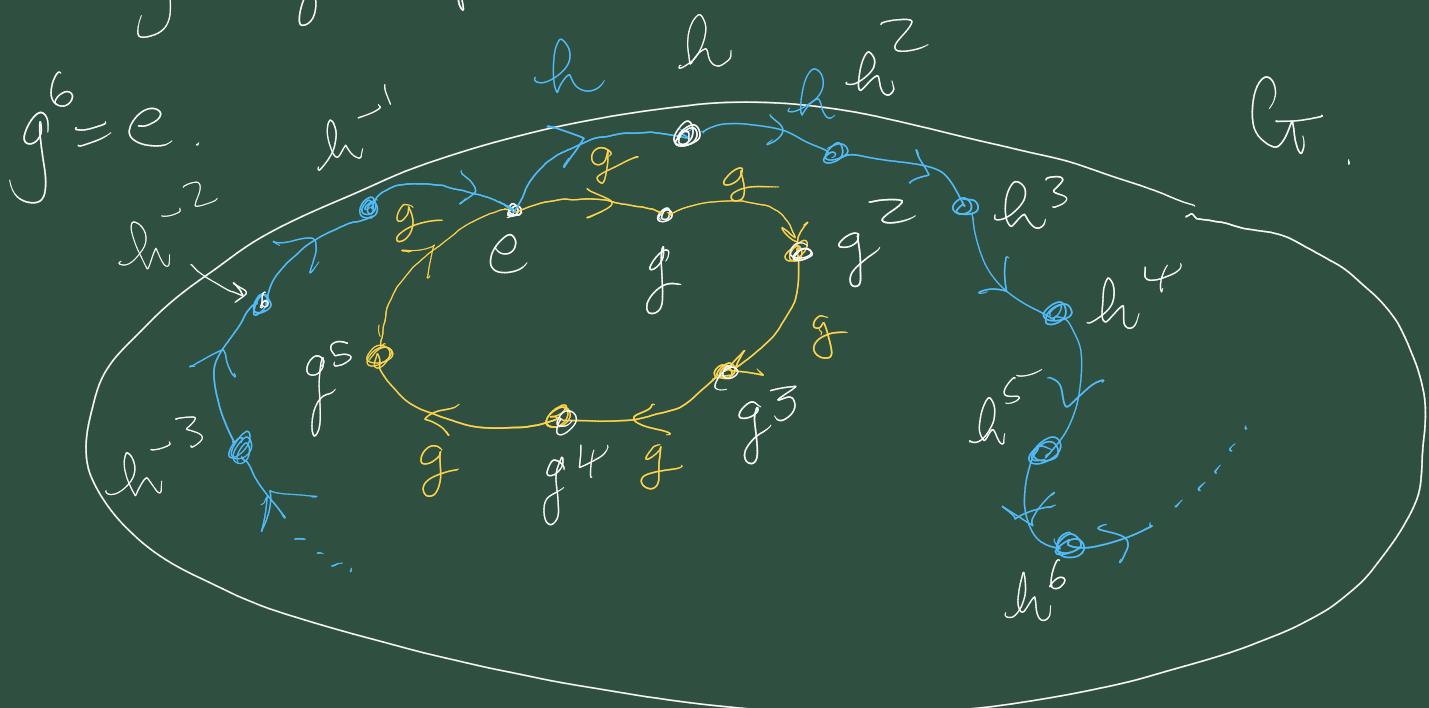
$$H_1 = \{e, r, r^2, r^3\}$$

$$H_2 = \{e, s\}$$



and in a sense we see that D_4 is composed of these two cycles / cyclic subgroups

This approach can be taken to any group



I'm suggesting the existence of two cyclic subgroups of G

$H_1 = \{e, g, g^2, g^3, g^4, g^5\}$ a finite cyclic subgroup

$H_2 = \{e, h, h^2, h^3, h^4, \dots, h^{-1}, h^{-2}, h^{-3}, h^{-4}, \dots\}$ an infinite cyclic subgroup

4.1. Other motivating examples.

Theorem 4.3.

Take a group G and element $a \in G$.
Then the set

$$\langle a \rangle := \left\{ a^k : k \in \mathbb{Z} \right\}$$

“power” in the group sense

forms a subgroup of G .

Moreover it's the smallest subgroup of

G containing a , i.e. given any subgroup H of G , if $a \in H$ then $\langle a \rangle \subseteq H$.

Proof Use prop 3-30 to show $\langle a \rangle$ is a subgroup of G .

$$|a| = \text{"order" of } a$$

= smallest positive integer exponent
 $k > 0$ such that $a^k = e$.

or $= \infty$ if no such k exists.

$$|a| = |\langle a \rangle|$$

↑
order
of a

↑
| subset |

= cardinality of subset.

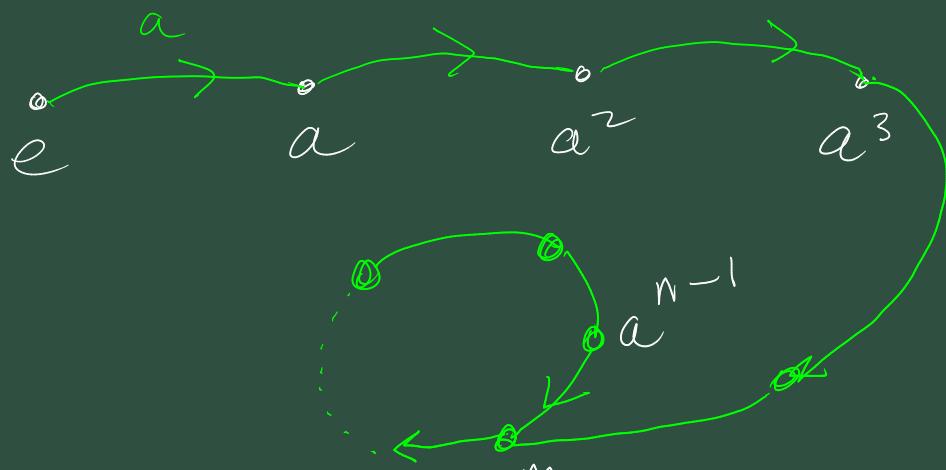
Ex 4.5

$$\mathbb{Z}_6 = \left\{ 0, 1, 1+1, 1+1+1, \dots \right\}$$

This shows G is abelian \blacksquare .

A subtle point

Cycles must repeat first at the identity.
ie. the following structure can not occur.



So suppose we had

$$a^n = a^m \quad \text{for two integers.}$$
$$0 < m < n$$

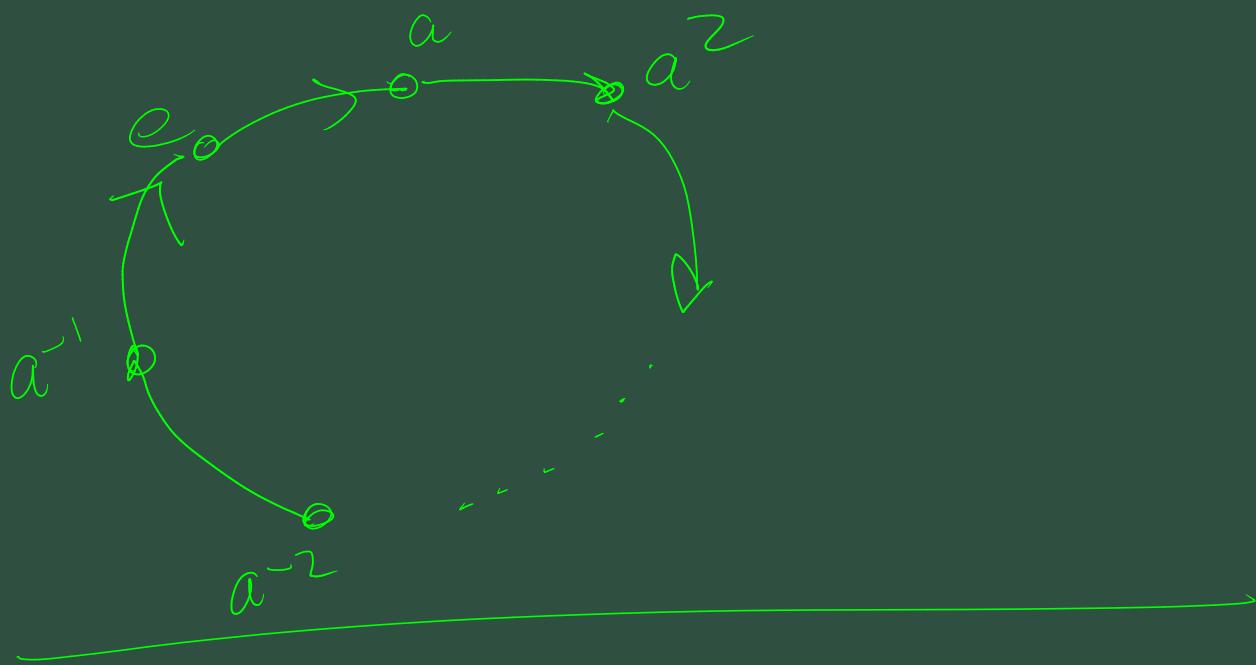
$$a^n = a^m$$

$$\Leftrightarrow a^{-m} a^n = a^{-m} a^m$$

$$\Leftrightarrow a^{n-m} = e$$

So the "first time" the cycle

closes in back at e.



Theorem 4.10

Every subgroup of a cyclic group is cyclic.

Proof. Suppose $G = \langle a \rangle$, i.e. a is a generator of G .

Let H be a subgroup of G . We will prove H is cyclic.

Special case: If $H = \{e\} = \langle e \rangle$

otherwise H has a non-identity element $g \in H$. Now

$$g = a^k, \text{ for some } k \in \mathbb{Z}.$$

and

$$g^{-1} \in H, \quad g^{-1} = a^{-k}$$

From this we see that H contains positive powers of a , as one of $k, -k$ is positive.

Let $m = \text{smallest strictly positive } k > 0$ exponent k , such that

$$\underline{a^k \in H}.$$

Claim: $H = \langle a^m \rangle$

Let $x \in H$.

we know $\underline{x = a^k}$, for some $k \in \mathbb{Z}$.

Divide k by m .

Since $x \in G$

$$G = \langle a \rangle$$

$$k = qm + r, \quad 0 \leq r < m$$

$$\begin{aligned} x = a^k &= a^{qm+r} \\ &= (a^m)^q a^r \\ &= h^q a^r, \quad \text{since } h = a^m \in H. \end{aligned}$$

$$\Rightarrow a^r = \underbrace{h^{-q}}_{\in H} \underbrace{x}_{\in H} \in H.$$

So we have $a^r \in H$, and $0 \leq r \leq m$

From the minimality of m we get

$$r = 0.$$

$$\Rightarrow k = q^m$$

$$\Rightarrow x = a^k = a^{q^m} = (a^m)^q$$

So any $x \in H$ can be written
as $(a^m)^q$ for some $q \in \mathbb{Z}$.

$$\Rightarrow H \subseteq \langle a^m \rangle$$

But we also know.

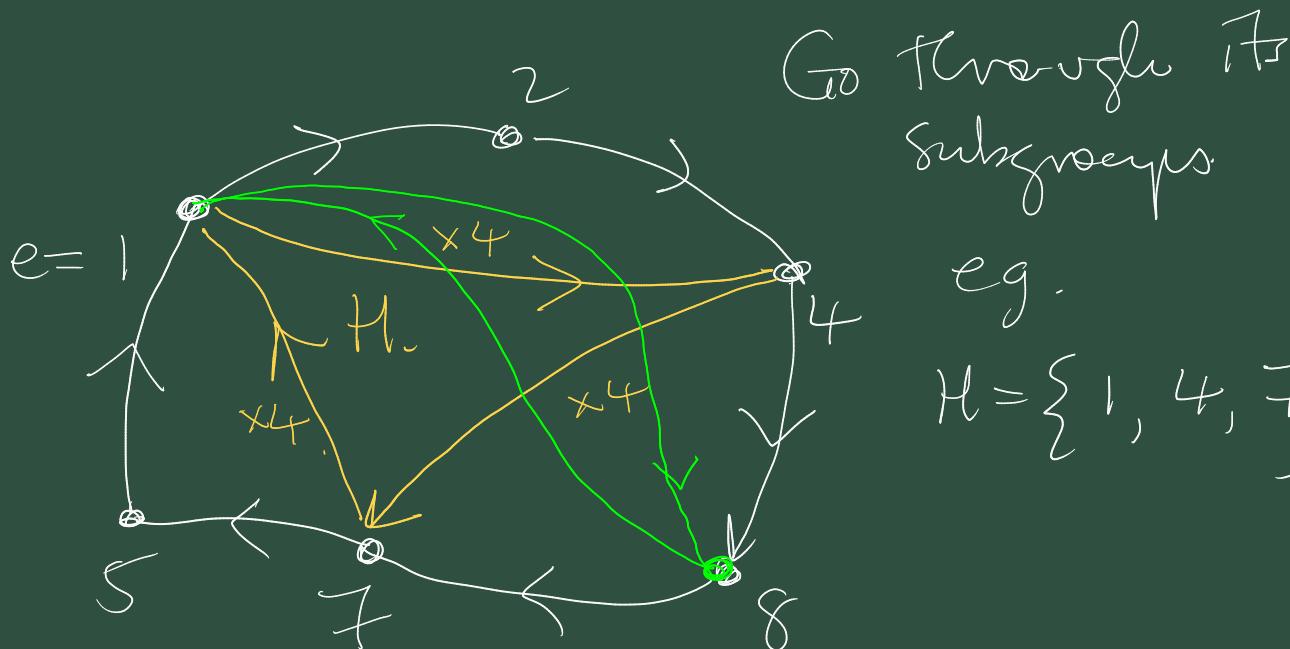
$$\langle a^m \rangle \subseteq H, \text{ since } a^m \in H.$$

$$\text{Therefore } H = \langle a^m \rangle$$

and H is cyclic as claimed.

Example:

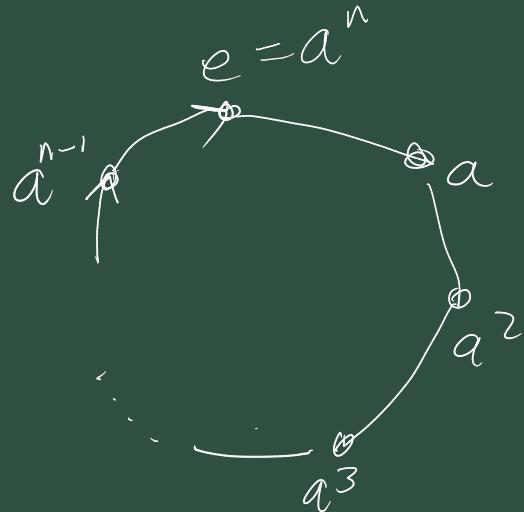
Consider $U(9) = \{1, 2, 4, 5, 7, 8\}$



Read through Prop 4.12, Theorem 4.13,

Prop 4.12

A nice picture makes the result clear.



Well looking at a^k for increasing powers $k=1, 2, 3, \dots$ is equivalent to walking around the cycle.

So clearly $a^k = e$ iff $n|k$.