

$$(\mathbb{Z}, +)$$

$$(\mathbb{Z}_n, +)$$

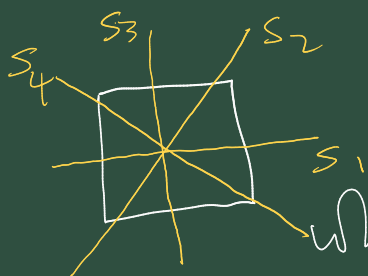
In both these groups, the group is "generated" by the element 1, in the whole group consists of

$$\mathbb{Z} = \{ 0, 1, 1+1, 1+1+1, 1+1+1+1, + \dots \\ -1, -1+ -1, -1+ -1+ -1, \dots \}$$

This is called a "cyclic" group.

Motivating example

Consider the group D_4 , the group of symmetries of a square.



$$D_4 = \{ e, r, r^2, r^3, s_1, s_2, s_3, s_4 \}$$

where r = rotation by a quarter turn ($\frac{2\pi}{4}$ radians) anti-clockwise.

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

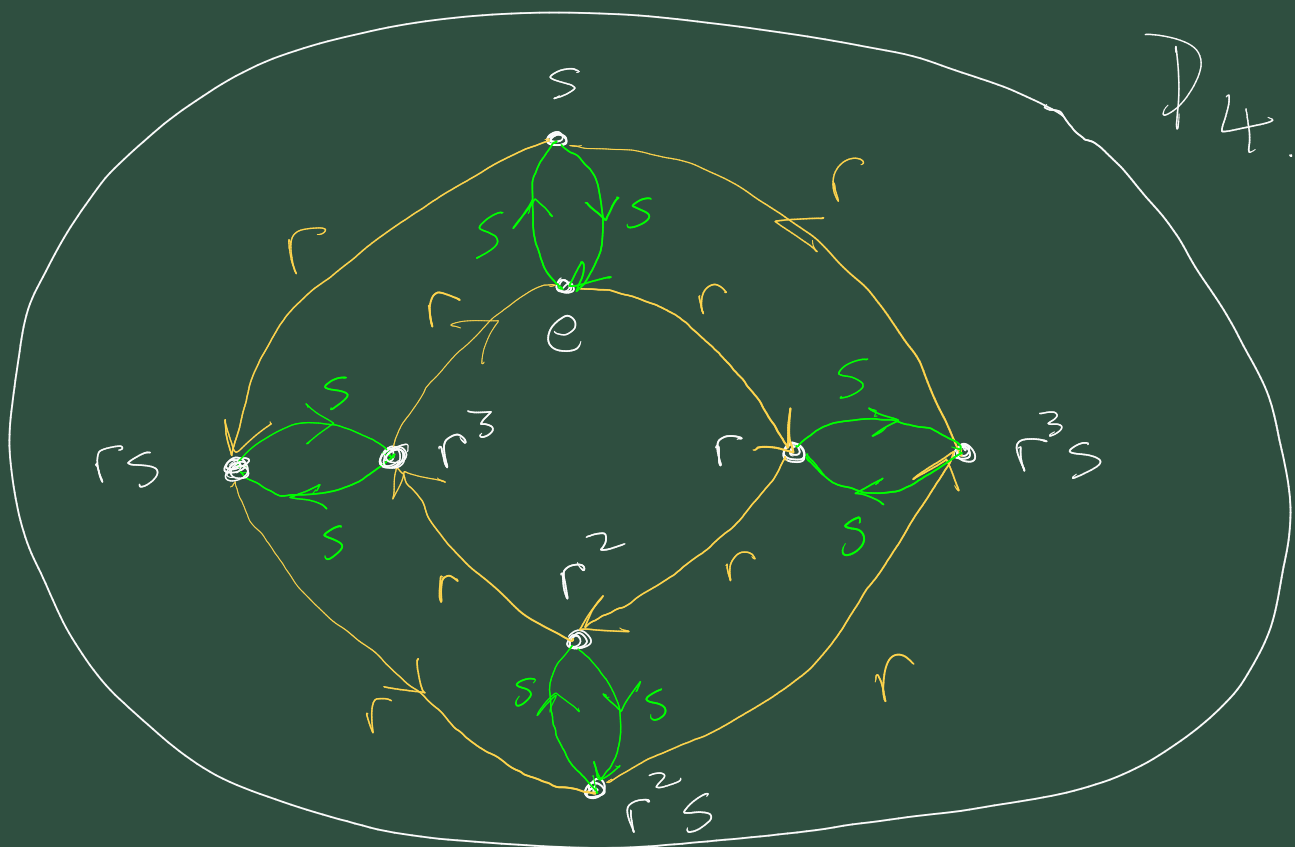
s_2 = reflection in the axis shown.

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.



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

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

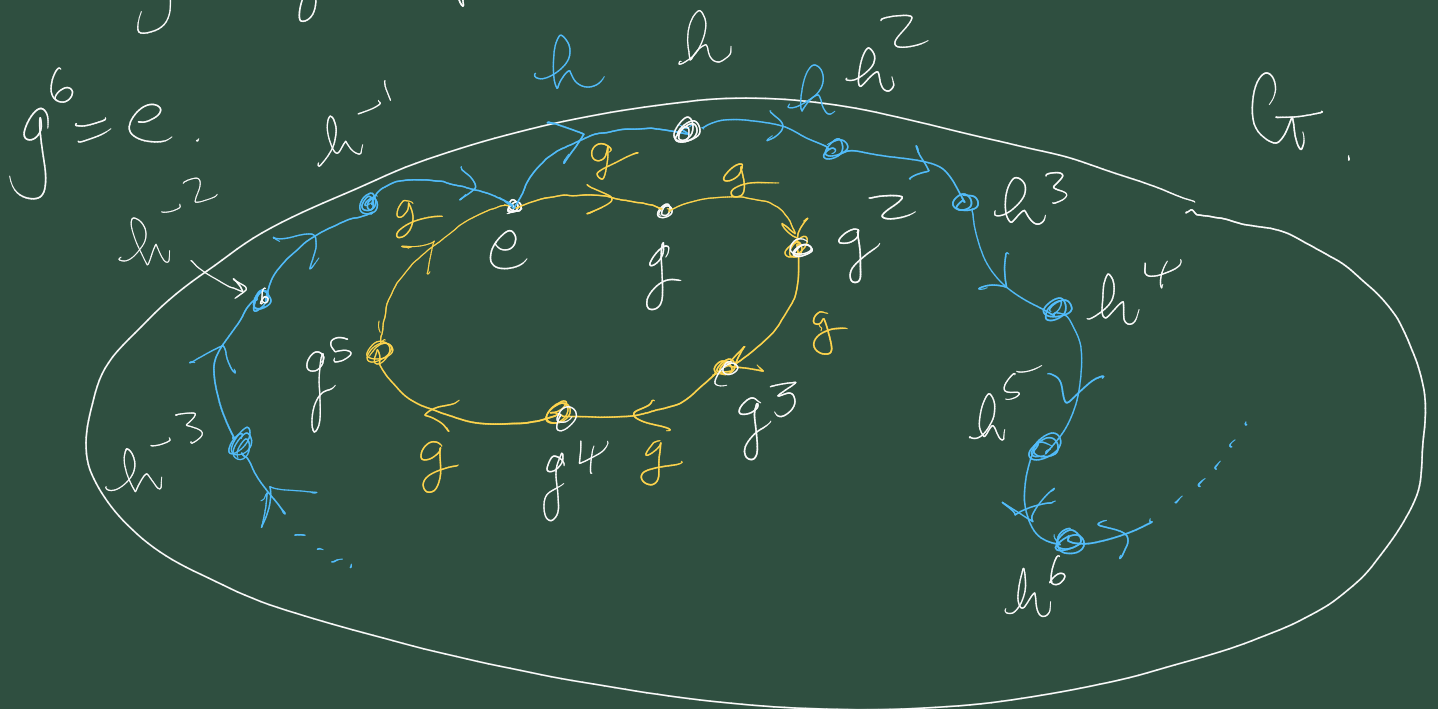
$$H_1 = \{e, r, r^2, r^3\}$$

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



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

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

“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 .

$|a| =$ "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

↑ $|\text{subset}|$
 $=$ cardinality of subset.

Ex 4.5

$$\mathbb{Z}_6 = \left\{ \underset{0}{1}, \underset{1}{1+1}, \underset{2}{1+1+1}, \underset{3}{1+1+1+1}, \dots, \underset{4}{1+1+1+1+1}, \underset{5}{1+1+1+1+1+1} \right\}$$

$$\Rightarrow a^r = \underbrace{h^{-1}}_{\in H} \underbrace{x}_{\in H} \in H.$$

So we have $a^r \in H$, and $0 \leq \underline{\underline{r}} < \underline{\underline{m}}$

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 knew.

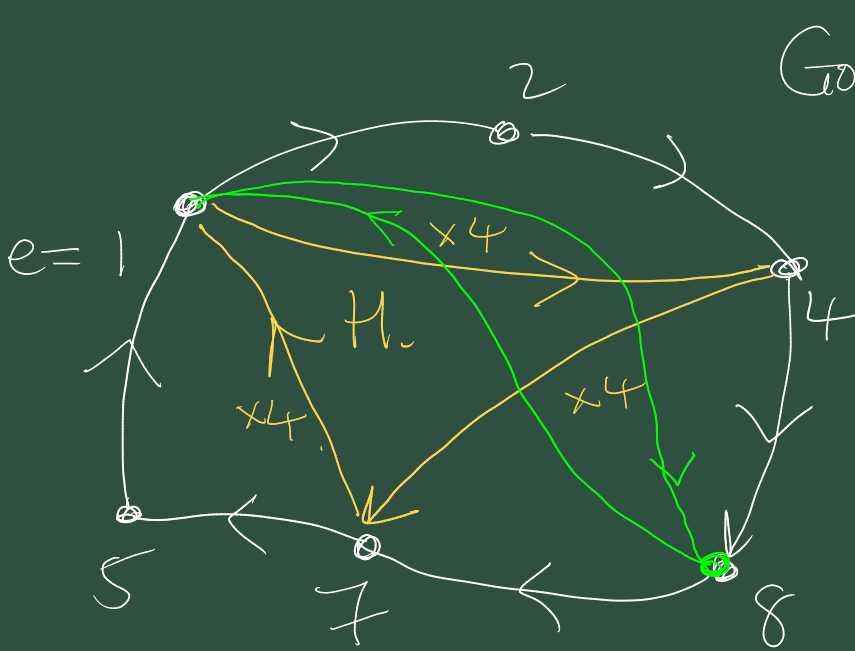
$$\langle a^m \rangle \subseteq H, \text{ since } a^m \in H.$$

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

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.

