# Chap 4 Cyclic groups

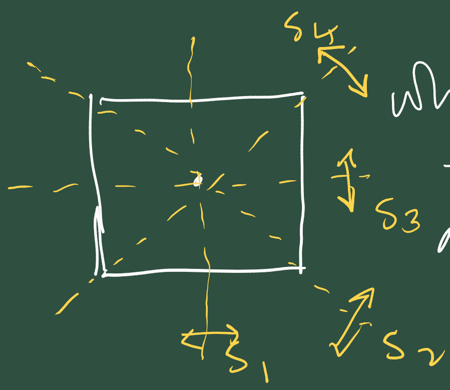
Concentrate on 4.1.

---

Motivation/example.

Consider $D_4$, the group all symmetries of the square under the operation of composition

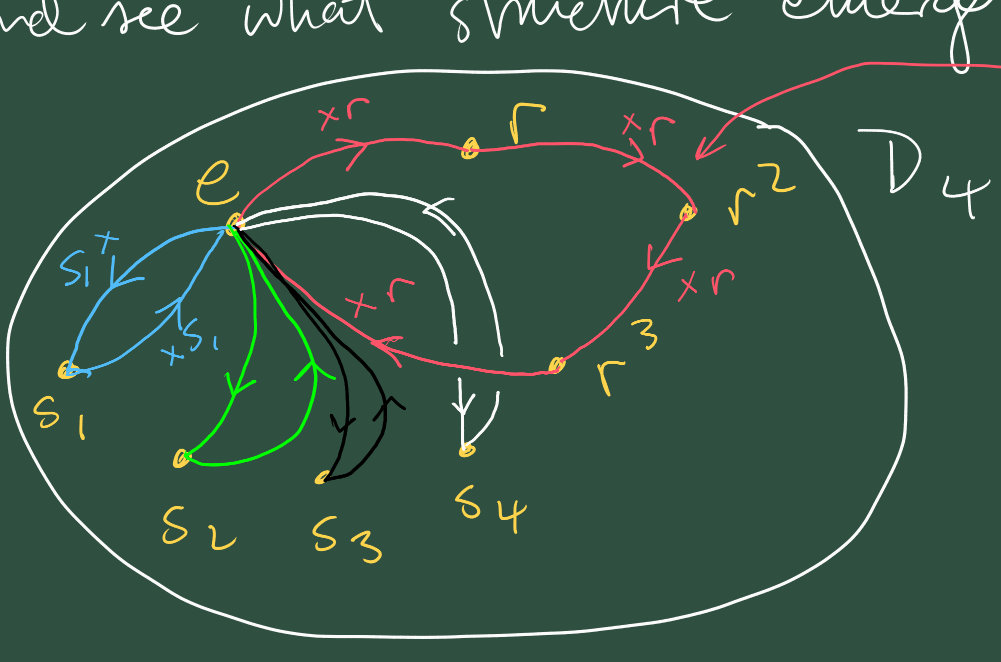
$$D_4 = \{e, r, r^2, r^3, s_1, s_2, s_3, s_4\}$$



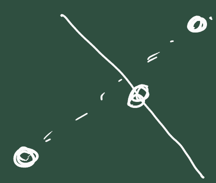

where $r$ is a rotation by $1/4$ of a turn, i.e. $\pi/2$ radians, in the anti-clockwise direction.

and four reflections $s_1, \dots, s_4$ in the lines shown.

Let's picture a set diagram of $D_4$ and see what structure emerges.




$$s_1^2 = s_1 \circ s_1 = e$$



Consider powers of elements
sequences of

ie. take $x \in D_4$, and look at $x^0 = e, x^1 = x, x^2, x^3, \ldots$

The structure that emerges is:

$D_4$ seems to be made of cycles. There is a 4-cycle of rotations, and four 2-cycles of reflections.

Moreover, each cycle is a subgroup of $D_4$.

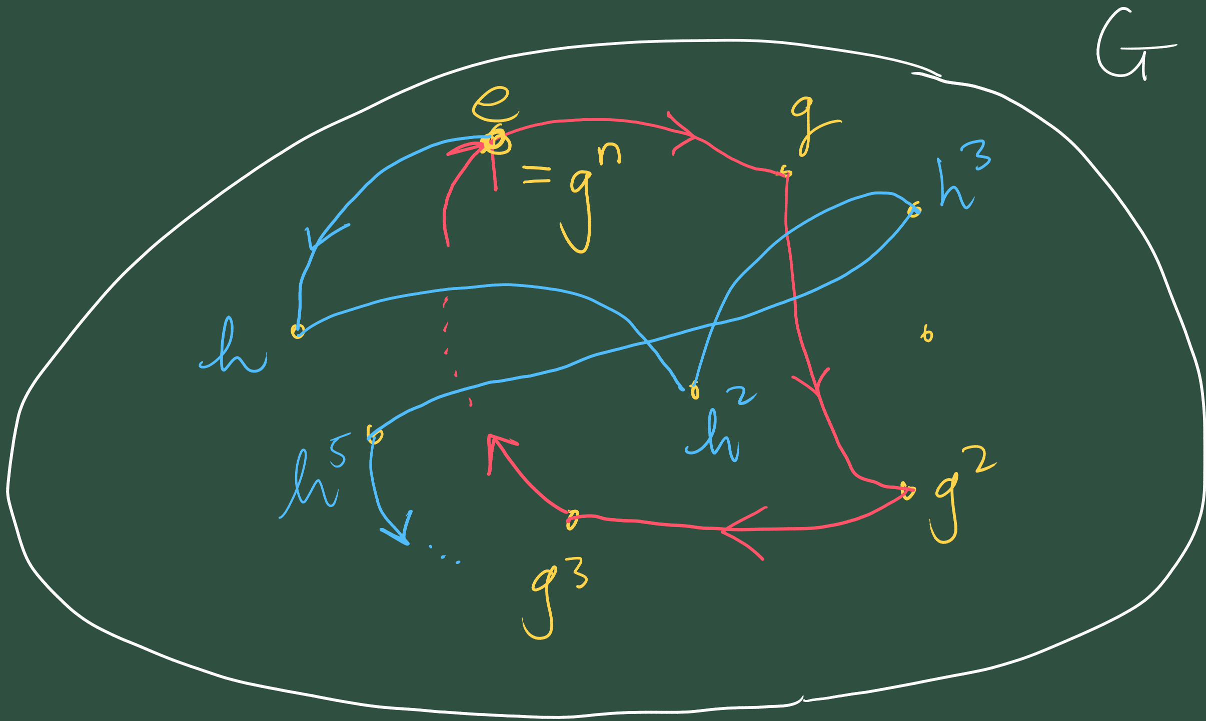
$H = \{e, r, r^2, r^3\}$ is a subgroup

$K = \{e, s_1\}$ is a subgroup

similarly for any other reflection

This picture of $D_4$ shows its decomposition into cycles (cyclic subgroups), and is an example of a (partial?) Cayley diagram for $D_4$.

This approach can be taken to any group $G$




Let $g \in G$. and look at it's cycle of powers.

$\{g^0 = e, g, g^2, g^3, \ldots$

if $|G| = \infty$, i.e. G is an infinite group then this cycle may turn out to be infinite, or it may not, and as pictured, we may have $g^n = e$, for some $n > 0$.

---

Ex 4.1 $\mathbb{Z}$, the integers under $+$

Consider $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$

- $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
- "$3\mathbb{Z}$ is a cyclic subgroup of $\mathbb{Z}$ generated by $3$"

<u>Ex 4.2</u> $(\mathbb{Q}^*, \times)$ the non-zero rationals under $\times$.

$$H = \{ 2^n : n \in \mathbb{Z} \}$$

$$= \{ \ldots, \tfrac{1}{16}, \tfrac{1}{8}, \tfrac{1}{4}, \tfrac{1}{2}, 1, 2, 4, 8, 16, 32, \ldots \}$$

- $H$ is a subgroup of $\mathbb{Q}^*$
- "$H$ is a cyclic subgroup of $\mathbb{Q}^*$ generated by $2$"

<u>Theorem 4.3</u> Let $G$ be a group with $a \in G$. We define $\langle a \rangle$ to be

$$\langle \underset{\text{generator}}{a} \rangle = \{ a^k : k \in \mathbb{Z} \}$$ "cyclic subgroup of $G$ generated by $a$"

- $\langle a \rangle$ is a subgroup of $G$
- $\langle a \rangle$ is the smallest subgroup of $G$ containing $a$. Or in other words, If

$H$ is any subgroup of $G$ then

$a \in H \Rightarrow \langle a \rangle \subseteq H$

The "order of $a$" is the size of $\langle a \rangle$ which may be infinite. written as $|a|$.

Ex 4.6 $U(9)$ = the multiplicative groups of units modulo 9

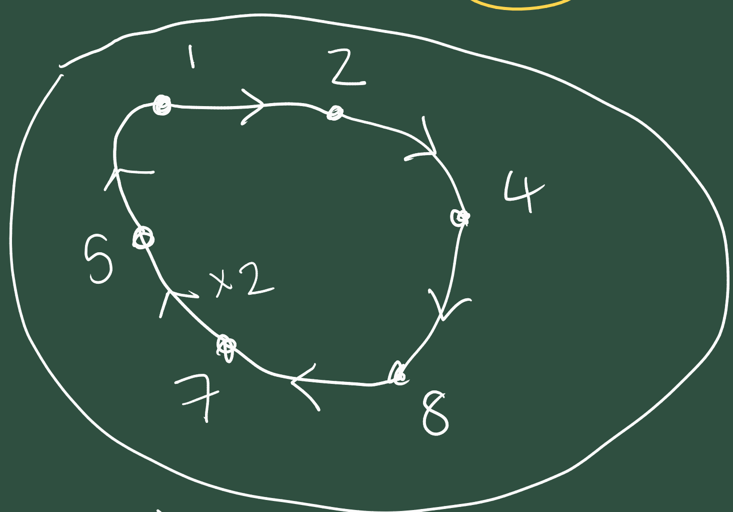
i.e. $U(9) = \{x \in \mathbb{Z}_9 : \gcd(x,9)=1\}$

$= \{1, 2, 4, 5, 7, 8\}$

in fact. $U(9) = \langle 2 \rangle$

$\{2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 7,$
$2^5 \equiv 5\} = U(9)$ $= \langle 5 \rangle$ Exercise.

$U(9)$




We say $U(9)$ is a "cyclic group"

because it is equal to the cyclic subgroup generated by one of its elements.

Note that $D_4$ is not cyclic, as all its cyclic subgroups are strict subgroups.

<u>Theorem 4.9</u> Every cyclic group is Abelian.

<u>Pf</u> Well if $G$ is cyclic then there exists ~~an~~ $g \in G$ such that

$$G = \langle g \rangle$$

Let $\underline{x, y \in G}$, then $x = g^n$, $y = g^m$, for some $n, m \in \mathbb{Z}$

$$\boxed{xy} = g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n \boxed{= yx}$$

$\blacksquare$

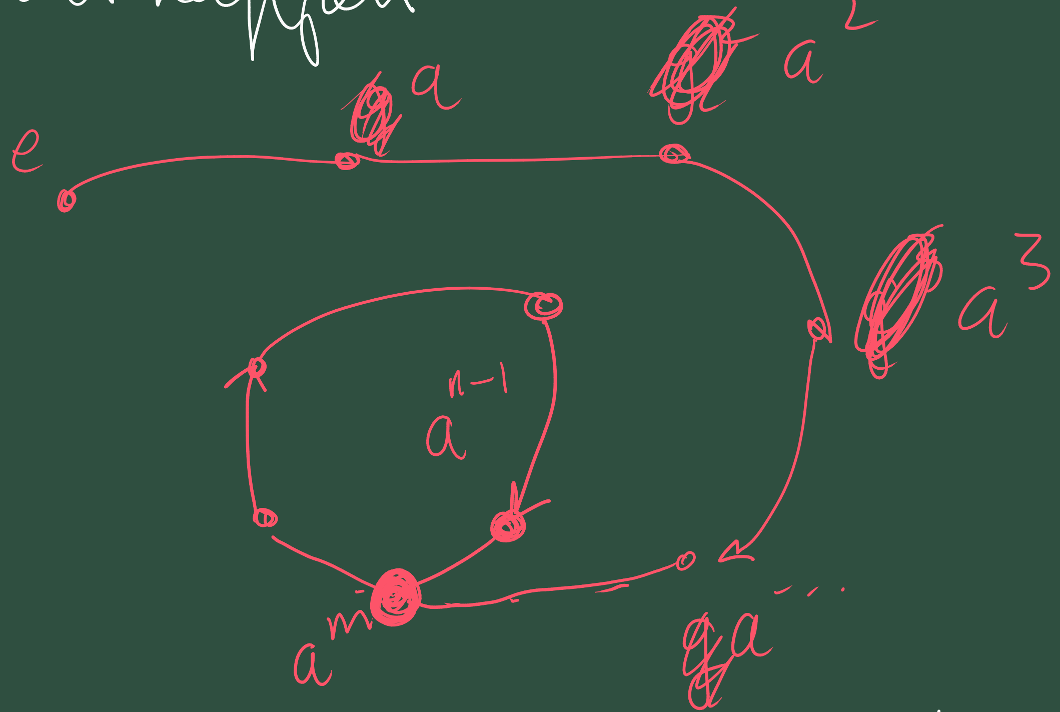
A subtle point

For a cycle $\{e = g^0, g, g^2, g^3, \dots\}$

if it closes it must close at $e$.

in other words, this kind of behaviour

can't happen




Suppose $a^n = a^m$ for two integers

$0 < m < n$

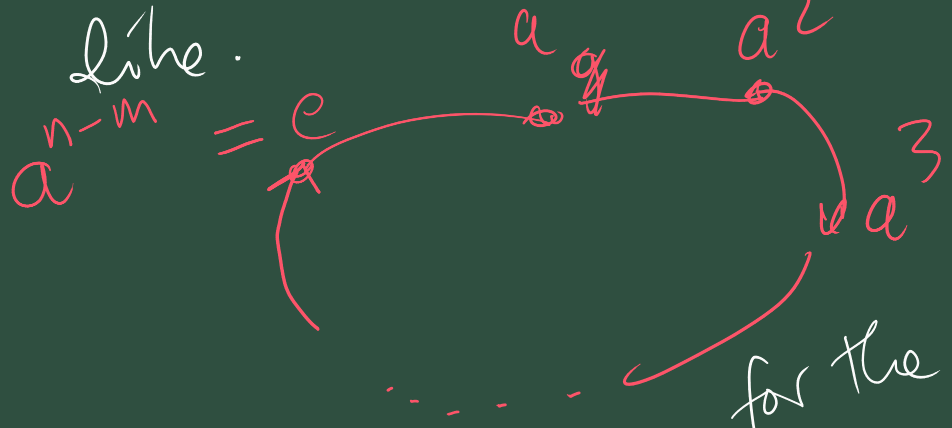
$$a^n = a^m$$

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

$$\Leftrightarrow \quad a^{n-m} = e \quad , \quad n - m > 0$$

ie. in fact the cycle must look

like.




So when cycles close for the first time, they do so at the identity

---

<u>Theorem 4.10</u> Every subgroup of a cyclic group is cyclic

<u>Proof</u> Suppose $G = \langle a \rangle$, for some $a \in G$.

Let $H$ be a subgroup of $G$.

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

Otherwise $H$ has non-identity elements.

Everything in $H$ is a power of $a$

if $g = a^n \in H$, for some $n \in \mathbb{Z}$.

then $g^{-1} = a^{-n} \in H$

So $H$ does contain powers of $a$, $a^k$, with positive exponents

Let $\boxed{m \text{ be the smallest strictly positive integer } (m>0) \text{ such that}}$

$\boxed{a^m \in H}$ $\Rightarrow$ $h = a^m$

Claim: $H = \langle a^m \rangle$, and thus $H$ is cyclic.

Pf: For any $h' \in H$, we know

$h' = a^k$, for some $k \in \mathbb{Z}$, since $(h') \in G$.

Divide $k$ by $m$.

$k = qm + r$, for some $q \in \mathbb{Z}$. and $0 \leq r < m$.

Consider $h'$

$$\boxed{h' = a^k} = a^{qm+r} = a^{qm} \cdot a^r$$

$$= (a^m)^q a^r$$

$$= \boxed{h^q \cdot a^r}$$

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

Almost a contradiction

$\Rightarrow r=0.$

$\Rightarrow k=qm$

and $\boxed{h' = a^k = a^{qm} = (a^m)^q}$

for some $q \in \mathbb{Z}$

So this implies that

$h' \in \langle a^m \rangle$

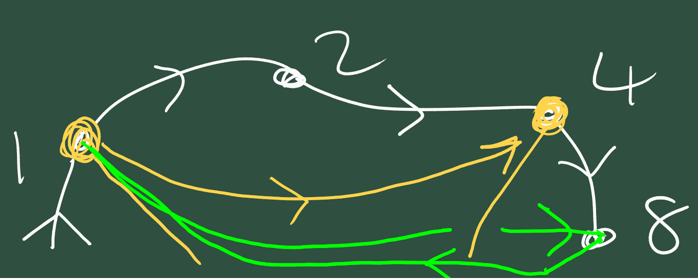
$\Rightarrow H \subseteq \langle a^m \rangle.$

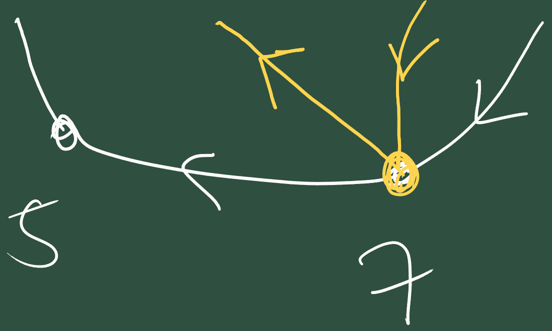
But since $a^m \in H$, we knew, by theorem 4.3., that $\langle a^m \rangle \subseteq H.$

Therefore $H = \langle a^m \rangle$, as claimed.

So $H$ is cyclic.

eg. $U(9) = \langle 2 \rangle$ a 6-cycle.





This shows U(9) is cyclic subgroups
can we form other subgroups.

Suppose H is a subgroup of U(9)

$$H=\{e, 7, 8, 7^2=4, 8\cdot 4=5, 5\cdot 4=2\} = U(9).$$

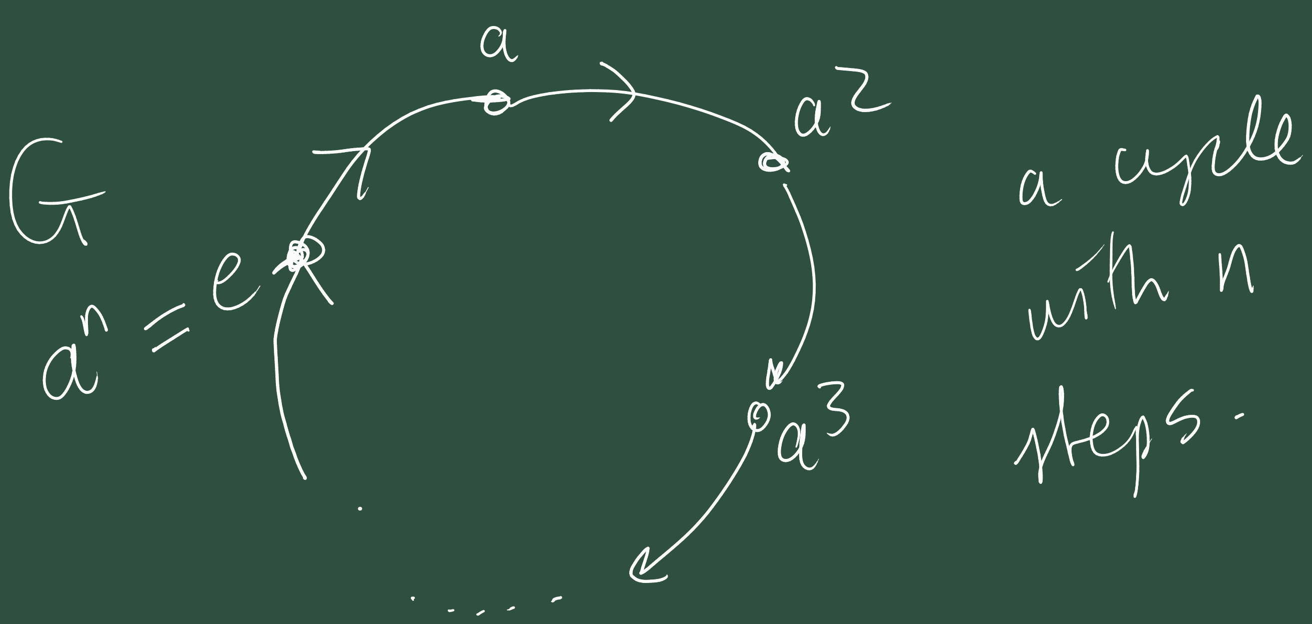
and trying other possibilities will always lead to one of the ~~..~~ three cyclic subgroups.

<u>Prop 4.12</u> Let $G=\langle a\rangle$, and ~~..~~ $|G|=|a|=n$

$$a^k=e \text{ iff } n \text{ divides } k.$$

<u>Pf</u> (both proof based on division with remainder).

But just look at cycle diagram.




Any "journey" along this path
"walk"
that starts and ends at $e$, must consist of a number of steps $k$, where $n | k$.

ie. $a^k = e \iff n | k$.

- $\gcd(a,b)$ makes no distinction about a 1st or 2nd element
- One can go ahead with Euclidean algorithm with $a, b$ in any order.

$35, 17.$

$35 = 2 \cdot 17 + 1$

$\vdots$

$17 = 0 \cdot 35 + 17$

$35 = \_ \ 17 + \_$