APPUNTI sul TUTORATO del 07/11/2024

Durante il tutorato di ieri abbiamo parlato di GRUPPI CICLICI.

Consideriamo il seguente "esercizio formativo":

ESERCIZIO FORMATIVO

Sia G gruppo ciclico, $G = (g)$ di cardinalità 12.

(i) Quanti sono gli elementi che generano G?

(ii) Quanti sono gli elementi di ordine 4?

Lavorando con gruppi ciclici è utile avere la seguente idea in mente (! almeno utile per me): siccome g genera G, tutti gli elementi di G sono della forma g^i per $i \in \mathbb{Z}$.

Mi piace visualizzare le cose in questo modo:

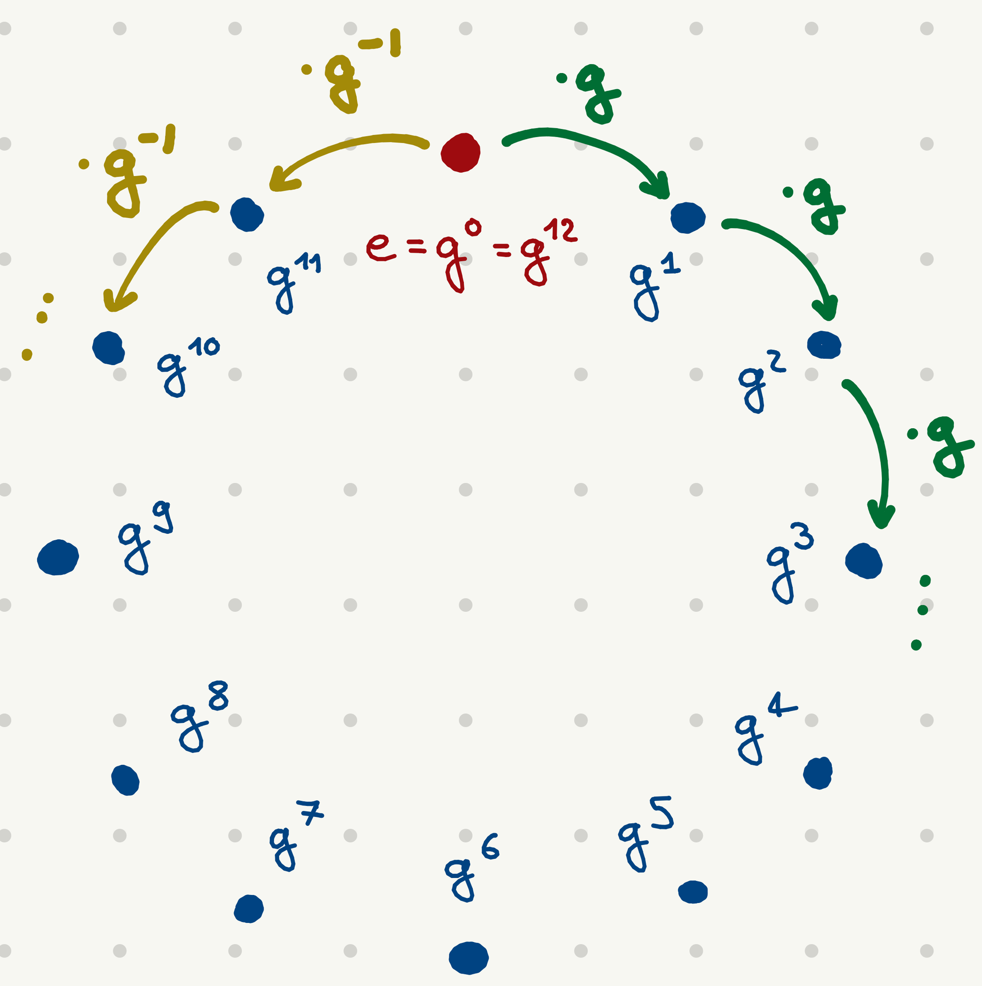
$$G = \left\{ \cdots \; g^{-2} \xleftarrow{\cdot g^{-1}} g^{-1} \xleftarrow{\cdot g^{-1}} e = g^0 \xrightarrow{\cdot g} g^1 \xrightarrow{\cdot g} g^2 \xrightarrow{\cdot g} g^3 \longrightarrow \cdots \right\}$$

cioè moltiplicando per g e g^{-1}, riesco a "raggiungere" tutti gli elementi del gruppo.

Nel nostro caso, però, il gruppo è FINITO, quindi moltiplicando iterativamente per g prima o poi ritorno su elementi già visitati e arriverò così in un "loop"!

Nell'esempio formativo...

Siccome $|G| = 12$ e $g \in G$ genera, dopo 12 passi (cioè moltiplicazioni per $\cdot g$) ritorno all'identità, come nel disegno.



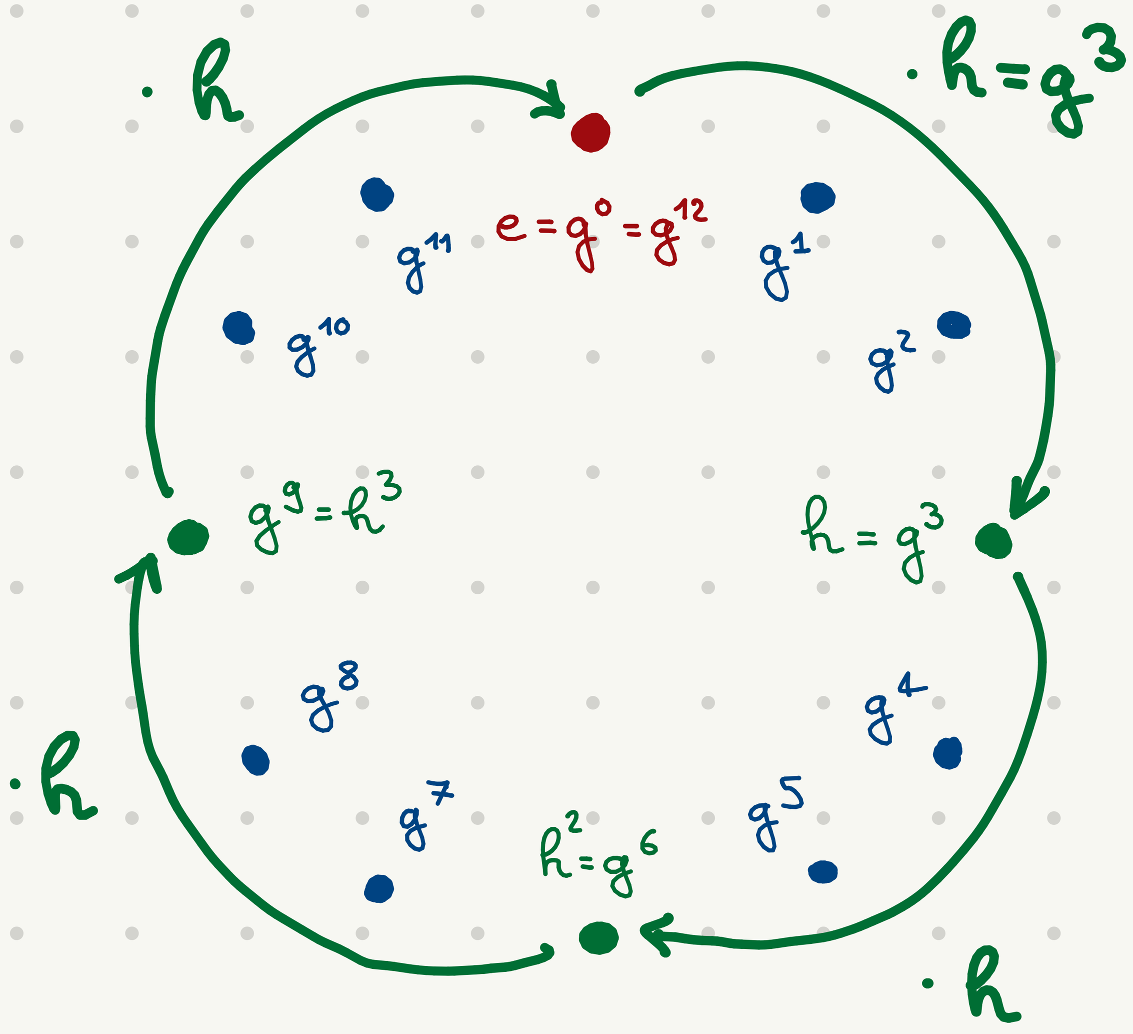
Vediamo di affrontare separatamente i due punti.

(i) Quando G è un gruppo ciclico finito possiamo tenere a mente la seguente proprietà:

$$h \in G \text{ genera il gruppo } G \iff \sigma(h) = |G|$$

Cerchiamo di spiegare intuitivamente perchè questo funziona: dire che "h genera G" significa che tutti gli elementi del gruppo vengono raggiunti da potenze di h.

Nel nostro esempio, se prendiamo $h = g^3$ vediamo cosa succede sul diagramma (a DX): partendo dall'elemento neutro $e = g^0 = h^0$, moltiplico iterativamente per h e riesco a raggiungere soltanto 4 elementi (in verde).



Segue che $h = g^3$ non genera. Infatti $\sigma(h) = 4$.

ESERCIZIO: prendere un altro elemento (tipo g^5) e fare lo stesso diagramma.

In un certo senso, quindi:

$$\sigma(h) = \#\{\text{elementi di } G \text{ ciclico "raggiunti da } h\text{"}\} = \#\{h^i \in G \mid i \in \mathbb{Z}\}.$$

Per questo motivo, h genera G se e solo se $\sigma(h) = |G|$.

La richiesta dell'esercizio è equivalente a chiedere: "Quanti sono gli elementi di ordine 12 in G?"

Aver fatto l'esempio $h = g^3$ ci aiuta: in quel caso, siccome l'esponente 3 e $|G| = 12$ hanno un fattore in comune (cioè 3 stesso), facendo le potenze $h^j = g^{i \cdot j}$, raggiungerò troppo presto una potenza di g^{12}, cioè l'identità.

Infatti: $h^4 = (g^3)^4 = g^{12} = e$ e quindi $o(h) \leq 4$.

Segue che preso $k = g^i \in G$ con $i \in \mathbb{Z}$, l'ordine di k può essere 12 soltanto se $MCD(i, 12) = 1$.

A lezione abbiamo infatti visto la Proposizione 7.5.1:

> Sia G gruppo ciclico finito. Esso ha $\phi(|G|)$ generatori.

e notate che la dimostrazione passa esattamente per quello che abbiamo intuitivamente visto negli esempi!

Segue che G ha $\phi(12) = \phi(3) \cdot \phi(4) = 4$ generatori.

(ii) Il punto precedente ci offre ispirazione anche per questa domanda: nell'esempio $h = g^3$ qual è la <u>minima</u> potenza di h, cioè h^d, che sarà l'elemento neutro?

Per $d > 0$ e $k = g^i$ abbiamo $k^d = g^{id}$, quindi vogliamo:
"$12 \mid id$" e "d minimo indice positivo per cui $12 \mid id$".

Se $i = 3$ vediamo subito che moltiplicare per $d = 4$ funziona ed è anche il minimo. Perchè?

Il motivo è che $d = 4$ è il minimo <u>divisore</u> di $|G|$ che rende $i \cdot d$ un multiplo di 12.

> ESERCIZIO / RIFLESSIONE: perchè è il minimo divisore?

> In particolare, nel prodotto $i \cdot d$, l'indice j minimo deve

"aggiungere" esattamente i fattori di $|G|$ che non ha i, in modo da ottenere $12 / i \cdot d$.

Cioè $d = \dfrac{|G|}{MCD(i, |G|)}$ sarà l'ordine di $k = g^i$.

Nell'esempio, $h = g^3$ e infatti $\sigma(h) = \frac{12}{MCD(3,12)} = 4$!

ESERCIZIO: fare gli esempi g^8, g^5 con $|G| = 12$ e disegnando il diagramma sopra.

Rigirando la formula sopra, gli elementi in $|G|$ di ordine d saranno g^i dove $MCD(i, |G|) = \dfrac{|G|}{d}$. ⊛

Da questa osservazione ritroviamo la Proposizione 7.5.3:

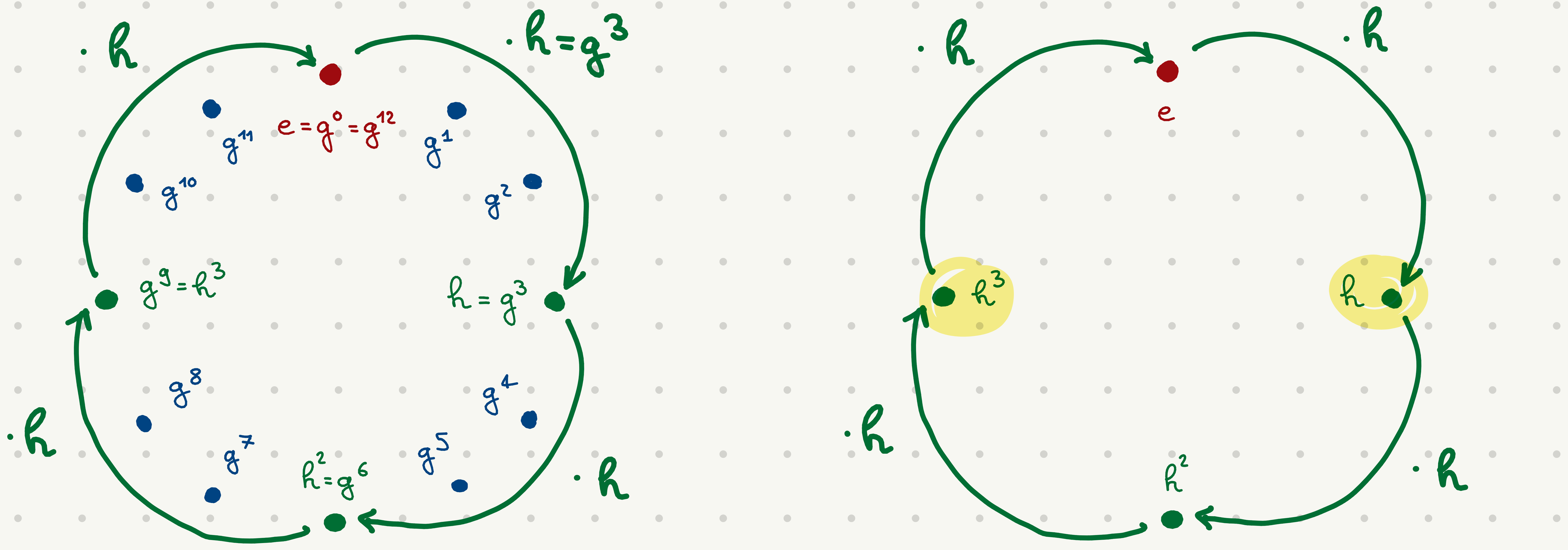
"Sia G ciclico e $d \mid |G|$. Allora G ha $\phi(d)$ elementi di ordine d."

Infatti per ⊛ gli elementi che hanno ordine d sono della forma $g^{k \cdot \frac{|G|}{d}}$, ovvero sono tutti contenuti nel sottogruppo $(g^{\frac{|G|}{d}}) \subset G$. Ma $|(g^{\frac{|G|}{d}})| = d$, quindi gli elementi di questo sottogruppo ciclico di ordine <u>esattamente</u> d sono i suoi generatori. Per il punto (i) sono $\phi(|(g^{\frac{|G|}{d}})|) = \phi(d)$.

Segue che G ha $\phi(4) = 2$ elementi di ordine 4. //

Concludiamo rivedendo questo ragionamento nel nostro esempio, con $h = g^3$ in $G = (g)$ ciclico di cardinalità 12.

Avevamo visto qual era il sottogruppo generato da h:



Schema del gruppo G ⟿ Schema di $(h) = (g^3)$

In questo esempio, quanti elementi di ordine 4 ha G?
Per il ragionamento sopra, questi elementi devono stare in (h) poiché $h = g^{\frac{12}{4}} = g^3$.
In questo sottogruppo (immagine a DX), gli elementi di ordine 4 saranno i generatori, che si osserva a mano essere proprio h, h^3 cioè g^3, g^9.
Guardacaso $\phi(4) = 2$, come previsto!

LEGENDA

- ☐ : esercizio / esempio.
- ☐ : attenti, questo ragionamento è puramente intuitivo e per nulla formale! Serve a capire l'idea che sta dietro una definizione / un passaggio.
- ☐ : fatto visto a lezione.