Gruppi ciclici

27 October 2022 11:18

Def. G è un gruppo ciclico se $\exists a \in G \mid G = (a) = \{a^k \mid k \in \mathbb{Z}\}$

Sia G un gruppo ciclico:

(i) i generatori hanno ordine pari alla cardinalità di G (i.e. $O(g) = \text{card } G$). Quali sono i generatori?

(ii) quali sono i sottogruppi?

Prop. G ciclico $\wedge$ $H < G$ $\wedge$ $H \neq \{e\} \rightarrow$
$\Longrightarrow H$ ciclico

Dimostrazione

Sia g un generatore di G (i.e. $G = (g)$). Sia k il minimo intero positivo t.c. $g^k \in H$.

Sia $g^a \in H$, $g^a = g^{bk+r} = g^r \in H$
(infatti $g^r = g^a g^{-bk} = g^a (g^k)^{-b} \in H$)

se r fosse positivo sarebbe minore di h, che è assurdo per la definizione di h.

Quindi $r = 0 \Rightarrow h \mid a$.

per la definizione di h.

Quindi $r = 0 \Rightarrow h \mid a$.

Pertanto, $\forall\, g^a \in H$, $g^a = (g^k)^i$, $i \in \mathbb{Z}$. D'altra parte $(g^k)^i \in H \ \forall\, i \in \mathbb{Z}$.

Perciò $H = (g^k)$.

$\boxtimes$

OSS. Tutti i sottogruppi di $\mathbb{Z}$ sono quindi ciclici, e pertanto della forma $\{nk \mid k \in \mathbb{Z}\}$ con $n \in \mathbb{Z}$.

Prop. Sia G un gruppo ciclico finito di ordine $\operatorname{card} G = n$ e sia g un generatore di G (i.e. $G = (g)$). Allora $\forall\, k \in \mathbb{Z}$, $(g^k) = (g^{(k,n)})$.

Dimostrazione

Sia $d = (k, n)$. $d \mid k \Rightarrow$
$\Rightarrow k = q \cdot d$, $q \in \mathbb{Z}$.

Per Bézout, $\exists\, x, y \in \mathbb{Z} \mid$
$d = kx + ny$

$$(g^k) = ((g^d)^q) \subseteq (g^d) =$$

$$= (g^{kx+ny}) = ((g^k)^x \underbrace{(g^n)^y}) =$$

$$= \left(g^{kx+ny} \right) = \left((g^k)^x \underbrace{(g^n)^y}_{e} \right) =$$

$$= \left((g^k)^x \right) \subseteq (g^k) \Longleftrightarrow$$

$$\Longleftrightarrow (g^k) \subseteq (g^d) \subseteq (g^k) \Longleftrightarrow$$

$$\Longleftrightarrow (g^k) = (g^d) = (g^{(k,n)}) \quad \square$$

OSS. g^d ha ordine $\frac{m}{d}$,

quindi: $o(g^k) = \frac{m}{d} = \frac{m}{(m,k)}$.

OSS. 2 gli elementi di ordine d sono tutti e soli i generatori di $(g^{m/d})$.

OSS. 3 esiste ed è unico il sottogruppo di G di ordine d, ossia $(g^{\frac{m}{d}})$.

es. su $\mathbb{Z}_{12}$

$([0]) = \{[0]\}$

$([1]) = \mathbb{Z}_{12}$

$([2]) = \{[2], [4], [6], [8], [10], [12]\}$

$([3]) = \{[3], [6], [9], [0]\}$

$([4]) = \{[4], [8], [12]\}$

$([4]) = \{[4], [8], [12]\}$

$\boxed{([5])} = \{[5], [10], [3], [8], [1], [6], [11], [4], [9], [2], [7], [0]\} = \mathbb{Z}_{12}$

...

si nota che $[1]$, $[5]$, $[7]$ e $[11]$ generano $\mathbb{Z}_{12}$.

Prop. Sia G un gruppo di ordine n finito t.c. per ogni divisore di n, G ha al più un sottogruppo di ordine d, allora G è ciclico.

Dimostrazione

Si definisce G_d il sottoinsieme di G con elementi di ordine d.

Ogni elemento di G_d genera un sottogruppo ciclico di ordine d, che per ipotesi è unico e ciclico di ordine d, che per ipotesi è unico e che ha esattamente $\varphi(d)$ generatori. Quindi

$$|G_d| \leq \varphi(d).$$

Tuttavia:

$$n = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n$$

Quindi $|G_d| = \varphi(d)$.

In particolare $|G_n| = \varphi(n) \geq 1$.

Quindi G ammette un generatore ed è ciclico.

$\boxtimes$

es. $\quad S_4 \supseteq \{ id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \}$ A

gli inversi sono loro stessi

$\underbrace{A < S_4}$ è chiuso sulla composizione

gruppo di

composizione $\underbrace{\qquad\qquad\qquad\qquad}_{\text{gruppo di Klein}}$

es. Se $|G| < 3$, allora è ciclico.

- $|G| = 1$, $G = \{e\} = (e)$ ✓
- $|G| = 2$, $G = \{e, a\}$
  - $a \cdot a \in G$

$a \cdot a = e$	$a \cdot a = a$
$G = (a)$	$a = e$
	impossibile ✓