Lezione 13 - 28/10/2022

Notazione - definizione

Sia G un **gruppo** e $g \in G$. Definiamo le **potenze** come segue

$$g^i = \begin{cases} g^{i-1} \cdot g & \text{se } i > 0 \\ e & \text{se } i = 0 \\ (g^{-1})^{-i-1} \cdot g^{-1} & \text{se } i < 0 \end{cases}$$

Nota: è una definizione induttiva

Osservazione: in notazione additiva si ha

$$\begin{aligned} g^i &\to ig \\ g^{-i} &\to -ig \end{aligned}$$

> ⚠️ Fare la **potenza** di un elemento x di un gruppo G equivale ad **iterare** a partire da x o da x^{-1} l'operazione del gruppo.

Proposizione

Se H, K sono **sottogruppi** di un gruppo G, anche $H \cap K$ lo è.
Dimostrazione: Per ipotesi

$$\begin{aligned} h_1 h_2^{-1} \in H \quad \forall h_1, h_2 \in H \ (1) \\ k_1 k_2^{-1} \in K \quad \forall k_1, k_2 \in K \ (2) \end{aligned}$$

Siano ora $x,\ y$ elementi qualsiasi di $H \cap K$. Devo dimostrare che

$$xy^{-1} \in H \cap K$$

ma se $x, y \in H \cap K$, in particolare $x, y \in H$ quindi per (1) $xy^{-1} \in H$ e $x, y \in K$, quindi per (2) $xy^{-1} \in K$. Dunque $xy^{-1} \in H \cap K$.

Osservazione: L'enunciato vale per una qualsiasi **famiglia di sottogruppi** di G

$$\alpha \in A \quad H_\alpha \leq G \iff \bigcap_{\alpha \in A} H_\alpha \leq G$$

Definizione - Sottogruppo generato

Sia G un **gruppo** e $X \leq G$. Si definisce **sottogruppo generato da** X l'insieme

$$< X >= \bigcap_{X \subseteq H \leq G} H$$

Caso speciale (importante): $X = \{g\}$ allora

$$< g >= \{g^i : i \in \mathbb{Z}\}$$

e prende il nome di **sottogruppo ciclico generato da** g**.**

Proposizione

Sia $X = \{x_1, x_2, ...\} \leq G$. Allora

$$< x >= \{t_1 \cdot ... \cdot t_r : r \in \mathbb{N},\ t_i \in X \text{ oppure } t_i^{-1} \in X\}$$

Idea: per generare un gruppo a partire dagli elementi di X devo prendere **tutti i possibili prodotti di elementi di** X **e dei loro inversi**.

Esempio: in $\mathbb{Z}$

$$< 2, 3 >= \{2s + 3t : s, t \in \mathbb{Z}\} = \mathbb{Z}$$

Definizione - Gruppo ciclico

Un **gruppo** G si dice **ciclico** se $\exists g \in G : G =< g >$.

Esempi:

1. $(\mathbb{Z}, +)$ è **ciclico**, generato da 1

$$n = n \cdot 1$$

Nota: anche -1 genera $\mathbb{Z}$ e **nessun altro intero** lo genera.

2. $(\mathbb{Z}_n, +)$ è ciclico, generato da $\bar{1}$

$$\bar{n} = n \cdot \bar{1}$$

Dimostreremo che $\mathbb{Z}_n$ ha $\phi(n)$ generatori.

Esempio:

- $\mathbb{Z}_6$ ha $\phi(6) = \phi(3)\phi(2) = 2$ generatori
- $\mathbb{Z}_8$ ha $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ generatori. Verifica:

$$\begin{aligned}
&< \bar{0} > = \{\bar{0}\} \\
&< \bar{1} > = \mathbb{Z}_8 \\
&< \bar{2} > = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\} \\
&< \bar{3} > = \{\underbrace{\bar{3}, \bar{6}}_{+3}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{0}\} = \mathbb{Z}_8 \\
&< \bar{4} > = \{\bar{4}, \bar{0}\} \\
&< \bar{5} > = \{\underbrace{\bar{5}, \bar{2}}_{+5}, \bar{7}, \bar{4}, \bar{1}, \bar{6}, \bar{4}, \bar{0}\} = \mathbb{Z}_8 \\
&< \bar{6} > = \{\bar{6}, \bar{4}, \bar{2}, \bar{0}\} \\
&< \bar{7} > = \{\bar{7}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0}\} = \mathbb{Z}_8
\end{aligned}$$

3. $(\mathbb{R} \setminus \{0\}, \cdot) \geq \{\pm 1\} \cong \mathbb{Z}_2$ ($\cong$ è il simbolo che indica un **isomorfismo**). Sia

$$\begin{aligned}
\phi : \{\pm 1\} &\to \mathbb{Z}_2 \\
1 &\mapsto \bar{0} \\
-1 &\mapsto \bar{1}
\end{aligned}$$

Si ha che

$$\phi(1 \cdot 1) = \phi(1) + \phi(1) = \bar{0} + \bar{0}$$
$$\phi(1 \cdot (-1)) = \phi(1) + \phi(-1) = \bar{0} + \bar{1} = \bar{1}$$
$$\phi((-1) \cdot (-1)) = \phi(-1) + \phi(-1) = \bar{1} + \bar{1} = \bar{0}$$

Definzione - Ordine

L'**ordine** di $g \in G$, denotato con $o(g)$, è il **minimo intero positivo**, se esiste, tale che

$$g^n = e$$

se tale n **non esiste**, si pone $o(g) = +\infty$.

Osservazione: in altri termini

$$o(g) = | < g > |$$

in particolare G è **ciclico se e solo se esiste** $g \in G$, con $o(g) = |G|$

Osservazione: se G è **ciclico**, allora è **abeliano**. Infatti, se $G =< g >,\ x, y \in G$

$$x = g^i,\ y = g^j$$
$$xy = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = yx$$

Il viceversa **non è vero**.

Esempio: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$

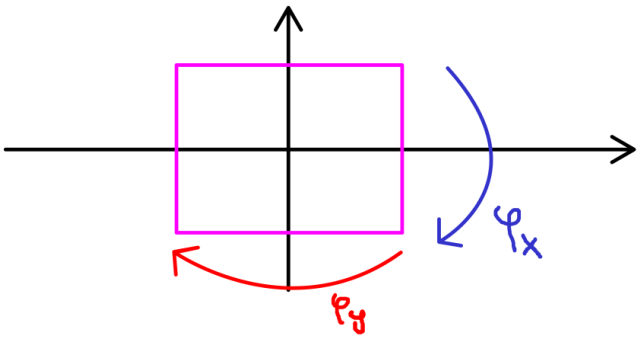
$$< (\bar{0}, \bar{0}) > = \{(\bar{0}, \bar{0})\}$$
$$< (\bar{1}, \bar{0}) > = \{(\bar{1}, \bar{0}), (\bar{0}, \bar{0})\}$$
$$< (\bar{0}, \bar{1}) > = \{(\bar{0}, \bar{1}), (\bar{0}, \bar{0})\}$$
$$< (\bar{1}, \bar{1}) > = \{(\bar{1}, \bar{1}), (\bar{0}, \bar{0})\}$$

Quindi tutti gli elmento diversi da $e = \{(\bar{0}, \bar{0})\}$ hanno ordine 2, quindi nessuno di essi ha ordine 4 e quindi il **gruppo non è ciclico**.

Il gruppo è chiaramente **abeliano**, ma **non è ciclico**.

Nota

Il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ è **isomorfo** al cosiddetto **gruppo di Klein**, delle **simmetrie di un rettangolo** con non è un quadrato:



$$V = \{Id, \phi_x, \phi_y, \phi_o\}$$
$$\phi_x(x,y) = (x,-y)$$
$$\phi_y(x,y) = (-x,y)$$
$$\phi_o(x,y) = (-x,-y)$$

Osservazione: abbiamo due gruppi di ordine 4 **non isomorfi** $\mathbb{Z}_4$ e V: il primo è **ciclico** mentre il secondo **non è ciclico**.

Proposizione

Sia G un **gruppo** e $g \in G$. Se $o(g) = +\infty$, allora $g^h \neq g^k$ per $h \neq k$. Se invece $o(g) = n$ allora

$$< g >= \{e, g, ..., g^{n-1}\}$$

e $g^h = g^k$ sse $h \equiv k \mod n$.

Dimostrazione: Supponiamo $o(g) = +\infty$ e $g^h = g^k$. Allora

$$g^{h-k} = e \Rightarrow h - k = 0 \Rightarrow h = k$$

Se $o(g) = n$, per definizione $e, g, ..., g^{n-1}$ sono **elementi distinti del sottogruppo** $< g >$ (se fosse $g^i = g^j,\ 1 \leq i \leq j < n$ avremmo $g^{i-j} = e$ con $i - j < n$ contro la definzione di $o(g)$).

Dunque basta vedere che ogni potenza di g è nella lista $\{e, g, ..., g^{n-1}\}$.

Consideriamo $g^s,\ s \in \mathbb{Z}$; $s = qn + r \quad 0 \leq r < n$

$$g^s = g^{qn+r} = g^{qn}g^r = (g^n)^q g^r = e^q g^r = eg^r = g^r \quad 0 \leq r \leq n-1$$

Supponiamo ora $g^h = g^k$

$$g^{h-k} = e \qquad h - k = q'n + r' \quad 0 \leq r' \leq n-1$$
$$g^{h-k} = g^{q'n+r'} = g^{r'} \Rightarrow r' = 0$$

ovvero $h - k = q'n$ ovvero $h \equiv k \mod n$.

Viceversa, $h \equiv k \mod n,\ h = k + tn$

$$g^h = g^{k+tn} = g^k g^{tn} = g^k (g^n)^t = g^k e^t = g^k e = g^k$$