Lezione 14 - 03/11/2022

Reminescenze gruppo ciclico

Ricordiamo che un gruppo G si dice ciclico se $\exists g \in G$: $G =< g >$.

Esempi:

1. $\mathbb{Z} =< 1 >$
2. $\mathbb{Z}_n =< \bar{1} >$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico

Osservazione: G ciclico $\Rightarrow G$ abeliano, ma non è vero il viceversa (come nell'esempio 3.).

Proposizione 1

Ogni sottogruppo di un gruppo ciclico G è **ciclico**.

Dimostrazione: sia $G =< g >$ e $H \leq G$.

Se $H = \{e\}$, allora $H =< e >$ quindi è **ciclico**.

Supponiamo $H \neq \{e\}$, quindi esiste $g^i \in H, i \neq 0$. Siccome $H \leq G$, se $g^i \in H$ anche $g^{-i} \in H$. Pertanto $\{i \in \mathbb{N}$: $g^i \in H\} \neq \emptyset$ e quindi **ammette minimo**, chiamiamolo m.

Dico che $H =< g^m >$. Poichè $g^m \in H$, $g^{km} \in H \; \forall k \in \mathbb{Z}$ (perché $H \leq G$), quindi $< g^m > \subseteq H$. Devo dimostrare l'inclusione contraria.

Sia $g^t \in H$

$$\begin{gathered} t = qm + r, \quad 0 \leq r < m \\ g^t = g^{qm+r} = g^{qm} g^r \\ g^r = g^t g^{-qm} \in H \end{gathered}$$

Per la **minimalità di** m segue che $r = 0$. Dunque $t = qm$ e quindi $g^t \in < g^m >$, che è quanto volevamo.

Proposizione 2

Sia $G =< g >$ un **gruppo ciclico finto** di ordine n. Allora

a. $H \leq G, \; |H| \mid n$ (la cardinalità di H divide n)
b. Se $k \mid |G|$, esiste **un unico** $H \leq G, \; |H| = k$

Dimostrazione a.: Sia $H \leq G$; per la $\text{prop } 1.\; H =< g^m >$;

$$(g^m)^n = (g^n)^m = e^m = e$$

quindi $o(g^m) \mid n$, dove $g^m = |H|$ e $n = |G|$ (in generle se $g^k = e \Rightarrow o(g) \mid k$).

Dimostrazione b.: Sia $k \mid n$; allora $| < g^{\frac{n}{k}} > | = k$.

Facciamo vedere che $< g^{\frac{n}{k}} >$ è l'**unico** sottogruppo di ordine k. Sia H un altro tale sottogruppo; $H =< g^h >$ dove h è il **minimo intero positivo** tale che $g^h \in H$

$$|H| = k = | < g^h > | = \frac{n}{h}$$

dunque $h = \frac{n}{k}$ e $H =< g^{\frac{n}{k}} >$.

Proposizione: Se $g \in G$ ha ordine finito n, allora

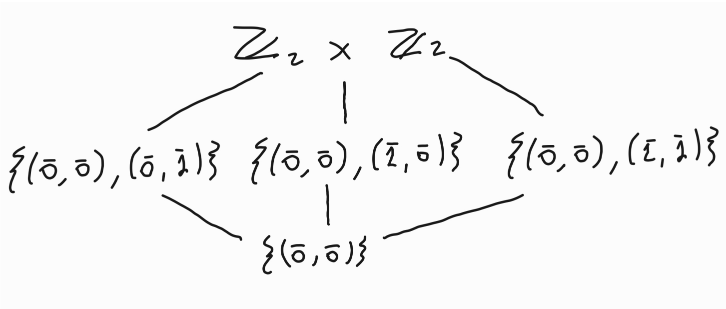
$$o(g^k) = \frac{n}{(n,k)}$$

Corollario delle prop 1. e 2.: Il **reticolo dei sottogruppi** di un gruppo cicliclo di ordine n è **isomorfo al reticolo dei divisori di** n.

Esempio: POSET dei sottogruppi di un gruppo:

$$H_1, H_2 \leq G \qquad H_1 \preccurlyeq H_2 \Leftrightarrow H_1 \subseteq H_2$$

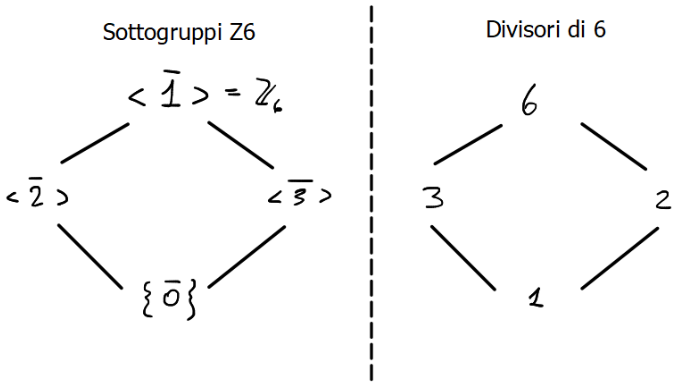
- $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{1})\}$



$\mathbb{Z}_6 =< \bar{1} >$

Abbiamo visto che il sottogruppo di ordine k è generato da $g^{\frac{n}{k}}$

$$\begin{array}{llll} n & k & & \\ 6 & 6 & \bar{1} & \\ & 3 & \bar{2} & < \bar{2} >= \{\bar{2}, \bar{4}, \bar{0}\} \\ & 2 & \bar{3} & < \bar{3} >= \{\bar{3}, \bar{0}\} \\ & 1 & \bar{0} & \end{array}$$



Proposizione 3

Sia $G =< g >$ un **gruppo ciclico** di ordine n. Allora $< g^i >$ genera G se e solo se $(i, n) = 1$.

<u>Dimostrazione</u>: g^i genera G se e solo se $o(g^i) = n$

$$n = o(g^i) = \frac{n}{(n,i)} \iff (n,i) = 1$$

Gruppo simmetrico

$$S_n = \{f : \{1, ..., n\} \to \{1, ..., n\} | f \text{ è biunivoca}\}$$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Per scrivere le permutazioni in modo più conveniente, introduciamo, fissata $\sigma \in S_n$, una **relazione di equivalenza** su $\{1, ..., n\}$

$$i \equiv_\sigma j \iff \exists k \in \mathbb{Z} : i = \sigma^k(j)$$

Esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 3 & 2 & 5 & 4 & 7 & 9 & 8 & 6 & 1 \end{pmatrix}$$

$$\begin{aligned} &1 \equiv_\sigma 10 \\ &2 \equiv_\sigma 3 \\ &4 \equiv_\sigma 5 \\ &6 \equiv_\sigma 7 \equiv_\sigma 9 \\ &8 \equiv_\sigma 8 \end{aligned}$$

quindi si ha che

$$\sigma = (1, 10)(2, 3)(4, 5)(6, 7, 9)$$

Tale rappresentazione viene chiamata **rappresentazione in cicli disgiunti.**

⚠️ Gli elementi in σ che restano fissati, come in questo caso l'8, non vengono riportati nella rappresentazione in cicli disgiunti.

Verifichiamo ora che $\equiv_\sigma$ è di equivlenza:

- **Riflessiva**: $i \equiv_\sigma i$ ovvio perché $i = \sigma^0(i)$
- **Simmetrica**: $i \equiv_\sigma j \Rightarrow j \equiv_\sigma i$. Vera in quanto $\exists k : i \in \sigma^k(j)$ e $j = \sigma^{-k}(i)$.
- **Transitiva**: $i \equiv_\sigma j,\ j \equiv_\sigma k \Rightarrow i \equiv_\sigma k$.

$$\begin{gathered} \exists t : i = \sigma^t(j) \\ \exists s : j = \sigma^s(k) \\ i = \sigma^t(j) = \sigma^t(\sigma^s(k)) = \sigma^{t+s}(k) \end{gathered}$$

  quindi $i \equiv_\sigma k$.

Definizione

Data $\sigma \in S_n$, un **ciclo** di σ è l'insieme ordinato

$$(x, \sigma(x), \sigma^2(x), ..., \sigma^{m-1}(x))$$

due cicli si dicono **disgiunti** se lo sono come insiemi.

Osservazione: possiamo interpretare un ciclo come la permutazione

$$x \mapsto \sigma(x), \sigma(x) \mapsto \sigma^2(x), ..., \sigma^{m-1}(x) \mapsto x$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 2 & 7 & 1 & 4 \end{pmatrix} = (1, 8, 3, 6, 7)(2, 5)$$

Esempio: trasformazione di cicli non disgiunti in cicli disgiunti

$$(1, 2, 3, 4)(2, 6, 4, 8)(8, 7, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 3 & 8 & 5 & 1 & 4 & 7 \end{pmatrix} = (1, 2, 6)(4, 8, 7)$$

Procediemento:

- Inizio dall'1 e lo faccio scorrere attraverso i vari cicli (non disgiunti) da **destra verso sinistra** e vedo dove va a finire:
    1. Nel ciclo $(8, 7, 3)$ l'1 non viene mappato da nessuna parte;
    2. Nel ciclo $(2, 6, 4, 8)$ l'1 non viene mappato da nessuna parte;
    3. Nel ciclo $(1, 2, 3, 4)$ l'1 viene mappato in 2, i cicli sono finiti e quindi nella permutazione avremo $\sigma(1) = 2$.
- Passo al 2 e faccio lo stesso procedimento:
    1. Nel ciclo $(8, 7, 3)$ il 2 non viene mappato da nessuna parte;
    2. Nel ciclo $(2, 6, 4, 8)$ il 2 viene mappato in 6, quindi ora nel prossimo ciclo dovrò controllare il 6 dove verrà mappato;
    3. Nel ciclo $(1, 2, 3, 4)$ il 6 non viene mappato da nessuna parte, i cicli sono finiti e quindi avremo $\sigma(2) = 6$.
- Passo al 3:
    1. Nel ciclo $(8, 7, 3)$ il 3 viene mappato in 8;
    2. Nel cilclo $(2, 6, 4, 8)$ l'8 viene mappato in 2;

3. Nel ciclo $(1,2,3,4)$ il 2 viene mappato in 3, quindi $\sigma(3)=3$.

- …

Infine vengono scritti i cicli disgiunti partendo dalla permutazione ottenuta.

Proposizione - Permutazione prodotto di cicli

Ogni permutazione è **prodotto dei suoi cicli**.

Dimostrazione: sia $\sigma \in S_n$ e siano $\gamma_1, ..., \gamma_k$ i suoi cicli. Poiché $\equiv_\sigma$ è una **relazione di equivalenza**, pensando i cilci come **insiemi** si ha

$$\bigcup_{i=1}^{k} \gamma i = \{1, ..., n\} \quad \gamma_i \cap \gamma_j = \emptyset,\ i \neq j$$

Dobbiamo far vedere che se penso $\gamma_1, ..., \gamma_k$ come **permutazioni** allora $\sigma = \gamma_1, ..., \gamma_k$, ovvero

$$\sigma(x) = (\gamma_1, ..., \gamma_k)(x)\ \forall x \in \{1, ..., n\}$$

Ora, ogni $x \in \{1, ..., n\}$ compare in **uno solo** dei cicli $\gamma_1, ..., \gamma_k$. Sia questo ciclo $\gamma_i = (x, \sigma(x), ..., \sigma^{m-1}(x))$. Per ogni $j \neq i$ e per ogni $y = \sigma^h(x)$ (ovvero per ogni y che compare nella scrittura di γ_i) risulta

$$\gamma_i(y) = y$$

dunque, $\forall x \in \{1, ..., n\}$

$$(\gamma_1, ..., \gamma_k)(x) = (\gamma_1, ..., \gamma_i)(x) = \gamma_1 ..., \gamma_{i-1}(\sigma(x)) = \sigma(x)$$

quindi $\sigma = \gamma_1, \gamma_2, ..., \gamma_k$.

Proposizione - Ordine di una permutazione

Se $\sigma = \gamma_1 ... \gamma_k$ è la **decomposizione in cicli disgiunti** di σ e γ_i ha lunghezza m_i, allora

$$o(\sigma) = \mathrm{m.c.m}\{m_1, ..., m_k\}$$

Dimostrazione: Ovvio dalla **definizione di ordine** e dal fatto che i cicli disgiunti **commutano**. Sia m_i l'ordine dell'i-esimo ciclo e $S = \mathrm{m.c.m}(m_1, ..., m_k)$ si ha che

$$\sigma^S = (\gamma_1, ..., \gamma_k)^S = \gamma_1^S ... \gamma_k^S$$

Esempi:

1. Calcolare l'ordine di

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$$

   Riportiamo σ in notazione in cicli disgiunti:

$$\sigma = (1, 2, 3)(4, 5, 6, 8)$$

   quindi $o(\sigma) = \text{m.c.m}(3, 4) = 12$.

2. Calcolare l'ordine di

$$\sigma = (1, 2, 3)(2, 3, 4)(3, 4, 5)$$

   Attenzione: non è 3 in quanto i cicli **non sono disgiunti**! Riportiamo σ in notazione in cilci disgiunti:

$$\sigma = (1, 2)(4, 5)$$

   quindi $o(\sigma) = \text{m.c.m}(2, 2) = 2$.

Notazione

I cicli di lunghezza m vengono chiamati m-cicli. I cicli di lunghezza 2 vengono chiamati **trasposizioni**.

Porposizione- Ciclo prodotto di trasposizioni

Ogni **ciclo** è **prodotto di trasposizioni**. In particolare, S_n è generato dalle trasposizioni.

Dimostrazione: ogni ciclo si può scrivere come prodotto di trasposizioni, ad esempio

$$(1, 2, ..., n) = (1, n)(1, n-1)(1, n-2)...(1, 3)(1, 2)$$

Ora **ogni permutazione è prodotto di cicli** e **ogni ciclo è prodotto di trasposizioni**, quindi **ogni permutazione è prodotto di trasposizioni**.

Osservazione: La scrittura come prodotto di trasposizioni non è unica

$$(1, 3) = (1, 2)(2, 3)(1, 2) = (2, 3)(1, 2)(2, 3)$$

Teorema

Se $\sigma = \tau_1 ... \tau_k = \tau'_1 ... \tau'_h$ con τ_i, τ'_j trasposizioni, allora $h \equiv k \mod z$.

Definizione - Parità delle permutazioni

Diciamo che σ è **pari** se si scrive come **prodotto di un numero pari di trasposizioni**, **dispari** altrimenti.

Esercizio: determinare ordine e parità della seguente permutazione

$$\sigma = (1,4,7,8)(2,9,7,6)(4,3,1,7)(2,9,5)$$

riportiamola in notazione in cicli disgiunti

$$\sigma = (1,6,2,8)(3,4)(5,9) \quad (*)$$

da cui deduciamo che $o(\sigma) = \text{m.c.m}(4,2,2) = 4$. Ora riportiamo i cicli disgiunti in prodotti di trasposizioni:

$$\sigma = (1,8)(1,2)(1,6)(3,4)(5,9)$$

da cui deduciamo che è **dispari**.

Definizione - Partizione di un numero naturale

Una **partizione** di $n \in \mathbb{N}$ è una sequenza di interi $\lambda_1 \geq ... \geq \lambda_k \geq 1$ tali che

$$\sum_{i=1}^{k} \lambda_i = n$$

Chiamiamo con $p(n)$ il **numero di partizioni** di n. Si ha che

$$\begin{array}{llllllll}
p(1) = 1 & & & & & & & \\
p(2) = 2 & 2 & 11 & & & & & \\
p(3) = 3 & 3 & 21 & 111 & & & & \\
p(4) = 5 & 4 & 31 & 22 & 211 & 1111 & & \\
p(5) = 7 & 5 & 41 & 32 & 311 & 221 & 2111 & 11111
\end{array}$$

Definizione - Struttura ciclica di una permutazione

Osserviamo che una permutazione di S_n individua, tramite la **decomposizione in cicli disgiunti**, una partizione di n che è detta **struttura ciclica** della permutazione.

La **struttura ciclica** della σ precedente $(*)$ è: 4221.

Esempio: $p(5) = 7$

		ordine	parità
5	$(1,2,3,4,5)$	5	p
41	$(1,2,3,4)$	4	d
32	$(1,2,3)(4,5)$	6	d
311	$(1,2,3)$	3	p
221	$(1,2)(3,4)$	2	p
2111	$(1,2)$	2	d
11111	id	1	p

Relazione coniugio

Ricordiamo che in un gruppo qualsiasi due elementi g_1, g_2 si dicono **coniugati** se esiste $g_3 \in G$:

$$g_1 = g_3 g_2 g_3^{-1}$$

Teorema

$\sigma, \tau \in S_n$ sono **coniugate** se e solo se hanno la **stessa struttura ciclica**.

Idea della dimostrazione: $\tau\sigma\tau^{-1}$ si ottiene dalla decomposizione in cicli disgiunti di σ sostituendo ad a la cifra $\tau(a)$.

$$\begin{aligned} \sigma &= (a,b,c,d)(e,f)(g,h) \\ \tau\sigma\tau^{-1} &= (\tau(a),\tau(b),\tau(c),\tau(d))(\tau(e),\tau(f))(\tau(g),\tau(h)) \end{aligned}$$

Esempio:

$$\begin{aligned} \sigma &= (1,2,3,4)(5,6)(7,8) \\ \sigma' &= (2,4,6,8)(7,1)(3,5) \end{aligned}$$

> ⚠️ Notare che σ e σ' hanno la **stessa struttura ciclica**: 422

una permutazione τ che **conigua** σ in σ' è

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 1 & 3 & 5 \end{pmatrix}$$

in quanto $\tau\sigma\tau^{-1} = \sigma'$:

$$\begin{aligned} \tau\sigma\tau^{1} &= (1,7)(2,4,6,8)(3,5) = \\ &= (2,4,6,8)(7,1)(3,5) = \sigma' \end{aligned}$$

⚠️ Ricordiamo che per risolvere questo tipo di esercizio si procede applicando le permutazioni da **destra verso sinistra**, quindi prima applico τ^{-1} e vedo dove viene mappato ogni elemento che man mano viene scelto, poi applico σ ed infine τ.
Ricordiamo inoltre che τ^{-1} vuol dire **leggere la permutazione al contrario**, quindi ogni elemento all'interno di un ciclo viene mappato in quello che si trova alla sua sinistra e non destra.