Lezione 15 - 04/11/2022

Osservazione - Il sottogruppo alterno

La mappa $\epsilon : S_n \to \{\pm 1\}$ definita come

$$\epsilon(\sigma) = \begin{cases} 1 & \sigma \text{ è pari} \\ -1 & \sigma \text{ è dispari} \end{cases}$$

è un **omomorfismo** di gruppi; questo è equivalente a dire che il **prodotto** di due permutaizioni pari **è pari** così come il prodotto di una permutazione pari ed una dispari e il prodotto di una permutazione dispari ed una pari **è dispari**. A sua volta questo segue dalle definizioni.

<u>Esempio</u>:

$$\sigma = \tau_1 ... \tau_6 \qquad \sigma' = \tau_1' ... \tau_8' \qquad \tau_i, \tau_j' \text{ trasposizioni}$$
$$\sigma\tau = \underbrace{\tau_1 ... \tau_6 \tau_1' ... \tau_8'}_{14 \text{ trasposizioni}}$$

In particolare

$$A_n = \{\sigma \in S_n : \sigma \text{ è pari}\}$$

è un sottogruppo di S_n e prende il nome di **sottogruppo alterno**.

Lemma - Cardinalità del sottogruppo alterno

$|A_n| = \dfrac{n!}{2}$ (ovvero sono metà pari e metà dispari)

Dimostrazione: basta costruire una **corrispondenza biunivoca**

$$\Phi : A_n \to \{\sigma \in S_n | \sigma \text{ è dispari}\}$$

Questo conclude perché se $a = |A_n|$

$$n! = a + |\{\sigma \in S_n : \sigma \text{ è dispari}\}| = 2a \Longrightarrow a = \frac{n!}{2}$$

Sia τ una permutazione **dispari fissata**

$$\Phi(\sigma) = \sigma\tau$$

$\Phi(\sigma)$ è dispri, perchè σ è pari, quindi Φ è effettivamente un'applicazione

$$A_n \to \{\sigma \in S_n : \sigma \text{ è dispari}\}$$

- Φ è **iniettiva**:

$$\begin{gathered} \Phi(\sigma) = \Phi(\sigma') \\ \sigma\tau = \sigma'\tau \\ \sigma\tau\tau^{-1} = \sigma'\tau\tau^{-1} \\ \sigma = \sigma' \end{gathered}$$

- Φ è **suriettiva**: $\alpha \in S_n$ dispari, $\alpha\tau^{-1} \in A_n$ e

$$\Phi(\alpha\tau^{-1}) = \alpha\tau^{-1}\tau = \alpha$$

Esercizio sulla relazione coniugio

Siano $\sigma = (1,5)(2,3,4)$ e $\tau = (1,4,3)(2,6,7,5)$

$$\tau\sigma\tau^{-1} = (\tau(1), \tau(1))(\tau(2), \tau(3), \tau(4)) = (4,2)(6,1,3)$$

derivata nel seguente modo

$$
\begin{aligned}
\tau\sigma\tau^{-1} : & 1 \to 3 \to 4 \to 3 \\
& 2 \to 5 \to 1 \to 4 \\
& 3 \to 4 \to 2 \to 6 \\
& 4 \to 1 \to 5 \to 2 \\
& 5 \to 7 \to 7 \to 5 \\
& 6 \to 2 \to 3 \to 1 \\
& 7 \to 6 \to 6 \to 7
\end{aligned}
$$

Calcolare τ tale che $\tau\sigma\tau^{-1} = \mu$ dove

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

$$
\begin{aligned}
\tau\sigma\tau^{-1} &= (\tau(1),\tau(2),\tau(3))(\tau(4),\tau(7),\tau(8)) = \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 9 & 5 & 6 & 7 & 2 & 1 & 8 \end{pmatrix}
\end{aligned}
$$

> ℹ️ In quanto in σ non sono presenti $5, 6$ e 9, in $\tau\sigma\tau^{-1}$ possono essere messi uno dei valori rimanenti a caso.

Lemma - Gli r-cicli di Sn

In S_n gli r-cicli sono

$$
\frac{1}{r} \cdot \frac{n!}{(n-r)!}
$$

Dimostrazione: Il **primo numero** del ciclo lo posso scegliere in n modi, **il secondo** in $n-1$, il terzo in $n-2$ …. l'**r-esimo** in $n-r+1$ modi. In totale

$$
n(n-1)...(n-r+1) = \frac{n!}{(n-r)!}
$$

Però ognuno dei cicli ottenuti in questo modo viene **contato r volte** (ci sono ripetizioni):

$$
(1,2,...,r) = (2,3,...,r,1) = (3,4,...,r,1,2)....
$$

Ad esempio in S_n ci sono $\binom{n}{2}$ trasposizioni.

Classi laterali e teorema di Lagrange

Sia G un gruppo e $H \leq G$; definiamo **due relazioni di equivalenza** ρ_d, ρ_s su G:

$$a\rho_d b \iff ab^{-1} \in H$$
$$a\rho_s b \iff b^{-1}a \in H$$

1. ρ_d, ρ_s sono relazioni di equivalenza
   - **Riflessiva**: $a\rho_d a \qquad aa^{-1} \in H \qquad e \in H$
   - **Simmetrica**: $a\rho_d b \Rightarrow b\rho_d a$

     $$ab^{-1} \in H \qquad (ab^{-1})^{-1} \in H$$
     $$(ab^{-1})^{-1} = ba^{-1} \Leftrightarrow b\rho_d a$$

   - **Transitiva**: $a\rho_d b,\ b\rho_d c \Rightarrow a\rho_d c$. Si ha che $ab^{-1} \in H$ e $bc^{-1} \in H$ e si ha che $H \leq G$.

     $$(ab^{-1})(bc^{-1}) \in H$$
     $$(ab^{-1})(bc^{-1}) = abb^{-1}c^{-1} = ac^{-1} \Leftrightarrow a\rho_d c$$

2. $\rho_d = \rho_s$ se G è **abeliano**.
3. <u>Esempio</u>: $G = \mathbb{Z}$ e $H = n\mathbb{Z}$. Sia $\rho = \rho_d = \rho_s$

   $$a\rho b \Leftrightarrow ab^{-1} \in H \rightarrow a - b \in n\mathbb{Z}$$

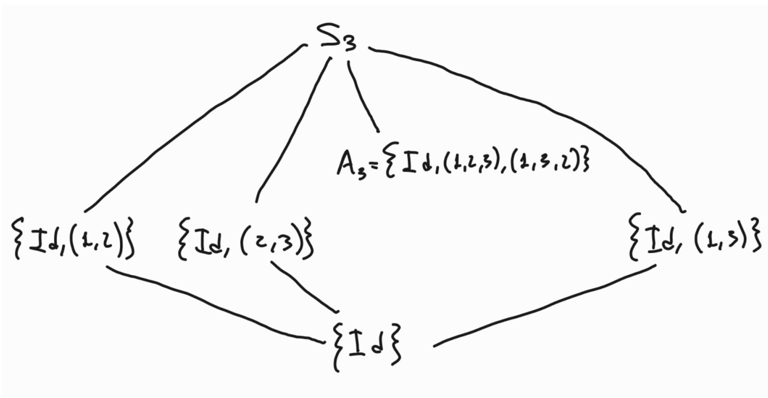
   che implica che ρ è precisamente la **congruenza mod n**.
4. Struttura delle **classi di equivalenza**
   - Classe **laterale destra** di $a \bmod H$

     $$\begin{aligned}\{b \in G : b\rho_d a\} &= \{b \in G : ba^{-1} \in H\} \\ &= \{b \in G : ba^{-1} = h \text{ per qualche } h \in H\} \\ &= \{b \in G : b = ha \text{ per qualche } h \in H\} \\ &= Ha \leftarrow \text{classe laterale destra di } a \bmod H\end{aligned}$$

   - Classe **laterale sinistra** di $a \bmod H$

$$
\begin{aligned}
\{b \in G : b\rho_s a\} &= \{b \in G : a^{-1}b \in H\} \\
&= \{b \in G : a^{-1}b = h \text{ per qualche } h \in H\} \\
&= \{b \in G : b = ah \text{ per qualche } h \in H\} \\
&= aH \leftarrow \text{classe laterale sinistra di } a \bmod H
\end{aligned}
$$

Esempio: $S_3 = \{Id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$



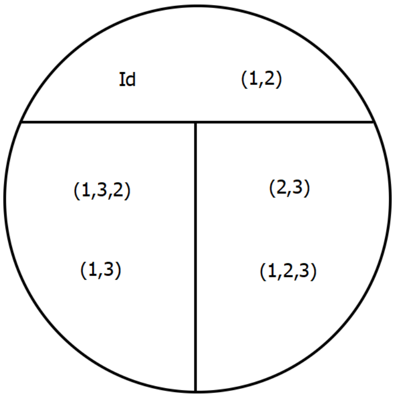
Poniamo $H = \{Id, (1,2)\}$ e troviamo le **classi laterali destre** e **sinistre** di $S_3 \bmod H$:

$$
\begin{aligned}
HId &= H \\
H(1,2) &= \{Id \cdot (1,2), (1,2)(1,2)\} = \{(1,2), Id\} = H \\
H(2,3) &= \{Id \cdot (2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\} \\
H(1,3) &= \{Id \cdot (1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\} \\
H(1,2,3) &= \{Id \cdot (1,2,3), (1,2)(1,2,3)\} = \{(1,2,3), (2,3)\} \\
H(1,3,2) &= \{Id \cdot (1,3,2), (1,2)(1,3,2)\} = \{(1,3,2), (1,3)\}
\end{aligned}
$$

Quindi si ha che

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

Che formano la seguente **partizione** di S_3:



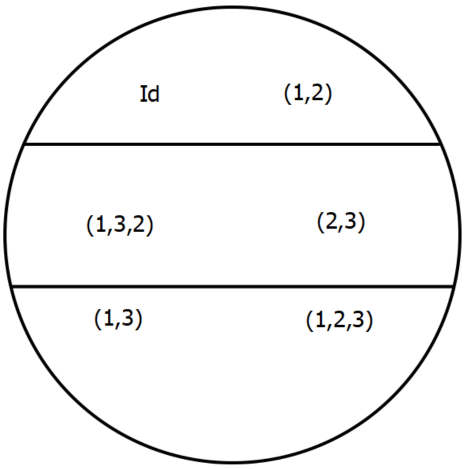
Passiamo ora alle **classi laterali sinistre**:

$$
\begin{aligned}
IdH &= H \\
(1,2)H &= \{(1,2)\cdot Id, (1,2)(1,2)\} = H \\
(2,3)H &= \{(2,3)\cdot Id, (2,3)(1,2)\} = \{(2,3), (1,3,2)\} \\
(1,3)H &= \{(1,3)\cdot Id, (1,3)(1,2)\} = \{(1,3), (1,2,3)\} \\
(1,2,3)H &= \{(1,2,3)\cdot Id, (1,2,3)(1,2)\} = \{(1,2,3), (1,3)\} \\
(1,3,2)H &= \{(1,3,2)\cdot Id, (1,3,2)(1,2)\} = \{(1,3,2), (2,3)\}
\end{aligned}
$$

Quindi si ha che

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

Che formano la seguente **partizione** di S_3:



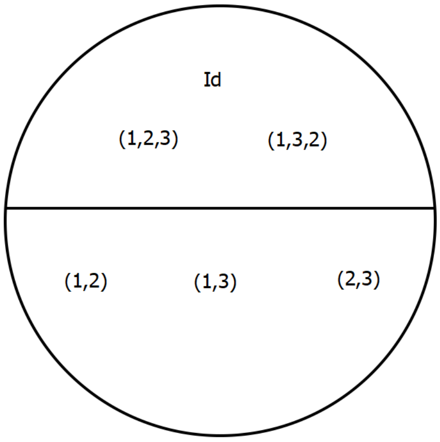
Sia ora $H = \{Id, (1,2,3), (1,3,2)\}$. Poichè H è un sottogruppo

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

Calcoliamo ora le **classi laterali destre**:

$$\begin{aligned} H(1,2) &= \{(1,2), (1,2,3)(1,2), (1,3,2)(1,2)\} \\ &= \{(1,2), (1,3), (2,3)\} = (1,2)H \\ H(2,3) &= \{(2,3), (1,2,3)(2,3), (1,3,2)(2,3)\} \\ &= \{(2,3), (1,2), (1,3)\} = (2,3)H \\ H(1,3) &= \{(1,3), (1,2,3)(1,3), (1,3,2)(1,3)\} \\ &= \{(1,3), (2,3), (1,2)\} = (1,2)H \end{aligned}$$

Che forma la seguente **partizione**



Teorema - Cardinalità classi laterali destre e sinistre

Tutte le **classi laterali destre e sinistre** hanno **la stessa cardinalità**, che è quella di H.

<u>Dimostrazione</u>: dati $a, b \in G$ costruiamo una **corrispondenza**

$$\alpha : Ha \to Hb$$
$$\alpha(ha) = hb$$

α è **biunivoca**

- **Iniettività**:

$$
\begin{aligned}
\alpha(ha) &= \alpha(h'a) \\
hb &= h'b \\
hbb^{-1} &= h'bb^{-1} \\
h &= h'
\end{aligned}
$$

- **Suriettività**: dato che $hb \in Hb$, risulta per definizione

$$hb = \alpha(ha)$$

Ora se prendo $b = e$ ottengo una corrispondenza biunivoca

$$\alpha : Ha \to He = H$$

Posso procedere allo stesso modo con i **laterali sinistri**:

$$
\begin{gathered}
\beta : aH \to bH \\
\beta(ah) = bh
\end{gathered}
$$

è una biezione, che da luogo ad una biezione $aH \leftrightarrow H$ quando prendo $b = e$. Quindi

$$
\begin{array}{ccccc}
aH & \leftrightarrow & H & \leftrightarrow & Ha \\
\beta \updownarrow & & & & \updownarrow \alpha \\
bH & & & & Hb
\end{array}
$$

Teorema - Teorema di Lagrange

Se G è un **gruppo finito** e $H \leq G$, detto $[G : H]$ il **numero di laterali** di H in G, risulta

$$|G| = [G : H]|H|$$

> ℹ️ $[G : H]$ si legge **indice di H in G**.

Corollario

Se $H \leq G$, G **finito** allora $|H| \mid |G|$

Dimostrazione: Abbiamo visto che tutte le classi laterali hanno la **stessa cardinalità** $|H|$. Poiché le classi laterali **formano una partizione** di G, l'ordine di G è quello di H moltiplicato per il numero di classi laterali denotato con $[G : H]$.