LEZIONE 5-10-20

ES: Sia G finito, $H \lneq G$. Allora

$$\bigcup_{g \in G} gHg^{-1} \neq G.$$

DIM Consideriamo $X = \{ gHg^{-1} : g \in G \}$ e l'azione di G su X

$\forall g \in G$, $K \in X$ allora $g \cdot K = gKg^{-1}$

Equiv: $\Phi : G \to S(X)$

$g \mapsto (K \mapsto gKg^{-1})$ ⌟

Quest'azione è TRANSITIVA: dati $K_1, K_2 \in X$ esiste $g \in G$

$g \cdot K_1 = K_2$.

⌜ Se $K_1 = aHa^{-1}$, $K_2 = bKb^{-1}$, allora

$$(ba^{-1}) \cdot K_1 = ba^{-1} a H a^{-1} a b^{-1} = bHb^{-1} = K_2$$ ⌟

⌜ Questo significa che G agisce su X con un'unica orbita ⌟

$$\Rightarrow |X| = |Orb(H)| = \frac{|G|}{|Stab_G(H)|} = \frac{|G|}{|N_G(H)|}$$

$Stab_G(H) = \{ g \in G : gHg^{-1} = H \} = N_G(H)$

Vogliamo dimostrare che

$G \neq \bigcup_{g \in G} gHg^{-1}$ ed è un'unione di $\frac{|G|}{|N_G(H)|}$ coniugati

ma $\frac{|G|}{|N_G(H)|} \leq \frac{|G|}{|H|}$ (poiché $H \leq N_G(H)$)

($|gHg^{-1}| = |H|$)

Dunque se $G = \bigcup_{g \in G} gHg^{-1}$ avremo che

$$|G| = \left| \bigcup_{g \in G} gHg^{-1} \right| = \left| \bigcup_{K \in X} K \right| \overset{(\leq)}{} \sum_{K \in X} |K|$$

$$= |H| \cdot \left| G / N_G(H) \right| \overset{(\leq)}{} |H| \cdot \frac{|G|}{|H|} = |G|$$

e dunque le due disuguaglianze dovranno essere uguaglianze.

Il primo $\leq$ vale se e solo se
- tutti i $K \in X$ sono disgiunti

oppure
- c'è un solo $K \in X$.

$H \in X$ ricavamente

Osserviamo che se ci fosse un solo $K \in X$ allora $G = \bigcup_{K \in X} K = K = H$,
e ciò è contro le ipotesi; inoltre
il primo caso non è possibile in quanto tutti i K contengono e.

Segue dunque che l'ipotesi di assurdo $G = \bigcup_{g \in G} gHg^{-1}$ è falsa e dunque la tesi. ∎

LEMMA: Supponiamo di avere un'azione di G su X transitiva.
Allora $\forall x, y \in X$ si ha che $\exists\, g \in G$

$$\mathrm{Stab}_G(x) = g \cdot \mathrm{Stab}_G(y) \cdot g^{-1}.$$

In particolare $\mathrm{Stab}_G(x) \simeq \mathrm{Stab}_G(y)$.

DIM: Per transitività $\exists\, g \in G$ tale che $y = g \cdot x$. Allora

$$\mathrm{Stab}_G(x) = \{a \in G : a \cdot x = x\}$$

$$\mathrm{Stab}_G(g \cdot x) = \{b \in G : b \cdot (g \cdot x) = g \cdot x\}$$

OSS: se l'azione non fosse trans., allora potremo restringerci ad un'orb:

se $y \in Orb_G(x)$
allora $\exists g \in G$
$Stab_G(y) = g\, Stab_G(x)\, g^{-1}$.

$$\{h \in G : g^{-1} \cdot h \cdot g \cdot x = g^{-1} \cdot g \cdot x = x\}$$

$$\{h \in G : (g^{-1} h g) \cdot x = x\}$$

$$\{h \in G : g^{-1} h g \in Stab_G(x)\}$$

$$g\, Stab_G(x)\, g^{-1} = \{h \in G : h \in g\, Stab_G(x)\, g^{-1}\}$$ ∎

ES: Sia G (finito) che agisce trans. su X, $|X| \geq 2$
Allora $\exists\, g \in G$ che agisce su X senza punti fissi, ovvero

$$g \cdot x \neq x \qquad \forall x \in X.$$

DIM: La tesi è equiv. a $g \notin Stab_G(x)\ \forall x \in X$.
Fissiamo allora $x_0 \in X$. Dal lemma precedente

$$\{Stab_G(x) : x \in X\} = \{a\, Stab_G(x_0)\, a^{-1} : a \in G\}$$

Vogliamo quindi $g \notin \bigcup_{x \in X} Stab_G(x) = \bigcup_{a \in G} a\, Stab_G(x_0)\, a^{-1}$.
Il primo esercizio ci dice che se $Stab_G(x_0) \lneq G$ allora effettivamente esiste un tale g.
Ma se per assurdo avessimo che $Stab_G(x_0) = G$ allora

$$|X| = |Orb_G(x_0)| = \frac{|G|}{|Stab_G(x_0)|} = 1,$$

e questo è assurdo poiché $|X| \geq 2$. ∎

AUTOMORFISMI DI $(\mathbb{Z}/p\mathbb{Z})^n$

Ricordiamo che $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ $\longleftrightarrow$ "matrici 1×1 invertibili su $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$"

$(x \mapsto ax) \longleftarrow\!\shortmid\ a$

(*) $\mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z})^2\right)$ $\quad (\mathbb{Z}/p\mathbb{Z})^2$ è generato da $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$

[è proprio una base come $\mathbb{F}_p$-spazio]

Allora $\varphi \in \mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z})^2\right)$ è determinato da

$$\varphi\left(\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}a\\c\end{pmatrix} \qquad \varphi\left(\begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}b\\d\end{pmatrix}$$

$\downarrow$ deve avere lo stesso ordine!

$(\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0)\}$

$\downarrow$ deve essere tale che $\left\langle \begin{pmatrix}a\\c\end{pmatrix}, \begin{pmatrix}b\\d\end{pmatrix} \right\rangle = (\mathbb{Z}/p\mathbb{Z})^2$ (p^2)

$\left\langle \begin{pmatrix}a\\c\end{pmatrix} \right\rangle$ (p) $\subseteq$ $\left\langle \begin{pmatrix}a\\c\end{pmatrix}, \begin{pmatrix}b\\d\end{pmatrix} \right\rangle$ ($p \cdot p^2$)

Ma $\left\langle \begin{pmatrix}a\\c\end{pmatrix}, \begin{pmatrix}b\\d\end{pmatrix} \right\rangle$ ha p el. se e solo se

$$\left\langle \begin{pmatrix}a\\c\end{pmatrix}, \begin{pmatrix}b\\d\end{pmatrix} \right\rangle = \left\langle \begin{pmatrix}a\\c\end{pmatrix} \right\rangle, \text{ cioè } \begin{pmatrix}b\\d\end{pmatrix} \in \left\langle \begin{pmatrix}a\\c\end{pmatrix} \right\rangle$$

$\Rightarrow$ Devo mandare $\begin{pmatrix}1\\0\end{pmatrix} \overset{\varphi}{\longmapsto} \begin{pmatrix}a\\c\end{pmatrix} \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0)\}$

e $\begin{pmatrix}0\\1\end{pmatrix} \overset{\varphi}{\longmapsto} \begin{pmatrix}b\\d\end{pmatrix} \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \left\langle \begin{pmatrix}a\\c\end{pmatrix} \right\rangle$

Dunque

$$\#\mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z})^2\right) = \sum_{\begin{pmatrix}a\\c\end{pmatrix} \neq (0)} \#\text{ scelte di } \begin{pmatrix}b\\d\end{pmatrix} \notin \left\langle \begin{pmatrix}a\\c\end{pmatrix} \right\rangle$$

$$= \#\text{scelte di } \varphi\left(\begin{pmatrix}1\\0\end{pmatrix}\right) \cdot \#\text{scelte } \varphi\left(\begin{pmatrix}0\\1\end{pmatrix}\right)$$

$$= (p^2-1)(p^2-p)$$

$\rightsquigarrow$ Possiamo pensare l'automorfismo come un automorfismo di $2p$ vett?

Sì

$$\varphi \longleftrightarrow \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in Aut\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2\right)$$

Infatti $\varphi\begin{pmatrix} x \\ y \end{pmatrix} = \varphi\left(x\begin{pmatrix} 1 \\ 0 \end{pmatrix} + y\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = x\varphi\begin{pmatrix} 1 \\ 0 \end{pmatrix} + y\varphi\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$= x\begin{pmatrix} a \\ b \end{pmatrix} + y\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ax + cy \\ bx + dy \end{pmatrix}.$$

$$= \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

Come mai OMOMORFISMI $\left(\mathbb{Z}/p\mathbb{Z}\right)^n \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^n$ sono la stessa cosa di

APPLICAZIONI LINEARI $\mathbb{F}_p^{\,n} \to \mathbb{F}_p^{\,n}$?

[$\Leftarrow$] $f : \mathbb{F}_p^{\,n} \longrightarrow \mathbb{F}_p^{\,n}$ lineare $\Rightarrow f(v+w) = f(v) + f(w)$ è omom!

[$\Rightarrow$] Sia $f : \mathbb{F}_p^{\,n} \longrightarrow \mathbb{F}_p^{\,n}$ omom.. Voglio dim che

$$f(\lambda v) = \lambda f(v) \qquad \forall \lambda \in \mathbb{F}_p,\ v \in \mathbb{F}_p^{\,n}$$

Ma λ è un intero modulo p: $\lambda = \bar{n}$ con $n \in \mathbb{Z}$.

Allora $f(\lambda v) = f(\underbrace{v + \cdots + v}_{n \text{ volte}}) = f(v) + \cdots + f(v) = \lambda f(v)$

TEOREMA (*) $Hom_{GRP}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^n, \left(\mathbb{Z}/p\mathbb{Z}\right)^m\right) \longleftrightarrow Hom_{Vect\text{-}\mathbb{F}_p}\left(\mathbb{F}_p^{\,n}, \mathbb{F}_p^{\,m}\right)$

(*) $Aut_{GRP}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^n\right) \longleftrightarrow Aut_{Vect\text{-}\mathbb{F}_p}\left(\mathbb{F}_p^{\,n}\right) \longleftrightarrow GL(n, \mathbb{F}_p)$

$= \{\text{matrici } M \in Mat(n, \mathbb{F}_p) : \det M \neq 0\}$

Segue che $\#\, Aut\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^n\right) =$

$$= (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1})$$

- $(p^n - 1)$: tutto tranne $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$
- $(p^n - p)$: tutto tranne i multipli della prima colonna $\rightsquigarrow p$ cose da evitare
- $(p^n - p^2)$: tutto tranne i vett. lin dip. dalle prime 2 colonne $\rightsquigarrow av_1 + bv_2$ $\rightsquigarrow p^2$ cose da evitare

GRUPPI LIBERI E PRESENTAZIONI

Vogliamo specificare come sono fatti i gruppi a partire dai loro generatori.

ES: Singolo generatore: due tipi: $\mathbb{Z} = \langle 1 \rangle = \langle x \rangle$ → non soddisfa alcuna relazione

$\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle = \langle x \mid x^n = 1 \rangle$ → soddisfa la rel. $x^n = 1$

ES: Gruppi con più generatori?

Esempio: 2 generatori

$G = \langle a, b \rangle \ni a, b, ab, ba, a^2, b^2, a^{-1}, a^{-1}b^3a^7b^{-2}, \dots$

Nella maggior parte dei casi alcuni di questi el. sono uguali.

ES: $S_3 = \langle \underbrace{(1\,2)}_{a}, \underbrace{(1\,2\,3)}_{b} \rangle \ni a, b, a^{-1} = a, b^{-1} = b^2, \dots$

DEF Sia X un insieme $X = \{x_1, x_2, \dots\}$. Poniamo

$$X^{-1} := \{x_1^{-1}, x_2^{-1}, \dots\}$$

l'INSIEME DEGLI INVERSI FORMALI di X.

L'ALFABETO corrispondente ad X è $X \cup X^{-1}$.

Le PAROLE di un alfabeto $\mathcal{A}$ sono gli elementi di $\bigcup_{n \geq 0} \mathcal{A}^n$.

Una parola è RIDOTTA se non compaiono mai x_i, x_i^{-1} consecutivamente.

Un gruppo $G \supseteq X$ è LIBERO SU X se tutte le parole ridotte rappresentano elementi diversi, e G è generato da X.

ES: Se $X = \{x\}$ allora le parole ridotte sono

(*) ε, la parola vuota

(*) $x \cdots x = x^n$

(*) $x^{-1} \cdots x^{-1} = x^{-n}$.

$\Rightarrow$ G è libero su X se e solo se $G \simeq \mathbb{Z}$

OSS. Dato H gruppo, allora $\mathrm{Hom}(\mathbb{Z}, H) \longleftrightarrow \{f : \mathbb{Z} \to H\} \hookrightarrow H$

$(\varphi = n \mapsto h^n) \longmapsto (1 \mapsto h) \longmapsto h$

TEOREMA Sia G un gruppo libero su X. Allora

$$\mathrm{Hom}(G, H) \longleftrightarrow \{f : X \to H\}$$

$$\begin{pmatrix} x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \cdots x_{i_k}^{\pm 1} \\ \downarrow \\ h_{i_1}^{\pm 1} h_{i_2}^{\pm 1} \cdots h_{i_k}^{\pm 1} \end{pmatrix} \longleftrightarrow \begin{pmatrix} x_1 \mapsto h_1 \\ x_2 \mapsto h_2 \\ \vdots \end{pmatrix}$$

PRESENTAZIONI DI GRUPPO

Sia H generato da n elementi $g_1, \dots, g_n$. Per il Teorema, c'è un omomorfismo

gpp. libero su n elementi $x_1, \dots, x_n$ $\leftarrow$ $F(n) \xrightarrow{\varphi} H$

$x_i \longmapsto g_i$

Tale omom. è suriettivo: $\mathrm{Im}\,\varphi < H$ contenente $g_1, \dots, g_n$, ma questi generano e quindi $\mathrm{Im}\,\varphi = H$.

Per il 1° Teorema di Isomorfismo: $F(n)/\ker\varphi \cong H$.

Una **PRESENTAZIONE** di H è dunque una scrittura del tipo

$$\langle x_1, \dots, x_n \mid \text{parole in } x_1^{\pm 1}, \dots, x_n^{\pm 1} \text{ che generano } \ker\varphi \rangle$$

ES: $D_n = \langle r, s \mid s^2, r^n, srsr \rangle$

questi el. generano $\ker\varphi$: sono parole in r, s (cioè el. di $F(2)$) sbustante in $F(2)$ ma che vengono mappate a id in D_n

$$= \langle r, s \mid s^2 = r^n = id, \; srs = r^{-1} \rangle$$

Es: $\mathbb{Z}_2\mathbb{Z} \times \mathbb{Z}_2\mathbb{Z} = \langle x, y \mid x^2 = y^2 = 1, \; xy = yx \rangle$

Omomorfismi a Partire da una Presentazione

Cor Sia $H = \langle x_1, \dots, x_n \mid w_1, \dots, w_n \rangle$, K altro gruppo. Allora

$$\mathrm{Hom}(H, K) \longleftrightarrow \left\{ f : \{x_1, \dots, x_n\} \to K \text{ tale che } f(x_i) \text{ rispetta le relazioni } w_1, \dots, w_n \right\}$$

Dim $H \simeq \dfrac{F(n)}{\langle w_1, \dots, w_n \rangle}$. Allora

$$\begin{array}{ccc} F(n) & \xrightarrow{\;\varphi\;} & \langle f(x_1), \dots, f(x_n) \rangle \leq K \\ \pi \downarrow & \nearrow \exists! \, \overline{\varphi} & \\ H & & \end{array}$$

Ma per ipotesi $f(x_i)$ rispettano le relazioni $\{w_j\}$, ovvero $\langle w_1, \dots, w_n \rangle \leq \mathrm{Ker}\, \varphi$. Per il 1° Teorema di Omom. posso allora considerare $\overline{\varphi} : H \cong \frac{F(n)}{\langle w_1, \dots, w_n \rangle} \longrightarrow \langle f(x_1), \dots, f(x_n) \rangle \leq K$ tale che $\varphi = \pi \overline{\varphi}$.

Dunque abbiamo associato ad ogni $f : \{x_1, \dots, x_n\} \to K$ t.c. i $f(x_i)$ soddisfano le relazioni un omom $\overline{\varphi} : H \to K$.

D'altro canto dato $\varphi : H \to K$ possiamo considerare $\varphi|_{\{x_1, \dots, x_n\}}$ che è una funzione $\{x_1, \dots, x_n\} \xrightarrow{f} K$ tale che $f(x_1), \dots, f(x_n)$ soddisfano le relazioni cercate. ∎

TEOREMA Esiste un unico gruppo libero su n el. a meno di isomorfismo.

DIM Dati $\langle x_1, \dots, x_n \rangle \xrightarrow[x_i \mapsto y_i]{f} \langle y_1, \dots, y_n \rangle$ per la proprietà del gruppo libero.

Dall'altro $\langle y_1, \dots, y_n \rangle \xrightarrow[y_i \mapsto x_i]{g} \langle x_1, \dots, x_n \rangle$ per la stessa prop.

Infine ovviamente $f \circ g = g \circ f = id$, dunque

$$\langle x_1, \dots, x_n \rangle \simeq \langle y_1, \dots, y_n \rangle$$ ∎

ES: $S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \ \tau\sigma\tau = \sigma^{-1} \rangle$

$\mathrm{Hom}(S_3, S_3)$? Basta dare $f(\sigma)$, $f(\sigma)$ tali che

$$f(\sigma)^3 = 1, \quad f(\tau)^2 = 1, \quad f(\tau\sigma\tau\sigma) = 1$$

$$\Updownarrow$$

$$f(\tau) f(\sigma) f(\tau) = f(\sigma)$$

$f(\sigma) \in \{1, \sigma, \sigma^2\}$

- $f(\sigma) = 1$: basta specificare $f(\tau)$ diverso da 1 o σ^2 → 4 tali omomorfismi $\tau \mapsto \tau, \sigma\tau, \sigma^2\tau$
- $f(\sigma) = \sigma$: $\begin{cases} f(\tau)^2 = 1 \\ f(\tau)\sigma f(\tau)^{-1} = \sigma^{-1} \end{cases}$ Vera per ogni trasposizione $\Rightarrow \tau \mapsto \tau, \sigma\tau, \sigma^2\tau$
- $f(\sigma) = \sigma^2$: come il caso 2

Di questi gli ultimi 6 sono automorfismi.