Lezione 14 Algebra I

Federico De Sisti

2024-12-02

1 Classi coniugate in S_n

Teorema 1 (Fondamentale)
Due permutazioni in S_n sono coniugate se e solo se hanno la stessa struttura ciclica

Dimostrazione (Già iniziata nella lezione precedente)
Avevamo dimostrato che se $\tau = (a_1, \dots, a_n) \in S_n$ e $\sigma \in S_n$
Allora
$\sigma\tau\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$
Da questo abbiamo dedotto che date $\sigma, \tau \in S_n$ qualsiasi, allora:
$\sigma\tau\sigma^{-1}$ *ha la stessa struttura ciclica di* τ
· *Vogliamo ora dimostrare il viceversa, ovvero: Date $\tau, \omega \in S_n$ vogliamo costruire σ tale che $\sigma\tau\sigma^{-1} = \omega$ (τ, ω con la stessa struttura ciclica)*
Per ipotesi, $\tau = \tau_1 \dots tau_h$ e $\omega = \omega_1 \dots \omega_h$ dove $h \geq 1, \tau_i, \omega_i$ sono $k_i -$ cicli
Denotiamo $\tau_i = (a^i_1{}^i_{k_i}), \omega = (b^i_1 \dots b_{k_i})$
Possiamo definire σ esplicitamente
Infatti
$\sigma\tau_i\sigma^{-1} = (\sigma(a^i_1) \dots \sigma(a^i_{k_i})$
Quindi
Definiamo $\sigma := \{\sigma(a^i_j) = b^i_j \quad \forall i \in \{1, \dots, h\}, j \in \{1, \dots, k\}, \sigma(t) = t$ se $t \neq a^i_j\}$
Allora $\sigma\tau_i\sigma^{-1} = \omega_i \quad \forall i = h$
$\Rightarrow \sigma\tau\sigma^{-1} = \sigma\tau_1 \dots \tau_h\sigma^{-1}$
$= (\sigma\tau_1\sigma^{-1}) \dots (\sigma\tau_h\sigma^{-1})$
$= \omega_1 \dots \omega_h = \omega$ □

Osservazione
Dato che la dimostrazione è costruttiva, è molto utile per risolvere gli esercizi.

2 Il gruppo p-Sylow

Idea
Prendiamo un gruppo finito.
Esistono sottogruppi di un dato ordine (divisore di $|G|$)?
Il risultato parziale che abbiamo è dato dal Teorema di Cauchy:
Se $\exists p$ primo e divide $|G|$, allora:
$\exists H \leq G$ t.c. $|H| = p$
Sylow, va avanti secondo questo filone:

Definizione 1
Sia G gruppo finito, $p, r, m \in \mathbb{Z}_{>0} t.c.$
$\cdot |G| = p^r \cdot m$
$\cdot p$ *primo* *(ogni gruppo finito ha queste caratteristiche)*
$\cdot MCD(p, m) = 1$
Un sottogruppo di ordine p^r in G si chiama $p-Sylow$
L'insieme dei $p-Sylow$ si denota con $Syl_p(G)$

Teorema 2 (I Teorema di di Sylow (1862-1872))
Se G gruppo finito, p primo che divide $|G|$, Allora:
$Syl_p(G) \neq \emptyset$

Dimostrazione
Sia $X := \{S \subseteq G : \ |S| = p^r\}$
Definisco un azione
$G \times X \to X$
$(g, s) \to gS = \{gs | s \in S\}$
Dalle osservazioni $\Rightarrow p \nmid |X|$
D'altra parte, x si decompone in G-orbite
Inoltre $|O_S| \cdot |Stab_S| = |G| = p^r \cdot m$
$\Rightarrow \exists$ *almeno un elemento $\underline{S} \in X t.c.\ \underline{S}| \not\equiv_p 0$*
Allora

$$\frac{|O_{\underline{S}}|}{|O_{\underline{S}}|} \cdot |Stab_{\underline{S}}| = \frac{p^r \cdot m}{|O_{\underline{S}}|} \in \mathbb{Z}.$$

Da cui segue che $|Stab_{\underline{S}}| \equiv_{p^r} 0$
$p^r \leq |Stab_{\underline{S}}$
L'idea ora è di dimostrare che $Stab_{\underline{S}} \in Syl_p(G)$
Essendo uno stabilizzatore, è sicuramente un sottogruppo, quindi basta dimostrare che $|Stab_{\underline{S}}| \leq p^r$
Osservazione/Esercizio
$\exists$ applicazione iniettiva, $Stab_{\underline{S}} \to p$ definita fissando un elemento qualsiasi $\underline{s} \in S$
$Stab_{\underline{S}} \to \underline{S}$
$g \to g\underline{s}$
dimostrare che questa funzione è iniettiva, questo porta alla conclusione che $|Stab_{\underline{S}}| \leq |\underline{S}| = p^r$ dato che $\underline{S} \in X$ □

Esempio
Sia $|G| = 12 = 2^2 \cdot 3 = 3 \cdot 4$
Dal I Teorema di Sylow segue:
$\cdot Syl_2(G) \neq 0 \Rightarrow \exists H \leq G : |H| = 4$
$\cdot Syl_3(G) \neq 0 \Rightarrow \exists H \leq G : |H| = 3$

Osservazione
$\cdot X = O_{S_1} \circ O_{S_2} \circ \ldots O_{S_r}$
$\Rightarrow |X| = \sum_{j=1}^{r} |O_{S_j}|$ Ma $|X| \not\equiv_p 0$

Idea
G gruppo, $|G| = p^r$
$MCD(p, m) = 1, p$ primo, $p, r, m \in \mathbb{Z}_{>0}$
Per il I teorema sappiamo che $(1) Syl_p(G) \neq 0$.
il II Teorema ci dirà che (2) Tutti i $p - Sylow$ sono tra loro coniugati.
Il (2) ci dice che $\rightarrow$ Un p-Sylow è normale se e solo se è l'unico p-Sylow.
Quanti sono i p-Sylow? Analogamente $n_p := |Syl_p(G)| =?$

Teorema 3 (II Teorema di Sylow)
Dati $H_1, H_2 \in Syl_p(G), \exists g \in G$ *t.c.* $\quad gH_1g^{-1} = H_2$

Dimostrazione
L'enunciato è equivalente a dimostrare che la seguente azione è transitiva.

$$\begin{aligned} G \times Syl_p(G) &\rightarrow Syl_p(G) \\ (g, H) \quad &\rightarrow gHg^{-1} \end{aligned}$$

o equivalentemente, che esiste un'unica orbita.
Per assurdo supponiamo che esistano due orbite distinte, O_H^G *e* O_K^G.
Passo 1
Denotiamo con $Stab_H^G$ *lo stabilizzatore di* H *rispetto a questa azione*

$$\begin{cases} |G| = |O_H^G| \cdot |Stab_H^G| = |O_H^G| \cdot [Stab_H^G : H] \cdot |H| \\ H \leq Stab_H^G \end{cases} .$$

Quindi $p \not| \, |O_H^G|$
Passo 2
Restringiamo l'azione

$$\begin{aligned} K \times O_H^G \rightarrow O_H^G \\ (k,S) \quad S\ k^{-1} \end{aligned}$$

Rispetto a questa azione abbiamo orbite diverse.
In particolare
$|O_H^G| = O_{H_1}^K \cup \ldots \cup O_{H_r}^K$

$$\begin{aligned} \Rightarrow |O_H^G| &= \sum_{i=1}^{r} |O_{H_i}^K| \\ &= \sum_{i=1}^{r} \frac{|K|}{Stab_{H_i}^K} \\ &= \sum_{i=1}^{r} \frac{p^r}{|Stab_{H_i}|} \end{aligned}$$

Dato che $p \not| |O_H^G|$ *deduciamo che* $\exists H_i$ *t.c.* $|O_{H_i}^K| = 1$
$\Rightarrow 1 = |O_{H_i}^K| = [K : Stab_{H_i}^G]$
Quindi K *stabilizza* H_i
$\Rightarrow kH_ik^{-1} = H_i \quad \forall k \in K$
$\Rightarrow KH_i = H_iK$
Passo 3 $KH_i = H_iK \Rightarrow KH_i \leq G$
$|KH_i| = \dfrac{|K| \cdot |H_i|}{|K \cap H_i|} = \dfrac{p^{2r}}{p^s}$ *con* $s < r$ *(poichè altrimenti* $K = H_i$*)*
$|KH_i| = p^{2r-s} = p^{r+t}$ *con* $t > r$
Ma $|KH_i|$ *divide* $|G| = p^r m$ *per Lagrange (assurdo)*

$\square$