# Libriccino degli esempi: ALGEBRA

**Dimostrazioni sui Gruppi**

Dat

## Gruppo simmetrico $S_n$:

Su $S_n$ può venir richiesto di risolvere alcune equazioni oppure, dato un elemento $\sigma \in S_n$, cercare $Cl(\sigma)\,; Z(\sigma)\,; N(\langle\sigma\rangle)$.

***Esempio 1 (Equazioni):***

Dire quando sono risolubili le seguenti equazioni in $S_n$:

| | |
|---|---|
| $x^2 = (123)$ | $x = (321)\rho \mid \rho^2 = \mathrm{Id}$, ossia un 2-ciclo, questo vale anche per i successivi. |
| $x^2 = (1234)$ | Mai, infatti nessun elemento al quadrato può dare un ciclo di lunghezza pari. |
| $x^2 = (1234)(56)$ | Mai, i due cicli pari dovrebbero avere stessa lunghezza. |
| $x^2 = (12)(34)$ | Si costruisce mettendo gli spazi dove dovrebbe esserci il secondo ciclo: $(1\blacksquare 2\blacksquare)$, quindi riempiendo gli spazi ottengo: $\{(1324)\,;(1423)\}$ |
| $x^2 = (123)(456)$ | $\{(142536)\,;\ (152634)\,;\ (162435)\,;(321)(654)\}$ |

***Esempio 2 (Centralizzatore):***

$\sigma = (123)(456) \in S_6$ ; determinare $|Cl(\sigma)|$ e $Z(\sigma)$.

Per cercare $|Cl(\sigma)|$ sfrutto il fatto che gli elemento coniugati di $\sigma$ hanno la stessa struttura, quindi caratterizzo gli elementi di $|Cl(\sigma)| = \binom{6}{3}\binom{3}{3} \cdot 2 \cdot \frac{1}{2} = 40\,; |Z(\sigma)| = \frac{|S_n|}{|Cl(\sigma)|} = \frac{6!}{40} = 18$

Per caratterizzare gli elementi considero che:

1- Tutti i cicli disgiunti da $\sigma$ vanno bene (Sono 0)

2- Tutto ciò che è generato dai cicli disgiunti da cui è formato: $H_1 = \{\mathrm{Id}, (123), (321)\}$ e $H_2 = \{\mathrm{Id}, (456), (654)\}$

Consideriamo dunque che $H_1H_2 \in Z(\sigma)$ e vale $|H_1H_2| = \frac{|H_1|\cdot|H_2|}{|H_1 \cap H_2|} = \frac{3\cdot 3}{1} = 9$

3- Infine le permutazioni che scambiano gli elementi, essendo due sarà un oggetto $\cong S_2$ ; cercandolo in maniera esplicita: $K = \langle(14)(25)(34)\rangle$

Ottengo quindi $|HK| = 18$ , quello che stavo cercando.

***Esempio 3 (Centralizzatore):***

$\sigma = (12)(345) \in S_6$ ; determinare $|Cl(\sigma)|$ e $Z(\sigma)$.

$|Cl(\sigma)| = \binom{n}{2}\binom{n-2}{3} \cdot 2 = \frac{n!}{2!(n-5)!}\,; |Z(\sigma)| = 6(n-5)!$ ed individuandoli otteniamo quelli generati dai cicli di $\sigma$: $H_1 = \{\mathrm{Id}\,;(12)\}\,; H_2 = \{\mathrm{Id}\,;(345)\,;(543)\}$ e i cicli distinti da $\sigma$ che sono $(n-5)!$, osserviamo inoltre che non esistono permutazioni interne in quanto i cicli di $\sigma$ hanno lunghezza diversa.

***Esempio 4 ($A_n$):***

Studiare lo stesso $\sigma = (123)$ su $S_4$ e su $A_4$.

$|Cl(\sigma)| = \binom{4}{3} \cdot 2 = 8$ in $S_4$ ; $|Z(\sigma)| = 3$ e quindi siccome $|A_n| = \frac{1}{2}|S_n|$ segue che essendo uno pari ed uno dispari debba essere quello pari dimezzato, $|Cl(\sigma)|_{A_4} = 4$ ; $|Z(\sigma)|_{A_4} = 3$.

***Esempio 5 ($A_n$):***

Studiare lo stesso $\sigma = (123)$ su $S_5$ e su $A_5$.

$|Cl(\sigma)| = \binom{5}{3} \cdot 2 = 20$ in $S_4$ ; $|Z(\sigma)| = 6$ quindi non posso usare il trucco di prima, cerco quindi di dimostrare che uno di loro è completamente contenuto in $A_n$, in questo caso l'intera orbita di $(123)$ è formata da elementi di $A_n$, quindi: $|Cl(\sigma)|_{A_5} = 20$ ; $|Z(\sigma)|_{A_5} = 3$

***Esempio 6 (<u>Normalizzatore</u>):***

Calcolare la cardinalità del normalizzatore di $\sigma = (123)(4567) \in S_7$.

Ricaviamo $|Cl(\sigma)| = \binom{7}{3}\binom{4}{4} \cdot 2! \cdot 3!$ ; $|Z(\sigma)| = 12$ inoltre sappiamo che:
$|N(\langle\sigma\rangle)| = |Z(\sigma)| \cdot |\mathrm{Aut}(\langle\sigma\rangle)|$
Studiando la cardinalità degli automorfismi (Basta assegnare il generatore essendo ciclico),
$|\mathrm{Aut}(\langle\sigma\rangle)| = \phi(12) = 4$ quindi $|N(\langle\sigma\rangle)| = 48$
Sono quelli di $Z(\sigma)$ combinati con gli automorfismi di $\langle\sigma\rangle$.

Gruppi di Sylow:

## <u>Anelli:</u>

Gli esercizi più standard riguardano piccole dimostrazioni sulle radici dei polinomi e il procedimento inverso, dato un elemento individuare il polinomio minimo per cui sia una radice.

***Esempio 1:***

Sia $\alpha \in \mathbb{C}$ una radice di $x^3 + 2x - 1$.
Trovare il polinomio minimo di $\alpha + 1$ ; $\alpha^{-1}$ ; $\alpha^2 + 1$ su $\mathbb{Q}$

Studiamo l'equazione data e cerchiamo di vedere se è fattorizzabile in $\mathbb{Q}$. Essendo irriducibile per verifica diretta sulle radici in $\mathbb{Q}$ ricaviamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Questo passaggio è importante per sapere la dimensione del polinomio che sto cercando.
Sfruttiamo quindi la condizione dettata dall'equazione, $\alpha^3 + 2\alpha - 1 = 0$:

$(\alpha - 1) \rightarrow g(x) = f(x - 1)$ quindi il p.m. è: $(x - 1)^3 + 2(x - 1) - 1$

$(\alpha^2+1)$ in questo caso non risulta evidente, costruiamo quindi il sistema lineare dato dall'equazione:
$(\alpha^2+1)^3 + a(\alpha^2+1)^2 + b(\alpha^2+1) + c = 0$ ; sfruttando l'equazione iniziale calcoliamo le potenze:
$(\alpha^2+1)^3 = \alpha^2 - \alpha + 2$ ; $(\alpha^2+1)^2 = \alpha + 1$ il sistema diventa dunque:
$(1+a)\alpha^2 + (-1+b)\alpha + (2+a+b+c) = 0$ lo uguagliamo a quello iniziale e troviamo il polinomio minimo: $\quad g(x) = x^3 - 2x^2 - 1$

$(\alpha^{-1}) \rightarrow$ osserviamo che per calcolare un inversa possiamo sfruttare il **polinomio reciproco** (Ossia quello calcolato invertendo l'ordine dei coefficienti), quindi $g(x) = -x^3 + 2x + 1$

***Esempio 2:***

Determinare il polinomio minimo di $\sqrt{2\sqrt{2}-3}$ su $\mathbb{Q}$.

Si procede cercando per prima cosa un polinomio che si annulli su quella radice, da quello estraiamo poi il polinomio minimo.
Eliminiamo una radice o un fattore dopo l'altro:

$$x^2 = 2\sqrt{2} - 3 \rightarrow x^2 + 3 = 2\sqrt{2} \rightarrow (x^2+3)^2 = 8 \rightarrow x^4 + 6x^2 + 1 = 0$$

Dimostrandone l'irriducibilità abbiamo concluso.

## Campi:

Gli esercizi standard sui campi sono la ricerca del campo di spezzamento di un polinomio e il corrispondente gruppo di Galois.

***Esempio 2:***

Calcolare il grado del campo di spezzamento e il gruppo di Galois di $f(x) = x^3 - 2$ su $\mathbb{Q}$.

Studio del campo di spezzamento:

Individuo le radici di $f(x) \rightarrow \{\sqrt[3]{2}, \varepsilon_3\sqrt[3]{2}, \varepsilon_3^2\sqrt[3]{2}\}$ con $\varepsilon_3 = \frac{-1+i\sqrt[3]{2}}{2}$ con polinomio minimo $x^2 + x + 1$

Il campo di spezzamento sarà $E = \mathbb{Q}(\varepsilon_3, \sqrt[3]{2})$ e siccome deve essere multiplo di tutti i fattori (3 e 2) e minore di 3! con 3 grado del polinomio avremo: $[E : \mathbb{Q}] = 6$

Studio del gruppo di Galois:

Sappiamo che (Avendo il polinomio 3 radici) il gruppo di Galois $Gal(E) < S_3$ quindi $Gal(E) \cong S_3$

Come è fatto? (Utile per poter costruirlo al contrario)

Cerco i sottogruppi di $G$

$\{\mathrm{Id}\}$ ; $G$ ; il 3-ciclo $H = \{\mathrm{Id}, (123), (321)\}$ ; i 3 gruppi generati dalle trasposizioni $M_1 = \{\mathrm{Id}, (12)\}$ ; $M_2 = \{\mathrm{Id}, (23)\}$ ; $M_3 = \{\mathrm{Id}, (13)\}$

Li associo ai campi secondo la corrispondenza di Galois:

$\{\mathrm{Id}\} \rightarrow$ tutto ciò che viene fissato da Id, tutto $E$.

$G \rightarrow$ ciò che è fissato da tutto, ossia $\mathbb{Q}$
$M_1$ ; $M_2$ ; $M_3 \rightarrow$ lasciano fissi $\mathbb{Q}(\varepsilon_3^2\sqrt[3]{2})$ ; $\mathbb{Q}(\sqrt[3]{2})$; $\mathbb{Q}(\varepsilon_3\sqrt[3]{2})$
Per capire cosa viene associato ad $H$ osserviamo che $\left|Gal({}^{E}/_{\mathbb{Q}(\varepsilon_3)}\right| = 3 = |H| \rightarrow H$ lo associamo a $\mathbb{Q}(\varepsilon_3)$.

***Esempio 3:***

Calcolare il grado del campo di spezzamento e il gruppo di Galois di $(x^3+1)(x^3-5)$ su $\mathbb{Q}$.

Studio del campo di spezzamento:

Studiamo i due diversi fattori:
$(x^3+1) = (x-1)(x^2-x+1)$ su $\mathbb{Q}$.
$(x^3-5)$ è irriducibile per Eisenstein.

Scriviamo la fattorizzazione in irriducibili:

$f(x) = (x-1)(x^2-x+1)(x^3-5)$

Individuiamo le radici dei fattori irriducibili:

$(x^2-x+1) \rightarrow \left\{\frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\right\}$
$(x^3-5) \rightarrow \left\{\sqrt[3]{5}, \varepsilon_3\sqrt[3]{5}, \varepsilon_3^2\sqrt[3]{5}\right\}$

Il campo di spezzamento è quindi (eliminando ciò che può essere ottenuto dal campo $\mathbb{Q}$):
$E = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{5}, \varepsilon_3)$
Cerchiamo di eliminare ciò che può essere ottenuto da un altro fattore, in questo caso:
$\varepsilon_3 = \frac{-1+i\sqrt{3}}{2} \rightarrow \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\varepsilon_3)$
Quindi $E = \mathbb{Q}(\varepsilon_3, \sqrt[3]{5})$

Individuiamo i gradi dei polinomi minimi (Per $\sqrt[3]{5}$ è 3 mentre per $\varepsilon_3$ è 2).
Quindi per il teorema di estensioni per torri, siccome le due estensioni non coincidono essendo una reale e l'altra immaginaria vale:

$$[\mathbb{Q}(\varepsilon_3, \sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon_3, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] \cdot [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 6$$

Studio del gruppo di Galois:

$G$ è isomorfo ad un sottogruppo di $S_3$ in quanto permuta le radici di $(x^3-5)$
$G$ ha cardinalità uguale al grado dell'estensione (6), quindi $G = S_3$

***Esempio 3 bis:***

Calcolare il grado del campo di spezzamento e il gruppo di Galois di $(x^3+1)(x^3-5)$ su $\mathbb{F}$.

Studio del campo di spezzamento:

Calcoliamo i possibili valori per $x^3$:

$$\begin{cases} 1^3=1 \\ 2^3=1 \\ 3^3=6 \\ 4^3=1 \\ 5^3=6 \\ 6^3=6 \end{cases}$$

Scriviamo la fattorizzazione in irriducibili:

$f(x) = (x-3)(x-5)(x-6)(x^3-5)$

Dove $(x^3-5)$ è irriducibile per verifica diretta.

Quindi il grado dell'estensione è 3 $\rightarrow E = \mathbb{F}_{7^3}$

Studio del gruppo di Galois:

Il gruppo di Galois ha ordine 3 quindi (A prescindere di quale $S_n$ sia sottogruppo) è isomorfo a $\mathbb{Z}/_{3\mathbb{Z}}$

**Notazione:**

Un gruppo di Galois di ordine primo *p* sarà isomorfo a $\mathbb{Z}/_{p\mathbb{Z}}$ che verrà indicato con $C_p$.