Gli automorfismi di $\mathcal{S}_n$

La struttura di $\mathcal{A}ut\,(\mathcal{S}_n)$

Riflessione 1. Con lo studio dei prodotti semidiretti è nata l'esigenza di studiare la possibile struttura del gruppo degli automorfismi di un dato gruppo. Vediamo quanto possiamo dire su $\mathcal{A}ut\,(\mathcal{S}_n)$; in particolare vogliamo dimostrare che:

$$\forall i \geq 3,\ i \neq 6,\ \mathcal{A}ut\,(\mathcal{S}_i) \ \simeq\ \mathcal{S}_i$$

Prima di arrivare alla dimostrazione vediamo alcuni risultati preliminari.

Osservazione 1. Siano H, K due gruppi e $H \xrightarrow{\phi} K$ un automorfismo. Allora dette $H_1, \ldots, H_i$ le classi di coniugio di H e $K_1, \ldots, K_j$ le classi di coniugio di K abbiamo che

$$\forall m_1^i,\ \exists n_1^j \ t.c.\ \phi(H_m) = K_n$$

Cioè un automorfismo manda classi di coniugio in classi di coniugio.

Dimostrazione. Sia $h_m \in H_m$ e $\gamma = \phi(h_m)$. Certamente γ appartiene ad una classe di coniugio in K (la sua classe di coniugio), che chiameremo K_n. Vogliamo a questo punto dimostrare

$$\phi(H_m) = K_n$$

'$\subseteq$' sia $h = sh_ms^{-1}$ un generico elemento di H_m, visto che ϕ è per ipotesi un automorfismo possiamo scrivere:

$$\phi(h) = \phi(sh_ms^{-1}) = \phi(s)\phi(h_m)\phi(s)^{-1} = \phi(s)\gamma\phi(s)^{-1} \in K_n$$

'$\supseteq$' Sia $k \in K_n$ un generico elemento della classe di coniugio di γ, sappiamo allora di poter scrivere, per qualche elemento $\check{k} \in K$, $k = \check{k}\gamma\check{k}^{-1}$. Ma la ϕ è una funzione bigettiva, esiste dunque $\check{h} \in H$ tale che $\phi(\check{h}) = \check{k}$. Sappiamo inoltre che $\check{h}h_m\check{h}^{-1}$ continua ad appartenere ad H_m. Possiamo quindi scrivere:

$$\phi(\check{h}h_m\check{h}^{-1}) = \check{k}\gamma\check{k}^{-1} = k$$

e visto che $\check{h}h_m\check{h} \in H_m$ abbiamo la tesi.

□

Definizione 1 (Automorfismi interni)**.** Sia $\mathcal{G}$ un gruppo e $\mathcal{G} \xrightarrow{C} \mathcal{A}ut\,(\mathcal{G})$ la funzione coniugio che associa ad ogni elemento $g \in \mathcal{G}$ il coniugio rispetto a g (che è sempre un automorfismo). Sappiamo dal corso di Aritmetica che C è un omomorfismo.
L'immagine di C viene detta insieme degli automorfismi interni e si scrive $Int(\mathcal{G})$. Quindi $Int(\mathcal{G}) < \mathcal{A}ut\,(\mathcal{G})$ sono i coniugi in $\mathcal{A}ut\,(\mathcal{G})$.

Teorema 1.

$$\forall n \geq 3,\ n \neq 6,\ \mathcal{A}ut\,(\mathcal{S}_n) \ \simeq\ \mathcal{S}_n$$

Dimostrazione. Notiamo innanzitutto che l'affermazione è falsa per $n = 2$, difatti $\mathcal{S}_2 \ \simeq\ \mathbb{Z}_2$ ma $\mathcal{A}ut\,(\mathcal{S}_2) \ \simeq\ \mathbb{Z}_2^* \ \simeq\ \{e\}$. Considerato allora $n \geq 3$, siano in $\mathcal{S}_n$,

$$T_1 = \{(a, b)\ t.c.\ a \neq b\} \subseteq \mathcal{S}_n$$
$$T_2 = \left\{(a_{(1,1)}, a_{(1,2)})(a_{(2,1)}, a_{(2,2)})\ t.c.\ (i, j) \neq (k, s) \implies a_{(i,j)} \neq a_{(k,s)}\right\} \subseteq \mathcal{S}_n$$
$$T_k = \left\{(a_{(1,1)}, a_{(1,2)}) \dots (a_{(k,1)}, a_{(k,2)})\ t.c.\ (i, j) \neq (k, s) \implies a_{(i,j)} \neq a_{(k,s)}\right\} \subseteq \mathcal{S}_n$$

Cioè T_i è l'insieme delle permutazioni che sono prodotto di i trasposizioni disgiunte. Abbiamo quindi che per ogni i, T_i è una classe di coniugio. Osserviamo inoltre che $\bigcup T_i$ è l'insieme di tutti e soli gli elementi di ordine 2 in $\mathcal{S}_n$.
Sia dunque $\phi \in \mathcal{A}ut\,(\mathcal{S}_n)$, per quanto appena detto sull'unione dei T_i e per l'Osservazione 1 possiamo dire che $\phi(T_1) = T_j$ per qualche j, infatti ϕ deve mandare elementi di ordine 2 in elementi con lo stesso ordine.
Contiamo quindi le cardinalità dei vari T_i, abbiamo che:

$$|T_1| = \binom{n}{2}$$
$$|T_k| = \frac{\binom{n}{2}\binom{n-2}{2} \cdot \ldots \cdot \binom{n-2(k-1)}{2}}{k!} = \frac{n \cdot \ldots \cdot (n - 2k + 1)}{2^k k!}$$

Se abbiamo che $\phi T_1 = T_k$ dobbiamo avere che le cardinalità dei due insiemi sono uguali. Possiamo dire:

$$|T_1| = |T_k| \iff 2^{k-1}k! = (n-2)(n-3) \cdot \ldots \cdot (n - 2k + 1)$$

Se $k = 2$ questa equazione diventa $4 = (n-2)(n-3)$, che non ha soluzioni intere. Nei casi $k \geq 3$ l'equazione è invece equivalente a:

$$2^{k-1} = (n-2)(n-3) \cdot \ldots \cdot (n - k + 1)\binom{n-k}{k}$$

Questa equazione, per i vari k:

$k = 3$ Nel caso $k = 3$ questa equazione ha soluzione solo se $n = 6$ (che infatti vedremo essere un caso particolare).

$k > 3$ In questi casi l'assurdo si ha dal fatto che vogliamo esprimere una potenza di 2 come prodotto di vari fattori fra cui sono presenti un numero pari e un numero dispari (i numeri sono $n - 2$ e $n - 3$, che quindi creano un assurdo per la fattorizzazione se $n > 4$ ma il caso $n = 4$ si esclude con una semplice verifica).

Sappiamo dunque che se ϕ è un automorfismo di $\mathcal{S}_n$ con $n \neq 6$ deve essere che $\phi(T_1) = T_1$. Ma sappiamo anche che ogni elemento di $\mathcal{S}_n$ può essere scritto come prodotto di elementi di T_1, quindi $\phi\,|_{T_1}$ determina completamente ϕ.

Per quanto visto possiamo dire che $\exists a_1, a_2 \in \{1, \dots, n\}$ tali che

$$\phi\big((1,2)\big) = (a_1, a_2)$$

Sappiamo inoltre che $(1,2)$ e $(1,3)$ non commutano, quindi non possono commutare nemmeno $\phi\big((1,2)\big)$ e $\phi\big((1,3)\big)$. Dobbiamo quindi avere (senza perdita di generalità)

$$\phi\big((1,3)\big) = (a_1, a_3)$$

e inoltre, per iniettività e dobbiamo avere $a_1 \neq a_2 \neq a_3 \neq a_1$. Notiamo che abbiamo:

$$\phi\big((2,3)\big) = \phi\big((1,3)(1,2)(1,3)\big) = (a_1, a_3)(a_1, a_2)(a_1, a_3) = (a_2, a_3)$$

Vogliamo dimostrare per induzione su i che $\phi\big((1,i)\big) = (a_1, a_i)$ e che tutti gli a_j sono due a due distinti. Sia dunque $i > 3$ e supponiamo quanto detto vero per tutti i numeri fino a $i-1$. Sappiamo che $(1,i)$ non commuta con $(1,2)$, possono esserci quindi solo due casi:

- $\phi\big((1,i)\big) = (a_2, a_i)$ per un certo a_i diverso da $a_1, a_2, \dots, a_{i-1}$. Ma allora avremmo che $\phi\big((1,i)\big)$ non commuta con $\phi\big((2,3)\big)$ mentre invece $(1,i)$ commuta con $(2,3)$. Assurdo.
- Deve quindi essere $\phi\big((1,i)\big) = (a_1, a_i)$. Ma allora, per iniettività della funzione, dobbiamo avere che $a_i \neq a_j$ per tutti gli $j < i$ (altrimenti $(1,i)$ e $(1,j)$ avrebbero la stessa immagine).

Abbiamo scoperto che ϕ altro non è che un coniugio, infatti vi è un coniugio che fa la stessa cosa: il coniugio rispetto a

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

Quindi C_σ e ϕ sono due automorfismi di $\mathcal{S}_n$ che coincidono sulle permutazioni del tipo $(1,i)$, ma allora (visto che sono omomorfismi) devono coincidere su tutto $\mathcal{S}_n$. Dobbiamo quindi avere $\phi = C_\sigma$.
Per concludere consideriamo l'omomorfismo:

$$\begin{array}{rccc} C: & \mathcal{S}_n & \longrightarrow & \mathcal{A}ut\,(\mathcal{S}_n) \\ & \sigma & & C_\sigma \end{array}$$

Sappiamo che, per $n \geq 3$, $Ker(C) = Z\,(\mathcal{S}_n) = \{e\}$, inoltre $Imm(C) = Int(\mathcal{S}_n) < \mathcal{A}ut\,(\mathcal{S}_n)$. Abbiamo quindi un omomorfismo iniettivo (quindi un automorfismo con l'immagine) tra $\mathcal{S}_n$ e $\mathcal{A}ut\,(\mathcal{S}_n)$ che ha come immagine $Int(\mathcal{S}_n)$ (il gruppo dei coniugi), dunque $\mathcal{S}_n \simeq Int(\mathcal{S}_n)$.
Concludiamo quindi dicendo che abbiamo dimostrato:

$$\mathcal{S}_n \simeq Int(\mathcal{S}_n) = \mathcal{A}ut\,(\mathcal{S}_n)$$

□