APPUNTI SUGLI AUTOMORFISMI ESTERNI DI S_6

GIOVANNI GAIFFI
ARGOMENTO FACOLTATIVO, CORSO DI ALGEBRA 1, ANNO 2010/2011

1. Premessa

Durante il corso avete visto, come esercizio, che, per $n \geq 3$ e $n \neq 6$, il gruppo $Aut(S_n)$ coincide con $Int(S_n)$, ossia tutti gli automorfismi del gruppo simmetrico sono interni, e $Int(S_n) \cong S_n$. Per $n = 2$, $S_2 \cong \mathbb{Z}_2$ e dunque $Aut(S_2) = \{e\}$. Ma cosa accade quando $n = 6$? In effetti in questo caso non è più vero che tutti gli automorfismi sono interni. Nelle pagine seguenti descriviamo un metodo per costruire (e contare) gli automorfismi esterni di S_6.

2. Breve ripasso sulle azioni dei gruppi

Sia G un gruppo e X un insieme. Una *azione* del gruppo G sull'insieme X è una mappa $G \times X \to X$ che manda la coppia (g, x) in $g \cdot x \in X$ e ha le seguenti proprietà:
a) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ per ogni $g_1, g_2 \in G$ e $x \in X$;
b) $e \cdot x = x$ per ogni $x \in X$ (dove e indica l'identità di G).

Esempio 2.1. Pensiamo per esempio al gruppo simmetrico S_n che agisce sull'insieme $\{1, 2, \ldots, n\}$ o al gruppo moltiplicativo $\mathbb{R} - \{0\}$ che agisce sul piano $\mathbb{R}^2$ attraverso la moltiplicazione per scalare: $t \cdot (x, y) = (tx, ty)$.

Osservazione 2.2. Nel seguito talvolta scriveremo gx invece di $g \cdot x$ (quando riterremo che non ci sia rischio di equivoci).

Proposizione 2.3. *Per ogni $g \in G$ l'applicazione $A_g = g\cdot \ : X \to X$ che manda x in $g \cdot x$ è bigettiva.*

Dimostrazione. La dimostrazione segue subito osservando che $A_{g^{-1}} = g^{-1}\cdot$ è l'applicazione inversa di A_g. □

Sia $S_X = Bij(X \to X)$ il gruppo delle funzioni bigettive dall'insieme X in sé (con la legge di composizione fra funzioni). In particolare, se X è finito e $|X| = n$, S_X è isomorfo a S_n.

Teorema 2.4. *La mappa $A : G \to S_X$ che associa a $g \in G$ la funzione bigettiva A_g è un omomorfismo di gruppi.*

Dimostrazione. Dati $g_1, g_2 \in G$ bisogna mostrare che $A_{g_1 g_2} = A_{g_1} A_{g_2}$. Preso $x \in X$, vale $A_{g_1 g_2}(x) = (g_1 g_2) \cdot x$ mentre $A_{g_1} A_{g_2}(x) = A_{g_1}(g_2 \cdot x) = g_1 \cdot (g_2 \cdot x)$ che è uguale a $(g_1 g_2) \cdot x$ per la definizione di azione.

□

Definizione 2.5. Data una azione del gruppo G sull'insieme X, si definisce l'*orbita* (detta anche la *G-orbita*) di un elemento $x \in X$ come il sottoinsieme di X:

$$Orb(x) = \{g \cdot x \mid \forall g \in G\}$$

L'insieme $Orb(x)$ si scrive anche $G \cdot x$.

Si osserva che le orbite di X costituiscono una partizione di X. Infatti ogni $x \in X$ appartiene certamente ad un orbita, la $G \cdot x$. D'altra parte, se $x \in G \cdot y$, allora $x = g \cdot y$ per un certo $g \in G$. Quindi $G \cdot x = G \cdot (g \cdot y)$, ma per la definizione di azione, $G \cdot (g \cdot y) = (Gg) \cdot y$. Ora la classe laterale Gg coincide con G, dunque $G \cdot x = G \cdot y$ e abbiamo mostrato che x appartiene ad una sola orbita in X.

Esempio 2.6. Sia H un sottogruppo di G. Facciamo agire H su G (pensato come insieme) mediante $h \cdot g = gh^{-1}$ dove a destra dell'uguale l'operazione è la moltiplicazione in G. Le orbite rispetto a questa azione sono i laterali destri gH di H in G.

Definizione 2.7. Lo *spazio delle orbite* di X rispetto all'azione di un gruppo Γ è l'insieme i cui elementi sono le orbite di X. Lo indicheremo come X/Γ.

Osservazione 2.8. La notazione concorda con quella usata per l'insieme G/H dei laterali destri di un sottogruppo H di G.

Si può pensare allo spazio delle orbite di X anche identificandolo col quoziente di X rispetto alla relazione di equivalenza data da:

$$x \sim y \text{ se e solo se } x \text{ e } y \text{ appartengono alla stessa orbita.}$$

3. Spazi di configurazioni

Dato un campo K, consideriamo la retta proiettiva $\mathbb{P}(K)$ ottenuta quozientando lo spazio $K^2 - \{(0,0)\}$ rispetto alla relazione:

$$(x, y) \sim (\gamma, \delta) \text{ se e solo se esiste } k \in K - \{0\} \text{ tale che } k(x, y) = (\gamma, \delta).$$

Definizione 3.1. Lo *spazio delle configurazioni* di $\mathbb{P}(K)$ di dimensione n è l'insieme

$$Conf_n(\mathbb{P}(K)) = \{(p_1, p_2, \dots, p_n) \in \mathbb{P}(K)^n \mid p_i \neq p_j \text{ se } i \neq j\}$$

Osservazione 3.2. Se $\mathbb{P}(K)$ è finito e ha q elementi, l'insieme $Conf_n(\mathbb{P}(K))$ è vuoto se $n > q$. Se invece $n = q$ allora $Conf_n(\mathbb{P}(K))$ ha esattamente $n! = q!$ elementi.

In queste dispense giocherà un ruolo importante lo spazio $Conf_6(\mathbb{P}(\mathbb{F}_5))$, dove $\mathbb{F}_5$ è il campo con 5 elementi. Lo spazio proiettivo $\mathbb{P}(\mathbb{F}_5)$ ha 6 elementi; li elenchiamo, scrivendo ognuno di essi anche in coordinate proiettive:

$$\begin{array}{rl} 0 & [1,0] \\ 1 & [1,1] \\ 2 & [1,2] \\ 3 & [1,3] \\ 4 & [1,4] \\ \infty & [0,1] \end{array}$$

Dunque $Conf_6(\mathbb{P}(\mathbb{F}_5))$ ha 6! elementi.

Entrano adesso in scena le proiettività. Osserviamo che il gruppo $PGL(K)$ delle proiettività di $\mathbb{P}(K)$ agisce sull'insieme $Conf_n(\mathbb{P}(K))$ con l'azione naturale componente per componente: se $\phi \in PGL(K)$ allora

$$\phi \cdot (p_1, p_2, \dots, p_n) = (\phi(p_1), \phi(p_2), \dots, \phi(p_n)).$$

Definizione 3.3. Chiamiamo $\mathcal{M}_n(K)$ lo spazio delle orbite di $Conf_n(\mathbb{P}(K))$ rispetto all'azione di $PGL(K)$:

$$\mathcal{M}_n(K) = Conf_n(\mathbb{P}(K))/PGL(K)$$

In questi appunti studieremo in particolare

$$\mathcal{M}_6(\mathbb{F}_5) = Conf_6(\mathbb{P}(\mathbb{F}_5))/PGL(\mathbb{F}_5) =$$
$$= \{(p_1, p_2, p_3, p_4, p_5, p_6) \in \mathbb{P}(\mathbb{F}_5)^6 \mid p_i \neq p_j \text{ se } i \neq j\}/PGL(\mathbb{F}_5)$$

Quanti sono gli elementi di questo insieme? Come è noto, una proiettività è univocamente determinata una volta che viene assegnato il suo valore su tre punti della retta proiettiva, dunque preso un qualunque elemento $(p_1, p_2, p_3, p_4, p_5, p_6)$ di una $PGL(\mathbb{F}_5)$-orbita in $Conf_6(\mathbb{P}(\mathbb{F}_5))$, c'è una e una sola proiettività $\phi \in PGL(\mathbb{F}_5)$ tale che $\phi(p_1) = 0, \phi(p_2) = 1, \phi(p_6) = \infty$. Per ogni $PGL(\mathbb{F}_5)$-orbita possiamo dunque scegliere uno e un solo rappresentante della forma

$$(0, 1, q_1, q_2, q_3, \infty) \quad \text{con } q_i \neq q_j \text{ se } i \neq j \text{ e } q_i \neq 0, 1, \infty \ \forall i$$

Gli elementi di $\mathcal{M}_6(\mathbb{F}_5)$ sono tanti quanti i rappresentanti delle orbite, che a questo punto si contano facilmente: abbiamo 3 scelte per q_1 (infatti deve essere diverso da $0, 1, \infty$), 2 per q_2 e q_3 a quel punto è determinato. In conclusione $\mathcal{M}_6(\mathbb{F}_5)$ ha 6 elementi...un ottimo terreno per una azione di S_6..

4. L'azione di S_6 su $\mathcal{M}_6(\mathbb{F}_5)$

Facciamo agire S_n su $Conf_n(\mathbb{P}(K))$ permutando le coordinate: se $\sigma \in S_n$ allora

$$\sigma \cdot (p_1, p_2, \ldots, p_n) = (p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}).$$

È immediato verificare che questa azione commuta con l'azione di $PGL(K)$ descritta nel paragrafo precedente. Consideriamo infatti $P = (p_1, p_2, \ldots, p_n) \in Conf_n(\mathbb{P}(K))$, $\sigma \in S_n$ e $\phi \in PGL(K)$ e verifichiamo che $\sigma \cdot (\phi \cdot P) = \phi \cdot (\sigma \cdot P)$:

$$(p_1, p_2, \ldots, p_n) \xrightarrow{\phi\cdot} (\phi(p_1), \phi(p_2), \ldots, \phi(p_n)) \xrightarrow{\sigma\cdot} (\phi(p_{\sigma(1)}), \phi(p_{\sigma(2)}), \ldots, \phi(p_{\sigma(n)}))$$
$$(p_1, p_2, \ldots, p_n) \xrightarrow{\sigma\cdot} (p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}) \xrightarrow{\phi\cdot} (\phi(p_{\sigma(1)}), \phi(p_{\sigma(2)}), \ldots, \phi(p_{\sigma(n)}))$$

Dunque l'azione di S_n "passa" allo spazio delle orbite $\mathcal{M}_n(K)$: se $\mathcal{O} \in \mathcal{M}_n(K)$ (dunque è una $PGL(K)$-orbita in $Conf_n(\mathbb{P}(K))$) e $Q \in Conf_n(\mathbb{P}(K))$ è un suo rappresentante possiamo definire, $\forall \sigma \in S_n$,

$$\sigma \cdot \mathcal{O} = \text{l'orbita a cui appartiene } \sigma \cdot Q$$

La commutatività fra le azioni di S_n e $PGL(K)$ garantisce che questa è una buona definizione: se $\phi \cdot Q$ (con $\phi \in PGL(K)$) è un altro rappresentante della $PGL(K)$-orbita $\mathcal{O}$, allora $\sigma \cdot (\phi \cdot Q) = \phi \cdot (\sigma \cdot Q)$ che è nella stessa $PGL(K)$-orbita di $\sigma \cdot Q$.

Venendo al caso che ci interessa, abbiamo dunque un'azione di S_6 su $\mathcal{M}_6(\mathbb{F}_5)$. Questa azione dà origine ad un automorfismo esterno di S_6. Per verificarlo ordiniamo i 6 elementi di $\mathcal{M}_6(\mathbb{F}_5)$:

$$L_1 = \text{orbita con rappresentante } (0, 1, 2, 3, 4, \infty)$$
$$L_2 = \text{orbita con rappresentante } (0, 1, 2, 4, 3, \infty)$$
$$L_3 = \text{orbita con rappresentante } (0, 1, 3, 2, 4, \infty)$$
$$L_4 = \text{orbita con rappresentante } (0, 1, 3, 4, 2, \infty)$$
$$L_5 = \text{orbita con rappresentante } (0, 1, 4, 2, 3, \infty)$$
$$L_6 = \text{orbita con rappresentante } (0, 1, 4, 3, 2, \infty)$$

Consideriamo la trasposizione $(1, 2) \in S_6$ e calcoliamo $(1, 2) \cdot L_1$. Sul rappresentante dell'orbita abbiamo:

$$(1, 2) \cdot (0, 1, 2, 3, 4, \infty) = (1, 0, 2, 3, 4, \infty)$$

Dobbiamo capire a quale orbita appartiene $(1,0,2,3,4,\infty)$. Per farlo basta trovare la proiettività che riporta questo elemento ad un rappresentante canonico, ossia la proiettività ϕ tale che $\phi(1)=0, \phi(0)=1, \phi(\infty)=\infty$.

Pensando le proiettività nella forma $\dfrac{ax+b}{cx+d}$ (con $ad-bc\neq 0$) la proiettività in questione è la $\phi = 1-x$. Applicandola a $(1,0,2,3,4,\infty)$ troviamo $(0,1,4,3,2,\infty)$ che è il rappresentante dell'orbita L_6 (ricordiamo che i numeri che compaiono sono elementi di $\mathbb{F}_5$ dunque per esempio $1-2=4$). Dunque $(1,2)\cdot L_1 = L_6$.

A questo punto, dato che l'azione di S_6 è ben definita, sappiamo anche che $(1,2)\cdot L_6 = L_1$. Calcoliamo adesso $(1,2)\cdot L_3$. Sul rappresentante dell'orbita abbiamo:

$$(1,2)\cdot(0,1,3,2,4,\infty) = (1,0,3,2,4,\infty)$$

Per capire a che orbita appartiene dobbiamo anche questa volta applicare la $\phi = 1-x$ e otteniamo $(0,1,3,4,2,\infty)$ che è il rappresentante dell'orbita L_4. Dunque $(1,2)\cdot L_3 = L_4$ e $(1,2)\cdot L_4 = L_3$.

Continuando allo stesso modo otteniamo che $(1,2)\cdot L_5 = L_6$ e $(1,2)\cdot L_6 = L_5$.

Sappiamo già abbastanza per capire che siamo in presenza di un automorfismo esterno di S_6. Questa azione infatti induce un omomorfismo (vedi Teorema 2.4)

$$\theta \,:\, S_6 \to S_{\mathcal{M}_6(\mathbb{F}_5)} \cong S_6$$

e abbiamo calcolato che $\theta((1,2)) = ((1,6)(2,5)(3,4))$. Se dimostriamo che θ è un automorfismo possiamo subito concludere che è esterno: infatti un automorfismo interno, ossia il coniugio per un elemento $\sigma\in S_6$, manda trasposizioni in trasposizioni.

Per ragioni di cardinalità ci basta dimostrare che l'omomorfismo θ è iniettivo.

Come sappiamo A_6 è semplice allora $Ker\ \theta \cap A_6$ è uguale a $\{e\}$ oppure ad A_6. Se fosse $Ker\ \theta = A_6$ allora l'immagine di θ conterrebbe al più 2 elementi, cosa che si esclude calcolando per esempio anche $\theta((3,4))$ e scoprendo che $\theta((34)) = (1,3)(2,5)(4,6)$.

Se invece $Ker\ \theta\cap A_6 = \{e\}$ e $Ker\ \theta \neq \{e\}$, allora sia $x\in Ker\ \theta$ una permutazione diversa da e: dunque x deve essere dispari. Ma x^2 è pari, e quindi è uguale a e. Allora x deve avere ordine 2 e ci sono solo due possibilità: può essere una trasposizione o un prodotto di tre trasposizioni disgiunte. Nel primo caso, siccome $Ker\ \theta$ è normale, allora dovrebbe contenere tutte le trasposizioni, e dunque tutto S_6, assurdo perché siamo nell'ipotesi $Ker\ \theta\cap A_6 = \{e\}$. Nel secondo caso $Ker\ \theta$ dovrebbe contenere tutti i prodotti di tre trasposizioni disgiunte: ma allora apparterrebbe a $Ker\ \theta$ anche

$$(1,2)(3,5)(4,6)(4,6)(1,3)(2,5) = (1,5)(2,3)$$

in contraddizione con $Ker\ \theta\cap A_6 = \{e\}$.

Dunque dobbiamo avere $Ker\ \theta = \{e\}$ e θ è un automorfismo esterno.

Esercizio 4.1. Dimostrare che $Int(S_n)$ ha indice 2 in $Aut(S_n)$, e dunque che $Aut(S_n)$ ha ordine 1440.