

Il gruppo degli automorfismi

di Gabriel Antonio Videtta

Nota. Nel corso del documento per (G, \cdot) si intenderà un qualsiasi gruppo. Si scriverà gh per indicare $g \cdot h$, omettendo il punto.

Definizione (gruppo degli automorfismi). Si definisce **gruppo degli automorfismi** di un gruppo G il gruppo $(\text{Aut}(G), \circ)$ dotato dell'operazione di composizione.

Si può associare ad ogni elemento $g \in G$ un automorfismo particolare φ_g determinato dalla seguente associazione:

$$h \xrightarrow{\varphi_g} ghg^{-1}.$$

Definizione (gruppo degli automorfismi interni). Si definisce **gruppo degli automorfismi interni** di un gruppo G il gruppo $(\text{Inn}(G), \circ)$ dotato dell'operazione di composizione, dove:

$$\text{Inn}(G) = \{\varphi_g \mid g \in G\}.$$

Gli automorfismi interni soddisfano alcune proprietà. Per esempio vale che:

$$\varphi_g \circ \varphi_h = \varphi_{gh},$$

così come vale anche che:

$$\varphi_g^{-1} = \varphi_{g^{-1}}.$$

Chiaramente $\text{Inn}(G) \leq \text{Aut}(G)$. Tuttavia vale anche che $\text{Inn}(G)$ è un sottogruppo normale di $\text{Aut}(G)$. Infatti, se $f \in \text{Aut}(G)$, vale che:

$$f \circ \varphi_g \circ f^{-1} = \varphi_{f(g)} \in \text{Inn}(G).$$

Inoltre, se G è abeliano, φ_g coincide con la sola identità Id (infatti, in tal caso, $\varphi_g(h) = ghg^{-1} = gg^{-1}h = h$).

Si dimostra adesso un teorema fondamentale che mette in relazione $\text{Inn}(G)$ con un gruppo quoziente particolare di G , $G/Z(G)$. Preliminarmente, si osserva che $Z(G)$ è un sottogruppo normale di G , e quindi $G/Z(G)$ è effettivamente un gruppo. Allora si può enunciare la:

Proposizione. $\text{Inn}(G) \cong G/Z(G)$.

Dimostrazione. Sia $\zeta : G \rightarrow \text{Inn}(G)$ la mappa che associa g al proprio automorfismo interno associato φ_g . Si osserva che ζ è un omomorfismo tra gruppi:

$$\zeta(gh) = \varphi_{gh} = \varphi_g \circ \varphi_h = \zeta(g) \circ \zeta(h).$$

Chiaramente ζ è una mappa surgettiva, e quindi $\text{Im } \zeta = \text{Inn}(G)$. Si osserva inoltre che $\text{Ker } \zeta$ è esattamente il centro di G , $Z(G)$. Infatti, se $g \in \text{Ker } \zeta$, vale che $\zeta(g) = \text{Id}$, e quindi che:

$$ghg^{-1} = h \implies gh = hg \quad \forall h \in G.$$

Allora, per il Primo teorema di isomorfismo, $G/\text{Ker } \zeta = G/Z(G) \cong \text{Inn}(G)$. \square

Il gruppo $G/Z(G)$ risulta particolarmente utile nello studio della commutatività del gruppo. Infatti vale la:

Proposizione. $G/Z(G)$ è ciclico se e solo se G è abeliano (e quindi se e solo se $G/Z(G)$ è banale).

Dimostrazione. Se G è abeliano, $G/Z(G)$ contiene solo l'identità, ed è dunque ciclico. Viceversa, sia $gZ(G)$ un generatore di $G/Z(G)$. Se $h, k \in G$, vale in particolare che esistono $m, n \in \mathbb{N}$ tali per cui $hZ(G) = g^mZ(G)$ e $kZ(G) = g^nZ(G)$. Allora esistono $z_1, z_2 \in Z(G)$ per cui $h = g^m z_1$ e $k = g^n z_2$.

Si conclude allora che:

$$hk = g^m z_1 g^n z_2 = g^n z_2 g^m z_1 = kh,$$

e quindi G è abeliano (da cui si deduce che $G/Z(G)$ è in realtà banale). \square

Allora, poiché $\text{Inn}(G) \cong G/Z(G)$, $\text{Inn}(G)$ è ciclico se e solo se G è abeliano (e dunque se e solo se è banale). Inoltre, il gruppo $\text{Inn}(G)$ risulta utile per definire in modo alternativo (ma equivalente) la nozione di *sottogruppo normale*. Infatti vale che:

Proposizione. Sia $H \leq G$. Allora $H \triangleleft G$ se e solo se H è φ_g -invariante per ogni $g \in G$ (ossia se $\varphi_g(H) \subseteq H$).

Dimostrazione. Se H è normale, allora $\varphi_g(h) = ghg^{-1}$ appartiene ad H per definizione. Allo stesso modo dire che H è φ_g -invariante equivale a dire che $gHg^{-1} \subseteq H$ per ogni $g \in G$. \square

In generale, se $H \triangleleft G$, vale che la restrizione $\varphi_g|_H$ è ancora un omomorfismo ed è in particolare un elemento di $\text{Aut}(H)$. Infatti $\varphi_g|_H$ è ancora iniettiva, e per ogni $h \in H$ vale che:

$$\varphi_g(g^{-1}hg) = h,$$

mostrando la surgettività di $\varphi_g|_H$ (infatti $g^{-1}hg \in H$).

Si può estendere questa idea considerando i sottogruppi di G che sono f -invarianti per ogni scelta di $f \in \text{Aut}(G)$.

Definizione (sottogruppo caratteristico). $H \leq G$ si dice **sottogruppo caratteristico** di G se H è f -invariante per ogni $f \in \text{Aut}(G)$.

In particolare, $H \leq G$ è un sottogruppo caratteristico di G se ogni automorfismo di G si riduce, restringendolo su H , ad un automorfismo di H . Infatti, se $f(H) \subseteq H$, vale anche che $f^{-1}(H) \subseteq H \implies H \subseteq f(H)$, e quindi $f(H) = H$ (da cui la surgettività dell'omomorfismo in H).

Chiaramente ogni sottogruppo caratteristico è un sottogruppo normale (infatti è in particolare φ_g -invariante per ogni scelta di $g \in G$), ma non è vero il contrario. Per esempio, si definisca l'automorfismo η per $(\mathbb{Q}, +)$ tale per cui:

$$x \xrightarrow{\eta} x/2.$$

Si osserva facilmente che η è un automorfismo. Dal momento che $(\mathbb{Q}, +)$ è abeliano, ogni suo sottogruppo è normale. In particolare $(\mathbb{Z}, +) \triangleleft (\mathbb{Q}, +)$. Tuttavia $\eta(\mathbb{Z}) \not\subseteq \mathbb{Z}$ (e quindi \mathbb{Z} non è caratteristico in \mathbb{Q}).

Esiste tuttavia, per qualsiasi scelta di gruppo G , un sottogruppo che è caratteristico, $Z(G)$ (oltre che G stesso ed il sottogruppo banale). Infatti, se $z \in Z(G)$ e $g \in G$, vale che:

$$f(z)g = f(z)f(f^{-1}(g)) = f(zf^{-1}(g)) = f(f^{-1}(g)z) = gf(z) \quad \forall f \in \text{Aut}(G),$$

e quindi $f(Z(G)) \subseteq Z(G)$ per ogni scelta di $f \in \text{Aut}(G)$.

Inoltre, se $H \leq G$ è l'unico sottogruppo di un certo ordine (o è comunque caratterizzato univocamente da una proprietà invariante per automorfismi), H è anche caratteristico (infatti gli automorfismi preservano le cardinalità essendo bigezioni).

Esempio ($\text{Aut}(S_3) \cong S_3$). Si osserva che $Z(S_3)$ deve essere obbligatoriamente banale¹. Infatti, se non lo fosse, $Z(S_3)$ potrebbe avere come cardinalità gli unici divisori positivi di $|S_3| = 6$, ossia 2, 3 e 6 stesso. In tutti e tre i casi $S_3/Z(S_3)$ sarebbe ciclico, e quindi S_3 sarebbe abeliano, \neq .

Poiché allora $Z(S_3)$ è banale, S_3 è isomorfo a $\text{Inn}(S_3) \leq \text{Aut}(S_3)$. Pertanto $|\text{Aut}(S_3)| \geq |S_3| = 6$. Ogni automorfismo è determinato dalle immagini dei propri generatori, e quindi ci sono al più $3 \cdot 2 = 6$ scelte dal momento che $S_3 = \langle (1, 2), (1, 2, 3) \rangle$. Allora $|\text{Aut}(S_3)| \leq 6$, da cui si deduce che $|\text{Aut}(S_3)| = 6$.

Dacché $\text{Aut}(S_3)$ ha lo stesso numero di elementi del suo sottogruppo $\text{Inn}(S_3)$, deve valere l'uguaglianza tra i due insiemi, e quindi $\text{Aut}(S_3) = \text{Inn}(S_3)$. Si conclude dunque che $\text{Aut}(S_3) \cong S_3$.

Si illustrano adesso dei risultati molto interessanti sui gruppi di automorfismi dei prodotti diretti, a partire dalla:

¹In generale $Z(S_n)$ è banale per $n \geq 3$.

Proposizione. Siano H e K due gruppi finiti di cardinalità coprime tra loro. Allora $H \times \{e\}$ e $\{e\} \times K$ sono caratteristici in $H \times K$.

Dimostrazione. Sia $\varphi \in \text{Aut}(H \times K)$. Si deve dimostrare che se $\varphi(h, e) = (h', k')$, allora $k' = e$. Chiaramente $\text{ord}(h, e) = \text{ord}(h) \mid |H|$. Allo stesso tempo $\text{ord}(h', k') = \text{mcm}(\text{ord}(h'), \text{ord}(k'))$. In particolare, dal momento che $\text{MCD}(|H|, |K|) = 1$, $\text{ord}(h', k') = \text{ord}(h') \text{ord}(k')$. Dacché φ è un automorfismo, $\text{ord}(h', k') = \text{ord}(h, e) = \text{ord}(h)$, e quindi $\text{ord}(h') \text{ord}(k') = \text{ord}(h)$. Allora $\text{ord}(k')$ deve dividere $|H|$, e quindi può valere soltanto 1, essendo $|H|$ e $|K|$ coprimi. Pertanto $k' = e$, e quindi $H \times \{e\}$ è caratteristico in $H \times K$. Analogamente si dimostra la tesi per $\{e\} \times K$. \square

Proposizione. Siano H e K due gruppi con $H \times \{e\}$ e $\{e\} \times K$ caratteristici in $H \times K$. Allora $\text{Aut}(H \times K) \cong \text{Aut}(H) \times \text{Aut}(K)$.

Dimostrazione. Nel corso della dimostrazione, se $\varphi \in \text{Aut}(H \times K)$, si denota con $\varphi_H = \iota_{H \hookrightarrow H \times \{e\}}^{-1} \circ \varphi|_{H \times \{e\}} \circ \iota_{H \hookrightarrow H \times \{e\}}$ la proiezione di φ su H a partire da H , e analogamente si fa lo stesso con φ_K . Tale notazione è ben definita dal momento che φ può sempre essere ristretta ad $H \times \{e\}$ (infatti è un sottogruppo caratteristico).

Sia allora $\alpha : \text{Aut}(H \times K) \rightarrow \text{Aut}(H) \times \text{Aut}(K)$ tale per cui $\varphi \xrightarrow{\alpha} (\varphi_H, \varphi_K)$. La mappa è ben definita dal momento che φ_H e φ_K sono due automorfismi di $\text{Aut}(H)$ e $\text{Aut}(K)$. Analogamente si definisce la mappa $\beta : \text{Aut}(H) \times \text{Aut}(K) \rightarrow \text{Aut}(H \times K)$ tale per cui $(\varphi_H, \varphi_K) \xrightarrow{\beta} [(h, k) \mapsto (\varphi_H(h), \varphi_K(k))]$.

Si verifica facilmente che α è un omomorfismo di gruppi, che $\alpha \circ \beta = \text{Id}_{\text{Aut}(H) \times \text{Aut}(K)}$ e che $\beta \circ \alpha = \text{Id}_{\text{Aut}(H \times K)}$, da cui segue la tesi. \square

Allo stesso modo si verifica che se α è un isomorfismo, allora $H \times \{e\}$ e $\{e\} \times K$ sono caratteristici in $H \times K$.

A partire dal precedente risultato, si dimostra facilmente che se $\text{MCD}(m, n) = 1$, allora:

$$\text{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/n\mathbb{Z}),$$

e quindi, ricordando che $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ per il Teorema cinese del resto e che $\text{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, vale che:

$$(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/mn\mathbb{Z})^*$$