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 $(\mathrm{Aut}(G), \circ)$ dotato dell'operazione di composizione.

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

$$h \overset{\varphi_g}{\longmapsto} ghg^{-1}.$$

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

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

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

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

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

Dimostrazione. Sia $\zeta : G \to \mathrm{Inn}(G)$ 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 $\operatorname{Im}\zeta = \mathrm{Inn}(G)$. Si osserva inoltre che $\operatorname{Ker}\zeta$ è esattamente il centro di G, $Z(G)$. Infatti, se $g \in \operatorname{Ker}\zeta$, vale che $\zeta(g) = \mathrm{Id}$, e quindi che:

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

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

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 $hZ(G) = g^m Z(G)$ e $kZ(G) = g^n Z(G)$. 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). □

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

Proposizione. Sia $H \leq G$. Allora $H \trianglelefteq G$ 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 $g \in G$. □

In generale, se $H \trianglelefteq G$, vale che la restrizione $\varphi_g|_H$ è ancora un omomorfismo ed è in particolare un elemento di $\mathrm{Aut}(H)$. 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 $f \in \mathrm{Aut}(G)$.

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

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:

$$x \overset{\eta}{\mapsto} x/2.$$

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:

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

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

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 ($\mathrm{Aut}(S_3) \cong S_3$)**.** Si[1] osserva che $Z(S_3)$ deve essere obbligatoriamente banale[2]. 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, $\lightning$.

Poiché allora $Z(S_3)$ è banale, S_3 è isomorfo a $\mathrm{Inn}(S_3) \leq \mathrm{Aut}(S_3)$. Pertanto $|\mathrm{Aut}(S_3)| \geq |S_3| = 6$. 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 $|\mathrm{Aut}(S_3)| \leq 6$, da cui si deduce che $|\mathrm{Aut}(S_3)| = 6$.

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

[1] Vale un fatto molto più generale: $\mathrm{Aut}(S_n) \cong S_n$ per ogni $n \geq 3$ con $n \neq 6$.
[2] In generale $Z(S_n)$ è banale per $n \geq 3$.

Esempio ($\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$)**.** Sia f un automorfismo di $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Allora, necessariamente, $f(\overline{1})$ deve essere un generatore di $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Si può quindi costruire un isomorfismo $\zeta : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^*$ tale per cui $f \overset{\zeta}{\mapsto} f(\overline{1})$.

Chiaramente ζ è un omomorfismo, infatti[3]:

$$\zeta(f \circ g) = f(g(\overline{1})) = f(\overline{1})g(\overline{1}) = \zeta(f)\zeta(g).$$

Inoltre $f(\overline{1}) = \overline{1} \implies f = \mathrm{Id}$, e quindi ζ è iniettiva. Infine, per ogni $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, si può costruire $f_a \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ di cui è immagine ponendo semplicemente che valga[4] $f_a(\overline{1}) = \overline{a}$. Si conclude quindi che ζ è un isomorfismo e dunque che vale il seguente isomorfismo:

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Il risultato è valido anche con $n = 0$, da cui si ricava che:

$$\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}^* \cong \{\pm 1\}.$$

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

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 $\varphi \in \mathrm{Aut}(H \times K)$. Si deve dimostrare che se $\varphi(h, e) = (h', k')$, allora $k' = e$. Chiaramente $\mathrm{ord}(h, e) = \mathrm{ord}(h) \mid |H|$. Allo stesso tempo $\mathrm{ord}(h', k') = \mathrm{mcm}(\mathrm{ord}(h'), \mathrm{ord}(k'))$. In particolare, dal momento che $\mathrm{MCD}(|H|, |K|) = 1$, $\mathrm{ord}(h', k') = \mathrm{ord}(h')\,\mathrm{ord}(k')$. Dacché φ è un automorfismo, $\mathrm{ord}(h', k') = \mathrm{ord}(h, e) = \mathrm{ord}(h)$, e quindi $\mathrm{ord}(h')\,\mathrm{ord}(k') = \mathrm{ord}(h)$. Allora $\mathrm{ord}(k')$ 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 $\{e\} \times K$. □

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

Dimostrazione. Nel corso della dimostrazione, se $\varphi \in \mathrm{Aut}(H \times K)$, si denota con $\varphi_H = \iota^{-1}_{H \hookrightarrow H \times \{e\}} \circ \varphi|_{H \times \{e\}} \circ \iota_{H \hookrightarrow H \times \{e\}}$ 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 $\alpha : \mathrm{Aut}(H \times K) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ tale per cui $\varphi \overset{\alpha}{\mapsto} (\varphi_H, \varphi_K)$. La mappa è ben definita dal momento che φ_H e φ_K sono due automorfismi di $\mathrm{Aut}(H)$ e $\mathrm{Aut}(K)$. Analogamente si definisce la mappa $\beta : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \to \mathrm{Aut}(H \times K)$ tale per cui $(\varphi_H, \varphi_K) \overset{\beta}{\mapsto} [(h, k) \mapsto (\varphi_H(h), \varphi_K(k))]$.

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

[3] Potrebbe non risultare completamente ovvio che valga $f(g(\overline{1})) = f(\overline{1})g(\overline{1})$. È necessario però ricordarsi che $\mathbb{Z}/n\mathbb{Z}$ è un gruppo definito sulla somma, e quindi vale sempre che $f(\overline{a}) = af(\overline{1}) = \overline{a}f(\overline{1})$.

[4] L'automorfismo è ben determinato dal momento che manda un generatore in un altro generatore.

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 $\mathrm{MCD}(m, n) = 1$, allora:

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

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 $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, vale che:

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

Esempio. ($\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$) Il gruppo $(\mathbb{Z}/p\mathbb{Z})^n$ ha una più facile visualizzazione se lo si pensa come spazio vettoriale su $\mathbb{Z}/p\mathbb{Z}$ (che per p primo è, per l'appunto, un campo). In tal caso, gli automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$ coincidono esattamente con gli endomorfismi invertibili di $\mathrm{End}((\mathbb{Z}/p\mathbb{Z})^n)$, e quindi vale in particolare che:

$$\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) \cong \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}).$$

In questo modo è estremamente più facile contare il numero di automorfismi di questo gruppo. È infatti sufficiente contare le possibili matrici invertibili con elementi in $\mathbb{Z}/p\mathbb{Z}$. Nella prima colonna di una matrice $A \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ possono essere effettuate $p^n - 1$ scelte (si esclude il vettore nullo); nella seconda è sufficiente scegliere un vettore che non stia in $(\mathbb{Z}/p\mathbb{Z})^n \setminus \mathrm{Span}(A^1)$, e quindi si hanno $p^n - p$ scelte; per la terza colonna se ne hanno $p^n - p^2$, ...

Si conclude dunque che vale la seguente identità:

$$|\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)| = \prod_{i=0}^{n-1}(p^n - p^i).$$

Se si prende m *square-free*[5], il risultato si può estendere facilmente su $\mathrm{Aut}((\mathbb{Z}/m)^n)$. Se infatti $m = p_1 \cdots p_k$, vale che:

$$\mathrm{Aut}((\mathbb{Z}/m\mathbb{Z})^n) \cong \mathrm{Aut}((\mathbb{Z}/p_1\mathbb{Z})^n \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^n) \cong \mathrm{Aut}((\mathbb{Z}/p_1\mathbb{Z})^n) \times \cdots \times \mathrm{Aut}((\mathbb{Z}/p_k\mathbb{Z})^n,$$

dove si è usato sia il Teorema cinese del resto, sia il fatto per cui $\mathrm{MCD}(p_i, p_j) = 1$ per $i \neq j$.

Esempio ($\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$ e altre proprietà)**.** Ora che è chiara la visualizzazione in senso vettoriale di $(\mathbb{Z}/p\mathbb{Z})^n$, si possono elencare alcune proprietà di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Innanzitutto, benché $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sia abeliano, $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ non lo è. Inoltre, ogni sottogruppo proprio e non banale di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non è caratteristico:

[5] Ossia m non è diviso da alcun quadrato; equivalentemente un primo che compare nella fattorizzazione di m compare con esponente unitario.

ogni tale sottogruppo è vettorialmente una retta (infatti $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ha dimensione due), e quindi è sufficiente costruire un automorfismo che manda tale retta in un'altra.

Infine, sempre perché $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, si può visualizzare facilmente l'isomorfismo tra $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ e S_3. Infatti, $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ si compone di 6 matrici, nella seguente bigezione con S_3:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftrightarrow e, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \leftrightarrow (1,2), \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \leftrightarrow (2,3),$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \leftrightarrow (1,3), \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \leftrightarrow (1,2,3) \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \leftrightarrow (1,3,2).$$

Infine, poiché $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3 \cong \mathrm{Aut}(S_3)$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e S_3 formano un esempio di gruppi non isomorfi (in particolare uno è abeliano e l'altro no) i cui gruppi di automorfismo sono isomorfi.