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 $\mathrm{Im}\,\zeta = \mathrm{Inn}(G)$. Si osserva inoltre che $\mathrm{Ker}\,\zeta$ è esattamente il centro di G, $Z(G)$. Infatti, se $g \in \mathrm{Ker}\,\zeta$, 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, $G/\mathrm{Ker}\,\zeta = G/Z(G) \cong \mathrm{Inn}(G)$. □

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).