Il teorema di corrispondenza e catene di sottogruppi normali

di Gabriel Antonio Videtta

Si illustra adesso un teorema che mette in corrispondenza i sottogruppi di G/H con i sottogruppi di G che contengono H. Benché questo teorema possa sembrare a prima vista di poca utilità, in realtà svela alcune proprietà che hanno portato allo sviluppo della celebre teoria di Galois. Non solo, guardando anche nelle piccole applicazioni, il teorema di corrispondenza permette di contare molto facilmente i sottogruppi di G/H, nonché di dimostrare l'esistenza di una catena di p-sottogruppi normali contenente tutti gli ordini possibili per un p-gruppo.

Teorema (di corrispondenza)**.** Sia H un sottogruppo normale di G. Allora la proiezione al quoziente $\pi_H : G \to G/H$ induce una bigezione tra l'insieme

$$X = \{K \leq G \mid H \subseteq K\}$$

dei sottogruppi di G che contengono H e l'insieme

$$Y = \{K' \leq G/H\}$$

dei sottogruppi di G/H. Tale bigezione preserva la normalità di un gruppo e il suo indice, ossia:

- $K \trianglelefteq G \iff K' \trianglelefteq G/H$,
- $[G : K] = [G/H : K']$,

dove $K \in X$ e $K' \in Y$ sono in corrispondenza biunivoca mediante π_H.

Dimostrazione. Sia $\alpha : X \to Y$ definita nel seguente modo:

$$K \overset{\alpha}{\mapsto} \pi_H(K),$$

dove si osserva che $\pi_H(K) = \{kH \mid k \in K\} = K/H \leq G/H$. Si definisce analogamente $\beta : Y \to X$ in modo tale che:

$$K' \overset{\beta}{\mapsto} \pi_H^{-1}(K').$$

Le due mappe sono entrambe ben definite (infatti $\pi_H^{-1}(K')$ è sempre un sottogruppo di G e contiene sempre H, dacché $H \in K'$, essendo l'identità di G/H). È dunque sufficiente mostrare che vale $\beta \circ \alpha = \mathrm{Id}_X$ e che $\alpha \circ \beta = \mathrm{Id}_Y$.

Siano quindi $K \in X$ e $K' \in Y$. Chiaramente $\pi_H(\pi_H^{-1}(K')) = K'$, dal momento che π_H è surgettiva; dunque $\alpha \circ \beta = \mathrm{Id}_Y$. Inoltre $\pi_H^{-1}(\pi_H(K)) = \pi_H^{-1}(K/H) = \{g \in G \mid gH \in K/H\} = K$[1], da cui $\beta \circ \alpha = \mathrm{Id}_X$. Quindi X e Y sono in corrispondenza biunivoca tramite α e β.

Rimane da dimostrare che α e β preservano la normalità e l'indice di sottogruppo. Se $K \trianglelefteqslant G$, allora chiaramente $K' = K/H \trianglelefteqslant G/H$ (infatti $gH\,kH\,g^{-1}H = (gkg^{-1})H$, dove $gkg^{-1} \in K$ per ipotesi di normalità). Sia ora $K' \trianglelefteqslant G/H$. Allora, se $k \in K$, $gH\,kH\,g^{-1}H = (gkg^{-1})H$, e per ipotesi di normalità deve esistere $k' \in K$ tale per cui $(gkg^{-1})H = k'H$, e quindi deve esistere $h \in H$ tale per cui $gkg^{-1} = k'h$. Dal momento che $H \subseteq K$, $gkg^{-1} \in K$, e quindi $K \trianglelefteqslant G$.

Per mostrare che l'indice di sottogruppo si preserva si dimostra che esiste lo stesso numero di classi laterali in G/K e $(G/H)/(K/H)$. Pertanto è sufficiente mostrare che:

$$xK = yK \iff xH(K/H) = yH(K/H), \qquad x, y \in G.$$

Infatti, in tal caso vi sarebbero esattamente $[G : K]$ classi laterali in $(G/H)/(K/H)$. Si consideri ora la classe laterale $xH(K/H)$:

$$xH(K/H) = \{xHkH \mid k \in K\} = \{(xk)H \mid k \in K\},$$

dove nell'ultima uguaglianza si è impiegata la normalità di H in G (altrimenti il prodotto non sarebbe ben definito). Analogamente $yH(K/H) = \{(yk)H \mid k \in K\}$. Quindi, se $xH(K/H) = yH(K/H)$, allora $xH = (yk)H$, con $k \in K$. Allora $x = ykh$ con $h \in H$. Poiché $H \subseteq K$, si deduce quindi che $xK = yK$. Infine, se $xK = yK$, esiste $k \in K$ tale per cui $x = yk$. Allora:

$$xH(K/H) = yH\,kH(K/H) = yH(K/H),$$

da cui la tesi. □

Esempio (I sottogruppi di $\mathbb{Z}/n\mathbb{Z}$)**.** Attraverso il teorema di corrispondenza è facile contare i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ senza ricorrere alla teoria sui gruppi ciclici finiti. Infatti, per il teorema di corrispondenza, i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono in esatta corrispondenza con i sottogruppi[2] $m\mathbb{Z}$ di $\mathbb{Z}$ tali per cui $n\mathbb{Z} \subseteq m\mathbb{Z}$. In particolare, $n\mathbb{Z} \subseteq m\mathbb{Z}$ se e solo se $m \mid n$, e quindi vi sono $d(n)$ possibili sottogruppi, che, tramite il teorema di corrispondenza, sono esattamente i sottogruppi della forma $m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\frac{n}{m}\mathbb{Z}$.

[1] Infatti se $gH = kH$ con $k \in K$, esiste un $h \in H$ tale per cui $g = kh$. Dal momento che $H \subseteq K$, g è dunque un elemento di K.

[2] Poiché $\mathbb{Z}$ è ciclico, ogni sottogruppo è della forma $m\mathbb{Z}$. In particolare, ogni sottogruppo di $\mathbb{Z}$ è anche un suo ideale, se si intende $\mathbb{Z}$ come anello, ed è dunque monogenerato in quanto $\mathbb{Z}$, essendo un anello euclideo, è anche un PID.

Si illustra allora il seguente fondamentale risultato sui p-gruppi, che è conseguenza del Teorema di corrispondenza e delle proprietà degli ordini di gruppi abeliani.

Proposizione. Sia G un p-gruppo di ordine p^n, con $n \in \mathbb{N}^+$. Allora esiste una successione H_1, ..., H_{n-1} di sottogruppi normali in G tali per cui:

$$\{e\} < H_1 < H_2 < \cdots < H_{n-1} < G, \qquad |H_i| = p^i.$$

Dimostrazione. Si dimostra la tesi per induzione su n. Per $n = 1$, la tesi è banale. Si ipotizzi allora che la tesi valga per $t < n$ con $t \in \mathbb{N}^+$. Se G è abeliano, allora G ammette un sottogruppo H_{n-1} di ordine p^{n-1}. Tale sottogruppo H_{n-1} ammette per ipotesi induttiva una successione H_1, ..., H_{n-2} di sottogruppi normali in H_{n-1} come desiderato dalla tesi. Poiché G è abeliano, tali sottogruppi sono normali anche in G, e quindi:

$$\{e\} < H_1 < \cdots < H_{n-1} < G.$$

Sia adesso G non abeliano. Allora $|Z(G)| < |G|$. Si può dunque considerare il gruppo quoziente $G/Z(G)$, di ordine strettamente inferiore a p^n. Per ipotesi induttiva esiste una catena di sottogruppi $\mathcal{H}_1$, ..., $\mathcal{H}_{k-1}$ normali in $G/Z(G)$ tale per cui:

$$\{e\} < \mathcal{H}_1 < \cdots < \mathcal{H}_{k-1} < G/Z(G), \qquad |\mathcal{H}_i| = p^i,$$

dove $|Z(G)| = p^{n-k}$.

Per il Teorema di corrispondenza, $\mathcal{H}_i$ corrisponde a un sottogruppo normale H_{n-k+i} di G contenente $Z(G)$ tale per cui $[G : H_{n-k+i}] = [G/Z(G) : \mathcal{H}_i]$. Allora vale che:

$$H_{n-k+i} = |Z(G)|\,|\mathcal{H}_i| = p^{n-k}p^i = p^{n-k+i},$$

e quindi H_{n-k+i} copre tutti gli esponenti di p da $n-k+1$ a $n-1$. Inoltre, tramite $\pi^{-1}_{Z(G)}$, vale anche che $H_{n-k+i} < H_{n-k+i+1}$[3]. Sempre per ipotesi induttiva (come nella costruzione di prima), $Z(G)$ ammette una catena di sottogruppi H_1, ..., H_{n-k-1} normali in $Z(G)$ tale per cui:

$$\{e\} < H_1 < \cdots < H_{n-k-1} < Z(G), \qquad |H_i| = p^i.$$

Poiché $Z(G)$ è il centro di G, tali sottogruppi sono normali anche in G. Ponendo allora $H_{n-k} := Z(G)$ si è costruita la catena desiderata:

$$\{e\} < H_1 < \cdots < H_{n-k} = Z(G) < H_{n-k+1} < \cdots < H_{n-1} < G.$$

□

[3]Segue dal fatto secondo cui $T/H < S/H \implies T < S$.