Il prodotto semidiretto

di Gabriel Antonio Videtta

Nota. Nel corso del documento con G un qualsiasi gruppo.

Siano H e K due gruppi. Allora, dato un omomorfismo $\varphi : K \to \mathrm{Aut}(H)$ e detto $\varphi_k := \varphi(k)$, si può costruire un gruppo su $H \times K$ detto **prodotto semidiretto** tra H e K, indicato con $H \rtimes_\varphi K$, dove l'operazione è data da:

$$(h,k)(h',k') = (h\,\varphi_k(h'), kk').$$

In questo gruppo l'inverso di (h,k) è dato da $(\varphi_k^{-1}(h^{-1}), k^{-1})$, infatti:

$$(h,k)(\varphi_k^{-1}(h^{-1}), k^{-1}) = (h\,\varphi_k(\varphi_k^{-1}(h^{-1})), kk^{-1}) = (e,e).$$

In particolare, se φ è banale, e quindi $k \overset{\varphi}{\mapsto} \mathrm{Id}_H$, $H \rtimes_\varphi K$ ha la stessa struttura usuale del prodotto diretto. Nel prodotto semidiretto $H \rtimes_\varphi K$ si possono identificare facilmente H e K nei sottogruppi $H \times \{e\}$ e $\{e\} \times K$.

Detto $\alpha : H \rtimes_\varphi K \to K$ la mappa che associa (h,k) a k, si verifica che α è un omomorfismo con $\ker \alpha = H \times \{e\}$. Pertanto $H \times \{e\}$ è un sottogruppo normale di $H \rtimes_\varphi K$, mentre in generale $K \times \{e\}$ non lo è.

Si illustra adesso un teorema che permette di decomporre, sotto opportune ipotesi, un gruppo in un prodotto semidiretto di due suoi sottogruppi:

Teorema (di decomposizione in prodotto semidiretto)**.** Siano[1] H e K due sottogruppi di G con $H \cap K = \{e\}$ e $H \trianglelefteq G$. Allora vale che $HK \cong H \rtimes_\varphi K$ con $\varphi : K \to \mathrm{Aut}(H)$ tale per cui[2] $k \overset{\varphi}{\mapsto} [h \mapsto khk^{-1}]$.

Dimostrazione. Si costruisce un isomorfismo tra $H \rtimes_\varphi K$ e HK. Sia $\alpha : H \rtimes_\varphi K \to HK$ tale per cui $(h,k) \overset{\alpha}{\mapsto} hk$. Si verifica che α è un omomorfismo:

$$\alpha((h,k)(h',k')) = \alpha(hkh'k^{-1}, kk') = hkh'k^{-1}kk' = hkh'k' = \alpha(h,k)\alpha(h',k').$$

Chiaramente α è iniettivo dal momento che $hk = e \implies h = k^{-1} \in H \cap K \implies h = k = e$. Infine α è surgettiva dal momento che $hk = \alpha(h,k)$, e quindi α è un isomorfismo. □

[1] Si osserva che questo teorema richiede *quasi* le stesse ipotesi del Teorema di decomposizione in prodotto diretto. L'unica ipotesi che manca è quella della normalità di K. Ciononostante, questo teorema copre anche il teorema analogo sul prodotto diretto: se K fosse normale, φ sarebbe l'identità (h e k commuterebbero), e quindi $H \rtimes_\varphi K$ sarebbe esattamente $H \times K$.

[2] Tale mappa è ben definita dal momento che H è normale in G.

Esempio ($S_n \cong \mathcal{A}_\mathrm{n} \rtimes_\varphi \langle\tau\rangle$)**.** Sia τ una trasposizione di S_n. Allora $\mathcal{A}_\mathrm{n}$ è normale in S_n, $\mathcal{A}_\mathrm{n} \cap \langle\tau\rangle = \{e\}$ e $|\mathcal{A}_\mathrm{n}|\,|\langle\tau\rangle| = |S_n| \implies S_n = \mathcal{A}_\mathrm{n}\langle\tau\rangle$. Allora, per il Teorema di decomposizione in prodotto semidiretto, vale che:

$$S_n \cong \mathcal{A}_\mathrm{n} \rtimes_\varphi \langle\tau\rangle,$$

con $\varphi : \langle\tau\rangle \to \mathrm{Aut}(\mathcal{A}_\mathrm{n})$ tale per cui $\tau \overset{\varphi}{\mapsto} [h \mapsto \tau h \tau^{-1}]$.

Esempio ($D_n \cong \mathcal{R} \rtimes_\varphi \langle sr^k\rangle$)**.** Sia sr^k una qualsiasi simmetria di D_n. Allora $\mathcal{R}$ è normale in D_n, $\mathcal{R} \cap \langle sr^k\rangle = \{e\}$ e $|\mathcal{R}|\left|\langle sr^k\rangle\right| = |D_n| \implies D_n = \mathcal{R}\langle sr^k\rangle$. Allora, come prima, vale che:

$$D_n \cong \mathcal{R} \rtimes_\varphi \langle sr^k\rangle,$$

con $\varphi : \langle sr^k\rangle \to \mathrm{Aut}(\mathcal{R})$ tale per cui $sr^k \overset{\varphi}{\mapsto} [h \mapsto sr^k h (sr^k)^{-1}]$.

Si illustra adesso un lemma che verrà riutilizzato successivamente per classificare i gruppi di ordine pq.

Lemma. Siano $\varphi, \psi : K \to \mathrm{Aut}(H)$ tali per cui esistono $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$ che soddisfano la seguente identità:

$$\alpha \circ \varphi_k \circ \alpha^{-1} = \psi_{\beta(k)} \qquad \forall\, k \in K.$$

Allora vale che $H \rtimes_\varphi K \cong H \rtimes_\psi K$.

Dimostrazione. Si costruisce la mappa $F : H \rtimes_\varphi K \to H \rtimes_\psi K$ tale per cui $(h,k) \overset{F}{\mapsto} (\alpha(h), \beta(k))$. Si verifica che F è un omomorfismo:

$$F(h\varphi_k(h'), kk') = (\alpha(h)\alpha(\varphi_k(h')), \beta(k)\beta(k')),$$

e quindi, poiché $\alpha \circ \varphi_k = \psi_{\beta(k)} \circ \alpha$:

$$F(h\varphi_k(h'), kk') = (\alpha(h)\psi_{\beta(k)}(\alpha(h')), \beta(k)\beta(k')) = F(h,k)F(h',k').$$

Chiaramente F è anche iniettiva e surgettiva, e quindi F è l'isomorfismo desiderato dalla tesi. □

Proposizione. Sia G un gruppo di ordine pq con p e q primi tali per cui $p < q$. Allora G è isomorfo a $\mathbb{Z}_{pq}$ se $p \nmid q - 1$. Altrimenti G è isomorfo a $\mathbb{Z}/pq\mathbb{Z}$ o a $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ con $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ univocamente determinata dalla relazione $\overline{1} \overset{\varphi}{\mapsto} f$ con f un qualsiasi elemento di ordine p di $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ (ossia φ non è banale).

Dimostrazione. Per il Teorema di Cauchy, esistono due elementi x e y di G con $\mathrm{ord}(x) = q$ e $\mathrm{ord}(y) = p$. Siano $H = \langle x\rangle$ e $K = \langle y\rangle$. Allora, poiché $[G : H] = p$ è il più piccolo primo che divide $|G| = pq$, H è normale. Inoltre $H \cap K = \{e\}$, dacché $|H \cap K| \mid \mathrm{MCD}(p,q) = 1$. Pertanto $|HK| = |H|\,|K| = pq \implies G = HK$.

Per il Teorema di decomposizione di un gruppo in un prodotto semidiretto, G è isomorfo al prodotto semidiretto $H \rtimes_\varphi K$ con $\varphi : K \to \mathrm{Aut}(H)$ tale per cui $k \overset{\varphi}{\mapsto} [h \mapsto khk^{-1}]$. Si osserva che $H \cong \mathbb{Z}/q\mathbb{Z}$, $\mathrm{Aut}(H) \cong \mathbb{Z}/q-1\mathbb{Z}$ e analogamente che $K \cong \mathbb{Z}/p\mathbb{Z}$.

Deve inoltre valere anche che $|\mathrm{Im}\,\varphi| \mid \mathrm{MCD}(|K|, |\mathrm{Aut}(H)|) = \mathrm{MCD}(p, q-1)$. Pertanto, se $p \nmid q-1$, $\mathrm{MCD}(p, q-1) = 1$, e quindi $\mathrm{Im}\,\varphi$ è banale. In tal caso φ è la mappa che associa ogni k all'identità di $\mathrm{Aut}(H)$, e quindi $G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$, dove si è usato il Teorema cinese del resto.

Altrimenti $\mathrm{MCD}(p, q-1) = p$, e quindi $\mathrm{Im}\,\varphi$ può essere banale (riconducendoci al caso di prima, in cui $G \cong \mathbb{Z}/pq\mathbb{Z}$), oppure $|\mathrm{Im}\,\varphi| = p$. Si mostra adesso che i prodotti semidiretti su φ non banale sono tutti isomorfi a prescindere dalla scelta di φ.

□