

Il prodotto semidiretto di gruppi, prima parte

dispense provvisorie del corso di Algebra 1 2010-2011

Alessio Del Vigna - Giovanni Gaiffi

19 novembre 2010

1 Prodotto semidiretto

La nozione di prodotto semidiretto generalizza quella di prodotto diretto.

Nella lezione precedente abbiamo dimostrato che se $M \triangleleft G$ e $N < G$ allora $MN < G$. In particolare, per quel che riguarda il prodotto fra due elementi m_1n_1 e m_2n_2 abbiamo osservato che

$$(m_1n_1)(m_2n_2) = m_1n_1m_2(n_1^{-1}n_1)n_2 = m_1(n_1m_2n_1^{-1})n_1n_2 \quad (1)$$

e abbiamo concluso che MN è chiuso per prodotto.

Supponiamo ora $M \cap N = \{e\}$ e $G = MN$: dal punto di vista insiemistico c'è una corrispondenza bigettiva naturale fra MN e $M \times N$, quella che manda mn in (m, n) , ma in generale non è vero che come gruppi $MN \cong M \times N$. Come vedremo, però, è possibile definire una particolare moltiplicazione sull'insieme $M \times N$ e ottenere un gruppo isomorfo a MN .

Definizione 1.1. Siano H e K gruppi e sia $\tau : K \rightarrow \text{Aut}(H)$ un omomorfismo. Si definisce *prodotto semidiretto* di H e K secondo τ , e si indica con $H \rtimes_{\tau} K$, il prodotto cartesiano $H \times K$ dotato dell'operazione seguente:

$$(h, k)(\bar{h}, \bar{k}) = (h \tau(k)(\bar{h}), k\bar{k}).$$

Osserviamo che $\tau(k)(\bar{h})$ è un elemento di H , infatti $\tau(k)$ è un automorfismo di H e viene applicato ad $\bar{h} \in H$.

Osservazione 1.1. Lasciamo come semplice verifica i seguenti fatti (alcuni visti a lezione).

- (1) $H \rtimes_{\tau} K$ è un gruppo con l'operazione della definizione, e l'elemento neutro è (e_H, e_K) , mentre l'inverso di (h, k) è $(\tau(k^{-1})(h^{-1}), k^{-1})$;
- (2) $H' = \{(h, e_K) \mid h \in H\} \triangleleft H \rtimes_{\tau} K$ e $H' \cong H$;
- (3) $K' = \{(e_H, k) \mid k \in K\} < H \rtimes_{\tau} K$ ed inoltre $(H \rtimes_{\tau} K)/H' \cong K' \cong K$.

Osservazione 1.2. Se τ è l'omomorfismo banale, ossia se $\tau(k) = id$ per ogni $k \in K$, allora l'operazione di prodotto semidiretto coincide col prodotto componente per componente. In tal caso $H \rtimes_{\tau} K = H \times K$.

Teorema 1.1. Sia G un gruppo, e siano $H \triangleleft G$ e $K < G$ due suoi sottogruppi tali che $H \cap K = \{e\}$ e $G = HK$. Allora

$$G \cong H \rtimes_{c_G} K,$$

dove $c_G : K \rightarrow \text{Aut}(H)$ è l'omomorfismo che associa ad ogni $k \in K$ l'automorfismo dato dal coniugio (in G) per k , ossia l'automorfismo $H \rightarrow H$ definito da $h \rightarrow khk^{-1}$.

Dimostrazione. La mappa

$$\begin{aligned} \phi : H \rtimes_{c_G} K &\longrightarrow G \\ (h, k) &\longmapsto hk \end{aligned}$$

definisce infatti un isomorfismo. Infatti è un omomorfismo per la regola (1) ricordata all'inizio della lezione; la condizione $H \cap K = \{e\}$ garantisce l'iniettività, la verifica della surgettività è immediata. \square

Esempio 1.1. Consideriamo \mathcal{S}_n , e i sottogruppi $\mathcal{A}_n \triangleleft \mathcal{S}_n$ e $\langle(12)\rangle < \mathcal{S}_n$. I due sottogruppi si intersecano solo nella permutazione identica, in quanto il secondo è generato da una permutazione dispari; inoltre, per questioni di cardinalità, deve essere $\mathcal{S}_n = \mathcal{A}_n \langle(12)\rangle$. Ma allora, per il teorema precedente

$$\mathcal{S}_n \cong \mathcal{A}_n \rtimes_{c_{\mathcal{S}_n}} \langle(12)\rangle.$$

Esempio 1.2. Sia $L = \{f_{a,b} : \mathbb{R} \rightarrow \mathbb{R} \mid f_{a,b}(x) = ax + b, a \neq 0, b \in \mathbb{R}\}$, con l'operazione data dalla composizione, il gruppo delle affinità su \mathbb{R} , e siano N ed M i gruppi delle omotetie e delle traslazioni su \mathbb{R} , ossia

$$N = \{f_{a,b} \in L \mid b = 0\} \cong \mathbb{R}^* \quad \text{e} \quad M = \{f_{a,b} \in L \mid a = 1\} \cong \mathbb{R}.$$

Non è difficile vedere che $M \triangleleft L$, in quanto $f_{a,b}^{-1} = f_{1/a, -b/a}$ e si verifica che $f_{a,b} f_{1,b'} f_{a,b}^{-1} = f_{1,ab'} \in M$. L'intersezione $M \cap N$ contiene un solo elemento, l'affinità $f_{1,0}$, elemento neutro di L ; $L = MN$ dato che $f_{a,b} f_{1,b'} = f_{a,ab'+b}$ e ogni affinità può essere espressa nella forma $f_{a,ab'+b}$ scegliendo opportunamente a, b', b . Ma allora

$$L \cong M \rtimes_{c_L} N.$$

Esempio 1.3. Consideriamo l'omomorfismo $\tau : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$ dove $\tau([1])$ è l'automorfismo che scambia le coordinate di ogni elemento di $\mathbb{Z}_3 \times \mathbb{Z}_3$. Costruiamo il prodotto semidiretto

$$G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\tau} \mathbb{Z}_2.$$

Osserviamo che il sottogruppo $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\tau} \{[0]\}$ è normale in G , e che $(\mathbb{Z}_3 \times \{[0]\}) \rtimes_{\tau} \{[0]\}$ è normale in $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\tau} \{[0]\}$, ma $(\mathbb{Z}_3 \times \{[0]\}) \rtimes_{\tau} \{[0]\}$ non è normale in G (basta calcolare il coniugio $(([0], [0]), [1]) (([1], [0]), [0]) (([0], [0]), [1]) \dots$).

Questo esempio illustra una tecnica generale di “costruzione” di gruppi. Dato un gruppo K , consideriamo il prodotto diretto $K \times K \times \dots \times K$ di n copie di K e facciamo agire S_n su $K \times K \times \dots \times K$ in modo ovvio permutando le coordinate (sia $\tau : S_n \rightarrow \text{Aut}(K \times K \times \dots \times K)$ il corrispondente omomorfismo). Allora si può costruire il seguente gruppo, che si chiama “prodotto intrecciato” di K e S_n :

$$G = (K \times K \times \dots \times K) \rtimes_{\tau} S_n.$$

Adesso un punto molto importante. Supponiamo di avere H e K gruppi. Considerato un omomorfismo $\tau : K \rightarrow \text{Aut}(H)$ possiamo costruire il prodotto semidiretto $H \rtimes_{\tau} K$ come detto prima. In generale esistono un certo numero di omomorfismi $K \rightarrow \text{Aut}(H)$ e quindi possiamo chiederci come variano le strutture di prodotto semidiretto al variare di τ . Per esempio vorremmo chiederci: se $\tau_1 \neq \tau_2$ allora è vero che $H \rtimes_{\tau_1} K \cong H \rtimes_{\tau_2} K$? La risposta a questa domanda è no; è possibile che omomorfismi diversi $K \rightarrow \text{Aut}(H)$ diano luogo a prodotti semidiretti isomorfi. Il seguente criterio è molto utile:

Proposizione 1.1. *Dati due gruppi H e K , siano $\phi, \psi : K \rightarrow \text{Aut}(H)$ due omomorfismi. Se esistono $\alpha \in \text{Aut}(H)$ e $\beta \in \text{Aut}(K)$ tali che*

$$\alpha \circ \phi(k) \circ \alpha^{-1} = \psi(\beta(k)) \quad \forall k \in K$$

allora $H \rtimes_{\phi} K \cong H \rtimes_{\psi} K$.

Dimostrazione. Consideriamo la seguente mappa:

$$\begin{aligned} \Xi : H \rtimes_{\phi} K &\longrightarrow H \rtimes_{\psi} K \\ (h, k) &\longmapsto (\alpha(h), \beta(k)) \end{aligned} \quad ,$$

e mostriamo che si tratta di un isomorfismo. Intanto mostriamo che Ξ è un omomorfismo:

$$\begin{aligned} \Xi((h, k)(h', k')) &= \Xi(h\phi(k)(h'), k\beta(k')) = (\alpha(h) \cdot (\alpha \circ \phi(k))(h'), \beta(k)\beta(k')) = \\ &= (\alpha(h) \cdot (\psi(\beta(k)) \circ \alpha)(h'), \beta(k)\beta(k')) = (\alpha(h), \beta(k))(\alpha(h'), \beta(k')) = \\ &= \Xi(h, k) \cdot \Xi(h', k'). \end{aligned}$$

L'iniettività segue da:

$$\Xi((h, k)) = (e_H, e_K) \iff (\alpha(h), \beta(k)) = (e_H, e_K) \iff (h, k) = (e_H, e_K),$$

dove l'ultima equivalenza vale per l'iniettività di α e β . Analogamente, la surgettività è data dal fatto che α e β sono automorfismi, e quindi anch'essi surgettivi. \square

Esempio 1.4. Classificare i gruppi di ordine 6.

Sia G un gruppo di ordine 6. Ci sono un sottogruppo di ordine 2 e uno di ordine 3, chiamiamoli $N_2(\cong \mathbb{Z}_2)$ e $N_3(\cong \mathbb{Z}_3)$ (non occorre invocare il teorema di Sylow per affermare ciò, basta per esempio il teorema di Cauchy). Inoltre N_3 ha indice 2 in G e quindi è normale: $N_3 \triangleleft G$. Per questioni di ordine degli elementi i due sottogruppi N_2 e N_3 hanno intersezione uguale a $\{e\}$ e quindi per motivi di cardinalità $G = N_2N_3$. Ma allora possiamo affermare

$$G \cong N_2 \rtimes_{c_G} N_3.$$

Per capire quanti prodotti semidiretti del tipo $\mathbb{Z}_2 \rtimes_{\tau} \mathbb{Z}_3$ esistono a meno di isomorfismo dobbiamo per prima cosa studiare gli omomorfismi $\tau : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_2)$. Ricordiamo che $\text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$: in definitiva stiamo cercando gli omomorfismi $\tau : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, che sono solo due.

Si osserva che quindi al massimo esistono due distinti prodotti semidiretti $\mathbb{Z}_3 \rtimes_{\tau} \mathbb{Z}_2$ e siccome conosciamo due gruppi, \mathbb{Z}_6 e \mathcal{S}_3 , di ordine 6 e non isomorfi fra loro, possiamo concludere che in effetti le distinte strutture di prodotto semidiretto sono proprio due (\mathbb{Z}_6 corrisponde al caso in cui τ è l'omomorfismo banale e dunque il prodotto è diretto).

L'esempio precedente si generalizza nel seguente modo:

Proposizione 1.2. *Consideriamo due numeri primi p e q , con $p > q$. Se q non divide $p-1$ esiste, a meno di isomorfismo, un solo gruppo di ordine pq , ossia \mathbb{Z}_{pq} . Se invece $q|p-1$ allora esistono a meno di isomorfismo due gruppi di ordine pq : uno è \mathbb{Z}_{pq} , l'altro non è abeliano.*

Dimostrazione. Sia G di ordine pq . Dal teorema di Cauchy (non occorre in questo caso invocare i teoremi di Sylow!) sappiamo che esistono due sottogruppi di ordine p e q , chiamiamoli N_p e N_q , isomorfi rispettivamente a \mathbb{Z}_p e a \mathbb{Z}_q . L'indice di N_p è q , il più piccolo primo che divide $o(G)$, e quindi, per un risultato visto durante il corso, N_p è normale in G . Essendo p e q due numeri primi distinti, l'intersezione fra N_p e N_q contiene, per ragioni di ordine degli elementi, solo l'elemento neutro del gruppo. Inoltre vale $N_p N_q = G$ per questioni di cardinalità. Possiamo quindi concludere che

$$G \cong N_p \rtimes_{c_G} N_q.$$

Adesso dobbiamo studiare gli omomorfismi $\tau : \mathbb{Z}_q \rightarrow \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ e a quali strutture di prodotto semidiretto danno luogo.

- Se $q \nmid (p-1)$ allora l'unico omomorfismo τ che possiamo costruire è quello che manda ogni elemento di \mathbb{Z}_q in $[0]$ in \mathbb{Z}_{p-1} : infatti l'immagine di un generatore di \mathbb{Z}_q deve avere ordine che divide q , dunque uguale a 1 o a q , ma dobbiamo escludere che tale ordine sia q in quanto in \mathbb{Z}_{p-1} , se $q \nmid (p-1)$, non ci sono elementi di ordine q . Allora si conclude che siamo nel caso del prodotto diretto

$$G = \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$$

(ricordiamo che $([1]_q, [1]_p)$ ha ordine pq).

- Se $q | (p-1)$ allora abbiamo diverse possibilità. Consideriamo un omomorfismo $\mathbb{Z}_q \rightarrow \mathbb{Z}_{p-1}$ (ricordiamo che $\mathbb{Z}_{p-1} \cong \text{Aut}(\mathbb{Z}_p)$); questo è completamente determinato dall'immagine di $[1]_q$, che può avere ordine 1 o q : se ha ordine

1 siamo nuovamente nel caso dell'omomorfismo banale, e dunque del prodotto diretto, già trattato; se ha ordine q abbiamo la possibilità di scegliere l'immagine come

$$1 \begin{bmatrix} p-1 \\ q \end{bmatrix}_{p-1}, 2 \begin{bmatrix} p-1 \\ q \end{bmatrix}_{p-1}, \dots, (q-1) \begin{bmatrix} p-1 \\ q \end{bmatrix}_{p-1},$$

che sono tutti e soli gli elementi di ordine q in \mathbb{Z}_{p-1} . In definitiva abbiamo $q-1$ omomorfismi non banali, che chiameremo $\phi_1, \dots, \phi_{q-1}$. Vogliamo mostrare che tutti questi omomorfismi inducono la stessa struttura sul prodotto semidiretto.

Consideriamo ϕ_1 e ϕ_j con $1 \neq j$: useremo la proposizione 1.1 per mostrare che inducono prodotti semidiretti isomorfi. Questo dimostra in particolare che tutte le ϕ_i inducono prodotti semidiretti isomorfi. Consideriamo $\alpha = id \in \text{Aut}(\mathbb{Z}_p)$ e $\beta_j \in \text{Aut}(\mathbb{Z}_q)$ tale che $\beta_j([1]_q) = [j]_q$. Visto che α è l'identità, dobbiamo verificare che $\phi_j([1]_q)$ e $\phi_1(\beta_j([1]_q))$ (che in base alla identificazione $\mathbb{Z}_{p-1} \cong \text{Aut}(\mathbb{Z}_p)$ sono elementi di \mathbb{Z}_{p-1}) coincidono¹. Infatti

$$\phi_j([1]_q) = j \begin{bmatrix} p-1 \\ q \end{bmatrix}_{p-1} = \phi_1([j]_q) = \phi_1(\beta_j([1]_q))$$

Esistono dunque al più due gruppi di ordine pq : $\mathbb{Z}_p \times \mathbb{Z}_q$ e $\mathbb{Z}_p \rtimes_{\tau} \mathbb{Z}_q$ con $\tau = \phi_i$ scelto un qualsiasi $i = 1, \dots, q-1$. Mostriamo adesso che sono diversi facendo vedere che il secondo non è abeliano. Prendiamo $a \in \mathbb{Z}_p$ e $b \in \mathbb{Z}_q$, allora (usando come di consueto la notazione additiva per i gruppi \mathbb{Z}_p e \mathbb{Z}_q e scrivendo per brevità i loro elementi senza parentesi quadre []) vale:

$$(a, b)(0, b) = (a + \tau(b)(0), 2b) = (a, 2b),$$

$$(0, b)(a, b) = (0 + \tau(b)(a), 2b) = (\tau(b)(a), 2b).$$

Siccome τ non è banale allora esisterà un $b \in \mathbb{Z}_q$ tale che $\tau(b) \neq id$ e quindi esiste un a tale che $\tau(b)(a) \neq a$ ². Scelti questi a e b possiamo concludere che $(a, b)(0, b) \neq (0, b)(a, b)$ e dunque $\mathbb{Z}_p \rtimes_{\tau} \mathbb{Z}_q$ non è abeliano.

□

¹Andrebbe verificato che $\phi_j([r]_q) = \phi_1(\beta_j([r]_q)) \forall [r]_q$ ma basta la verifica su un generatore, visto che ϕ_j e $\phi_1 \circ \beta_j$ sono omomorfismi da \mathbb{Z}_q a \mathbb{Z}_{p-1} .

²Gli omomorfismi ϕ_i andavano da \mathbb{Z}_q a $\mathbb{Z}_{p-1} \cong \text{Aut}(\mathbb{Z}_p)$. Abbiamo detto che $\tau = \phi_i$ quindi, per essere rigorosi, $\tau(b)$ è un elemento di \mathbb{Z}_{p-1} . Quando abbiamo scritto $\tau(b) \neq id$ e $\tau(b)(a)$ abbiamo invece interpretato $\tau(b)$ come automorfismo di \mathbb{Z}_p .

Esempio 1.5. Le considerazioni dell'esempio precedente mostrano che, preso un primo dispari p , ci sono solo due gruppi di ordine $2p$. Uno è \mathbb{Z}_{2p} e l'altro? Sappiamo che il gruppo diedrale D_p è un gruppo di ordine $2p$ non abeliano. Si tratta dunque proprio del gruppo che stiamo cercando.