Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 24-04-2020

Prodotto semidiretto di sottogruppi

Definizione

Se $H < G$, $K \triangleleft G$, $H \cap K = \{1\}$ e $HK (= KH) = G$, si dice che G è prodotto semidiretto dei sottogruppi K e H, e si indica $G = K \rtimes H$ o $G = H \ltimes K$.

Osservazione

Se anche $H \triangleleft G$, si dice che G è prodotto (diretto) di K e H e si può scrivere $G = K \times H$ o $G = H \times K$.

Esempio

- $D_n = \langle R \rangle \rtimes \langle S \rangle$.
- $S_n = A_n \rtimes \langle \sigma \rangle$ con σ trasposizione.
- $S_4 = V_4 \rtimes S_3$ (con $S_3 = \{\sigma \in S_4 \,:\, \sigma(4) = 4\} < S_4$) e $A_4 = V_4 \rtimes A_3$.
- $\#G = pq$ con $p < q$ primi $\implies$ $G = K \rtimes H$ con $H \cong C_p$ p-Sylow e $K \cong C_q$ q-Sylow.

Condizioni equivalenti

Proposizione

$K \triangleleft G$, $\pi\colon G \to G/K$ proiezione $\implies$ sono equivalenti:

1. *$\exists\, H < G$ tale che $G = K \rtimes H$;*
2. *$\exists\, H < G$ tale che $\pi|_H\colon H \to G/K$ è un isomorfismo;*
3. *$\exists\, f\colon G/K \to G$ omomorfismo tale che $\pi \circ f = \mathrm{id}_{G/K}$.*

Osservazione

- Se in 1 (o in 2) $H \triangleleft G$ (e quindi $G = K \times H$), allora $\exists\, p\colon G \to K$ omomorfismo tale che $p|_K = \mathrm{id}_K$ (e $\ker(p) = H$).
- In generale le condizioni 1, 2, 3 possono non essere soddisfatte e, anche quando lo sono, H e f possono non essere unici. In particolare, se G è abeliano (additivo), le condizioni valgono $\iff$ K è addendo diretto di G (Proposizione 11.4 delle dispense sui moduli), e in questo caso H ne è un complementare.

Dimostrazione della Proposizione

$1 \implies 2$ $\pi|_H = \pi \circ i$ omomorfismo (con $i\colon H \to G$ inclusione).

$$\ker(\pi|_H) = H \cap \ker(\pi) = H \cap K = \{1\} \implies \pi|_H \text{ iniettivo.}$$
$$\operatorname{im}(\pi|_H) = \pi(H) = (HK)/K = G/K \implies \pi|_H \text{ suriettivo.}$$

$2 \implies 3$ $f := i \circ (\pi|_H)^{-1}\colon G/K \to G$ omomorfismo tale che

$$\pi \circ f = \pi \circ i \circ (\pi|_H)^{-1} = \pi|_H \circ (\pi|_H)^{-1} = \mathrm{id}_{G/K}.$$

$3 \implies 1$ $H := \operatorname{im}(f) < G$.

$g \in H \cap K \implies \exists x \in G/K$ tale che $g = f(x)$ (perché $g \in H$) $\implies x = \pi(f(x)) = \pi(g) = \bar{1}$ (perché $g \in K$) $\implies g = f(x) = f(\bar{1}) = 1 \implies H \cap K = \{1\}$.

$g \in G \implies b := f(\pi(g)) \in H$; $a := gb^{-1}$ tale che $\pi(a) = \pi(g)\pi(b)^{-1} = \pi(g)\pi(f(\pi(g)))^{-1} = \pi(g)\pi(g)^{-1} = \bar{1}$ $\implies a \in K \implies g = ab \in KH \implies G = KH$.

Operazione in un prodotto semidiretto

$g, g' \in G = K \rtimes H \implies \exists!\, a, a' \in K$ e $b, b' \in H$ tali che
$g = ab$ e $g' = a'b' \implies$

$$gg' = aba'b' = aba'b^{-1}bb' \quad \text{con} \quad aba'b^{-1} \in K \text{ e } bb' \in H.$$

Se $\Gamma\colon G \to \mathrm{Aut}(G)$ è l'omomorfismo che definisce l'azione per coniugio, $\forall\, c \in G$ posso considerare $\Gamma(c)|_K \in \mathrm{Aut}(K)$ (perché $K \triangleleft G$) e ottengo un omomorfismo

$$\theta\colon H \to \mathrm{Aut}(K) \qquad b \mapsto \Gamma(b)|_K$$

tale che $ba'b^{-1} = \Gamma(b)(a') = \theta(b)(a')$, e quindi

$$gg' = a\theta(b)(a')bb' \quad \text{con} \quad a\theta(b)(a') \in K \text{ e } bb' \in H.$$

Prodotto semidiretto di gruppi

Definizione-Proposizione

H e K gruppi, $\theta\colon H \to \mathrm{Aut}(K)$ omomorfismo. Il prodotto semidiretto di K e H rispetto a θ, denotato con $K \rtimes_\theta H$ o $H \ltimes_\theta K$, è il gruppo costituito dall'insieme $K \times H$ con l'operazione

$$(a, b)(a', b') \mapsto (a\theta(b)(a'), bb').$$

In particolare $K \rtimes_\theta H = K \times H$ se θ è l'omomorfismo banale.

Osservazione

È facile vedere che $G = K \rtimes_\theta H \implies G = K' \rtimes H'$ con $K \cong K' := K \times \{1\} \lhd G$ e $H \cong H' := \{1\} \times H < G$ (esercizio).
Inoltre $H' \lhd G \iff \theta$ è banale: se θ è banale, $G = K \times H$, quindi $H' \lhd G$. Viceversa, se $H' \lhd G$, allora $\forall\, a \in K$ e $\forall\, b \in H$
$(a, 1)(1, b)(a, 1)^{-1} = (a, b)(a^{-1}, 1) = (a\theta(b)(a^{-1}), b) \in H' \implies$
$1 = a\theta(b)(a^{-1}) = a\theta(b)(a)^{-1} \implies \theta(b)(a) = a \implies \theta$ è banale.
In particolare $K \rtimes_\theta H$ abeliano $\iff$ H, K abeliani e θ banale.

Dimostrazione della Definizione-Proposizione

- L'operazione è associativa: $\forall\, a, a', a'' \in K$ e $\forall\, b, b', b'' \in H$

$$\begin{aligned}((a,b)(a',b'))(a'',b'') &= (a\theta(b)(a'),bb')(a'',b'')\\ &= (a\theta(b)(a')\theta(bb')(a''),bb'b'')\end{aligned}$$

$$\begin{aligned}(a,b)((a',b')(a'',b'')) &= (a,b)(a'\theta(b')(a''),b'b'')\\ &= (a\theta(b)(a'\theta(b')(a'')),bb'b'')\end{aligned}$$

e le due espressioni sono uguali perché (tenendo conto che $\theta(b)\colon K \to K$ è un omomorfismo e che $\theta(bb') = \theta(b)\circ\theta(b')$)

$$\theta(b)(a'\theta(b')(a'')) = \theta(b)(a')\theta(b)(\theta(b')(a'')) = \theta(b)(a')\theta(bb')(a'').$$

- L'elemento neutro è $(1,1)$ (esercizio).
- $(a,b)^{-1} = (\theta(b^{-1})(a^{-1}),b^{-1})$ $\forall\, a \in K$ e $\forall\, b \in H$ (esercizio):

Automorfismi dei gruppi ciclici

$\mathrm{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^* \ \forall\, n > 0$. Infatti la funzione

$$f : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}^* \qquad \alpha \mapsto \alpha(\bar{1})$$

è un isomorfismo:

- f è ben definita perché α isomorfismo $\implies$ $\mathrm{ord}(\alpha(\bar{1})) = \mathrm{ord}(\bar{1}) = n \implies \alpha(\bar{1}) \in \mathbb{Z}/n\mathbb{Z}^*$;
- f è biunivoca perché $\forall\, a \in \mathbb{Z}\ \exists!\, \alpha : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ omomorfismo tale che $\alpha(\bar{1}) = \bar{a}$ e α iniettivo $\iff$ α suriettivo $\iff$ $\mathrm{ord}(\alpha(\bar{1})) = n \iff \alpha(\bar{1}) \in \mathbb{Z}/n\mathbb{Z}^*$;
- f è un omomorfismo perché $\forall\, \alpha, \beta \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, se $f(\alpha) = \alpha(\bar{1}) = \bar{a}$ e $f(\beta) = \beta(\bar{1}) = \bar{b}$, allora

$$f(\alpha \circ \beta) = \alpha(\beta(\bar{1})) = \alpha(\bar{b}) = b\alpha(\bar{1}) = b\bar{a} = \overline{ba} = \bar{a}\bar{b} = f(\alpha)f(\beta).$$

$\mathrm{Aut}(\mathbb{Z}) = \{\pm \mathrm{id}_{\mathbb{Z}}\} \cong C_2$: $\forall\, a \in \mathbb{Z}\ \exists!\, \alpha : \mathbb{Z} \to \mathbb{Z}$ omomorfismo tale che $\alpha(1) = a$ e α iniettivo $\iff$ $a \neq 0$, α suriettivo $\iff$ $a = \pm 1$.

Altri gruppi di automorfismi

p primo, $n > 0 \implies \mathrm{Aut}(C_p^n) \cong \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$:

$C_p^n \cong (\mathbb{Z}/p\mathbb{Z})^n$ abeliano tale che $p\mathbb{Z} \subseteq \mathrm{Ann}_{\mathbb{Z}}((\mathbb{Z}/p\mathbb{Z})^n) \implies$

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

Dunque $\#\mathrm{Aut}(C_p^2) = \#\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = (p-1)^2 p(p+1)$, e in particolare $\#\mathrm{Aut}(C_2^2) = 6 \implies \mathrm{Aut}(C_2^2) \cong S_3$, dato che $\forall\, K$ campo $\mathrm{GL}_2(K)$ non è abeliano, perché per esempio

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Anche $\mathrm{Aut}(S_3) \cong S_3$:

$\mathrm{Int}(S_3) \cong S_3/Z(S_3) = S_3/\{1\} \cong S_3$ e basta vedere che $\#\mathrm{Aut}(S_3) \leq 6$, vero perché $f \in \mathrm{Aut}(S_3)$ è determinato da $f|_{\{2\text{-cicli}\}} \in S(\{2\text{-cicli}\}) \cong S_3$.

Isomorfismo tra prodotti semidiretti

Proposizione

$\theta, \theta' \colon H \to \mathrm{Aut}(K)$ *omomorfismi tali che* $\theta = \theta' \circ \alpha$ *per qualche* $\alpha \in \mathrm{Aut}(H) \implies K \rtimes_\theta H \cong K \rtimes_{\theta'} H$.

Dimostrazione.

Poiché α è biunivoca, anche la funzione

$$f \colon K \rtimes_\theta H \to K \rtimes_{\theta'} H \qquad (a, b) \mapsto (a, \alpha(b))$$

lo è. Inoltre f è un omomorfismo perché

$$f((a,b)(a',b')) = f((a\theta(b)(a'), bb')) = (a\theta(b)(a'), \alpha(bb')) =$$
$$(a\theta'(\alpha(b))(a'), \alpha(b)\alpha(b')) = (a, \alpha(b))(a', \alpha(b')) = f((a,b))f((a',b'))$$

$\forall\, a, a' \in K$ e $\forall\, b, b' \in H$. □

Corollario

H e K gruppi con $H \cong C_p$ per qualche primo p.

1. $\exists\, \theta\colon H \to \mathrm{Aut}(K)$ omomorfismo non banale $\iff$ $p \mid \#\mathrm{Aut}(K)$.
2. Se $\mathrm{Aut}(K)$ ha un unico sottogruppo di ordine p, allora $K \rtimes_\theta H \cong K \rtimes_{\theta'} H$ per ogni coppia $\theta, \theta'\colon H \to \mathrm{Aut}(K)$ di omomorfismi non banali.

Dimostrazione.

1. Poiché H è semplice, $\exists\, \theta$ non banale $\iff$ $\exists\, \theta$ iniettivo $\iff$ $\exists\, H' < \mathrm{Aut}(K)$ tale che $H' \cong H$ $\iff$ $p \mid \#\mathrm{Aut}(K)$.
2. Se H' è l'unico sottogruppo di ordine p di $\mathrm{Aut}(K)$ e θ e θ' sono non banali, allora sono iniettivi e $\mathrm{im}(\theta) = \mathrm{im}(\theta') = H'$. Dunque esistono isomorfismi $\tilde{\theta}, \tilde{\theta}'\colon H \to H'$ tali che $\theta = i \circ \tilde{\theta}$ e $\theta' = i \circ \tilde{\theta}'$ (con $i\colon H' \to \mathrm{Aut}(K)$ l'inclusione). Allora $\tilde{\theta} = \tilde{\theta}' \circ \alpha$ e quindi $\theta = \theta' \circ \alpha$ con $\alpha := \tilde{\theta}'^{-1} \circ \tilde{\theta} \in \mathrm{Aut}(H)$.

Classificazione dei gruppi di ordine pq

$\#G = pq$ con $p < q$ primi.

- $q \not\equiv 1 \mod p \implies G \cong C_{pq}$.
- $q \equiv 1 \mod p \implies G \cong C_{pq}$ o $G \cong C_q \rtimes_\theta C_p$ con $\theta\colon C_p \to \mathrm{Aut}(C_q)$ omomorfismo non banale; inoltre $C_q \rtimes_\theta C_p$ non è abeliano e, a meno di isomorfismo, non dipende da θ.

Dimostrazione.

So già che $G \cong C_q \rtimes_\theta C_p$ per qualche omomorfismo

$$\theta\colon C_p \to \mathrm{Aut}(C_q) \cong \mathbb{Z}/q\mathbb{Z}^* \cong C_{q-1}.$$

Se θ è banale $G \cong C_q \times C_p \cong C_{pq}$, e θ è banale se $q \not\equiv 1 \mod p$, perché in quel caso $p \nmid \#\mathrm{Aut}(C_q) = q - 1$.
Se invece $q \equiv 1 \mod p$, esiste θ non banale, $C_q \rtimes_\theta C_p$ non è abeliano e, a meno di isomorfismo, non dipende da θ perché $\mathrm{Aut}(C_q) \cong C_{q-1}$ ha un unico sottogruppo di ordine p. □