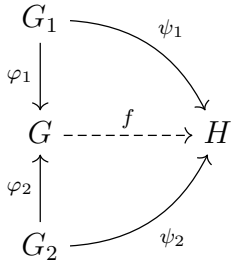
Prodotto libero di gruppi

14 dicembre 2014

Definizione 1. *Siano G_1 e G_2 due gruppi (in notazione moltiplicativa). Consideriamo una terna $(G, \varphi_1, \varphi_2)$, dove G è un terzo gruppo e $\varphi_i : G_i \to G$ è un morfismo (per $i = 1, 2$). Diciamo che $(G, \varphi_1, \varphi_2)$ è un* prodotto libero *di G_1 e G_2, se vale la seguente proprietà: per ogni gruppo H e per ogni coppia di morfismi $\psi_i : G_i \to H$, $i = 1, 2$ esiste un unico morfismo $f : G \to H$ tale che il diagramma*

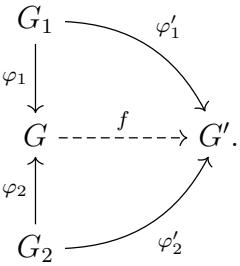


(0.1)

commuti.

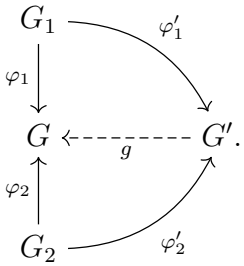
Proposizione 2. *Se $(G, \varphi_1, \varphi_2)$ e $(G', \varphi_1', \varphi_2')$ sono due prodotti liberi di G_1 e G_2, allora esiste un unico isomorfismo $f : G \xrightarrow{\cong} G'$ tale che $f\varphi_i = \varphi_i'$.*

Dimostrazione. Siccome $(G, \varphi_1, \varphi_2)$ è un prodotto libero, esiste un unico morfismo $f : G \to G'$ che fa commutare il diagramma



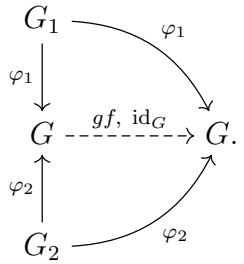
(0.2)

Siccome $(G', \varphi_1', \varphi_2')$ è un prodotto libero, esiste un unico morfismo $g : G' \to G$ che fa commutare il diagramma



(0.3)

D'altro canto gf e id_G fanno commutare il diagramma seguente



(0.4)

Siccome $(G, \varphi_1, \varphi_2)$ è un prodotto libero, il morfismo che fa commutare questo diagramma è unico, quindi $gf = \mathrm{id}_G$. Per lo stesso motivo, siccome $(G', \varphi_1', \varphi_2')$ è un prodotto libero, $fg = \mathrm{id}_{G'}$. Quindi $g = f^{-1}$ ed f è un isomorfismo. □

Per dimostrare che il prodotto libero esiste bisogna fare una costruzione un po' lunga.

Fissiamo G_1 e G_2. Usiamo sempre la notazione moltiplicativa e indichiamo con 1_G l'elemento neutro del gruppo G. Quando non c'è rischio di confondersi scriviamo semplicemente 1. Sostituendo eventualemente G_2 con un altro gruppo a lui isomorfo possiamo supporre che gli insiemi $G_1 - \{1\}$ e $G_2 - \{1\}$ siano disgiunti. Poniamo $A^* := (G_1 - \{1\}) \sqcup (G_1 - \{1\})$ e $A := A^* \sqcup \{1\}$. Chiamiamo A^* *alfabeto* e chiamiamo *lettere* i suoi elementi. Una *parola* nell'alfabeto A^* è una successione $\{x_n\}_{n\in\mathbb{N}}$ di elementi di A che è definitivamente uguale ad 1, cioè tale che esista k tale che $x_n = 1$ per ogni $n > k$. Il k minimo con questa proprietà si chiama *lunghezza* della parola. Se $k = 0$ la successione $\{x_n\}$ è tale che $x_n = 1$ per ogni $n \geq 1$. Questa successione si chiama *parola*

vuota o *parola di lunghezza 0* e si indica con 1. Se invece $k > 0$ la parola è una successione $\{x_n\}_{n\in\mathbb{N}}$, tale che $x_n = 1$ per $n > k$ e $x_k \neq 1$. Una parola di lunghezza k è identificata dai suoi primi k termini, per cui la possiamo scrivere nel modo seguente

$$w = x_1 \cdots x_k.$$

Sia $w = x_1 \cdots x_k$ una parola di lunghezza $k > 0$. Supponiamo che valga la condizione seguente:

a) $x_n \neq 1$ per ogni $n, 1 \leq n \leq k$.

Allora per ogni $n, 1 \leq n \leq k$, esiste un indice $i_n \in \{1, 2\}$ tale che $x_n \in G_{i_n} - \{1\}$.

Definizione 3. *Una parola $w = x_1 \cdots x_k$ di lunghezza $k > 0$ è* ridotta *se oltre ad (a) vale la condizione*

b) $i_n \neq i_{n+1}$ per ogni $n, 1 \leq n \leq k-1$.

Inoltre consideriamo per definizione la parola vuota come una parola ridotta.

Indichiamo con $G_1 * G_2$ l'insieme formato da tutte le parole ridotte (inclusa la parola vuota). Vogliamo definire su $G_1 * G_2$ una struttura di gruppo sfruttando la giustapposizione di parole. In generale se $w_1 = x_1 \cdots x_k$ e $w_2 = y_1 \cdots y_l$, non è detto che la successione $x_1 \cdots x_n y_1 \cdots y_l$ sia una parola ridotta. Può succedere per esempio che x_n e y_1 stiano entrambi in G_1. Quindi la concatenazione pura e semplice non definisce una operazione su $G_1 * G_2$. Procediamo invece come segue. Innanzitutto poniamo $1 \cdot w = w \cdot 1 := w$ per ogni $w \in G_1 * G_2$. Quindi definiamo il prodotto di parole ricorsivamente. Supponiamo di sapere moltiplicare due parole rispettivamente di lunghezza $n' < n$ e $m' < m$. Date $w = x_1 \cdots x_n$ e $w' = y_1 \cdots y_m$ poniamo

$$w \cdot w' := \begin{cases} x_1 \cdots x_n y_1 \cdots y_m & \text{se } x_n \text{ e } y_1 \text{ non stanno} \\ & \text{nello stesso gruppo} \\ x_1 \cdots x_{n-1}(x_n y_1) y_2 \cdots y_m & \text{se } x_n \text{ e } y_1 \text{ stanno nello} \\ & \text{stesso gruppo e } x_n \neq y_1^{-1} \\ (x_1 \cdots x_{n-1}) \cdot (y_2 \cdots y_m) & \text{se } x_n \text{ e } y_1 \text{ stanno nello} \\ & \text{stesso gruppo e } x_n = y_1^{-1}. \end{cases} \tag{0.5}$$

Nei primi due casi otteniamo una parola ridotta (verificare!). Nel terzo caso ci riconduciamo a calcolare il prodotto di due parole di lunghezza rispettivamente $n-1$ ed $m-1$.

Osserviamo che c'è una applicazione naturale che associa alla lettera $a \in A^*$ la parola ridotta $w = a$. In questo modo otteniamo una mappa iniettiva $\varphi : A^* \hookrightarrow G_1 * G_2$ che ha per immagine l'insieme delle parole di lunghezza 1. Il più delle volte identificheremo $a \in A^*$ con la parola $\varphi(a)$.

Teorema 4. *$(G_1 * G_2, \cdot)$ è un gruppo.*

Dimostrazione. Per costruzione la parola vuota 1 è un elemento neutro bilatero. L'inverso della parola ridotta $x_1 \cdots x_n$ è la parola ridotta $x_n^{-1} \cdots x_1^{-1}$. Questo si può dimostrare per induzione su k sfruttando la definizione 0.5 (ci si trova sempre nel terzo caso). L'unica cosa che resta da verificare è l'associatività. Procediamo nel modo seguente, detto trucco di van der Waerden. Sia H l'insieme di tutte le applicazioni biunivoche di $G_1 * G_2$ in sé stesso. H è un gruppo rispetto alla composizione. Data una lettera $x \in A^*$, sia $L_x : G_1 * G_2 \to G_1 * G_2$ l'applicazione definita dalla formula

$$L_x(w) := x \cdot w$$

dove il prodotto $x \cdot w$ è quello appeno definito in $G_1 * G_2$. Vogliamo verificare che $L_{x^{-1}} \circ L_x = \mathrm{id}_{G_1 * G_2}$. Infatti scriviamo $w = z_1 \cdots z_k$. Come al solito dobbiamo distinguere 3 casi. Nel primo caso x e z_1 appartengono allo stesso gruppo e $xz_1 \neq 1$, nel secondo caso x e z_1 appartengono allo stesso gruppo e $xz_1 = 1$, nel terzo caso x e z_1 appartengono a gruppi diversi. Nel primo caso, cioè se x e z_1 appartengono allo stesso gruppo G_s e $xz_1 \neq 1$, si ha $x \cdot w = (xz_1)z_2 \cdots z_k$ (qui (xz_1) è un elemento di G_s e pertanto è una lettera) e dunque

$$\begin{aligned}(L_{x^{-1}} \circ L_x)(w) = x^{-1} \cdot (x \cdot w) = x^{-1} \cdot (xz_1)z_2 \cdots z_k = \\ = (x^{-1}xz_1)z_2 \cdots z_k = z_1 z_2 \cdots z_k = w.\end{aligned}$$

Una verifica analoga dimostra che anche negli altri due casi si ha $(L_{x^{-1}} \circ L_x)(w) = w$. Pertanto $L_{x^{-1}} \circ L_x = \mathrm{id}_{G_1 * G_2}$. Allo stesso modo $L_x \circ L_{x^{-1}} = \mathrm{id}_{G_1 * G_2}$, dunque $L_x \in H$ e $L_{x^{-1}} = (L_x)^{-1} =$. Abbiamo così definito una mappa $L : A^* \to H, x \mapsto L_x$. Ora estendiamo L a $G_1 * G_2$. Se $w = x_1 \cdots x_n \in G_1 * G_2$, poniamo $L_w := L_{x_1} \circ \cdots \circ L_{x_n}$. Vogliamo dimostrare che date due parole ridotte $w, w' \in G_1 * G_2$ si ha $L_w \circ L_{w'} = L_{w \cdot w'}$. Procediamo

per induzione sulla lunghezza di w e w'. Se una delle due parole ha lunghezza 0 è ovvio. Supponiamo $w = x_1 \cdots x_k$ e $w = y_1 \cdots y_m$ con $k, m > 0$. Allora

$$L_w \circ L_{w'} = (L_{x_1} \circ \cdots \circ L_{x_{k-1}}) \circ (L_{x_k} \circ L_{y_1}) \circ (L_{y_2} \circ \cdots \circ L_{y_m}).$$

Come al solito distinguiamo 3 casi a seconda di cosa combinano x_k e y_1. Se x_k e y_1 stanno in gruppi distinti, la parola $x_1 \cdots x_k y_1 \cdots y_m$ è ridotta ed è uguale a $w \cdot w'$. Pertanto $L_w \circ L_{w'} = L_{w \cdot w'}$. Se invece x_k e y_1 stanno nello stesso gruppo e $x_k y_1 \neq 1$, è sufficiente provare che $L_{x_k} \circ L_{y_1} = L_{(x_k y_1)}$. Questa verifica è simile a tutte le altre già fatte e viene lasciata come esercizio. Infine, se x_k e y_1 stanno nello stesso gruppo e $x_k y_1 = 1$, basta sfruttare il fatto che $L_{x_k} \circ L_{y_1} = \mathrm{id}_{G_1 * G_2}$. Date $w, w', w'' \in G$ si ha

$$(w \cdot w') \cdot w'' = L_{w \cdot w'}(w'') = L_w(L_{w'}(w'')) = w \cdot (w' \cdot w'').$$

Ciò prova che l'operazione di $G_1 * G_2$ è associativa. □

In sostanza il trucco di van der Waerden permettedi provare l'associatività direttamente solo nel caso (più semplice) delle parole di lunghezza 1.

Indichiamo con $\varphi_i : G_i \longrightarrow G_1 * G_2$ la mappa che manda 1 in 1 e che su $G_i - \{1\}$ coincide con φ. In altre parole se $x \in G_i - \{1\}$, allora $\varphi_i(x)$ è la parola di lunghezza 1 formata dalla sola lettera x. φ_i è un morfismo iniettivo di gruppi e $G_1 * G_2$ è generato da $\varphi_1(G_1) \cup \varphi_2(G_2) = \varphi(A) \cup \{1\}$ (dimostrare!).

Possiamo finalmente dimostrare che il prodotto libero esiste.

Teorema 5. *Dati due gruppi G_1 e G_2 la terna $(G_1 * G_2, \varphi_1, \varphi_2)$ è un prodotto libero di G_1 e G_2.*

Dimostrazione. Sia H un gruppo e siano $\psi_i : G_i \to H$ morfismi qualsiasi. Dobbiamo provare che esiste un morfismo f che rende commutativo il diagramma (0.1). Definiamo f nel modo seguente. Se $w = x_1 \cdots x_k \in G_1 * G_2$ con $x_n \in G_{i_n}$ per $n = 1, \ldots, k$, poniamo

$$f(w) := \psi_{i_1}(x_1) \cdots \psi_{i_k}(x_k).$$

Sfruttando ancora una volta la definizione (0.5) si verifica che f è un morfismo. Evidentemente f fa commutare il diagramma. Infine se f' è un altro morfismo che fa commutare il diagramma, allora $f'(w) = f(w)$ per ogni parola $w \in \varphi_1(G_1) \cup \varphi_2(G_2)$. Ma siccome quest'ultimo insieme genera $G_1 * G_2$, segue $f' = f$. Dunque f è unico. □

Per approfondire si può consultare [1, p. 64 sgg.], [4, VIII, §3], [3, Ch. III] e [2].

Osserviamo che la tecnica per costruire $G_1 * G_2$ non è unica. Quindi in alcuni testi si trovano strategia alternative.

Riferimenti bibliografici

[1] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[2] M. Manetti. *Topologia*. Springer. xii, 297 p., 2008.

[3] W. S. Massey. *Algebraic topology: an introduction*. Springer-Verlag, New York, 1977. Reprint of the 1967 edition, Graduate Texts in Mathematics, Vol. 56.

[4] G. Zappa. *Fondamenti di teoria dei gruppi. Vol. II*, volume 18 of *Consiglio Nazionale delle Ricerche Monografie Matematiche*. Edizioni Cremonese, Rome, 1970.