

# Prodotto di sottogruppi e ordini di gruppi abeliani

di Gabriel Antonio Videtta

**Nota.** Nel corso del documento per  $(G, \cdot)$  si intenderà un qualsiasi gruppo.

Si introduce in questo documento la nozione di prodotto di sottogruppi, ripresa poi nella dimostrazione di un lemma fondamentale per lo studio dei gruppi abeliani.

**Definizione** (prodotto di sottogruppi). Siano  $H$  e  $K$  due sottogruppi di  $G$ . Si definisce il loro prodotto  $HK$  come:

$$HK = \{hk \mid h \in H, k \in K\} \subseteq G.$$

In realtà, il concetto di “prodotto di sottogruppi” non è del tutto nuovo nello studio dell’Algebra per uno studente che ha già seguito con successo un corso di Algebra lineare. Infatti, la somma di due sottospazi vettoriali è un prodotto di sottogruppi, per quanto la scrittura  $V + W$  possa trarre in inganno (infatti uno spazio vettoriale è in particolare un gruppo abeliano). L’unica, cruciale, differenza sta nel fatto che una somma di sottospazi è sempre un sottospazio, mentre  $HK$  potrebbe non esserlo, come mostra la:

**Proposizione.** Siano  $H$  e  $K$  due sottogruppi di  $G$ . Allora  $HK$  è un sottogruppo di  $G$  se e solo se  $HK = KH$ .

*Dimostrazione.* Se  $HK$  è un sottogruppo di  $G$ , si verifica facilmente che  $HK = KH$ . Infatti, se  $k \in K$  e  $h \in H$ ,  $kh$ , che appartiene chiaramente a  $KH$ , deve appartenere anche ad  $HK$  dal momento che è l’inverso dell’elemento  $h^{-1}k^{-1} \in HK$  (infatti  $HK$  è un gruppo); pertanto  $KH \subseteq HK$ . Analogamente, sia  $x$  un elemento di  $HK$ . Allora  $x$  ammette un inverso in  $HK$ , e quindi  $x^{-1} = hk$ , con  $h \in H$ ,  $k \in K$ . Allora  $x = k^{-1}h^{-1} \in KH$ , da cui  $HK \subseteq KH$  e quindi  $HK = KH$ .

Sia ora  $HK = KH$ . Chiaramente  $e \in HK$ . Siano  $x = h_1k_1$  e  $y = h_2k_2$  elementi di  $HK$  con  $h_1, h_2 \in H$  e  $k_1, k_2 \in K$ . Allora  $xy = h_1k_1h_2k_2$ ; tuttavia  $k_1h_2$  si può riscrivere per ipotesi (essendo  $KH \subseteq HK$ ) come  $hk$  con  $h \in H$  e  $k \in K$ . Allora  $xy = h_1hkk_2 \in HK$ , e quindi  $HK$  è chiuso per l’operazione di gruppo di  $G$ . Inoltre  $x^{-1} = k_1^{-1}h_1^{-1} \in KH$ , e quindi, per ipotesi,  $x^{-1} \in HK$ , da cui la tesi.  $\square$

Quindi, se un gruppo è abeliano, vale sempre la relazione  $HK = KH$ , e dunque  $HK$  è sempre un sottogruppo (e quindi si sostituisce con più tranquillità alla notazione  $HK$  la più familiare  $H + K$ ). In realtà, però, si può indebolire questa ipotesi richiedendo la normalità di  $H$  o  $K$  (come suggerisce la notazione  $H = KHK^{-1}$ ), come mostra la:

**Proposizione.** Siano  $H$  e  $K$  due sottogruppi di  $G$ . Allora, se  $H \triangleleft G$ ,  $HK = KH$ .

*Dimostrazione.* Siano  $h \in H$  e  $k \in K$ . Si consideri l'elemento  $hk \in HK$ . Poiché  $H$  è normale,  $k^{-1}hk \in H$ , e quindi  $k^{-1}hk = h'$  con  $h' \in H$ , da cui  $HK \subseteq KH$ . Analogamente si mostra anche l'altra inclusione.  $\square$

Come studiato nell'ambito dell'Algebra lineare, l'intersezione dei sottogruppi  $H$  e  $K$  gioca un ruolo fondamentale nel considerare l'insieme  $HK$ . In particolare, ci si chiede quando il prodotto  $hk$  è univocamente rappresentato (ossia  $hk = h'k' \implies h = h'$  e  $k = k'$ ). Si può rispondere a questa domanda in due modi: mostrando sotto quali ipotesi si trova un isomorfismo tra  $HK$  e  $H \times K$  (che dunque codifica l'unicità tramite l'uguaglianza delle coordinate), o determinando la cardinalità di  $HK$  per  $G$  finito (e dunque l'unicità dipende dall'uguaglianza  $|HK| = |H||K|$ , dal momento che se le scritture sono uniche, tutti i prodotti tra elementi di  $H$  e di  $K$  sono distinti). In entrambi i casi si giungerà alla conclusione secondo cui  $H \cap K$  deve essere banale<sup>1</sup>

**Proposizione** (cardinalità di  $HK$ ). Sia  $G$  un gruppo finito. Siano  $H$  e  $K$  due sottogruppi di  $G$ . Allora vale che  $|HK| = \frac{|H||K|}{|H \cap K|}$ .

*Dimostrazione.* Si costruisca la relazione di equivalenza  $\sim$  su  $H \times K$  in modo tale che:

$$(h, k) \sim (h', k') \stackrel{\text{def}}{\iff} hk = h'k'.$$

Allora chiaramente  $|H \times K / \sim| = |HK|$  (infatti ad ogni classe di equivalenza corrisponde esattamente un unico elemento di  $HK$ ).

Si esamini la classe di equivalenza di  $(h, k) \in H \times K$ . Si mostra che ogni elemento di tale classe è della forma  $(ht, t^{-1}k)$  con  $t \in H \cap K$ . Sia infatti  $(h_1, k_2) \in [(h, k)]_{\sim}$ . Allora:

$$h_1k_1 = hk \implies h^{-1}h_1 = kk_1^{-1} \in H \cap K.$$

Pertanto, se  $h^{-1}h_1 = kk_1^{-1} = t$ , vale che  $h_1 = ht$  e che  $k_1 = t^{-1}k$ . Quindi ogni classe di equivalenza contiene esattamente  $|H \cap K|$  elementi. Poiché  $\sim$  induce una partizione di  $H \times K$  in classi di equivalenza, vale dunque che:

$$|H||K| = |H \times K| = |H \times K / \sim| |H \cap K| = |HK| |H \cap K|,$$

da cui la tesi.  $\square$

<sup>1</sup>Mantenendo l'analogia con l'Algebra lineare, vale infatti che  $V+W = V \oplus W$  se e solo se  $V \cap W = \{0\}$ . Si mostrerà che sotto le stesse ipotesi anche un prodotto di sottogruppi è un prodotto diretto (tramite isomorfismo).

*Dimostrazione alternativa.* Si osserva che vale la seguente identità:

$$HK = \bigcup_{h \in H} hK.$$

Poiché gli  $hK$  rappresentano delle classi laterali sinistre di  $G$ , se  $h' \in H$ , o  $hK = h'K$  o  $hK \cap h'K = \emptyset$ . Se  $hK = h'K$ , allora  $hh^{-1} \in K$ , e quindi  $hh^{-1} \in H \cap K$ . Vi sono dunque esattamente  $|H \cap K|$  istanze della classe  $hK$  nell'unione considerata all'inizio della dimostrazione. Allora:

$$|HK| = \frac{|H| |K|}{|H \cap K|},$$

dove  $|K|$  è il numero di elementi di ogni classe  $hK$ . □

Pertanto, se le scritture sono uniche,  $H \cap K$  deve essere per forza banale (infatti deve valere  $|H \cap K| = 1$ ). Questo risultato può essere rafforzato dalla:

**Proposizione.** Siano  $H$  e  $K$  due sottogruppi normali di  $G$  tali che  $H \cap K = \{e\}$ . Allora  $HK \cong H \times K$ .

*Dimostrazione.* Si costruisce la mappa  $\rho : H \times K \rightarrow HK$  in modo tale che:

$$(h, k) \xrightarrow{\rho} hk.$$

Si osserva che ogni elemento  $h$  di  $H$  commuta con ogni elemento  $k$  di  $K$ . Se infatti si considera il commutatore  $g = [h, k]$ , vale che:

$$g = \underbrace{(hkh^{-1})}_{\in K} k \in K, \quad g = h^{-1} \underbrace{(kh^{-1}k^{-1})}_{\in H} \in H.$$

Pertanto  $g \in H \cap K \implies [h, k] = e \implies hk = kh$ . Allora  $\rho$  è un omomorfismo, infatti:

$$\rho((hh', kk')) = hh'kk' = hkh'k' = \rho((h, k))\rho((h', k')).$$

Chiaramente  $\rho$  è surgettiva. Inoltre  $\rho((h, k)) = e \implies h = k^{-1} \in H \cap K$ , e dunque  $h = k = e$ , da cui l'iniettività di  $\rho$  e la tesi. □

Inoltre, se  $G = G_1 \times G_2$  con  $G_1$  e  $G_2$  gruppi, si possono trovare facilmente due copie isomorfe di  $G_1$  e  $G_2$  in  $G$ , ossia  $G'_1 = G_1 \times \{e\}$  e  $G'_2 = \{e\} \times G_2$ . Vale inoltre che  $G'_1, G'_2 \trianglelefteq G$  e dunque, per la proposizione precedente<sup>2</sup>, che  $G \cong G'_1 \times G'_2$ .

In particolare vale il seguente risultato, considerando  $\langle x \rangle \cap \langle y \rangle = \{e\}$ :

**Proposizione.** Siano<sup>34</sup>  $x, y$  due elementi di  $G$  che commutano con  $\text{MCD}(\text{ord}(x), \text{ord}(y)) = 1$ . Allora  $\text{ord}(xy) = \text{ord}(x) \text{ord}(y)$ .

<sup>2</sup>Infatti  $G'_1 \cap G'_2 = \{(e, e)\}$ .

<sup>3</sup>In generale, se  $\text{MCD}(\text{ord}(x), \text{ord}(y)) > 1$ , non vale che  $\text{ord}(xy) = \text{mcm}(\text{ord}(x), \text{ord}(y))$ , benché sicuramente  $\text{ord}(xy) \mid \text{mcm}(\text{ord}(x), \text{ord}(y))$ , sempre a patto che  $x$  e  $y$  commutino. È sufficiente considerare in  $\mathbb{Z}/6\mathbb{Z}$  gli elementi  $\bar{1}$  e  $\bar{2}$ : infatti  $\text{ord}(\bar{1}) = 6$  e  $\text{ord}(\bar{2}) = 3$ , ma  $\text{ord}(\bar{1} + \bar{2}) = \text{ord}(\bar{3}) = 2 \neq 6$ .

<sup>4</sup>A prescindere da quanto valga  $\text{MCD}(\text{ord}(x), \text{ord}(y))$ , se  $x$  e  $y$  commutano, esiste però sempre un elemento  $g \in G$  tale per cui  $\text{ord}(g) = \text{mcm}(\text{ord}(x), \text{ord}(y))$ .

*Dimostrazione.* Chiaramente  $\text{ord}(xy) \mid \text{ord}(x) \text{ord}(y)$ , dal momento che  $(xy)^{\text{ord}(x) \text{ord}(y)} = x^{\text{ord}(x) \text{ord}(y)} y^{\text{ord}(x) \text{ord}(y)} = e$ , dove si è usato che  $x$  e  $y$  commutano. Sia allora  $k = \text{ord}(xy)$ . Vale allora che  $x^k y^k = e \implies x^k = y^{-k} \in \langle x \rangle \cap \langle y \rangle$ . Tuttavia  $|\langle x \rangle \cap \langle y \rangle| \mid \text{MCD}(|\langle x \rangle|, |\langle y \rangle|) = \text{MCD}(\text{ord}(x), \text{ord}(y)) = 1$ , e quindi  $\langle x \rangle \cap \langle y \rangle = \{e\}$ . Allora deve valere che  $x^k = y^{-k} = e \implies \text{ord}(x), \text{ord}(y) \mid k$ , da cui si deduce che  $\text{ord}(x) \text{ord}(y) \mid k = \text{ord}(x) \text{ord}(y)$ . Si conclude dunque che  $\text{ord}(xy) = \text{ord}(x) \text{ord}(y)$ .  $\square$

Si può adesso dimostrare il seguente fondamentale teorema per i gruppi abeliani:

**Teorema.** Sia  $G$  un gruppo abeliano finito di ordine  $n$ . Allora, se  $m$  divide  $n$ , esiste un sottogruppo di  $G$  di ordine  $m$ .

*Dimostrazione.* Si dimostra preliminarmente che se  $p^k$  divide  $n$ , dove  $p$  è un numero primo e  $k \in \mathbb{N}^+$ , allora  $G$  ammette un sottogruppo di ordine  $p^k$ . Si mostra la tesi per induzione su  $k$ .

Se  $k = 1$  la tesi è valida per il Teorema di Cauchy, completando il passo base. Si ipotizzi adesso che per ogni  $t < k$  valga la tesi. Si consideri un sottogruppo  $H$  di  $G$  di ordine  $p$  (ancora una volta questo sottogruppo esiste per il Teorema di Cauchy). Poiché  $G$  è abeliano,  $H$  è normale in  $G$ , e quindi si può considerare il gruppo quoziente  $G/H$ . Per il Teorema di Lagrange,  $p^{k-1}$  divide  $|G/H|$ , e quindi, per l'ipotesi induttiva, esiste un sottogruppo  $T$  di  $G/H$  di ordine  $p^{k-1}$ .

Si consideri la proiezione al quoziente  $\pi_H : G \rightarrow G/H$ . Poiché  $\pi_H$  è un omomorfismo,  $\pi_H^{-1}(T)$  è un sottogruppo. Inoltre, questo sottogruppo di  $G$  ha ordine  $p^k$ , dal momento che  $H$  ha ordine  $p$  (e quindi ogni elemento di  $T$  corrisponde tramite la controimmagine a  $p$  elementi), completando il passo induttivo.

Sia ora  $m$  scomposto nella sua fattorizzazione in primi  $p_1^{k_1} \cdots p_s^{k_s}$ . Per il risultato precedente,  $G$  ammette dei sottogruppi  $H_1, \dots, H_s$  di ordine  $p_1^{k_1}, \dots, p_s^{k_s}$ . Poiché  $G$  è abeliano, tutti questi sottogruppi sono normali e si può dunque considerare il prodotto dei sottogruppi  $H_1 \cdots H_s$  (che è dunque un sottogruppo). Poiché  $\text{MCD}(p_1^{k_1}, p_2^{k_2}) = 1$ ,  $H_1 \cap H_2$  è banale e vale che  $|H_1 H_2| = |H_1| |H_2| = p_1^{k_1} p_2^{k_2}$ . Allora, poiché  $\text{MCD}(p_1^{k_1} p_2^{k_2}, p_3^{k_3}) = 1$ , anche  $(H_1 H_2) \cap H_3$  è banale e dunque  $|H_1 H_2 H_3| = p_1^{k_1} p_2^{k_2} p_3^{k_3}$ . Proseguendo induttivamente si mostra dunque che  $H_1 \cdots H_s$  è un sottogruppo di  $G$  di ordine  $m$ .  $\square$