Capitolo 1

Prodotto libero di gruppi

Queste dispense sono basate su degli appunti forniti da alcuni studenti, che ringrazio.

Osservazione 1. Abbiamo già incontrato $\mathbb{Z}^k$ e l'abbiamo presentato come gruppo abeliano libero di rango k. Abbiamo visto che una delle ragioni di questo nome è dovuta al fatto che, dato un gruppo abeliano A, e considerata una base[1] $v_1, \ldots, v_k$ di $\mathbb{Z}^k$, per ogni scelta di k elementi $a_1, a_2, ..., a_k$ di A (non necessariamente distinti), è possibile trovare un omomorfismo da $\mathbb{Z}^k$ ad A che mandi v_i in a_i per ogni i. Nel creare un omomorfismo, insomma, si è liberi di decidere l'immagine degli elementi v_i.

Definizione 1 (Prodotto libero di gruppi)**.** Sia $\{\mathcal{G}_i\}_{i\in I}$ un insieme di gruppi. Se un gruppo $\mathcal{G}$ soddisfa tutte le seguenti condizioni:

- $\forall i \in I,\ \exists \phi_i \in Hom(\mathcal{G}_i, \mathcal{G})$. (Vedremo poi che non è restrittivo chiedere che questi omomorfismi siano iniettivi).
- $\forall H$ gruppo e per ogni insieme di omomorfismi $\left\{\mathcal{G}_i \xrightarrow{\psi_i} H\right\}_{i\in I}$ esiste un unico omomorfismo $\mathcal{G} \xrightarrow{f} H$ tale che siano commutativi i seguenti diagrammi:

$$\begin{array}{ccc} \mathcal{G}_i & \xrightarrow{\phi_i} & \mathcal{G} \\ & \searrow^{\psi_i} & \downarrow f \\ & & H \end{array}$$

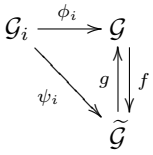
diremo che $\mathcal{G}$ è un prodotto libero dei $\mathcal{G}_i$ (rispetto alle mappe ϕ_i).

Teorema 1. *Dato un insieme $\{\mathcal{G}_i\}_{i\in I}$ di gruppi, il loro prodotto libero, se esiste, è unico a meno di isomorfismo.*

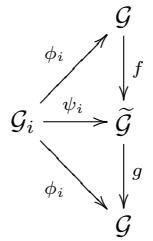
Dimostrazione

[1] Come per gli spazi vettoriali, una base è un insieme di elementi linearmente indipendenti e che generano (si considerano le combinazioni lineari a coefficienti in $\mathbb{Z}$

Supponiamo per assurdo che anche $\widetilde{\mathcal{G}}$ sia il prodotto libero dello stesso insieme di gruppi. Allora avremmo i diagrammi:



e sappiamo che esistono un'unica f ed un'unica g tali che tutti questi diagrammi commutino. Se riuscissimo ad ottenere che $f \circ g$ e $g \circ f$ sono le identità allora avremmo che entrambe sono isomorfismi e avremmo concluso. Analizziamo dunque $g \circ f$ utilizzando i diagrammi:



Sappiamo che $g \circ f : \mathcal{G} \to \mathcal{G}$ fa commutare il diagramma, ma anche l'identità $id : \mathcal{G} \to \mathcal{G}$ lo fa commutare. Possiamo comunque concludere, per l'unicità richiesta dalla definizione di prodotto libero, che $g \circ f = id : \mathcal{G} \to \mathcal{G}$. Analogamente si dimostra che $f \circ g = id : \widetilde{\mathcal{G}} \to \widetilde{\mathcal{G}}$.

Teorema 2. *Dato un insieme $\{\mathcal{G}_i\}_{i \in I}$ di gruppi, il loro prodotto libero esiste.*

Dimostrazione
Definiamo lista a coefficienti nei $\mathcal{G}_i$ una qualunque sequenza ordinata finita $(x_1, \ldots, x_k)$ con le seguenti proprietà:

- ogni elemento x_j che compare nella lista appartiene ad uno dei gruppi $\mathcal{G}_i$ per qualche i.
- due termini consecutivi appartengono a due $\mathcal{G}_i$ diversi.
- nessun termine è l'identità per qualche $\mathcal{G}_i$.

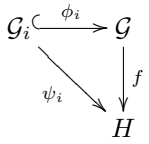
Il numero naturale k viene detta lunghezza della lista. Si aggiunge all'insieme delle liste anche la lista vuota (l'unica di lunghezza 0). L'insieme delle liste è infinito, e lo indicheremo con W. Descriviamo adesso un'azione di $\mathcal{G}_i$ su W. Sia $g \in \mathcal{G}_i$ e $X = (x_1, \ldots, x_k)$ allora:

- se $x_1 \notin \mathcal{G}_i$:
  a) Se $g \neq e_{\mathcal{G}_i}$ allora $g \cdot X = (g, x_1, \ldots, x_k)$. (Notiamo che se $X = (\,)$ allora $g \cdot (\,) = (g)$.
  b) Se $g = e_{\mathcal{G}_i}$ allora $g \cdot X = X$
- se $x_1 \in \mathcal{G}_i$:
  c) se $g \neq x_1^{-1}$ allora $g \cdot X = (gx_1, \ldots, x_k)$.

d) se $g = x_1^{-1}$ allora $g \cdot X = (x_2, \ldots, x_k)$ in particolare $g \cdot (g^{-1}) = ()$

Questa in effetti è un'azione di $\mathcal{G}_i$ su W. Sappiamo dunque che tale azione induce un omomorfismo $\mathcal{G}_i \xrightarrow{\phi_i} Big(W)$ che è anche iniettivo (per capire che due elementi di $\mathcal{G}_i$ hanno immagini diverse basta vedere come agiscono sulla lista vuota).
Chiamiamo allora $\mathcal{G}$ il sottogruppo di $Big(W)$ generato da $\phi(\mathcal{G}_i)$ al variare di $i \in I$.
D'ora in poi, se ci converrà per alleggerire la notazione, potremo leggere i $\mathcal{G}_i$ direttamente in $\mathcal{G}$, visto che i vari ϕ_i sono omomorfismi iniettivi. Quindi possiamo dire che ogni elemento di $\mathcal{G}$ è prodotto di un numero finito di elementi dei vari $\mathcal{G}_i$.

Dobbiamo verificare che $\mathcal{G}$ è il prodotto libero dei gruppi $\mathcal{G}_i$, cioè che comunque si scelga un gruppo H e una famiglia di omomorfismi $\{\psi_i : \mathcal{G}_i \to H\}_{i \in I}$, esiste un unico omomorfismo f tale che i seguenti diagrammi siano commutativi:



Per verificarlo premettiamo una definizione e un lemma.

Definizione 2 (Forma ridotta)**.** Diciamo che (con la notazione appena introdotta) $X = g_1 g_2 \ldots g_m$ è una *scrittura in forma ridotta* dell'elemento $X \in \mathcal{G}$ se:

- due fattori consecutivi stanno in due gruppi diversi.
- nessuno dei g_i è l'identità del suo gruppo.

Lemma 1. *La forma ridotta di un elemento $X \in \mathcal{G}$ esiste ed è unica.*

Dimostrazione
Per prima cosa si osserva che la forma ridotta di un elemento esiste: dato un elemento $X \in \mathcal{G}$ espresso come prodotto finito di vari elementi appartenenti ai gruppi $\mathcal{G}_i$ è infatti possibile scriverlo in forma ridotta con un numero finito di passaggi (se ci sono due fattori consecutivi che appartengono allo stesso gruppo si considera il loro prodotto, se, ad un certo punto si ottiene l'identità di un gruppo $\mathcal{G}_i$ la si elimina, etc...). Supponiamo per assurdo di avere due forme ridotte differenti:

$$X = g_1 \cdot \ldots \cdot g_m = h_1 \cdot \ldots \cdot h_k$$

Ogni elemento di $\mathcal{G}$ agisce su $Big(W)$. Consideriamo allora l'azione di $X \in \mathcal{G} \subseteq Big(W)$ sulla lista vuota; se vale l'uguaglianza delle due scritture di X allora devono anche valere le uguaglianze:

$$X \cdot (\,) = (g_1 \cdot \ldots \cdot g_m) \cdot (\,) = (g_1 \cdot \cdots \cdot g_{m-1}) \cdot (g_m) = (g_1, \ldots, g_m)$$
$$X \cdot (\,) = (h_1 \cdot \ldots \cdot h_k) \cdot (\,) = (h_1 \cdot \cdots \cdot h_{k-1}) \cdot (h_k) = (h_1, \ldots, h_k)$$

Dunque abbiamo

$$(g_1, \ldots, g_m) = (h_1, \ldots, h_k)$$

che è possibile solo se $m = k$ e le componenti sono uguali due a due.

Torniamo adesso alla dimostrazione del fatto che $\mathcal{G}$ è il prodotto libero dei gruppi $\mathcal{G}_i$. Dividiamo in due parti gli elementi di $\mathcal{G}$, pensando alla loro forma ridotta.

- Se la forma ridotta di un elemento X è $X = g_i$ con $g_i \in \mathcal{G}_i$ per un certo $i \in I$, allora perché i diagrammi commutino si deve porre $f(X) = \psi_i(g_i)$.
- Se la forma ridotta di un elemento X è $X = g_{i_1} g_{i_2} \cdots g_{i_k}$, con $g_{i_j} \in \mathcal{G}_{i_j}$, allora dato che vogliamo che f sia un omomorfismo dobbiamo porre

$$f(X) = \psi_{i_1}(g_{i_1}) \cdot \ldots \cdot \psi_{i_k}(g_{i_k})$$

Il fatto che la forma ridotta di un elemento sia unica ci dice innanzitutto che la funzione f è ben definita su ogni elemento $X \in \mathcal{G}$. Si verifica inoltre facilmente che f è un omomorfismo.

Esempio 1. Siano $\mathcal{G}_1 = \mathbb{Z}_2 = \{e, x_1\}$, $\mathcal{G}_2 = \mathbb{Z}_2 = \{e, x_2\}$. Il prodotto libero viene indicato con $\mathbb{Z}_2 * \mathbb{Z}_2$ (in generale si usa il simbolo $*$ per indicare il prodotto libero) e alcuni suoi elementi sono: x_1, x_1x_2, $x_1x_2x_1$, che sono tutti scritti in forma ridotta (e questo mostra che sono elementi diversi fra loro). In particolare abbiamo che $x_1x_2 \neq x_2x_1$. Inoltre x_1x_2 e x_2x_1 sono l'uno l'inverso dell'altro e hanno ordine infinito.

Esempio 2. Siano $\mathcal{G}_1 = \ldots = \mathcal{G}_m = \mathbb{Z}$ e consideriamo il loro prodotto libero che si può scrivere come:

$$\mathcal{G} = \prod_{i=1}^{m\ *} \mathbb{Z}$$

$\mathcal{G}$ è detto *gruppo libero su m generatori*. Se indichiamo ogni copia di $\mathbb{Z}$ con la notazione moltiplicativa, e scriviamo $\mathcal{G}_1 = \mathbb{Z} = (x_1)$, $\mathcal{G}_2 = \mathbb{Z} = (x_2)$, ..., $\mathcal{G}_m = \mathbb{Z} = (x_m)$, etc..allora $\mathcal{G}$ consiste di tutte le forme ridotte in cui ogni fattore è del tipo $x_i^{a_i}$ con a_i intero non nullo. Il gruppo libero su n generatori è unico a meno di isomorfismo, per il Teorema 1.

Esempio 3. Sia K un gruppo finito generato da m elementi $\{k_1, \ldots, k_m\}$. Consideriamo allora $\mathcal{G} = \prod_{i=1}^{m\ *} \mathbb{Z}$, con le notazioni dell'esempio precedente. Sappiamo che esiste un omomorfismo Γ da $\mathcal{G}$ a K ottenuto mandando per ogni $i = 1, ..., m$ il generatore x_i di $\mathcal{G}$ nel generatore k_i di K. Questo ci fornisce anche una successione esatta corta:

$$\{e\} \longrightarrow Ker\ \Gamma \longrightarrow \mathcal{G} \xrightarrow{\Gamma} K \longrightarrow \{e\}$$

Abbiamo dunque per il primo teorema di omomorfismo:

$$K \simeq {}^{\mathcal{G}}\!/_{Ker\ \Gamma}$$

Quindi K è determinato dalla conoscenza di $Ker\ \Gamma$. Osserviamo ora che $Ker\ \Gamma$ è un sottogruppo normale di $\mathcal{G}$. Se riusciamo a trovare degli elementi $r_1, ..., r_s$ di $Ker\ \Gamma$ che lo generano, diremo che K è *finitamente presentato* tramite i generatori $x_1, ..., x_m$ di $\mathcal{G}$ e le *relazioni* $r_1, ..., r_s$. Osserviamo che quando diciamo che $r_1, ..., r_s$ generano $Ker\ \Gamma$, intendiamo che lo generano come sottogruppo normale, ossia che $Ker\ \Gamma$ è il più piccolo sottogruppo normale di $\mathcal{G}$ che contiene gli elementi $r_1, ..., r_s$. In maniera equivalente, possiamo dire che $Ker\ \Gamma$ è dato da tutti i possibili prodotti finiti degli elementi $r_1, ..., r_s$, dei loro inversi, e di tutti i coniugati degli elementi $r_1, ..., r_s$ e dei loro inversi.

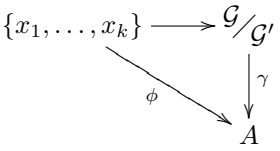
Osservazione 2. Che relazioni vi sono tra $\mathcal{G} = \prod_{i=1}^{k} {}^{*} \mathbb{Z}$, cioè il gruppo libero su k generatori, e $\mathbb{Z}^k$, il gruppo abeliano libero di rango k?
Consideriamo $\mathcal{G}'$, il sottogruppo dei commutatori (o derivato) di $\mathcal{G}$. Sappiamo che $\mathcal{G}/\mathcal{G}'$ è abeliano, dimostriamo che in effetti è isomorfo al gruppo abeliano libero di rango k.
Vediamo due differenti dimostrazioni:

- Sappiamo che un elemento di $\mathcal{G}$ è è dato da una espressione ridotta (che chiameremo 'parola'); quozientare per $\mathcal{G}'$ significa rendere il gruppo abeliano, questo ci permette quindi di scambiare l'ordine delle 'lettere' e di raggruppare i contributi di ogni singolo gruppo. Cioè una generica parola $x \in \mathcal{G}$ potrà essere scritta come:

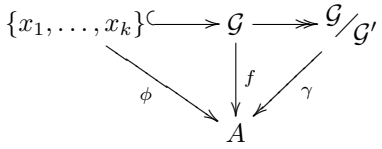
  $$x = x_1^{a_1} \cdot \ldots \cdot x_k^{a_k}$$

  Ma l'insieme degli elementi di questo tipo è isomorfo a $\mathbb{Z}^k$, come si verifica immediatamente.

- Proviamo una dimostrazione 'più astratta'. Sappiamo che $\mathbb{Z}^k$ è il gruppo abeliano libero. Ci è sufficiente dimostrare che anche $\mathcal{G}/\mathcal{G}'$ è il gruppo abeliano libero di rango k, è cioè sufficiente dimostrare che per ogni gruppo abeliano A esiste un unico omomorfismo γ che renda commutativo il seguente diagramma:

  Per vedere questo ci ricordiamo intanto che $\mathcal{G}$ è il gruppo libero, e dunque possiamo scrivere:

  sapendo che esiste un unico omomorfismo f che fa quanto richiesto. Certamente i commutatori di $\mathcal{G}$ appartengono al Ker di f, visto che sappiamo che ogni quoziente abeliano di $\mathcal{G}$ deve essere ottenuto quozientando per un sottogruppo contenente il sottogruppo dei commutatori. Ma allora possiamo dire che l'omomorfismo f passa al quoziente. Abbiamo quindi un omomorfismo γ (data dal passaggio al quoziente della f) che fa commutare il diagramma rappresentato nella figura sopra. Va dimostrata l'unicità di γ. Ma in realtà γ è completamente determinato dalle immagini di $x_1\mathcal{G}', \ldots, x_k\mathcal{G}'$ che sono già decise da ϕ.

Proposizione 1. *Siano F e G sono due gruppi liberi su due diversi insiemi di generatori S e T finiti. Allora*

$$F \simeq G \iff |S| = |T|$$

Osservazione 3. Osserviamo che in virtù di questa proposizione è ben definito il *rango* di un gruppo libero su un numero finito di generatori (la proposizione vale anche nel caso infinito, ma non approfondiremo in questo corso...).

Dimostrazione
Supponiamo innanzitutto $F \cong G$. Abbiamo allora:

$$\mathbb{Z}^{|S|} \cong {}^{F}\!/_{F'} \cong {}^{G}\!/_{G'} \cong \mathbb{Z}^{|T|}$$

Questo conclude, ricordandoci che S e T sono finiti e del teorema di classificazione dei gruppi abeliani finitamente generati.
L'altra implicazione è immediata.

Esempio 4. Siano $R \cong S \cong \mathbb{Z}$ due gruppi isomorfi a $\mathbb{Z}$ generati rispettivamente da ρ e da σ. Abbiamo allora:

$$\mathcal{D}_n \cong S * R/[(\rho^n, \sigma^2, \sigma\rho\sigma\rho)]$$

Con le parentesi quadre, in questo caso, indichiamo il generato dagli elementi indicati e da tutti gli elementi a loro coniugati (come abbiamo già osservato, infatti, il nucleo deve essere normale nel suo gruppo di appartenenza, in questo caso il gruppo libero).
Per dimostrare questo isomorfismo dovremmo vedere che (utilizzando la notazione della successione corta vista nell'ultima osservazione, in particolare la funzione Γ manda l'elemento ρ di $S * R$ nell'elemento $\bar{\rho}$ di $\mathcal{D}_n$, un generatore delle rotazioni, e fa lo stesso con σ e la riflessione che conosciamo):

$$Ker\ \Gamma = [(\rho^n, \sigma^2, \sigma\rho\sigma\rho)]$$

Si vede facilmente che gli elementi indicati sono contenuti nel $Ker\ \Gamma$; ma è meno immediato vedere che vale il contrario; si procede nella dimostrazione per induzione: si esplicitano quali sono gli elementi contenuti nel $Ker\ \Gamma$ al variare della lunghezza della loro forma ridotta e si vede che sono quelli descritti:

Lunghezza $= 1$ Abbiamo che $g \in Ker\ \Gamma \iff g = \rho^{cn} \vee g = \sigma^{d2}$.

Lunghezza $= 2$ Vi sono solo due casi: $g = \rho^a\sigma^b$ oppure $g = \sigma^b\rho^a$. Osservando che l'immagine rispetto a Γ di g risulta, rispettivamente: $\bar{\rho}^a\bar{\sigma}^b$ oppure $\bar{\sigma}^b\bar{\rho}^a$, possiamo dire che in entrambi i casi dobbiamo avere: $a = cn$ e $b = 2d$.

Lunghezza ≥ 3 Nel leggere la parola che esprime $g \in Ker\ \Gamma$ troviamo sicuramente all'inizio una espressione del tipo $\sigma^{2j}\sigma\rho^a\sigma$ con $j \in \mathbb{Z}$ oppure $\sigma^{2j}\rho^a\sigma\rho^b$ con $j \in \mathbb{Z}$. Vediamo cosa succede nel primo caso (il secondo è analogo). Possiamo scrivere:

$$\sigma^{2j}\sigma\rho^a\sigma = \sigma^{2j}(\sigma\rho^a\sigma\rho^a)\rho^{-a}$$

Si dimostra facilmente che σ^{2j} e $(\sigma\rho^a\sigma\rho^a)$ appartengono a $[((\rho^n, \sigma^2, \sigma\rho\sigma\rho))]$. Siccome l'elemento g appartiene a $Ker\ \Gamma$ si conclude che anche l'elemento g', ottenuto da g sostituendo la parte iniziale $\sigma^{2j}\sigma\rho^a\sigma$ con ρ^{-a}, appartiene a $Ker\ \Gamma$. Ma la lunghezza di g' è inferiore a quella di g e per induzione possiamo dire che $g' \in [((\rho^n, \sigma^2, \sigma\rho\sigma\rho))]$. Da questo si conclude subito che $g = \sigma^{2j}(\sigma\rho^a\sigma\rho^a)g' \in [((\rho^n, \sigma^2, \sigma\rho\sigma\rho))]$

Facciamo un accenno ora a quello che è conosciuto come il problema della parola: dato un gruppo presentato come quoziente di un gruppo libero per delle relazioni, esiste un algoritmo per decidere se due parole sono uguali?
Sono stati individuati gruppi finitamente presentati nei quali il problema della parola è indecidibile[2], e comunque, in generale, non è un problema semplice.
In generale è anche difficile riconoscere se due quozienti di un gruppo libero sono isomorfi fra loro. Il caso del prossimo esempio è di questo tipo ma è invece di facile soluzione.

Esempio 5. Indichiamo con $F(a,b)$ il gruppo libero con generatori a, b e con $F(a,c)$ il gruppo libero con generatori a, c. Consideriamo:

$$F(a,b)\big/_{[(baba^{-1})]} \qquad\qquad F(a,c)\big/_{[(a^2c^2)]}$$

questi due gruppi sono isomorfi?
La risposta è sì. Consideriamo l'omomorfismo:

$$\begin{array}{rccc} f: & F(a,b) & \longrightarrow & F(a,c) \\ & a & & a \\ & b & & ca \end{array}$$

sappiamo che esiste un unico f omomorfismo che fa quanto richiesto perché $F(a,b)$ è un gruppo libero. Consideriamo anche l'omomorfismo (sempre unico):

$$\begin{array}{rccc} g: & F(a,c) & \longrightarrow & F(a,b) \\ & a & & a \\ & c & & ba^{-1} \end{array}$$

Possiamo vedere facilmente che $g \circ f$ e $f \circ g$ sono le identità, quindi f e g sono entrambi isomorfismi.
Per concludere ci basta dimostrare che $f([(baba^{-1})]) = [(a^2c^2)]$. Cominciamo col dimostrare che:

$$f(baba^{-1}) = caacaa^{-1} = caac = ca^2c \in [(a^2c^2)]$$

Ma questo è vero, infatti $[(a^2c^2)]$ è normale, dunque possiamo dire:

$$a^2c^2 \in [(a^2c^2)] \implies ca^2c^2c^{-1} = ca^2c \in [(a^2c^2)]$$

A questo punto è immediato anche verificare che $g(a^2c^2) \in [(baba^{-1})]$ e concludere ricordando che $g \circ f$ e $f \circ g$ sono le identità.

[2]Rimaniamo vaghi su cosa questo vuole dire... Nei corsi di logica approfondirete.