Presentazione di gruppi

Sia G un gruppo e X un suo sottoinsieme non vuoto, indichiamo con

$$\bar{Gp}(X) = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} | x_i \in X, \epsilon_i = \pm 1\}$$

dove gli elementi di questo insieme sono da intendersi come stringhe di simboli.

Se $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots\dots x_n^{\epsilon_n}$ e $y_1^{\eta_1} y_2^{\eta_2} \dots\dots y_m^{\eta_m}$ sono prodotti in X essi sono *identici* se

$$m = n, \quad , \quad x_i = y_i, \quad , \quad \epsilon_i = \eta_i \qquad i = 1, 2, \dots, n$$

Due prodotti sono *differenti* se non sono identici. Due prodotti differenti possono dar luogo allo stesso elemento di G. Per esempio se $X = \{x, y\} \subseteq G$, i prodotti $xx^{-1}xy$ e xy sono differenti ma individuano lo stesso elemento di G. Se un prodotto contiene la successione xx^{-1} oppure $x^{-1}x$ per qualche $x \in X$, possiamo convenire di ridurre la sua lunghezza cancellando x e x^{-1}. Un prodotto si dice *ridotto* se non è possibile operare tali cancellazioni. A partire da un prodotto possiamo effettuare un numero finito di cancellazioni, ottenendo infine un prodotto ridotto che prende il nome di *forma ridotta* del prodotto considerato:

$$Gp(X) = \left\{w | w = 1_G \vee w \quad \textbf{elemento ridotto di} \quad \bar{Gp}(X)\right\}$$

Se G è il gruppo ciclico infinito generato da $\{x\}$, i prodotti ridotti in X sono solo di due tipi: $xx \dots x = x^r$ oppure $x^{-1}x^{-1} \dots x = x^{-r}$ dove r è un intero positivo. Se $x^m = x^n$ allora $m = n$ cioè prodotti ridotti differenti danno luogo a differenti elementi.

Questa proprietà si esprime dicendo che $\{x\}$ è un insieme libero di generatori di G.

Un gruppo G si dice *generato liberamente* da un suo sottoinsieme X se

1. $X \neq \emptyset$
2. $Gp(X) = G$
3. due prodotti ridotti differenti di X danno due elementi differenti non unitari di G.

Segue, dalla condizione 3, che se $x \in X$ allora $x^{-1} \notin X$ e che $1 \notin X$.

Un insieme X di generatori di G che soddisfi la condizione 3 è chiamato un *insieme libero di generatori di* G.

Un gruppo G è *libero* se è il gruppo banale con la sola identità o se ha un insieme libero di generatori. Se X è un insieme libero di generatori di G si dice che G è libero su X.

Osservazioni 0.1

1. *Il gruppo ciclico infinito è sottogruppo di un qualunque gruppo libero non banale. Infatti se* $G = Gp(X)$ *e* $x \in X, \quad x \neq 1$, *allora* $Gp(\{x\})$ *è un gruppo ciclico infinito.*
2. *Ogni gruppo finito non banale non è libero.*
3. *Se* G *è libero, generato da* X, *e* X *contiene almeno due elementi,* G *non è abeliano. Infatti se* $x, y \in X, \quad x \neq y$ *allora* xy *e* yx *sono prodotti ridotti differenti, quindi* $xy \neq yx$
4. *Il prodotto diretto di gruppi ciclici infiniti non è libero.*

Teorema 0.2 *Se F è un gruppo libero sull'insieme X e $f : X \to G$ è una funzione dall'insieme X in un gruppo G, esiste uno e un solo omomorfismo $\tilde{f} : F \to G$ che estende f.*

Dimostrazione

Ogni elemento di F è esprimibile in modo unico nella forma $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots\ldots x_n^{\epsilon_n}$ con $x_i \in X, \epsilon_i = \pm 1$, quindi necessariamente deve essere: $\tilde{f}(x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots\ldots x_n^{\epsilon_n}) = f(x_1)^{\epsilon_1} f(x_2)^{\epsilon_2} \ldots\ldots f(x_n)^{\epsilon_n}$. Ne segue che $\tilde{f}$ è unico per costruzione ed è un omomorfismo.

Se A è un insieme qualunque, esiste il gruppo libero generato da A che indichiamo con $F(A)$.

$F(A)$ è l'insieme delle parole ridotte sull'alfabeto A cioè l'insieme di tutti i prodotti ridotti del tipo $a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots\ldots a_n^{\epsilon_n}$ con $a_i \in A, \epsilon_i = \pm 1$ e della parola vuota 1.

L'operazione su $F(A)$ si ottiene riducendo due parole scritte di seguito.

Il gruppo libero sull'insieme vuoto è il gruppo unitario.

Se G è un gruppo, indicheremo con $T(G)$ (componente di torsione)il sottoinsieme di G costituito dagli elementi di periodo finito,

$$T(G) = \{a \in G | a^n = 1, \texttt{per qualche}\, n > 0\}$$

La componente di torsione di un gruppo non abeliano non è, in generale, un sottogruppo.

Per esempio, nel gruppo diedrale infinito, con due generatori a e b e le relazioni $a^2 = b^2 = 1$generatori a e b sono entrambi elementi di torsione, mentre $a \cdot b$ ha ordine infinito.

Se G è libero allora $T(G) = \{0\}$

Il teorema 0.2 ci consente di fornire una "presentazione di gruppi" in termini di gruppi liberi.

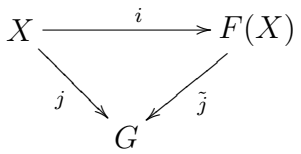
Una *presentazione di un gruppo* è una coppia $\langle X|R\rangle$ dove X è un insieme di generatori del gruppo libero $F(X)$ ed R è un sottoinsieme di $F(X)$.

Il gruppo presentato da $\langle X|R\rangle$ è il gruppo quoziente $F(X)/N$ dove N è il sottogruppo normale generato da R.

Teorema 0.3 *Ogni gruppo è isomorfo a un quoziente di un gruppo libero.*

Dimostrazione.

Sia G un gruppo e $X \subseteq G$ un insieme di generatori di G. Si consideri $F(X)$, l'inclusione $i : X \to F(X)$ e l'inclusione $j : X \to G$. Per il teorema precedente esiste uno e un solo $\tilde{j} : F(X) \to G$ tale che $\tilde{j}i = j$.



L'omomorfismo $\tilde{j}$ è suriettivo perché $\tilde{j}(F(X))$ è un sottogruppo che contiene X, quindi G risulta isomorfo al quoziente di $F(X)$ sul nucleo di $\tilde{j}$.

Una *presentazione* $\langle X|R\rangle$ è *finita* se sia X che R sono insiemi finiti.

Un gruppo G è *finitamente presentato* se ha una presentazione finita.

Esempi 0.4 *I seguenti primi 3 gruppi hanno presentazione finita, mentre il quarto non è finitamente generato:*

1. $\mathbf{Z}_3 = \langle a|a^3\rangle$
2. $\mathbf{Z} \times \mathbf{Z} = \langle a, b|aba^{-1}b^{-1}\rangle$
3. $\langle a, b|a^n, b^2, a^{-1}bab\rangle$ *è il gruppo diedrico di ordine n*
4. *Il gruppo dei razionali* $\mathbf{Q}$ *non è finitamente presentato, infatti se per assurdo* $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_n}{s_n}$ *fosse un insieme di generatori, si consideri un primo p che non divide nessun* s_i *e allora non è possibile scrivere:* $\frac{1}{p} = a_1\frac{r_1}{s_1} + a_2\frac{r_2}{s_2} + \ldots + a_n\frac{r_n}{s_n}$ *con* a_i *interi.*

Un gruppo può avere molte presentazioni diverse, per esempio $\langle x, y|xyxy^{-1}x^{-1}y^{-1}\rangle$ e $\langle a, b|a^3, b^{-2}\rangle$ sono presentazioni di gruppi isomorfi.

Non è possibile dare una soluzione generale al problema di sapere se due rappresentazioni distinte determinano gruppi isomorfi.

Ci sono però trasformazioni che non cambiano il gruppo. Tra queste molto importanti sono le equivalenze di Tietze.

Trasformazioni di Tietze

Sia $G = \langle X|R\rangle$ un gruppo di presentazione finita, con generatori $X = \{x_1, x_2 \ldots, x_n\}$ e relazioni $R = \{r_1, r_2 \ldots, r_m\}$.

Operiamo su G con delle trasformazioni (o equivalenze) di Tietze che ci permetteranno di passare da questa presentazione ad un'altra presentazione con altri generatori ed altre relazioni.

Tali trasformazioni sono di due tipi a seconda che si aggiunga o tolga una relazione oppure un generatore:

1. Se s è una conseguenza di $R = \{r_1, r_2 \ldots, r_m\}$ (cioè si ottiene come prodotto di r_i), allora $G = \langle X|R\rangle = \langle x_1, x_2 \ldots, x_n | r_1, r_2 \ldots, r_m, s\rangle$

2. Se $\xi \in F(X)$, allora $G = \langle X|R\rangle = \langle X \cup \{y\} \,|R \cup y\xi^{-1}\rangle =$

   $\langle x_1, x_2 \ldots, x_n, y | r_1, r_2 \ldots, r_m, y\xi^{-1}\rangle$

   che scriveremo anche nella forma:

   $\langle x_1, x_2 \ldots, x_n, y | r_1, r_2 \ldots, r_m, y = \xi\rangle$

Teorema 0.5 *Date due presentazioni finite $\langle X|R\rangle$ e $\langle X'|R'\rangle$ di uno stesso gruppo, esiste una successione finita di trasformazioni di Tietze che porta da $\langle X|R\rangle$ a $\langle X'|R'\rangle$.*

Esempi 0.6 *1. I gruppi presentati da $\langle x, y | xyxy^{-1}x^{-1}y^{-1}\rangle$ e da $\langle a, b | a^3b^{-2}\rangle$, sono isomorfi.*

1 $\langle x, y | xyx = yxy\rangle$ *con 2 volte passo 2 otteniamo*

2 $\langle x, y, a, b | xyx = yxy, a = xy, b = xyx\rangle$ *con 3 volte passo 1 otteniamo*

3 $\langle x, y, a, b | xyx = yxy, a^3 = b^2, a = xy, b = xyx, x = a^{-1}b, y = b^{-1}a^2\rangle$ *con 3 volte passo 1 otteniamo*

4 $\langle x, y, a, b | a^3 = b^2, x = a^{-1}b, y = b^{-1}a^2\rangle$ *con 2 volte passo 2 otteniamo*

5 $\langle a, b | a^3 = b^2\rangle$

2. I gruppi presentati da $\langle x, y, z | xyz = yzx\rangle$ e da $\langle x, y, a | xa = ax\rangle$, sono isomorfi.

1 $\langle x, y, z | xyz(yzx)^{-1}\rangle$ *con passo 2 otteniamo*

2 $\langle x, y, z, a | xyz(yzx)^{-1}, a(yz)^{-1}\rangle$ *con passo 1 otteniamo*

3 $\langle x, y, z, a | xyz(yzx)^{-1}, a(yz)^{-1}, xa(ax)^{-1} \rangle$ *con passo 1 otteniamo*

4 $\langle x, y, z, a | a(yz)^{-1}, xa(ax)^{-1} \rangle$ *con passo 1 otteniamo*

5 $\langle x, y, z, a | a(yz)^{-1}, xa(ax)^{-1}, z(y^{-1}a)^{-1} \rangle$ *con passo 1 otteniamo*

6 $\langle x, y, z, a | xa(ax)^{-1}, z(y^{-1}a)^{-1} \rangle$ *con passo 2 otteniamo*

7 $\langle x, y, a | xa(ax)^{-1} \rangle$

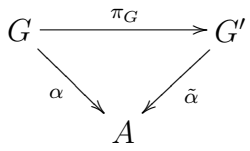
Gruppi abeliani finitamente presentati

Dato un gruppo $G = \langle X|R\rangle$, si possono aggiungere ad R i commutatori di X: S.

In tal modo si ottiene il gruppo abeliano $G' = \langle X|R \cup S\rangle$, che si chiama abelianizzazione di G.

Tale gruppo G' gode della seguente proprietà universale ed è da essa caratterizzato:

- *G' è l'unico gruppo abeliano (a meno di isomorfismi) tale che: esiste un omomorfismo $\pi_G : G \to G'$ con la seguente proprietà: per ogni gruppo abeliano A e per ogni omomorfismo $\alpha : G \to A$ esiste uno e un solo $\tilde{\alpha} : G' \to A$ per cui $\tilde{\alpha}\pi_G = \alpha$:*



Un gruppo libero abeliano è la abelianizzazione di un gruppo libero. Se $F(x_1, x_2, \ldots x_n)$ è il gruppo libero generato da $x_1, x_2, \ldots x_n$, e S è l'insieme dei commutatori di $x_1, x_2, \ldots x_n$, $\langle x_1, x_2, \ldots x_n|S\rangle$ è il gruppo libero abeliano su n generatori, di rango n. Il gruppo $\mathbf{Z}^n$ è libero per ogni $n \geq 1$ e i gruppi abeliani liberi finitamente generati sono tutti di questa forma, infatti si ha il seguente

Teorema 0.7 *Se G è un gruppo abeliano, si ha:*

1. *$T(G)$ è un suo sottogruppo.*
2. *Se G è libero allora $T(G) = \{0\}$*

Dimostrazione.

Se $a, b \in T(G)$ si ha $a^n = b^m = 1$ con $n, m > 0$. Ma allora $(ab^{-1})^{nm} = a^{nm}b^{-nm} = 1$ e $nm > 0$. Quindi $ab^{-1} \in T(G)$. Ciò prova che $T(G)$ è un sottogruppo di G. Se poi G è libero e X è un sistema libero di generatori, per ogni $a \in T(G)$ possiamo scrivere $a = \prod_{i=0}^{s} x_i^{\epsilon_i}$. Essendo $a^n = 1$, per qualche $n > 0$, si ottiene $\prod_{i=0}^{s} x_i^{n\epsilon_i}$. Poiché $\{x_1, \ldots, x_s\} \subseteq X$ e X è un sistema libero di generatori, si ottiene $n\epsilon_i = 0$ per ogni i e quindi $n_i = 0$ per ogni i.

Definizione 0.8 *$T(G)$ è chiamato* sottogruppo di torsione di G.

Se $T(G)$ è il sottogruppo banale G è detto privo di torsione.

Teorema 0.9 *Per un gruppo abeliano finitamente presentato G sono fatti equivalenti*

1. *G è libero*
2. *T(G)=0*
3. *G è isomorfo a $\mathbf{Z}^n$ per qualche $n \geq 0$*

Il teorema 0.9 ci dice che, per i gruppi abeliano finitamente presentati essere privo di torsione ed essere libero sono condizioni equivalenti.

Il teorema 0.9 non è vero per i gruppi che non sono finitamente presentati.

Infatti il gruppo dei razionali $\mathbf{Q}$ è privo di torsione ma non è libero.

Infatti se esis tesse un insieme libero di generatori, questo non potrebbe contenere un solo elemento perché $\mathbf{Q}$ non è isomorfo a $\mathbf{Z}$; (si può osservare, per esempio, che in $\mathbf{Q}$ ogni elemento non nullo è divisibile per due). D'altra parte $\mathbf{Q}$ non ammette un insieme libero di generatori con almeno due elementi:

supponiamo per assurdo che esista X insieme libero di generatori di $\mathbf{Q}$ e che $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in X$, $\frac{p_1}{q_1} \neq \frac{p_2}{q_2}$, con $q_1, q_2 \geq 1$ e $p_1, p_2 \neq 0$, allora $p_2 q_1 \frac{p_1}{q_1} + (p_1)(-q_2)\frac{p_2}{q_2} = 0$. Poiché$\frac{p_1}{q_1}, \frac{p_2}{q_2} \in X$, $p_2 q_1 = (p_1)(-q_2) = 0$ ma $p_2 q_1, (p_1)(-q_2)$ sono entrambi non nulli.

Definizione 0.10 $\mathbf{Z}^n$, $n \geq 1$, *è detto gruppo abeliano libero di rango* n.

Il gruppo ciclico $\mathbf{Z}^n/n\mathbf{Z}$, essendo finito, non è mai un gruppo libero, qualunque sia $n \geq 1$.

Un gruppo infinito, anche se finitamente generato, non è necessariamente libero. Ad esempio il gruppo $(\mathbf{Z}^n/n\mathbf{Z}) \times \mathbf{Z}$ è infinito ma non libero perché in un gruppo abeliano libero non ci sono elementi di ordine finito. Ciò è conseguenza delle seguenti osservazioni.

Ogni gruppo abeliano finitamente generato è somma diretta di gruppi ciclici, come si può dedurre dai seguenti due teoremi di caratterizzazione.

1 Teorema 0.11 *Se* G *è un gruppo abeliano finitamente generato, allora:*

1. *G è isomorfo a*

   - $\mathbf{Z}^n$ *oppure*
   - $\mathbf{Z}^n \bigoplus_1^r \mathbf{Z}_{d_i}$
     dove $n \geq 0$, d_1 *sono numeri interi* ≥ 2 *e se* $i < j$, d_i *divide* d_j *e sono univocamente individuati da* G.

2 Teorema 0.12 *Se G è un gruppo abeliano finitamente generato, allora:*

1. *G è isomorfo a*

   - $\mathbf{Z}^n$ *oppure*
   - $\mathbf{Z}^n \bigoplus_1^r \mathbf{Z}_{d_i}$ *dove* $n \geq 0$, d_1 *sono numeri interi potenze di numeri primi*

Si pu concludere che ogni gruppo abeliano finitamente generato è somma di un gruppo libero $\mathbf{Z}^n$, dove n si chiama *rango* del gruppo G, e del gruppo di torsione $T(G)$ che ha due rappresentazioni canoniche.

Esempi 0.13

- $\mathbf{Z}/15\mathbf{Z} \cong \mathbf{Z}_{15}$ *può essere visto come somma diretta di due sottogruppi ciclici di ordine* 3 *e* 5*:* $\mathbf{Z}_{15} \cong \{0, 5, 10\} \oplus \{0, 3, 6, 9, 12\}$.

- *I gruppi di ordine* 8 *sono*
  - $\mathbf{Z}_8$
  - $\mathbf{Z}_2 \oplus \mathbf{Z}_4$
  - $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$

- $\mathbf{Z}_{36} \cong \mathbf{Z}_4 \oplus \mathbf{Z}_9$

- $\mathbf{Z}_2 \oplus \mathbf{Z}_{18} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_9$
- $\mathbf{Z}_6 \oplus \mathbf{Z}_{20} \oplus \mathbf{Z}_{36} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{12} \oplus \mathbf{Z}_{180}$.