

Gruppi liberi e relazioni

Sofia Tirabassi

Introduzione

Nota: In questo seminario lavoriamo in gruppi qualsiasi, in generale **NON** abeliani

Sia S un sottoinsieme (anche infinito) di un gruppo (G, \cdot) , con il simbolo $\langle S \rangle$ si indica il più piccolo sottogruppo di G che contiene S che è detto il sottogruppo di G generato da S . Quindi

$$\langle S \rangle := \bigcap_{\substack{H \supset S \\ H < G}} H = \{1, s_1 \cdots s_n \mid n \in \mathbb{N} \text{ e } s_i \in S \text{ o } s_i^{-1} \in S\}$$

Se $\langle S \rangle = G$ si dice che S genera G e gli elementi di S si dicono *generatori* di G ; se $|S| < \infty$, dove con $|S|$ si è indicata la cardinalità di S , si dice che G è *finitamente generato*.

Quando si lavora con un gruppo, soprattutto quando si vuole fare dell'algebra su di esso, ci si accorge che l'unico modo che abbiamo per fare dei conti è conoscere i generatori del gruppo e le varie relazioni che intercorrono tra questi.

Esempio 1. $\mathbb{Z}/6\mathbb{Z}$ è un gruppo *ciclico* e ha ordine 6. Una volta fissato un suo generatore a e imposta la regola che $6a = 0^1$, possiamo facilmente individuare i suoi sottogruppi, il periodo dei suoi elementi, costruire (quando esiste) un morfismo di gruppi iniettivo da $\mathbb{Z}/6\mathbb{Z}$ ad un qualsiasi altro gruppo G ...

Esempio 2. Prendiamo ora in considerazione il gruppo delle permutazioni su tre lettere, S_3 . Visto che non è un gruppo troppo grande, per capire come

¹Sono in notazione additiva

è fatto possiamo elencare tutti i suoi elementi:

$$S_3 = \{1, (12), (13), (23), (123), (132)\}.$$

Oppure possiamo fissare un insieme di suoi generatori e vedere le relazioni che intercorrono tra essi. Ad esempio facendo un po' di conti si vede che $(23) = (12)(123)$, $(132) = (123)^2$ e $(13) = (12)(123)^2$, quindi possiamo dedurre che $S_3 = \langle (12), (123) \rangle$. Inoltre questi due suoi generatori non sono liberi, ma hanno dei vincoli. Ad esempio si ha che $(12)^2 = 1$, $(123)^3 = 1$, oppure che $(12)(123)^2 = (123)(12)$.

Gli esempi precedenti trattano gruppi finiti, un modo semplice per riuscire a fare dei conti in essi è scrivere la loro tavola di moltiplicazione. Un'altra maniera di procedere, molto più utile in quanto si può utilizzare anche con gruppi infiniti è quella di trovare tutte le relazioni tra i generatori del gruppo. Purtroppo l'insieme delle relazioni tra gli elementi di un gruppo in generale non è finito, quindi è impensabile descriverle tutte elencandole una ad una. Da questi due esempi e dalle considerazioni che li hanno seguiti risulta evidente come i gruppi ciclici siano considerevolmente più facili da trattare di quelli che ciclici non sono. Già passando da uno a due generatori la situazione si complica parecchio. Ciò è una diretta conseguenza del fatto che tutti i gruppi ciclici possono essere visti come quozienti di \mathbb{Z} , il gruppo su cui è facile far di conto per autonomia. Infatti richiamiamo la proprietà di rappresentazione di $(\mathbb{Z}, +, 0)$

Teorema 1. *Dato un qualsiasi gruppo (G, \cdot) ed un suo elemento g , esiste un unico morfismo di gruppi $h : \mathbb{Z} \longrightarrow G$ tale che $h(1) = g$; h è il morfismo definito dalla mappa $n \mapsto g^n$.*

Supponiamo ora che, nelle notazioni precedenti, il gruppo G sia ciclico e che l'elemento g sia un suo generatore. Allora il morfismo h certamente suriettivo, e quindi, grazie al teorema fondamentale di isomorfismo di gruppi, possiamo affermare che $G \simeq \mathbb{Z}/\text{Ker } h$.

E se G non fosse ciclico?

Purtroppo in questo caso gli interi non ci possono aiutare più di tanto. Occorre quindi costruire un nuovo gruppo, indicato con FG^S (dove le lettere

FG stanno ad indicare le iniziali delle parole inglesi *free group*), tale che sia generato dagli elementi di un insieme S e tale che per ogni gruppo G generato da S esista N sottogruppo normale di FG^S tale che $G \simeq FG^S/N$. FG^S verrà detto *gruppo libero su S* mentre il sottogruppo N sarà l'*insieme delle relazioni tra i generatori di G* .

Procediamo ora ad una descrizione più formale

1 Il Gruppo Libero

Un insieme S di elementi di un gruppo che non soddisfano nessun'altra relazione all'infuori di quelle che derivano dagli assiomi della definizione stessa di gruppo (e.g. $a \cdot a^{-1} = a^{-1} \cdot a = 1$) è detto *libero*. Un gruppo che possiede un insieme libero di generatori è detto *libero*.

Esempio 3. 1. $\{1, 0\} \subset \mathbb{Z}/3\mathbb{Z}$ non è libero. Infatti i suoi due elementi soddisfano la relazione $3 \cdot 1 = 0$, non richiesta dagli assiomi della definizione di gruppo.

2. $\{1\} \subset \mathbb{Z}$ è libero. Da ciò segue subito che \mathbb{Z} è un gruppo libero.

Descriviamo come sono fatti i gruppi liberi. Sia S un insieme arbitrario (finito o infinito) di simboli o *alfabeto*, $S = \{a, b, c, \dots\}$, chiamiamo *parola nell'alfabeto S* , o semplicemente *parola*, una qualunque successione finita di elementi di S in cui sono ammesse ripetizioni. Ad esempio a , aa , $abbac$ sono parole. Indichiamo con W l'insieme di tutte le parole su S e definiamo su di esso un'operazione mediante la giustapposizione:

$$(ac, abbc) \mapsto acabbc$$

Notiamo che questa legge di composizione delle parole è associativa e per di più possiamo considerare la parola vuota, che d'ora in avanti indicheremo con il simbolo 1 , come elemento neutro di quest'operazione. Purtroppo l'insieme $(W, \cdot, 1)$ non è un gruppo, perchè non abbiamo definito cosa sono gli inversi delle parole. Sia quindi S' l'insieme costituito dai simboli di S e dai simboli s^{-1} per ogni $s \in S$:

$$S' = \{a, a^{-1}, b, b^{-1}, \dots\}.$$

Sia W' l'insieme delle parole su S' . Se una parola $w \in W'$ è della forma

$$\dots xx^{-1} \dots \quad \text{oppure} \quad \dots x^{-1}x \dots$$

per qualche $x \in S$, possiamo convenire di ridurre la sua lunghezza cancellando x e x^{-1} . Una parola si dice *ridotta* se non è possibile operare tali cancellazioni. A partire da una parola w possiamo effettuare un numero finito² di cancellazioni, ottenendo infine una parola *ridotta* w_0 che prende il nome di *forma ridotta* di w . A questo punto ci si può chiedere se a partire da una parola w la sua forma ridotta sia univocamente determinata da w . Infatti a partire da una parola w è possibile operare le cancellazioni in più modi: ad esempio se $w = babb^{-1}acc^{-1}$ possiamo scegliere di eliminare prima la coppia bb^{-1} e poi la coppia cc^{-1} o possiamo scegliere di invertire l'ordine delle due operazioni. La proposizione seguente ci assicura che la definizione di forma ridotta di una parola w sia ben posta.

Proposizione 2. *Esiste un'unica forma ridotta di una parola assegnata a w .*

Dimostrazione. Si procede per induzione sulla lunghezza di w . Se w è ridotta non vi è nulla da dimostrare. Supponiamo quindi che w non sia ridotta e che per tutte le parole non ridotte di lunghezza minore di w la proposizione sia vera. Il fatto che w non sia ridotta implica che esiste un coppia di sue lettere che possono essere cancellate, diciamo la coppia sottolineata:

$$w = \dots \underline{xx^{-1}} \dots ,$$

dove con x denotiamo un qualsiasi elemento di S' con la convenzione ovvia che se $x = a^{-1}$, allora $x^{-1} = a$. Se si riuscisse a mostrare che è possibile ottenere ogni forma ridotta w_0 di w cancellando per prima la coppia $\underline{xx^{-1}}$, allora la proposizione seguirà per induzione sulla parola accorciata $\dots \cancel{xx^{-1}} \dots$ così ottenuta. Sia w_0 una forma ridotta di w . Sappiamo che w_0 è ottenuta da w mediante una successione finita di cancellazioni. La prima possibilità è che la coppia $\underline{xx^{-1}}$ venga cancellata in qualche passo di questa successione. Allora potremmo ordinare le operazioni e cancellare

²Le cancellazioni accorciano la lunghezza della parola w che è finita, quindi in un numero finito di passi si arriva o ad una parola ridotta od alla parola vuota, che è altresì ridotta. Ne segue che l'algoritmo ha termine in un numero finito di passi.

$\underline{xx^{-1}}$ per prima. Ed in questo caso avremmo ottenuto il risultato cui anelavamo.

D'altra parte, la coppia $\underline{xx^{-1}}$ non può restare in w_0 , poichè w_0 è ridotta. Se la coppia stessa non è stata cancellata, allora deve essere stato cancellato uno dei suoi elementi, con un'operazione della forma

$$\dots \cancel{x}^{-1} \underline{\cancel{x}^{-1}} \dots \quad \text{oppure} \quad \dots \underline{x} \cancel{x}^{-1} \cancel{x} \dots .$$

Si noti che in entrambi i casi la parola ottenuta mediante questa cancellazione è la stessa di quella che si sarebbe ottenuta cancellando la coppia originaria $\underline{xx^{-1}}$. Ci ritroviamo così nel primo caso e l'asserto è dimostrato. \square

Due parole w e w' sono dette *equivalenti*, e si scrive $w \sim w'$ se hanno la stessa forma ridotta. Questa è una relazione di equivalenza e la prossima proposizione ci dice che il prodotto per giustapposizione si “comporta bene” se si passa al quoziente.

Proposizione 3. *I prodotti di parole equivalenti sono equivalenti: se $w \sim w'$ e $v \sim v'$, allora $wv \sim w'v'$.*

Dimostrazione. Per ottenere la parola ridotta equivalente al prodotto wv , possiamo innanzitutto cancellare quanto più possibile dalle parole w e v , per ridurle rispettivamente alle loro forme ridotte w_0 e v_0 . Ora possiamo continuare a cancellare in w_0v_0 , se possibile. Adottando lo stesso procedimento a w' e v' , arriveremo nuovamente alla parola w_0v_0 , dopo aver ridotto w' e v' . e quindi continuando a ridurre giungeremo alla stessa forma ridotta. \square

Una diretta conseguenza di questo risultato è il seguente:

Teorema 4. *Denotiamo con FG^S l'insieme quoziente dell'insieme delle parole W' con la relazione di equivalenza appena introdotta. Allora FG^S è un gruppo rispetto alla legge di composizione indotta da W' :*

$$[w]_{\sim} [v]_{\sim} \stackrel{\text{def}}{=} [wv]_{\sim} \quad (1)$$

Dimostrazione. La proposizione 3 ci assicura che l'operazione sulle classi di equivalenza definita in (1) sia ben definita. L'associatività di questa

composizione ed il fatto che la classe della parola vuota 1 sia un'identità discendono direttamente dalle proprietà corrispondenti in W' . Resta da verificare che tutti gli elementi di FG^S siano invertibili. Ma è chiaro che se $w = xy \cdots z$, allora la classe di $z^{-1} \cdots y^{-1}x^{-1}$ è l'inversa di w . \square

Definizione 1. Il gruppo FG^S delle classi di equivalenza delle parole sull'alfabeto S è detto *gruppo libero* sull'insieme S

Osservazione 1. Notiamo che possiamo considerare l'insieme S come un sottoinsieme di FG^S mediante l'inclusione $I_S : S \rightarrow FG^S$ definita dalla mappa $s \mapsto [s]_{\sim}$. Si vede subito che S è un'insieme libero di generatori per FG^S e quindi che FG^S è un gruppo libero.

Osservazione 2. I sottogruppi di gruppi liberi sono anch'essi liberi.

La proposizione 2 ci assicura che un elemento del gruppo libero corrisponde ad un uica parola ridotta di W' . Per moltiplicare parole ridotte basta unire e cancellare:

$$(ab^{-1}c)(c^{-1}a) = ab^{-1}a$$

Per le parole ridotte si può introdurre la notazione esponenziale:

$$\overbrace{a \cdots a}^{n \text{ volte}} = a^n$$

Osservazione 3 (Notazione). D'ora in avanti, per alleggerire la notazione, userò la scrittura \bar{w} piuttosto che $[w]_{\sim}$ per indicare la classe di equivalenza di una parola nel gruppo libero.

2 Relazioni

Andiamo ora a vedere come sia possibile studiare un gruppo il cui insieme dei generatori non sia libero usando gli strumenti che abbiamo introdotto nella sezione precedente. Enunciamo prima di tutto una caratteristica propria dei gruppi liberi che non è altro che un'estensione della proprietà di rappresentazione di \mathbb{Z} .

Teorema 5 (Proprietà di rappresentazione del gruppo libero). *Sia FG^S il gruppo libero su un insieme $S = \{a, b, \dots\}$ e sia G un gruppo. Ogni applicazione tra insiemi $f : S \rightarrow G$ si estende in modo unico ad un morfismo di gruppi $\varphi : FG^S \rightarrow G$ definito dalle mappe*

$$\bar{s} \mapsto f(s) \quad \forall s \in S; \quad (2)$$

$$\overline{s^{-1}} \mapsto f(s)^{-1} \quad \forall s \in S; \quad (3)$$

$$\overline{w} = [\dots x \dots y^{-1} \dots]_{\sim} \mapsto \dots f(x) \dots f(y)^{-1} \dots \quad \forall x, y \in S. \quad (4)$$

Equivalentemente, nelle notazioni precedenti, esiste un unico morfismo di gruppi φ tale per cui il seguente diagramma commuti

$$\begin{array}{ccc} FG^S & \xrightarrow{\varphi} & G \\ & \swarrow i_S \quad \searrow f & \\ & S & \end{array}$$

Dimostrazione. Bisogna vedere che due parole equivalenti w e w' di W' corrispondano allo stesso elemento di G . Ciò è evidente in quanto la cancellazione in una parola non cambia il prodotto corrispondente in G . Inoltre il fatto che la moltiplicazione in FG^S sia definita per giustapposizione ci dice subito che la φ così definita è un omomorfismo di gruppi. Esso rappresenta l'unico modo di estendere f ad un morfismo. \square

Se nelle notazioni precedenti S è un sottoinsieme di G ed f è l'inclusione canonica, il teorema 5 definisce un morfismo $\varphi : FG^S \rightarrow G$ che agisce come la mappa $\bar{x} \mapsto x$. Se poi S è un insieme di generatori per G , φ sarà suriettivo. Infatti, preso $g \in G$, avremo che $g = s_1 \cdots s_n$ con $n \in \mathbb{N}$ e $s_i \in S$ o $s_i^{-1} \in S$. Per come abbiamo costruito la φ si ha subito che $\varphi(\overline{s_1 \cdots s_n}) = g$. In queste condizioni il primo teorema di isomorfismo di gruppi ci dice che $G \simeq FG^S / \text{Ker } \varphi$. Gli elementi di $\text{Ker } \varphi$ prendono il nome di *relazioni* tra i generatori di G . Quindi una relazione è una classe di equivalenza di una parola w tale che $\varphi(\overline{w}) = 1$, cioè è un'identificazione del tipo $\overline{w} = 1$.

Sia ora R è un sottoinsieme di un gruppo G , possiamo definire il sottogruppo normale di G generato da R come il sottogruppo intersezione di

tutti i sottogruppi normali di G contenenti R ; scriveremo

$$\langle R \rangle_N = \bigcap_{\substack{N \supset R \\ N \triangleleft G}} N.$$

Si ha che $\langle R \rangle_N$ è normale in G , in realtà è il più piccolo³ sottogruppo normale di G che contiene R , e quindi è ben definita la struttura di gruppo sul quoziente $FG^S / \langle R \rangle_N$. Se R è un sottoinsieme di GF^S e G è un gruppo tale che $G \simeq FG^S / K$, dove K denota il sottogruppo normale di GF^S generato da R diremo che G è *definito dalle relazioni* R . Se R è finito diremo che G è *finitamente presentato*. Conoscendo un insieme di generatori di G ed un insieme di generatori del suo gruppo delle relazioni possiamo effettuare facilmente calcoli nel gruppo libero quozientato e quindi in G .

Osservazione 4 (Notazione). In generale per indicare gruppi finitamente generati e finitamente presentati si usa la notazione

$$G = \langle g_1, \dots, g_n; r_1, \dots, r_m \rangle$$

Dove i g_i sono i generatori del gruppo G , mentre gli r_i sono i generatori del gruppo delle relazioni di G .

Esempio 4 (D_n).

Mostreremo che il gruppo delle simmetrie di un poligono regolare di n lati, D_n è definito dalle relazioni

$$x^n, y^2, xyxy \tag{5}$$

nel gruppo libero generato da x e y che indicheremo con FG . Prendiamo per buono che D_n è generato dalla rotazione ρ di un angolo di $2\pi/n$ e dalla riflessione σ lungo un asse di simmetria del poligono. certo tra ρ e σ sussistono le relazioni

$$\rho^n = 1, \quad \sigma^2 = 1, \quad \sigma\rho\sigma\rho = 1; \tag{6}$$

³Notiamo come $\langle R \rangle_N$ in generale contenga strettamente $\langle R \rangle$. Infatti i suoi elementi sono sia prodotti del tipo $r_1 \cdots r_n$ con $n \in \mathbb{N}$ e $r_i \in R$ o $r_i^{-1} \in R$ sia gli coniugati di quest'ultimi

chiamiamo N il sottogruppo normale di FG generato dagli elementi della (5). E sia $\varphi : FG \rightarrow D_n$ il morfismo definito da $x \mapsto \rho$ e da $y \mapsto \sigma$. Certo $\text{Ker } \varphi \supseteq N$ e quindi è ben definita la mappa

$$\begin{aligned} \tilde{\varphi} : FG/N &\longrightarrow D_n \\ gN &\longmapsto \varphi(g) \end{aligned}$$

Inoltre la $\tilde{\varphi}$ è suriettiva in quanto la φ è tale. Se dimostriamo che $|FG/N| \leq 2n$ avremmo necessariamente che $\tilde{\varphi}$ è pure iniettiva e di qua l'asserto.

Siano quindi $\bar{x} = xN$ e $\bar{y} = yN$ in FG/N . Dato che x^n, y^2 e $xyxy$ sono in N , valgono le relazioni $\bar{x}^n = 1$, $\bar{y}^2 = 1$ e $\bar{x}\bar{y}\bar{x}\bar{y} = 1$. In particolare vale che $\bar{y}\bar{x} = \bar{x}^{-1}\bar{y}$ il che implica che $\bar{y}\bar{x}^k = \bar{x}^{-k}\bar{y}$. Si vede che l'insieme $\{\bar{x}^k, \bar{x}^k\bar{y}, k = 0, \dots, n-1\}$ è chiuso rispetto alla moltiplicazione, all'inversione ed inoltre ha 1 come un suo elemento. In parole povere è un sottogruppo di FG/N e contiene i suoi generatori \bar{x} e \bar{y} . Segue immediatamente che

$$FG/N = \{\bar{x}^k, \bar{x}^k\bar{y}, k = 1, \dots, n-1\}.$$

Quindi $|FG/N| \leq 2n$ da cui deduciamo che $D_n \simeq FG/N$.

Esempio 5 (I gruppi abeliani).

Consideriamo il gruppo generato da due elementi, x e y con l'unica relazione $xyx^{-1}y^{-1}$. In generale se x e y sono elementi di un gruppo, l'elemento

$$xyx^{-1}y^{-1}$$

è detto il loro *commutatore*. Esso gode della proprietà di essere uguale a 1 se, e solo se, gli elementi x e y commutano tra loro. Quindi imponendo la relazione $xyx^{-1}y^{-1}$ otteniamo un gruppo i cui generatori x e y commutano tra loro.

Sia ora FG il gruppo libero generato da x e y e sia N il suo sottogruppo normale generato dal loro commutatore. Dimostriamo che il gruppo quoziente è abeliano.

Indichiamo le classi xN e yN con i simboli \bar{x} e \bar{y} rispettivamente. Poiché il commutatore appartiene ad N , \bar{x} e \bar{y} commutano in FG/N . Allora $\bar{y}\bar{x}\bar{y}^{-1} = \bar{x}$, il che implica $\bar{x}\bar{y}^{-1} = \bar{y}^{-1}\bar{x}$, cioè \bar{x} commuta con \bar{y}^{-1} . Inoltre \bar{x}

commuta ovviamente con se stesso ed il suo inverso, pertanto esso commuta con qualsiasi parola in $S' = \{\bar{y}, \bar{x}, \bar{y}^{-1}, \bar{x}^{-1}\}$ e così pure y . Segue per induzione che due qualsiasi parole in S' commutano tra loro, e poichè \bar{y} e \bar{x} generano il gruppo, FG/N è commutativo.

Il gruppo che abbiamo appena costruito è detto *gruppo abeliano libero su due elementi*, in quanto i suoi elementi non soddisfano altra relazione fuorchè quelle derivanti dagli assiomi di gruppo e la proprietà commutativa. In generale, per costruire il gruppo libero abeliano su n elementi x_1, \dots, x_n dobbiamo quozientare il gruppo libero su n elementi con il suo sottogruppo normale generato da TUTTI i commutatori dei generatori:

$$N = \langle \{x_i x_j x_i^{-1} x_j^{-1} \mid i, j = 1, \dots, n; i \neq j\} \rangle$$

Conclusioni

Negli esempi che abbiamo visto la conoscenza delle relazioni e dei generatori ci ha permesso di maneggiare un gruppo abbastanza facilmente. Ciò tuttavia può trarre in inganno, perchè i calcoli in un insieme arbitrario di relazioni spesso non sono affatto semplici. Per esempio supponiamo di cambiare leggermente le relazioni che definiscono il gruppo diedrale sostituendo y^2 con y^3 :

$$G = \langle x, y; x^n, y^3, xyxy \rangle .$$

Questo gruppo è molto complicato e si dimostra che per $n > 5$ è addirittura infinito.

Inoltre è stato dimostrato che in generale non esiste alcun algoritmo per risolvere in un tempo predeterminato il *problema della parola per i gruppi*, cioè il determinare se due parole rappresentano lo stesso elemento in un quoziente FG/N . Ciò nonostante i gruppi liberi e le relazioni sono uno strumento davvero potente: essi ci permettono di descrivere i gruppi finitamente generati e finitamente rappresentati con un numero finito di parametri, e ciò ci dà, tra le altre cose, la possibilità di far capire ad un calcolatore la struttura algebrica su cui stiamo lavorando. Concludiamo riprendendo gli esempi esposti all'inizio di questo seminario:

1. \mathbb{Z}_6 è il gruppo $\langle c; c^n \rangle$. In generale il gruppo ciclico di ordine n ha la rappresentazione $\langle c; c^n \rangle$.
2. Analogamente si dimostra che S_3 ha la seguente rappresentazione $\langle a, b; a^3, b^2 (ab)^2 \rangle$.

Riferimenti bibliografici

- [1] M. Artin *Algebra*, Bollati Boringhieri, Torino 1997
- [2] N. Jacobson *Basic Algebra I*, W. H. Freeman and Company, San Francisco 1973