Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

PRESENTAZIONI DI GRUPPI CON GENERATORI E RELAZIONI

Relatore:
Chiar.mo Prof.
Luca Migliorini

Presentata da:
Viola Pipa

III Sessione
Anno Accademico 2014-2015

Indice

Introduzione

La struttura di gruppo è una delle strutture algebriche piú semplici e importanti della matematica. Un gruppo si può descrivere in vari modi. Uno dei piú interessanti è la presentazione per generatori e relazioni. Sostanzialmente presentare un gruppo per generatori e relazioni significa dire quali specifiche "regole di calcolo" e semplificazione valgono nel gruppo in considerazione oltre a quelle che derivano dagli assiomi di gruppo. Questo porta in particolare alla definizione di gruppo libero. Un gruppo libero non ha regole di calcolo oltre quelle derivanti dagli assiomi di gruppo. Ogni gruppo è un quoziente di un gruppo libero su un appropriato insieme di generatori per un sottogruppo normale, generato dalle relazioni. In questa tesi si ricordano le definizioni piú importanti ed elementari della teoria dei gruppi, e si passa in seguito a discutere il gruppo libero e le presentazioni di gruppi con generatori e relazioni, dando alcuni esempi. La tesi si conclude illustrando un algoritmo molto interessante, l'algoritmo di Coxeter e Todd, per enumerare le classi laterali di un sottogruppo quando si ha un gruppo presentato per generatori e relazioni.

Capitolo 1

Richiami di teoria dei gruppi

Definizione 1.0.1. Sia I un insieme. Una operazione binaria in I è una applicazione $\circ : I \times I \to I$. Indicheremo $\circ(a, b) = a \circ b$.

Notiamo che il fatto che l'applicazione mandi coppie di elementi di I in elementi di I permette l'iterazione di questa operazione. Ad esempio dati tre elementi a, b, c è definito l'elemento $a \circ (b \circ c)$, cosí come l'elemento $(a \circ b) \circ c$. In generale questi elementi sono diversi.

Osservazione 1. Si può definire la nozione di elemento neutro a sinistra e a destra. $e_S \in I$ è un elemento neutro a sinistra se $e_S \circ a = a$ per ogni a, analogamente e_D è un elemento neutro a destra se $a \circ e_D = a$ per ogni a. Ponendo $a = e_D$ nella prima troviamo che se esistono elementi neutri destri e sinistri questi sono necessariamente uguali e unici. Assumeremo che questo accada e chiameremo l'elemento neutro (a destra e sinistra) e.

Osservazione 2. Avendo un elemento neutro e, si può definire la nozione di elemento inverso a sinistra e a destra. $\hat{a}_S \in I$ è un elemento inverso a sinistra di a se $\hat{a}_S \circ a = e$, analogamente $\hat{a}_D$ è un elemento inverso a destra se $a \circ \hat{a}_D = e$. Se l'operazione è associativa, cioè $(a \circ b) \circ c = a \circ (b \circ c)$, si vede, calcolando $\hat{a} \circ a \circ \hat{a}_D$ nei due modi possibili, che inverso a sinistra e a destra, se esistono, sono uguali. Osserviamo anche che in questo caso $(a^{-1})^{-1} = a$.

Fatte queste considerazioni possiamo definire la struttura di gruppo.

Definizione 1.0.2. Un gruppo è una coppia $(G, \circ)$, dove G è un insieme e $\circ$? una legge di composizione binaria interna con le proprietà:

1. Per ogni $a, b, c \in G$ si ha $(a \circ b) \circ c = a \circ (b \circ c)$ (proprietà associativa)
2. Esiste un elemento $e \in G$, detto neutro, tale che per ogni $a \in G$ si ha $a \circ e = e \circ a = a$.
3. Per ogni elemento $a \in G$ esiste un elemento $b \in G$ tale che $a \circ b = b \circ a = e$. Si dice che b è l'inverso di a e si indica a^{-1}.

Osservazione 3. L'inverso di un elemento scritto come prodotto di altri elementi, è il prodotto degli inversi presi con l'ordine invertito:

$$(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1},$$

come si verifica facilmente calcolando il prodotto di $(a_1 \cdots a_n)$ con $a_n^{-1} \cdots a_1^{-1}$ e usando l'associatività dell'operazione.

Se $\circ$ è una operazione che definisce una struttura di gruppo sull'insieme G, possiamo definire una nuova operazione $\hat{\circ}$ mediante

$$a \hat{\circ} b := b \circ a.$$

Si può verificare che anche questa operazione definisce una struttura di gruppo. Il gruppo $(G, \hat{\circ})$ cosí ottenuto si dice il gruppo opposto a $(G, \circ)$.

Definizione 1.0.3. Un gruppo abeliano è un gruppo $(G, \circ)$ la cui composizione interna è commutativa, cioè $a \circ b = b \circ a$ qualunque siano a e b.

Definizione 1.0.4. Un gruppo $(G, \circ)$ si dice finito se l'insieme G è un insieme finito. In tal caso il numero dei suoi elementi si indica con $|G|$ e si dice l'ordine del gruppo. Se l'insieme G non è finito si dice che il gruppo è infinito.

Notazione. Nel seguito ometteremo spesso di indicare l'operazione $\circ$, limitandoci a indicare l'insieme G. Inoltre spesso ometteremo di indicare l'operazione anche nelle espressioni di elementi del gruppo, che saranno semplicemente giustapposti. Quindi ad esempio scriveremo ab per indicare $a \circ b$.

Dato un elemento $a \in G$ di un gruppo, si possono considerare le sue potenze a^n, per $n \geq 0$, definite induttivamente come segue:

$$a^0 = e, \text{ e } a^n := a(a^{n-1}).$$

Osserviamo che la notazione a^{-1} è compatibile, nel senso che $e = a^0 = a(a^{-1})$. Pertanto in un gruppo possiamo definire a^n per ogni $n \in \mathbb{Z}$, e si ha

1. $a^m a^l = a^{m+l}$
2. $(a^m)^l = a^{ml}$.

Definizione 1.0.5. Dato un gruppo G, si dice che un elemento $a \in G$ ha ordine finito se esiste un $n \in \mathbb{N}, n \neq 0$ tale che $a^n = e$. In tal caso l'ordine di a è definito come il piú piccolo intero positivo per cui questo succede: Quindi a ha ordine n se $a^n = e$, ma $a^l \neq e$ per ogni $0 < l < n$.

Osservazione 4. In un gruppo finito ogni elemento ha ordine finito. Infatti $a \mapsto a^n$ definisce una applicazione $\mathbb{N} \to G$. Avendo $\mathbb{N}$ cardinalità infinita, segue che l'applicazione non può essere iniettiva, quindi esistono $m, n \in \mathbb{N}$ distinti tali che $a^n = a^m$. Supponiamo per esempio $n > m$. Moltiplicando per a^{-m} si ha $a^{n-m} = e$, cioè a ha ordine finito minore o uguale a $n - m$.

Definizione 1.0.6. Un gruppo G si dice ciclico se esiste un elemento a, detto generatore, tale che ogni elemento del gruppo si scrive come potenza di a.

Osserviamo che se a ha ordine n, allora $a^{-1} = a^{n-1}$, e che anche a^{-1} ha ordine n. Infatti da $a^n = e$ segue, calcolando l'inverso $(a^n)^{-1} = e^{-1} = e$, ma $(a^n)^{-1} = a^{-n} = (a^{-1})^n$.

Definizione 1.0.7. Si dice che due elementi $a, b \in G$ sono coniugati se esiste $c \in G$ tale che $b = cac^{-1}$.

Questo definisce una relazione d'equivalenza: Infatti

1. (PROPRIETA' RIFLESSIVA) un elemento è sempre coniugato a sé stesso: $a = eae^{-1}$.
2. (PROPRIETA' SIMMETRICA) Se $b = cac^{-1}$ allora, moltiplicando a sinistra per c^{-1} e a destra per c, si ha $a = c^{-1}bc$.
3. (PROPRIETA' TRANSITIVA) se $b = cac^{-1}$, e $g = dbd^{-1}$, allora si ha $g = dcac^{-1}d^{-1} = dca(dc)^{-1}$.

Si ha pertanto che l'insieme G è suddiviso in classi disgiunte di elementi: due elementi sono coniugati se e solo se appartengono alla stessa classe. Queste classi si dicono classi di coniugio.

Osservazione 5. L'elemento neutro è coniugato solo con se stesso.

Osservazione 6. In un gruppo abeliano gli elementi sono coniugati solo con se stessi.

Definizione 1.0.8. Si dice che due elementi $a, b \in G$ commutano se $ab = ba$. Ogni elemento commuta con l'identità e ogni elemento commuta con le sue potenze, positive o negative. Naturalmente in un gruppo abeliano due qualsiasi elementi commutano.

Esempio 1. L'insieme dei numeri interi $\mathbb{Z}$ con l'operazione di addizione è un gruppo abeliano. L'elemento neutro è $0 \in \mathbb{Z}$, dato $a \in \mathbb{Z}$ il suo inverso è $-a$. Analogamente sono gruppi abeliani l'insieme dei numeri razionali, (rispetto alla somma), l'insieme dei numeri reali, sempre rispetto alla somma, e dei numeri complessi.

Esempio 2. L'insieme dei numeri razionali non nulli è un gruppo abeliano rispetto all'operazione di prodotto. Analogamente sono gruppi abeliani rispetto all'operazione di prodotto l'insieme dei numeri reali non nulli e l'insieme dei numeri complessi non nulli.

Esempio 3. Dato un intero positivo N l'insieme $\mathbb{Z}/N\mathbb{Z}$ delle classi resto modulo N è un gruppo abeliano.

Esempio 4. L'insieme delle matrici quadrate invertibili, a coefficienti interi, o razionali, o reali o complessi, è un gruppo.

Esempio 5. Dato un insieme I l'insieme $\mathrm{Aut}(I)$ delle applicazioni biunivoche di I in sé è un gruppo rispetto alla operazione di composizione di applicazioni. Se $I = \{1, \cdots, n\}$ il gruppo $\mathrm{Aut}(I)$ non è altro che il gruppo simmetrico S_n delle permutazioni su n elementi.

Definizione 1.0.9. Siano G_1, G_2 due gruppi. Un omomorfismo di gruppi è una applicazione $\phi : G_1, G_2$ con la proprietà

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2), \text{ per ogni } g_1, g_2 \text{ in } G.$$

Osservazione 7. Se ϕ è un omomorfismo di gruppi, ponendo $g_1 = e$ si trova $\phi(g_2) = \phi(eg_2) = \phi(e)\phi(g_2)$ per ogni g_2, il che assicura che $\phi(e) = e$. Ponendo $g_1 = g_2^{-1}$ si trova che $\phi(g^{-1}) = (\phi(g))^{-1}$.

Osservazione 8. L'applicazione identica Id : $G \to G$, definita $Id(g) = g$ per ogni g, è banalmente un omomorfismo di gruppi. Se $\phi : G_1 \to G_2$ e $\psi : G_2 \to G_3$ sono due omomorfismi di gruppi, allora la loro composizione $\psi \circ \phi : G_1 \to G_3$ è un omomorfismo.

Definizione 1.0.10. Se un omomorfismo di gruppi è biunivoco come applicazione di inisemi si verifica che l'applicazione inversa è ancora un omomorfismo. Si dice in tal caso che si ha un isomorfismo di gruppi, e i due gruppi si dicono isomorfi.

Esempio 6. Se un gruppo G è ciclico infinito con generatore a, l'applicazione $\mathbb{Z} \to G$ definita $n \mapsto a^n$ è un isomorfismo di gruppi. Se il gruppo G è ciclico con generatore a di ordine N si verifica che l'applicazione $\mathbb{Z}/N\mathbb{Z} \to G$ che manda $n \mapsto a^n$ è ben definita ed è un isomorfismo di gruppi. notiamo che una scelta diversa del generatore definisce isomorfismi diversi. Tutti i gruppi ciclici di ordine N fissato sono comunque isomorfi, e indicheremo con C_N un tale gruppo.

Osservazione 9. Semplici considerazioni di primalità mostrano che se G è ciclico di ordine N con generatore a, un altro elemento, necessariamente della forma a^q è ancora un generatore se e solo se q e N sono primi tra loro.

Definizione 1.0.11. Un isomorfismo di gruppi $G \to G$ si dice un automorfismo di G.

Definizione 1.0.12. Preso $g \in G$, l'applicazione $\gamma_g : G \to G$ definita da $\gamma_g(a) = gag^{-1}$ si dice coniugio per g, e si verifica essere un automorfismo di gruppi.

Un automorfismo della forma γ_g per qualche g si dice interno. Ovviamente in un gruppo abeliano gli automorfismi interni sono uguali all'dentità.

Osservazione 10. l'insieme Aut(G) degli automorfismi di un gruppo è a sua volta un gruppo rispetto alla composizione. L'elemento neutro è l'applicazione identica.

Capitolo 2

Sottogruppi e sottogruppi normali

In questo capitolo G indicherà sempre un gruppo.

Definizione 2.0.13. Un sottoinsieme $H \subseteq G$ si dice un sottogruppo se per ogni coppia di elementi $a, b \in H$ si ha che $ab \in H$ e $a^{-1} \in H$. Si scrive in questo caso $H < G$.

Osservazione 11. Un gruppo possiede sempre due sottogruppi detti banali (distinti a meno che il gruppo non contenga un solo elemento): $H = \{e\}$, e $H = G$.

Se H è un sottogruppo di G, l'insieme H con l'operazione ereditata da G è a sua volta un gruppo. Osserviamo che se K è un sottogruppo di H che è un sottogruppo di G allora K è un sottogruppo di G. Osserviamo anche che l'applicazione di inclusione $i : H \to G$ è un omomorfismo di gruppi. Notiamo che banalmente un sottogruppo di un gruppo finito è ancora finito.

Esempio 7. $\mathbb{Z}$ è un sottogruppo di $\mathbb{Q}$, che è un sottogruppo di $\mathbb{R}$.

Esempio 8. Dato $a \in G$, l'insieme $\{a^n\}_{n\in\mathbb{Z}}$ delle potenze di a è un sottogruppo detto il sottogruppo generato da a. E' chiaramente un gruppo ciclico.

Proposizione 2.0.1. *Un sottogruppo di un gruppo ciclico è ciclico.*

Dimostrazione. Supponiamo a sia un generatore di G, e $H < G$. Se $H = \{e\}$ non c'è niente da mostrare quindi supponiamo $H \neq \{e\}$. Osserviamo che in H esistono elementi che si possono scrivere come potenze positive di a, perché se $a^k \in H$ allora $(a^k)^{-1} = a^{-k} \in H$. Ogni elemento di H è una potenza di a. Prendiamo allora l'elemento

a^k di H che si può scrivere come potenza di a con esponente positivo minimo. Mostriamo che a^k genera a, cioè che ogni altro elemento di H è una potenza di a^k. Se esiste un elemento a^l che non è una potenza di a^k significa che l non è un multiplo di k e poiché $l > k$ per definizione di k, si può scrivere $l = mk + r$, con r, k interi positivi e $r < k$. Ma allora, per le proprietà delle potenze in un gruppo,

$$a^l = (a^k)^m a^r, \text{ cioè } a^r = a^l((a^k)^m)^{-1}.$$

Quindi $a^r \in H$ ma questo è assurdo perché $r < k$ mentre abbiamo scelto k come il minimo esponente.

Osservazione 12. Si verifica immediatamente che se $H_1, \cdots H_r$ sono sottogruppi allora la loro intersezione $H_1 \cap \cdots \cap H_r$ è un sottogruppo. La stessa cosa vale anche per una famiglia infinita di sottogruppi. Notiamo invece che la proprietà analoga non vale invece per l'unione di sottogruppi. In generale l'unione di sottogruppi non è un sottogruppo. Questo motiva la nozione introdotta piú avanti di sottogruppo generato da un insieme di elementi o da un insieme di sottogruppi.

Se H è un sottogruppo di G si possono definire due relazioni di equivalenza su G:

1. $a \overset{S}{\sim} b$ se esiste $h \in H$ tale che $a = hb$.
2. $a \overset{D}{\sim} b$ se esiste $h \in H$ tale che $a = bh$.

Verifichiamo che la prima è una relazione di equivalenza, la verifica per la seconda è analoga:

1. (PROPRIETA' RIFLESSIVA) $a \overset{S}{\sim} a$ perché $a = ea$, ed $e \in H$.
2. (PROPRIETA' SIMMETRICA)

   Se $a \overset{S}{\sim} b$ allora $a = hb$ per qualche $h \in H$. Ma allora, moltiplicando a sinistra per h^{-1}, si ha $b = h^{-1}a$ e, poiché $h^{-1} \in H$, si ha $b \overset{S}{\sim} a$.
3. (PROPRIETA' TRANSITIVA) se $a \overset{S}{\sim} b$ allora $a = hb$ per qualche $h \in H$. Se $b \overset{S}{\sim} c$ allora $b = kc$ per qualche $k \in H$. Sostituendo si trova $a = (hk)c$, e poiché da $h, k \in H$ segue $hk \in H$, si vede che $a \overset{S}{\sim} c$.

Si vede quindi che ognuna di queste relazioni ripartisce l'insieme G in classi di equivalenza, disgiunte, dette rispettivamente *laterali sinistri* e *laterali destri*. Il laterale sinistro che contiene l'elemento $g \in G$ si indica Hg, quello destro gH. Osserviamo che g non è univocamente identificato dal laterale, è soltanto un rappresentante della classe di equivalenza. Osserviamo che il laterale destro e sinistro dell'elemento neutro coincidono e non sono altro che il sottogruppo H.

Osservazione 13. L'applicazione $aH \mapsto Ha^{-1}$ definisce una biiezione tra l'insieme dei laterali destri e sinistri di un gruppo. E' ben definita nel senso che non dipende dai rappresentanti stessi: infatti se $aH = a'H$ significa che $a' = ah$ per qualche $h \in H$. Ma a $a'H$ associamo $H(a')^{-1} = Hh^{-1}a^{-1} = Ha^{-1}$. Questo spiega la forma, a prima vista strana, della applicazione. Quindi la cardinalità dei due insiemi di laterali è la stessa. Nel caso di gruppi finiti questa osservazione si può raffinare e porta all'importante teorema seguente.

Teorema 2.0.2. (Teorema di Lagrange) *Se G è un gruppo finito e H è un suo sottogruppo, allora tutti i laterali, destri e sinistri, hanno cardinalità $|H|$, l'ordine di H divide l'ordine di G, e il numero dei laterali, sinistri o destri, è uguale a $|G|/|H|$.*

Dimostrazione. Mostriamo che ogni laterale contiene esattamente $|H|$ elementi. Consideriamo i laterali sinistri, la verifica per i laterali destri essendo del tutto analoga: consideriamo un laterale sinistro Hg. L'applicazione di insiemi (non è un omomorfismo di gruppi) $D_g : H \to G$ definita $D_g(h) = hg$ ha come immagine esattamente Hg. Basta quindi mostrare che è iniettiva per concludere $|H| = |Hg|$. Se si ha $D_g(h_1) = D_g(h_2)$ vuol dire che $h_1 g = h_2 g$. Moltiplicando a sinistra per g^{-1} si trova che $h_1 = h_2$. Gli altri enunciati sono adesso immediati: scegliamo in ogni laterale un elemento: abbiamo cosı $g_1, \cdots g_r$ e $G = Hg_1 \coprod \cdots Hg_r$, quindi $|G| = \sum_{i=1}^{r} |Hg_i|$, ma per quanto abbiamo appena mostrato, $|Hg_i| = |H|$ per ogni i, quindi $|G| = r|H|$.

Definizione 2.0.14. L'intero $|G|/|H|$ si dice l'indice di H in G.

Considerando il sottogruppo generato da un elemento si trova:

Corollario 2.0.3. *In un gruppo finito G ogni elemento ha ordine che divide l'ordine di G.*

Corollario 2.0.4. *Un gruppo finito G tale che $|G|$ è primo contiene solo i sottogruppi banali ed è ciclico.*

La seconda affermazione segue dal fatto che il sottogruppo generato da un qualsiasi elemento $\neq e$ non essendo banale deve coincidere con tutto il gruppo.

Definizione 2.0.15. Dato un insieme di elementi, che per semplicità supponiamo finito, $g_1, \cdots, g_n \in G$, consideriamo l'intersezione di tutti i sottogruppi di G che li contengono. Per quanto detto prima questa intersezione è un sottogruppo che contiene $g_1, \cdots, g_n$ ed è il piú piccolo sottogruppo con questa proprietà. Lo si indica con $< g_1, \cdots, g_n >$ e si chiama il sottogruppo generato da $g_1, \cdots, g_n$. Piú generalmente se $H_1, \cdots H_n$ sono dei sottogruppi di G, si può considerare l'intersezione di tutti i sottogruppi di G che contengono $H_1 \cup \cdots \cup H_n$. Abbiamo un sottogruppo $< H_1, \cdots H_n >$ detto il sottogruppo generato da $H_1, \cdots H_n$.

Faremo in seguito alcune considerazioni sulla forma degli elementi di $< g_1, \cdots, g_n >$.
La seguente definizione è estremamente importante per quanto segue

Definizione 2.0.16. Un gruppo G si dice finitamente generato se esiste un sottoinsieme finito $\{g_1, \cdots, g_n\} \subseteq G$ tale che $G =< g_1, \cdots, g_n >$.

Osserviamo che un gruppo finito è banalmente finitamente generato: basta prendere tutti i suoi elementi come insieme di generatori. Il gruppo $\mathbb{Z}$ è finitamente generato, in quanto 1 è un generatore. Invece il gruppo $\mathbb{Q}$ non è finitamente generato, né tantomeno lo è $\mathbb{R}$. Un esempio non immediato di gruppo finitamente generato è il gruppo $GL(n, \mathbb{Z})$ delle matrici invertibili di ordine un intero n a coefficienti interi.

Dato un omomorfismo $\phi : G \to H$ di gruppi questo individua due sottogruppi, uno di G_2 e uno di G_1

Definizione 2.0.17. Definiamo $\text{Im}\phi = \{h \in H : \text{ esiste } g \in G \text{ con } \phi(g) = h\}$.

Si vede che $\text{Im}\phi$ è un sottogruppo di H che si dice l'immagine di ϕ.

Definizione 2.0.18. Definiamo $\text{Ker}\phi = \{g \in G : \text{ con } \phi(g) = e\}$

Anche in questo caso si vede che Kerϕ è un sottogruppo di G che si dice il nucleo di ϕ.

Il nucleo di un omomorfismo è un sottogruppo di natura speciale. Supponiamo infatti che $g \in \text{Ker}\phi$, e sia $\gamma \in G$ una altro elemento. Consideriamo il coniugato di g mediante γ, ovvero l'elemento $g' = \gamma g \gamma^{-1}$ e calcoliamo

$$\phi(g') = \phi(\gamma g \gamma^{-1}) = \phi(\gamma)\phi(g)\phi(\gamma^{-1}) = \phi(\gamma)e\phi(\gamma^{-1}) = e.$$

Abbiamo quindi che anche $g' \in \text{Ker}\phi$. In altre parole, il sottogruppo Kerϕ, se contiene un elemento, contiene anche tutti i suoi coniugati. Sottogruppi con questa proprietà sono estremamente importanti e si dicono normali.

Definizione 2.0.19. Un sottogruppo $H < G$ si dice normale, e si scrive $H \triangleleft G$, se da $h \in H$ segue $ghg^{-1} \in H$ per ogni $g \in G$.

Osservazione 14.

1. I due sottogruppi banali sono normali.
2. L'intersezione di sottogruppi normali è un sottogruppo normale.
3. Un sottogruppo di un gruppo abeliano è necessariamente normale.

Quanto discusso sopra dimostra dunque

Teorema 2.0.5. *Il nucleo di un omomorfismo di gruppi è un sottogruppo normale.*

Dato un elemento $g \in G$ e un sottogruppo $H < G$ si indica gHg^{-1} il sottoinsieme degli elementi della forma ghg^{-1} al variare di $h \in H$. Si verifica senza difficoltà che H è ancora un sottogruppo, che si dice il sottogruppo coniugato di H mediante g. La definizione di sottogruppo normale si può anche enunciare dicendo: Un sottogruppo è normale se coincide con tutti i suoi coniugati.

La proprietà piú importate dei sottogruppi normali è che laterali destri e sinistri coincidono e si può definire una struttura di gruppo sull'insieme di questi laterali:

Teorema 2.0.6. *Sia G un gruppo e H un suo sottogruppo normale.*

1. *Per ogni elemento $g \in G$, il laterale destro e sinistro coincidono.*

2. *presi due laterali g_1H e g_2H, se si definisce l'operazione*

$$(g_1H)(g_2H) := g_1g_2H$$

definisce una struttura di gruppo sull'insieme dei laterali .

Dimostrazione. 1. Sia gh un elemento del laterale destro gH. Poiché H è normale, si ha che $ghg^{-1} =: h' \in H$. Ma allora $gh = h'g \in Hg$. Quindi abbiamo mostrato che $gH \subseteq Hg$. Lo stesso ragionamento mostra l'inclusione opposta.

2. Ci limitiamo a mostrare che l'operazione è ben definita, non dipende cioè dalla scelta di g_1 e g_2. Prendiamo $g_1h_1 \in g_1H$ e $g_2h_2 \in g_2H$. Allora, per la normalità di H si ha che esiste $h_1' \in H$ tale che $h_1g_2 = g_2h_1'$, quindi $g_1h_1g_2h_2 = g_1g_2h_1'h_2 \in g_1g_2H$. Questo mostra che la definizione è ben posta.

Definizione 2.0.20. Sia G un gruppo e H un suo sottogruppo normale. L'insieme dei suoi laterali dotato dell'operazione sopra definita si dice gruppo quoziente e si indica con G/H.

Esempio 9. Consideriamo il gruppo abeliano $\mathbb{Z}$ dei numeri interi. E' ciclico, generato da 1 (o anche da -1). Quindi ogni suo sottogruppo è ciclico per quanto abbiamo già dimostrato e sarà generato da un qualche N. In altre parole i sottogruppi di $\mathbb{Z}$ sono dati da tutti i multipli $N\mathbb{Z}$ di un numero dato. Questi sottogruppi sono necessariamente normali in quanto il gruppo è abeliano. Il gruppo quoziente di $\mathbb{Z}$ per $n\mathbb{Z}$ è il gruppo ciclico con N elementi delle classi di resto modulo N.

Si ha l'importante

Teorema 2.0.7. Teorema di omomorfismo. *Dato un omomorfismo $\phi : G_1 \to G_2$, si ha un omomorfismo di gruppi*

$$G/\mathrm{Ker}\phi \simeq \mathrm{Im}\phi.$$

In particolare, se ϕ è suriettivo, si ha $G_2 \simeq G/\mathrm{Ker}\phi$. Viceversa, se $H \triangleleft G$, l'applicazione $G \to G/H$ che manda g nel suo laterale gH è un omomorfismo suriettivo con nucleo esattamente H. In particolare si vede che ogni sottogruppo normale è il nucleo di un omomorfismo.

Un sottogruppo normale interessante è il cosiddetto centro.

Definizione 2.0.21. Dato un gruppo G si definisce

$$Z(G) = \{g \in G \text{ tali che } gh = hg \text{ per ogni } h \in G\}.$$

che si dice il centro del gruppo.

Il centro è un sottogruppo normale, perché se $g \in G$ e $z \in Z(G)$ allora $gz = zg$, quindi $gzg^{-1} = z \in Z(G)$. E' anche evidentemente un gruppo abeliano. Un gruppo è abeliano se coincide col suo centro.

Capitolo 3

Il gruppo libero su un insieme

Sia G un gruppo finitamente generato. Sia $X \subseteq G$ un suo sottoinsieme. Abbiamo definito il sottogruppo $< X >$ generato da questo insieme come il piú piccolo sottogruppo che lo contiene. Chiaramente ogni elemento della forma $x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}$ (una "parola" in X), con $x_1 x_2 \cdots x_r \in X$ e $a_1 a_2 \cdots a_r \in \mathbb{Z}$ deve appartenere a $< X >$. Viceversa l'insieme degli elementi che ammettono una tale scrittura è chiaramente un sottogruppo: l'elemento neutro ad esempio si scrive x^0 per un qualsiasi elemento $x \in X$, se ho due elementi $x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}$ e $\hat{x_1}^{a_1} \hat{x_2}^{a_2} \cdots \hat{x_s}^{a_s}$ anche il loro prodotto $x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r} \hat{x_1}^{a_1} \hat{x_2}^{a_2} \cdots \hat{x_s}^{a_s}$ ha la stessa forma, infine $(x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r})^{-1} = x_r{}^{-a_r} \hat{x_{r-1}}{}^{-a_{r-1}} \cdots \hat{x_1}{}^{-a_1}$.

La scrittura $x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}$ è però non unica: ad esempio, banalmente, possiamo inserire in qualsiasi posto l'espressione x^0 per un qualche x, oppure una espressione $x^n x^{-n}$, oppure, se è presente un simbolo x^a, possiamo sostituirlo con qualunque sequenza $x^{a-b} x^b$. A parte questi casi banali, però la non unicità può dipendere dalla struttura del gruppo. Ad esempio in un gruppo ciclico di ordine N, ogni espressione x^N, con $x \neq e$, può essere "semplificata", visto che ogni elemento ha ordine che divide N. Tale situazione è specifica per il gruppo che consideriamo, e non accade in altri gruppi, ad esempio in $\mathbb{Z}$. Per fare un altro esempio, se prendiamo il gruppo delle permutazioni dell'insieme $\{1, \cdots n\}$, e chiamiamo σ_i la permutazione che scambia i con $i+1$ lasciando gli altri elementi invariati, è noto che $\{\sigma_1, \cdots, \sigma_{n-1}\}$ è un insieme di generatori del gruppo. Ogni apparizione di σ_i^2 in una parola può essere semplificata. Analogamente a ogni espressione $\sigma_i \sigma_j$, con $|j-i| > 1$, si può sostituire $\sigma_j \sigma_i$, in quanto si vede che tali elementi commutano.

Queste semplificazioni dipendono quindi non dalle relazioni puramente di gruppo, ma dalle "regole di calcolo" specifiche del gruppo che si sta considerando. Vogliamo definire, dato un insieme di simboli X, un gruppo in cui le uniche regole di calcolo siano quelle che derivano dagli assiomi di gruppo. Tale gruppo è il gruppo libero sull'insieme X. La definizione di tale gruppo è piuttosto astratta.

Sia $X = \{x_\alpha\}_{\alpha\in\Lambda}$ un insieme non vuoto finito, oppure infinito. Consideriamo tutte le sequenze finite, che chiameremo parole, di elementi di del tipo $s = x_1x_2x\cdots x_n$ in cui sono ammesse le ripetizioni degli elementi. L' insieme di tutte queste sequenze lo indichiamo con $S = \{s_a\}_a \in I$ Nell' insieme delle sequenze definiamo un'operazione $*$ detta prodotto, scrivendo semplicemente una sequenza dopo l'altra. In questo modo l' insieme di tutte le sequenze ha una legge di composizione interna che risulta associativa: Se $s_1 = x_1x_2\cdots x_n, s_2 = y_1y_2\cdots y_m$ e $s_3 = z_1z_2\cdots z_p$, allora

$$(s_1 * s_2) * s_3 = (x_1x_2\cdots x_ny_1y_2\cdots y_m) * z_1z_2\cdots z_p =$$

$$x_1x_2\cdots x_ny_1y_2\cdots y_mz_1z_2\cdots z_p = x_1x_2\cdots x_n * (y_1y_2\cdots y_mz_1z_2\cdots z_p) = s_1 * (s_2 * s_3).$$

Per costruire il gruppo occorre avere un elemento neutro e l'inverso di ogni elemento. Come elemento neutro si introduce la sequenza vuota, cio? la sequenza senza elementi, che indichiamo con e. Per quanto riguarda l'inverso di una parola, la formula che abbiamo osservato nel primo capitolo ci suggerisce che $(x_1x_2\cdots x_n)^{-1} = x_n^{-1}\cdots x_2^{-1}x_1$. Quindi prima di tutto dobbiamo aggiungere al nostro insieme X l'insieme X' dei simboli x_α^{-1} e considerare le parole in questi nuovi simboli. Quindi ogni parola si scrive $x_1^{\sigma_1}x_2^{\sigma_2}\cdots x_n^{\sigma_n}$ con $\sigma_i = \pm 1$. Però per come abbiamo definito l'operazione $*$, si ha che $x_1x_2\cdots x_nx_n^{-1}\cdots x_2^{-1}x_1^{-1}$ non è la parola vuota. Questo ci forza a definire una relazione di equivalenza che permette di cancellare le parole del tipo xx^{-1}. Introduciamo allora la relazione d'equivalenza generata dalle equivalenze $xx^{-1} \sim e$. in altri termini, due parole si dicono equivalenti se si può passare dall'una all'altra togliendo un certo numero di sottoparole xx^{-1} e aggiungendone altre. Una parola si dice ridotta se non contiene alcuna sequenza xx^{-1}, e si vede facilmente che ogni parola è equivalente a una e una sola parola ridotta. Si vede allora che l'operazione sulle classi di equivalenza è ben definita e soddisfa gli assiomi di gruppo, con elemento neutro dato dalla classe di equivalenza di $e = \{$ parola vuota $\}$, e inversa definita come sopra. L'operazione sulla parole ridotte consiste nel giustapporre due parole ridotte e poi ridurre la parola risultante.

Definizione 3.0.22. Il gruppo appena definito si dice gruppo libero sull'insieme X, e si indica con $F<X>$. Se $X = \{1, \cdots n\}$ il gruppo si indica F_n e si dice il gruppo libero su n generatori.

Quando un simbolo x è ripetuto consecutivamente n volte in una parola lo scriviamo x^n. Se il simbolo è x^{-1} lo scriviamo x^{-n}. Osserviamo che questa notazione è coerente, in quanto x^n è proprio il prodotto nel gruppo libero dell'elemento x con se stesso iterato n volte.

Osservazione 15. Se X contiene un solo elemento x il gruppo libero contiene solo le parole $x \cdots x =: x^n$ e i loro inversi, quindi $F_1 \simeq \mathbb{Z}$.

Osserviamo che in modo analogo dati due gruppi G, H si può costruire quello si chiama il loro prodotto libero $G * H$, i cui elementi sono parole $g_1 h_1 \cdots g_n h_n$ con gli elementi (si intende che si può sempre inserire l'elemento neutro in qualsiasi posto, quindi non è restrittivo considerare che le parole inizino con un elemento di G e terminino con uno di H), con le regole di composizione

$$(g_1 h_1 \cdots g_n h_n) * (g'_1 h'_1 \cdots g'_m h'_m) = g_1 h_1 \cdots g_n h_n g'_1 h'_1 \cdots g'_m h'_m \text{ se } h_n, g'_1 \neq e,$$

e

$$(g_1 h_1 \cdots g_n h_n) * (g'_1 h'_1 \cdots g'_m h'_m) = g_1 h_1 \cdots (g_n g'_1) h'_1 \cdots g'_m h'_m \text{ se } h_n = e,$$

$$(g_1 h_1 \cdots g_n h_n) * (g'_1 h'_1 \cdots g'_m h'_m) = g_1 h_1 \cdots g_n (h_n h'_1) \cdots g'_m h'_m \text{ se } g'_1 = e.$$

Osservazione 16. Notiamo che il gruppo appena definito $G*H$ è molto diverso in generale dal prodotto diretto $G \times H$, i cui elementi sono le coppie $(g, h) \in G \times H$ con l'operazione di prodotto definita da

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

ed elemento neutro (e, e). L'applicazione $G * H \to G \times H$ che manda l'elemento $(g_1 h_1 \cdots g_n h_n)$ nella coppia $(g_1 \cdots g_n, h_1 \cdots h_n)$ risulta essere un omomorfismo suriettivo, ma non certamente iniettivo: ad esempio siano $g \in G \setminus \{e\}$ e $h \in H \setminus \{e\}$. Gli elementi gh e hg (o, piú precisamente data la nostra notazione, $ehge$) hanno la stessa immagine $(g, h) \in G \times H$ senza essere uguali in $G * H$. In altre parole, tutti gli elementi $ghg^{-1}h \in G * H$ appartengono al nucleo dell'omomorfismo appena definito.

Osservazione 17. Dalle definizioni risulta immediatamente che

$$F_n = \mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}.$$

Una delle proprietà piú importanti del gruppo libero è la seguente

Teorema 3.0.8. Proprietà universale del gruppo libero *Sia $F < X >$ il gruppo libero sull' insieme X e sia G un gruppo. Ogni applicazione tra insiemi $f : X \to G$ si estende in modo unico ad un omomorfismo di gruppi $\Phi : F<X> \to G$.*

Dimostrazione. Si definisce $\Phi(x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n}) := f(x_1)^{\sigma_1} f(x_2)^{\sigma_2} \cdots f(x_n)^{\sigma_n}$. poiché $\Phi(xx^{-1}) = f(x)f(x^{-1}) = e$, la definizione è ben posta, e si verifica immediatamente che è un omomorfismo di gruppi.

L'immagine dell'omomorfismo Φ è esattamente il sottogruppo generato dall'insieme $f(X)$. In particolare se $f(X)$ è un insieme di generatori l'immagine è tutto il gruppo G, e perciò per il teorema di omomorfismo si ha $G \simeq F<X>/\mathrm{Ker}\Phi$. Quindi

Corollario 3.0.9. *Ogni gruppo è quoziente di un gruppo libero per un sottogruppo normale. Se un gruppo è finitamente generato e ammette un insieme con n generatori lo si può presentare come quoziente del gruppo libero F_n.*

Piú precisamente la scelta di un insieme di generatori X per G equivale alla scelta di un isomorfismo $G \simeq F<X>/\mathrm{Ker}\Phi$.

Lo stesso principio porta a concludere che se si hanno due gruppi G_1, G_2 con omomorfismi $\phi_1 : G_1 \to G$ e $\phi_2 : G_2 \to G$, allora si definisce $\Phi : G_1 * G_2 \to G$ che ha come immagine il sottogruppo generato da $\mathrm{Im}G_1 \cup \mathrm{Im}G_2$.

Capitolo 4

Relazioni

Preso il gruppo libero $F<X>$ sull'insieme X, supponiamo di avere un certo numero, che per semplicità supponiamo finito, di elementi

$$R_1, \cdots, R_m \in F<X> .$$

Consideriamo l'intersezione R di tutti i sottogruppi normali di $F<X>$ che contengono $R_1, \cdots, R_m$. Per quanto osservato in precedenza, R è un sottogruppo normale. Possiamo allora considerare il gruppo quoziente

$$F<X> /R,$$

e si ha l'omomorfismo suriettivo

$$\phi : F<X> \to F<X> /R.$$

Mediante ϕ gli elementi di R vanno nell'elemento neutro. In altri termini, nel gruppo quoziente, gli elementi di R diventano "regole di semplificazione". Ad esempio, se partiamo da F_2, con generatori $\{a, b\}$, e consideriamo la parola $R_1 = aba^{-1}b^{-1}$, questo vuole dire che nel gruppo quoziente introduciamo la regola di semplificazione $aba^{-1}b^{-1} = e$, per cui certe parole che non erano semplificabili in F_2 adesso lo diventano: non è difficile capire cosa succede in questo caso. Se ho ad esempio una parola, che in generale sarà della forma $a^{n_1}b^{m_2}a^{n_2}....a^{n_k}b^{m_k}$ a una successione ba si può sostituire, in F_2/R, $ba(a^{-1}b^{-1}ab) = ab$, quindi la relazione introdotta permette di scambiare a nostro piacimento a e b. Pertanto ogni parola in $F < X > /R$ si può porre nella forma $a^n b^m$, con

$m, n \in \mathbb{Z}$. A questo punto è quasi immediato verificare che l'applicazione $F_2 \to \mathbb{Z}^{\oplus 2}$, ottenuta mandando $a^{n_1}b^{m_2}a^{n_2}....a^{n_k}b^{m_k}$ in $(\sum n_i, \sum m_i)$ passa al quoziente F_2/R, visto che $aba^{-1}b^{-1} \to (0,0)$, e definisce un isomorfismo $F_2/R \simeq \mathbb{Z}^{\oplus 2}$. In questo caso particolare abbiamo descritto cioè quella che si chiama una presentazione di $\mathbb{Z}^{\oplus 2}$ con generatori e relazioni.

Definizione 4.0.23. Un gruppo G si dice presentato con generatori e relazioni quando è dato un insieme $X = \{g_\alpha\}$ di suoi generatori, e un insieme $\mathcal{R}$ di parole in $F<X>$ tali che l'applicazione naturale

$$F<X> \to G,$$

che manda gli elementi di X negli elementi stessi in G, passa al quoziente (ovvero manda gli elementi di $\mathcal{R}$ nell'elemento neutro di G) a un isomorfismo

$$G = F<X>/R,$$

dove R è il piú piccolo sottogruppo normale che contiene $\mathcal{R}$.

La coppia $(X, \mathcal{R})$, con X considerato semplicemente come insieme di simboli, si dice una presentazione del gruppo. Gli esempi che vedremo saranno di gruppi finitamente generati e insiemi finiti di relazioni. Quindi indicheremo un gruppo presentato come

$$(x_1, \cdots, x_N, R_1(x_1, \cdots, x_N), \cdots, R_M(x_1, \cdots, x_N))$$

sottintendendo che le relazioni contengono anche gli inversi degli x_i. Spesso le relazioni, invece che come parole, vengono indicate come uguaglianze. Ad esempio la relazione vista prima $aba^{-1}b^{-1}$ può anche essere indicata $ab = ba$, che si ottiene scrivendo $aba^{-1}b^{-1} = e$ e poi moltiplicando a destra per ba.

Osservazione 18. Se si hanno due presentazioni $(X, \mathcal{R})$ e $(X, \mathcal{R}')$ con lo stesso insieme di generatori, e con la proprietà che $\mathcal{R}' \subseteq \mathcal{R}$, segue dalla costruzione che $F<X>/R$ è un quoziente di $F<X>/R'$.

Esempio 10. Se X consiste di un solo elemento il gruppo è necessariamente ciclico. In tal caso la presentazione $(\{x\}, x^n)$ definisce il gruppo ciclico di ordine n.

Esempio 11. Supponiamo di avere due gruppi G_1, G_2 con rispettive presentazioni $(X, \mathcal{R})$ e $(Y, \mathcal{S})$. Il loro prodotto libero $G_1 * G_2$ ha allora presentazione $(X \coprod Y, \mathcal{R} \coprod \mathcal{S})$. Una presentazione per il prodotto diretto $G_1 \times G_2$ si ottiene invece prendendo come insieme di generatori $X \coprod Y$ (dove la notazione di unione disgiunta serve a enfatizzare il fatto che prendiamo i generatori come simboli distinti), e come relazioni tutte quelle di $\mathcal{R} \coprod \mathcal{S}$ e in piú ogni relazione $xyx^{-1}y^{-1}$ per $x \in X$ e $y \in Y$. Stabiliamo cioè che i generatori di G_1 e quelli di G_2 commutano tra loro. Grazie a queste ultime relazioni ogni parola si può portare nella forma $W_1(\{x_\alpha\})W_2(\{y_\beta\})$, e definire cosí una applicazione in $G_1 \times G_2$ mandando tale parola in $(W_1(\{x_\alpha\}), W_2(\{y_\beta\}))$.

Dato un gruppo presentato, un suo elemento può essere scritto in molti modi diversi, e analogamente un gruppo può avere molte diverse presentazioni. Ad esempio non è assolutamente evidente dalla presentazione se il gruppo definito è finito o no, e neppure addirittura se è il gruppo banale o meno. Nel 1911 Max Dehn ha formulato i tre seguenti problemi di decisione che si sono rivelati molto importanti nei loro sviluppi:

Sia data una presentazione $(X, \mathcal{R})$ di un gruppo G

1. **Problema della Parola** Date due parole W_1 e W_2 nei simboli X (e loro inversi), decidere se queste rappresentano lo stesso elemento in G. Equivalentemente, data una parola W, decidere se questa appartiene al piú piccolo sottogruppo normale di $F < X >$ che contiene $\mathcal{R}$.

2. **Problema del coniugio** Date due parole W_1 e W_2 nei simboli X (e loro inversi), decidere se queste rappresentano elementi coniugati in G

3. **Problema dell'isomorfismo** Data un'altra coppia $(X', \mathcal{R}')$, decidere se questa definisce un gruppo isomorfo a G.

Questi tre problemi sono in generale indecidibili, e l'interesse maggiore sta nella possibilità di risolverli in casi particolari. Altresí indecidibile è il problema se una data presentazione definisce un gruppo finito o meno. Osserviamo che il primo problema in particolare ammonta alla possibilità di trovare un algoritmo per portare una qualsiasi parola in "forma normale" unica.

Esempio 12. Consideriamo un gruppo con due generatori a, b con le relazioni $a^2, b^n, abab$. Partendo da una qualsiasi parola, innanzitutto la si può ridurre, usando le prime due relazioni, in modo che appaiano solo potenze di a con esponente al piú 1 e potenze di b con esponente al piú $n-1$. Poi, se abbiamo una sequenza ba, la terza relazione dà , moltiplicata a sinistra per a e tenendo conto della prima relazione:

$$bab = a, \text{ quindi } ba = ab^{-1} = ab^{n-1},$$

l'ultima uguaglianza tenendo conto della terza relazione. Quindi ogni parola si arriva a scrivere in modo unico come $e, b, \cdots, b^{n-1}, a, ab, \cdots, ab^{n-1}$. Il gruppo ha quindi $2n$ elementi. Tale gruppo è noto come gruppo diedrale. È il gruppo di simmetria di un poligono regolare con n lati. L'elemento a di ordine 2 è una simmetria, l'elemento b una rotazione di un angolo di $2\pi/n$ radianti. Le tre relazioni assumono un significato geometrico evidente.

Esempio 13. Consideriamo $\sigma_1, \cdots, \sigma_n$ dei generatori, con le relazioni come quelle che abbiamo trovato nel gruppo simmetrico, cioè

$$\sigma_i^2, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ per } |i-j| > 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}.$$

La terza relazione, detta relazione di treccia, si può scrivere anche nella forma $(\sigma_i\sigma_{i+1})^3$. Partendo da queste regole di calcolo possiamo semplificare notevolmente una qualsiasi parola: innanzitutto la prima relazione dice che $\sigma_i = \sigma_i^{-1}$, quindi in particolare in una parola si possono fare trasformazioni fino a che ogni generatore σ_i, se appare, appare con esponente 1. La seconda relazione dice che si può "far scorrere" un qualsiasi generatore a meno che l'indice contiguo differisca di 1, nel qual caso usiamo la terza relazione. Come abbiamo già detto queste relazioni sono soddisfatte dalle trasposizioni nel gruppo simmetrico, per cui si ha sicuramente un omomorfismo suriettivo del gruppo con queste relazioni nel gruppo simmetrico. Si può mostrare in realtà che tale omomorfismo è un isomorfismo, quella data è cioè una presentazione del gruppo simmetrico.

Esempio 14. Se nella presentazione precedente si tolgono le relazioni σ_i^2 si trova un gruppo infinito, che risulta uno dei gruppi piú interessanti in topologia, il gruppo delle trecce su n capi.

Capitolo 5

L'algoritmo di Coxeter-Todd

Concludiamo questo lavoro illustrando, senza fornire le dimostrazioni, che sono piuttosto laboriose, l'algoritmo di Coxeter-Todd, un metodo per enumerare le classi laterali di un gruppo G presentato con generatori e relazioni rispetto all'azione di un sottogruppo H, di cui si fornisce un insieme di generatori. Supponiamo quindi di avere un insieme finito di generatori

$$\{g_1, \cdots, g_n\}.$$

Abbiamo poi un insieme finito di relazioni

$$r_1(\cdots g_i, g_i^{-1}, \cdots), \cdots, r_m(\cdots g_i, g_i^{-1}, \cdots)$$

che danno una presentazione di G. Il sottogruppo H è generato in G da un certo numero di elementi $h_1, \cdots h_k$. Vogliamo enumerare i laterali sinistri (ad esempio) di H e capire l'azione di G su questi laterali.

Costruiamo una "matrice" nel seguente modo: Aggiungiamo all'insieme dei generatori i loro inversi:

$$\mathbb{E} := \{g_1, \cdots, g_n, g_1^{-1}, \cdots, g_n^{-1}\}.$$

Le righe della prima matrice M sono etichettate con numeri interi positivi che rappresentano i laterali, di cui non conosciamo a priori il numero, mentre le colonne hanno come indici gli elementi di $\mathbb{E}$. Assegnamo il numero **1** al laterale H. Dato un laterale "**k**", moltiplicando a destra per un generatore $g \in \mathbb{E}$ si avrà un altro laterale $\mathbf{k}g$ cui sarà stato assegnato un altro intero, diciamo **l**. Allora poniamo $M(\mathbf{k}, g) = \mathbf{l}$. Ogni volta che

viene definito un nuovo laterale si aggiunge una riga e si aggiungono alla sua relativa riga tutte le informazioni che già abbiamo. Scriviamo le relazioni

$$r_1 = g_{1_1} \cdots g_{1_{t_1}}, r_2 = g_{2_1} \cdots g_{2_{t_2}}, \cdots r_m = g_{m_1} \cdots g_{m_{t_m}}, \text{ con } g_{a_{b_c}} \in \mathbb{E},$$

e costruiamo una matrice M_i per ogni relazione, le cui righe sono gli interi positivi corrispondenti ai laterali, e le colonne sono gli elementi g_{i_k} della relazione considerata presi nel loro ordine. Osserviamo che questa notazione introduce una certa ambiguità in quanto uno stesso elemento può apparire piú volte nella stessa relazione. L'elemento di posto $(\mathbf{a}, g_{i_k})$ di M_i è il laterale $\mathbf{a}g_{i_1} \cdots g_{i_k}$. Quindi poiché stiamo considerando delle relazioni abbiamo sicuramente che $M_i(\mathbf{a}, g_{i_{t_i}}) = \mathbf{a}$. Ogni volta che viene definito un nuovo laterale si aggiungono alla sua relativa riga tutte le informazioni che abbiamo su esso. Ogni generatore $h_\alpha = g_{\alpha_1} \cdots g_{\alpha_{t_\alpha}}$ del nostro sottogruppo H ha infine assegnata una riga corrispondente a H, mentre le colonne sono le sottoparole $g_{\alpha_1}, g_{\alpha_1}g_{\alpha_2}$ etc. che, come nel caso delle matrici M_j indichiamo mediante il loro ultimo elemento. In corrispondenza con g_{α_s} poniamo il laterale $S_j(\mathbf{1}, g_{\alpha_s}) = Hg_{\alpha_1} \cdots g_{\alpha_s}$. Poiché $g_{\alpha_1} \cdots g_{\alpha_{t_\alpha}} \in H$ abbiamo $S_j(\mathbf{1}, g_{\alpha_{t_\alpha}}) = \mathbf{1}$.

Ogni volta che si riesce a completare una riga nelle matrici M_i o S_j si ha una informazione del tipo $\mathbf{k}g = \mathbf{l}$ e anche $\mathbf{l}g^{-1} = \mathbf{k}$, sull'azione dell'ultimo elemento della relazione o del sottogruppo su un laterale, che riportiamo nella matrice M: Se i corrispondenti posti $M(\mathbf{k}, g)$ e $M(\mathbf{l}, g^{-1})$ erano vuoti si aggiunge il termine corrispondente nella matrice M. Se invece erano già occupati, ad esempio $M(\mathbf{k}, g) = \mathbf{l}'$, siamo forzati a dedurre che $\mathbf{l} = \mathbf{l}'$ il che permette di eliminare la riga $\max(\mathbf{l}, \mathbf{l}')$, e modificare di conseguenza tutte e matrici sostituendo a $\max(\mathbf{l}, \mathbf{l}')$ il laterale $\min(\mathbf{l}, \mathbf{l}')$. Si può dimostrare che, se il numero dei laterali è finito, questo processo termina con tutte le matrici M, M_i, S_j riempite, il che permette di enumerare i laterali e conoscere l'azione di G come permutazione di questi.

Facciamo un esempio, che prendiamo da [5]. Consideriamo G generato da due elementi g_1, g_2 con le relazioni $r_1 = g_1^2, r_2 = g_2^2, r_3 = (g_1g_2)^3$, e prendiamo H generato da $g_1g_2g_1g_2$. Notiamo che G non è altro che il gruppo simmetrico su tre elementi. Come detto, $\mathbf{1}$ denota il laterale H, quindi poniamo $\mathbf{2} = Hg_1$ e $\mathbf{3} = Hg_2$. Dalle prime due relazioni sappiamo che $\mathbf{2}g_1 = \mathbf{1}$ e $\mathbf{3}g_2 = \mathbf{1}$. Introduciamo anche $\mathbf{4} = Hg_1g_2$. Sicuramente

$\mathbf{4}g_2 = Hg_1 = \mathbf{2}$. Quindi abbiamo la matrice

	g_1	g_2	g_1^{-1}	g_2^{-1}
1	**2**	**3**	**2**	**3**
2	**1**	**4**	**1**	**4**
3	?	**1**	?	**1**
4	?	**2**	?	**2**

Dove temporaneamente mettiamo un ? nel posto Hg_2g_1 e nel posto $Hg_1g_2g_1$ Compiliamo la matrice S: Dobbiamo calcolare

1. $Hg_1 = \mathbf{2}$
2. $Hg_1g_2 = \mathbf{4}$
3. $Hg_1g_2g_1 =$?
4. $Hg_1g_2g_1g_2 = H = \mathbf{1}$ in quanto $g_1g_2g_1g_2 \in H$, e questo determina il termine mancante $Hg_1g_2g_1 = (Hg_1g_2g_1g_2)g_2 = Hg_2 = \mathbf{3}$.

Quindi

	g_1	g_2	g_1	g_2
1	**2**	**4**	**3**	**1**

Le matrici relative alle relazioni g_1^2, g_2^2 non dicono niente di nuovo in quanto ne abbiamo già tenuto conto quindi scriviamo la matrice per la relazione $g_1g_2g_1g_2g_1g_2$ non tenendo conto in un primo tempo di quanto già sappiamo, cioè $Hg_1g_2g_1 = \mathbf{3}$.

	g_1	g_2	g_1	g_2	g_1	g_2
1	**2**	**4**	?	?	**3**	**1**
2	**1**	**3**	?	?	**4**	**2**
3	?	?	4	**2**	1	**3**
4	?	?	**3**	**1**	**2**	**4**

Ad esempio la prima colonna è ricavata come segue: $\mathbf{1} = H$, quindi al posto $(1, g_1)$ mettiamo $Hg_1 = \mathbf{2}$, al posto $(1, g_2)$ mettiamo $Hg_1g_2 = \mathbf{4}$, al posto $(1, g_1)$ mettiamo $Hg_1g_2g_1$ cui non abbiamo ancora dato un nome. Al posto successivo non abbiamo assegnato un numero in quanto ancora non teniamo conto della matrice S. L'ultimo coefficiente è sicuramente **2** in quanto stiamo moltiplicando per una relazione. Ma $Hg_1g_2g_1g_2g_1g_2 = H$ implica $Hg_1g_2g_1g_2g_1 = (Hg_1g_2g_1g_2g_1g_2)g_2 = Hg_2 = \mathbf{3}$.

Se inseriamo l'informazione $Hg_1g_2g_1 = \mathbf{3}$ e $Hg_1g_2g_1g_2 = \mathbf{1}$ la prima riga della matrice per la relazione diventa

	g_1	g_2	g_1	g_2	g_1	g_2
1	**2**	**4**	**3**	**1**	**3**	**1**

Ma dalla quinta colonna di questa riga vediamo $\mathbf{1}g_1 = \mathbf{3}$ quindi dal confronto con la definizione $\mathbf{1}g_1 = \mathbf{2}$ deduciamo $\mathbf{2} = \mathbf{3}$, cioè $Hg_1 = Hg_2$, quindi anche $\mathbf{4} = Hg_1g_2 = Hg_2^2 = H$ cioè $\mathbf{1} = \mathbf{4}$. Concludiamo che ci sono due laterali, $\mathbf{1} = H$ e $\mathbf{2} = Hg_1$, sui quali l'azione di G è descritta dalle prime righe della matrice M.

Bibliografia

[1] M. Artin "Algebra", Bollati-Boringhieri 1997.

[2] H. S. M. Coxeter, W. O. J.; Moser, Generators and Relations for Discrete Groups. Ergebnisse der Mathematik und ihrer Grenzgebiete 14 (4th ed.). Springer-Verlag 1980.

[3] H. S. M. Coxeter, J. A. Todd, "A practical method for enumerating cosets of a finite abstract group". Proceedings of the Edinburgh Mathematical Society. Series II 5: 2634. (1936).

[4] W. Magnus, A. Karras, D. Solitar "Combinatorial group theory," J. Wiley 1966.

[5] A. Seress, "An Introduction to Computational Group Theory". Notices of the American Mathematical Society 1997.