ìM

Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

GIOCHI DI PAROLE E GRUPPI LIBERI

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
LIBERO VERARDI

Presentata da:
SARA GARAFFONI

I Sessione
Anno Accademico 2013/2014

A Francesco,
e alla mia famiglia.

Introduzione

La struttura di gruppo è una delle strutture algebriche più semplici e fondamentali della matematica. Un gruppo si può descrivere in vari modi. Noi abbiamo illustrato la presentazione tramite generatori e relazioni, che consiste sostanzialmente nell'elencare le "regole di calcolo" che valgono nel gruppo considerato, oltre a quelle che derivano dagli assiomi di gruppo. L'idea principale di questa tesi è quella di mostrare come un argomento così tecnico e specifico possa essere reso "elementare" e anche divertente. Siamo infatti partiti dalla costruzione di un gioco, inventando regole da aggiungere di volta in volta. Abbiamo poi tentato di spiegare il medesimo concetto da un punto di vista teorico, tramite la teoria dei gruppi liberi. Si tratta di gruppi che hanno un insieme di generatori soddisfacenti unicamente alle relazioni che sono conseguenza degli 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. Infine si è illustrato il problema della parola formulato da Max Dhen nel 1911, e si è visto come tale problema è risolubile per i gruppi liberi.

Indice

Capitolo 1

Monoidi e gruppi di parole

In questo capitolo cerchiamo, mediante l'uso di parole, alcuni esempi di monoidi e di gruppi, finiti o infiniti.

Ai numeri naturali sono associati vari monoidi, con le operazioni di addizione, moltiplicazione, MCD e mcm. Per costruire altri esempi di monoidi e di gruppi ci si può servire di un qualsiasi oggetto. In particolare, usiamo delle lettere.
Occorre sottolineare che, in questo contesto, il ruolo delle lettere non è quello di variabili su un insieme, ma di *indeterminate*, ossia di oggetti astratti, estranei agli insiemi numerici, manipolati con regole stabilite di volta in volta.

1) Quello che si può fare è mettere le lettere in fila e contarle. Si ottiene così un insieme di parole nell'alfabeto $\{a\}$:

1	a	aa	aaa	$aaaa$	$aaaaa$	$aaaaaa$	...
0	1	2	3	4	5	6	...

Il simbolo 1 rappresenta qui una parola vuota di lettere, e ogni numero in basso esprime la lunghezza della parola di lettere sovrastante. Ora, date due parole, possiamo ottenerne una nuova "sommandole". Chiamiamo *concatenazione* questo procedimento, che indichamo con &:

$$aaa \ \& \ aaaaa = aaaaaaaa$$

Questa operazione è associativa, commutativa ed ha come elemento neutro la parola vuota.

Nota. Si tratta di un modo primitivo di rappresentare il monoide $(\mathbb{N}, +, 0)$, che è libero da regole. I nostri antenati paleolitici rappresentavano i numeri mediante sequenze finite di tacche, assimilabili alle parole formate da una sola lettera, ripetuta quante volte si vuole. Le operazioni su $\mathbb{N}$ sono definibili a partire da questa primitiva rappresentazione.

Ora proviamo ad inventare regole per complicare questa struttura così elementare; per esempio:

2) Fissato un numero n > 0, "mangiare" ogni parola di n lettere, ossia sostituirla con la parola vuota. In simboli, $\underbrace{aaa...a}_{n} = 1$

Usiamo volutamente il termine "mangiare", tratto dal gioco degli scacchi o della dama, per enfatizzare questo approccio informale ai gruppi finitamente presentati.

Fissiamo $n = 5$. Allora avremo il 4 come lunghezza massima, e le parole possibili saranno solo cinque:

$$1 \qquad a \qquad aa \qquad aaa \qquad aaaa.$$

Quando concateniamo le parole, ogni volta che abbiamo 5 lettere in fila le mangiamo, ossia ogni parola di cinque lettere equivale alla parola vota.

Possiamo riassumere in una tabella i 25 risultati possibili:

&	1	a	aa	aaa	aaaa
1	1	a	aa	aaa	$aaaa$
a	a	aa	aaa	$aaaa$	1
aa	aa	aaa	$aaaa$	1	a
aaa	aaa	$aaaa$	1	a	aa
$aaaa$	$aaaa$	1	a	aa	aaa

Nota. Quello che si ottiene per ogni lunghezza massima prefissata $n > 0$ è chiaramente il *gruppo ciclico di ordine* n che contiene esattamente n elementi. Si tratta inoltre di un altro modo di rappresentare il gruppo delle rotazioni del piano di ampiezza $\frac{2\pi k}{n}, 0 \leqslant k \leqslant n-1$ intorno ad un centro O fissato.

3) Fissati m, n > 0, sostituire ad ogni parola di n lettere una parola lunga m. In simboli, $\underbrace{aaa...a}_{n} \longrightarrow \underbrace{aaa...a}_{m}$ (regola monodirezionale).

Se $m = n$ non succede niente. Se $n < m$ otteniamo un monoide commutativo, con 1 come elemento neutro e ∞ come elemento assorbente: infatti, non appena arriviamo ad n lettere, immediatamente la lunghezza "esplode" e diventa infinita. Prendiamo $n = 4$ ed $m = 5$ e riassumiamo nella seguente tabella le 25 possibili concatenazioni.

&	1	a	aa	aaa	∞
1	1	a	aa	aaa	∞
a	a	aa	aaa	∞	∞
aa	aa	aaa	∞	∞	∞
aaa	aaa	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞

Nota. La percezione visiva consente all'uomo di riconoscere modeste quantità di oggetti senza contare. È accertato che possiamo individuare, con un colpo d'occhio, e senza contare, fino a tre oggetti, e dopo ci sia solo una generica moltitudine. Somiglia un po' a quello che succede in questo caso, come si vede dalla tabella.
Il monoide ottenuto, commutativo e con elemento neutro 1, ha ∞ come elemento assorbente.
Per analogia, se definiamo la somma di angoli consecutivi (quindi con lo stesso vertice) come la loro unione, otteniamo l'angolo giro come elemento assorbente in luogo del simbolo ∞. In questo caso abbiamo un monoide commutativo, ma con la potenza del continuo.

Resta il caso di $n > m$. Qui abbiamo un limite massimo alla lunghezza delle parole uguale ad $n - 1$, perchè ogni volta che si arriva ad n, il numero scende ad $m < n$. In questo caso si ottengono monoidi commutativi non regolari, ma talora privi di elemento assorbente.

Poniamo $n = 4$, $m = 3$. Le parole possibili saranno allora:

$$1 \qquad a \qquad aa \qquad aaa$$

In questo caso, come si vede dalla seguente tabella di moltiplicazione, l'elemento assorbente è la parola aaa:

&	1	a	aa	aaa
1	1	a	aa	aaa
a	a	aa	aaa	aaa
aa	aa	aaa	aaa	aaa
aaa	aaa	aaa	aaa	aaa

Se invece $n = 5$ e $m = 3$ otteniamo un monoide privo di elemento assorbente:

&	1	a	aa	aaa	$aaaa$
1	1	a	aa	aaa	$aaaa$
a	a	aa	aaa	$aaaa$	aaa
aa	aa	aaa	$aaaa$	aaa	$aaaa$
aaa	aaa	$aaaa$	aaa	$aaaa$	aaa
$aaaa$	$aaaa$	aaa	$aaaa$	aaa	$aaaa$

Vediamo ora cosa succede se aggiungiamo un'altra lettera, prendiamo b. Avremo allora delle parole sull'alfabeto $\{a,b\}$.

4) Il gioco di base, libero da regole, è come quello del caso precedente, ma l'assenza di regole crea qualche complicazione, non è lecito per esempio scambiare lettere diverse:

1	a, b	aa, ab, ba, bb	aaa, aab, aba, baa, abb, bab, bba, bbb	...
0	1	2	3	...

Le parole distinte di data lunghezza $n \geq 0$ sono 2^n. La concatenazione di due parole ne produce una nuova la cui lunghezza è uguale alla somma delle lungezze delle due parole iniziali, e la parola vuota non produce variazioni se concatenata

con altre parole. Osserviamo che scambiando i due termini nella concatenazione si ottengono in generale risultati diversi:

$$aab \,\&\, bb = aabbb \qquad\qquad bb \,\&\, aab = bbaab$$

Nota. Nell'insieme composto da due lettere diverse l'operazione di concatenazione è automaticamente associativa ed ha come elemento neutro la parola vuota. Inoltre la lunghezza della somma è la somma delle lunghezze, e vale la legge di cancellazione. Si ottiene quindi il *monoide libero* $(F_2, \&, 1)$ su due generatori.

Ora introduciamo mano a mano delle regole.

5) Commutatività: $ba = ab$

Ora, per ogni $n \geq 0$ ci sono solo n+1 parole distinte di lunghezza n. Se aggiungendo la convenzione di collocare sempre prima la a della b otteniamo un modo canonico di rappresentare gli elementi:

1	a, b	aa, ab, bb	aaa, aab, bbb	...
0	1	2	3	...

Nota. In questo caso si ottiene un monoide commutativo regolare. Si tratta di un altro modo di rappresentare la somma diretta del monoide additivo $(\mathbb{N}, +, 0)$ con se stesso o il monoide moltiplicativo dei monomi monici in due indeterminate.

6) Commutatività e opposti: $ba = ab$**,** $ab = 1$

Tale regola implica solo parole formate da lettere uguali, una per ogni lunghezza possibile, come mostra la tabella seguente:

...	$bbbb$	bbb	bb	b	1	a	aa	aaa	$aaaa$	...
...	-4	-3	-2	-1	0	1	2	3	4	...

La concatenazione di due parole della stessa lettera ne fa sommare le lunghez-

ze, mentre in caso di lettere diverse le lunghezze si sottraggono. Concatenando una parola di 'a' e una di 'b' della stessa lunghezza si ottiene la parola vuota. Si ottiene chiaramente un *isomorfismo* con il gruppo $(\mathbb{Z}, +)$ dei numeri interi.

Ora imponiamo che la massima lunghezza di una parola di 'a' o di una parola di 'b' siano limitate. Per esempio stabiliamo di "mangiare" tre 'a' o due 'b' consecutive. Allora si ottiene la situazione seguente:

1	a, b	aa, ab, ba	aab, aba, baa, bab	...
0	1	2	3	...

Sono possibili quindi solo parole in cui non compaiono mai tre 'a' o due 'b' consecutive. Si ottiene un insieme infinito di parole che, rispetto alla concatenazione, forma un gruppo non commutativo numerabile. Per esempio,

$$(aababaababababab)^{-1} = baabaabaababaaba$$

Aggiungiamo regole per poter scambiare in qualche modo le due lettere.

7) Commutatività e limitatezza: $ba = ab, bb = 1, aaa = 1$**.**

Le parole possibili sono sei:

$$1 \qquad a \qquad b \qquad aa \qquad ab \qquad aab$$

Riportiamo la tavola dei risultati delle 36 concatenazioni:

&	1	a	aa	b	ab	aab
1	1	a	aa	b	ab	aab
a	a	aa	1	ab	aab	b
aa	aa	1	a	aab	b	ab
b	b	ab	aab	1	a	aa
ab	ab	aab	b	a	aa	1
aab	aab	b	ab	aa	1	a

Osserviamo che ogni parola ha l'inversa; si tratta infatti di un gruppo.

Nota. L'operazione di concatenazione è ancora associativa ed ha come elemento neutro la parola vuota. In questo caso è anche commutativa, ed ogni elemento ha l'inverso. Si ottiene così un gruppo abeliano di ordine 6, *somma diretta* dei due gruppi ciclici di ordine 3 (generato da 'a') e 2 (generato da 'b'), quindi *isomorfo* al gruppo ciclico di ordine 6.
La regola 7) si generalizza variando le lunghezze massime delle parole di 'a' o di 'b'. Per ogni m, n interi positivi, si ottiene un insieme di $m \cdot n$ parole. In definitiva si ottiene sempre un gruppo abeliano di ordine m·n, *somma diretta* dei due gruppi ciclici di ordine m ed n.

8) Inversione e limitatezza: $ba = aab, bb = 1, aaa = 1$**.**

Anche in questo caso si hanno a disposizione solo sei parole diverse:

$$1 \qquad a \qquad b \qquad aa \qquad ab \qquad aab$$

Come si vede dalla seguente tavola di concatenazione, ogni parola ha l'inversa, quindi come nel caso precedente, si ha un gruppo, senza però la proprietà commutativa:

&	1	a	aa	b	ab	aab
1	1	a	aa	b	ab	aab
a	a	aa	1	ab	aab	b
aa	aa	1	a	aab	b	ab
b	b	aab	ab	1	aa	a
ab	ab	b	aab	a	1	aa
aab	aab	ab	b	aa	a	1

La regola $ba = aab$ è detta *di inversione* perchè la parola aa è inversa della parola a : lo scambio delle 'a' e delle 'b' sostituisce alla parola a la sua inversa.

Nota. In questo caso si ottiene un gruppo non abeliano di ordine 6, detto *gruppo diedrale* D_3 che è il gruppo delle simmetrie di un triangolo equilatero. Se la lunghezza della parola di 'a' che viene mangiata è $m > 2$, e nella regola d'inversione la parola ba diventa la sequenza di m-1 'a' e una 'b', si ottengono gruppi non abeliani di ordine 2m, detti *gruppi diedrali* D_{m}. Se $m = 2$ si ottiene invece un gruppo abeliano di ordine 4.

La regola precedente si generalizza variando le lunghezze massime delle parole di 'a' o di 'b' e la regola d'inversione, ma non in modo arbitrario, per evitare giochi banali, o in cui resta un solo tipo di lettera. Capire quali insiemi di regole producono giochi banali è un problema estremamente difficile, così come è altrettanto difficile sapere se alla fine avremo un numero finito o infinito di parole. Si veda per questo aspetto l'ultimo capitolo.

Notazione esponenziale L'uso di lettere per rappresentare parole, specie se lunghe, diventa pesante. Introduciamo allora, per comodità, la notazione esponenziale. In luogo di scrivere $n \geq 2$ lettere uguali consecutive, "compattiamo" la scrittura: $\underbrace{aaa...a}_{n}$ lo denotiamo con a^n.
In questo modo, una parola per esempio nell'alfabeto a, b può essere scritta nella forma $a^{n_1}b^{m_1}a^{n_2}b^{m_2}...$ con $n_i, m_i \in \mathbb{N}$.
Allora il gruppo diedrale D_3 ha per elementi: 1, a, a^2, b, ab, a^2b.
L'unico pericolo è quello di scambiare erroneamente di posto le potenze delle lettere, pur non avendo definito alcuna regola di commutatività. Nei monomi dell'algebra classica la commutatività delle lettere è implicitamente postulata, ma qui non si tratta di monomi, bensì di parole.

Riassumiamo quello che abbiamo ottenuto nei vari punti.
Possiamo adottare la convenzione di scrivere ogni gioco nel modo seguente:
scriviamo entro due parentesi a punta la lista delle lettere da usare, e poi la lista delle regole date.

1) $\langle a|\emptyset\rangle$

2) $\langle a|a^n = 1\rangle$

3) $\langle a|a^n = a^m\rangle$

4) $\langle a, b|\emptyset\rangle$

5) $\langle a, b | ab = ba \rangle$

6) $\langle a, b | ab = ba = 1 \rangle$

7) $\langle a, b | ab = ba, a^3 = 1 = b^2 \rangle$

8) $\langle a, b | ba = a^2 b, a^3 = 1 = b^2 \rangle$

Chiamiamo *generatori* le lettere che possiamo usare e *relazioni* le varie regole del gioco. Vedremo che si tratta di una struttura algebrica molto importante.

Capitolo 2

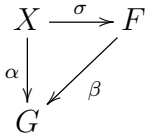
Gruppi Liberi e Presentazioni

Ora formalizziamo le costruzioni del capitolo precedente mediante la teoria dei gruppi liberi. In generale le dimostrazioni non saranno riportate.

2.1 Gruppi Liberi

Rifacendoci al capitolo precedente potremmo dire che un gruppo libero non ha "regole di gioco", come nel primo esempio ($\langle a|\emptyset\rangle$), che, con un'opportuna convenzione, vedremo essere un gruppo e non solo un monoide.

Definizione 2.1. Siano F un gruppo, X un sottoinsieme non vuoto di F, e σ: $X \longrightarrow F$ una funzione. Allora F, o più precisamente (F, σ), è detto *libero* su X se ad ogni funzione α da X ad un gruppo G corrisponde un unico omomorfismo β: $F \longrightarrow G$ tale che $\alpha = \beta \circ \sigma$; tale equazione esprime la commutatività del seguente diagramma:



La funzione σ: $X \longrightarrow F$ è necessariamente iniettiva. Supponiamo che $\sigma(x_1)$=$\sigma(x_2)$ e $x_1 \neq x_2$. Sia G un gruppo con almeno due elementi distinti g_1 e g_2 e scegliamo una funzione α: $X \longrightarrow G$ tale che $\alpha(x_1)$=g_1 e $\alpha(x_2)$=g_2. Allora $\beta(\sigma(x_1))$=$\beta(\sigma(x_2))$, da cui $\alpha(x_1)$=$\alpha(x_2)$ e g_1=g_2, che è una contraddizione. Chiaramente F è libero anche su Im σ, e Im $\sigma \hookrightarrow$ F sostituisce σ. Da qui un gruppo libero è sempre libero

su un sottoinsieme: in questo caso la commutatività del diagramma ci dice che la restrizione di β a X è α, cosicché β è l'unica estensione di α ad f. Un'altra conseguenza è che Im σ genera F.

Proposizione 2.1. *Se X è un insieme non vuoto, esistono un gruppo F e una funzione σ: X $\longrightarrow$ F tale che (F, σ) è libero su X e F=$\langle$Im $\sigma\rangle$.*

Dimostrazione. Scegliamo un insieme disgiunto da X, con la stessa cardinalità: per convenzione lo denotiamo con $X^{-1} = \{x^{-1} | x \in X\}$ dove x^{-1} è un simbolo. Chiamiamo *parola* in X una sequenza finita di simboli appartenenti ad $\{X \cup \mathrm{X}^{-1}\}$, scritta nella forma:

$$w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r},$$

$x_i \in$X, $\varepsilon_i = \pm 1$, $r \geq 0$: se $r = 0$ la sequenza è vuota e w è la *parola vuota*, che denotiamo con 1. Si avrà che due parole sono uguali se e solo se hanno gli stessi elementi nelle posizioni corrispondenti. Il prodotto tra due parole $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ e $v = y_1^{r_1} \cdots y_s^{r_s}$ è la la concatenazione, quindi:

$$wv = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} y_1^{r_1} \cdots y_s^{r_s},$$

con la convenzione che $w1 = w = 1w$. Definiamo inversa di w la parola $w^{-1} = x_r^{-\varepsilon_r} \cdots x_1^{-\varepsilon_1}$ e $1^{-1} = 1$.
Sia S l'insieme di tutte le parole di X. Definiamo una relazione di equivalenza su S nel modo seguente.
Due parole w e v sono equivalenti (in simboli w) se è possibile passare da una parola all'altra mediante una successione finita di operazioni del tipo:
(a) inserimento in w di una coppia di termini consecutivi xx^{-1} oppure $x^{-1}x$, con $x \in X$;
(b) cancellazione in w di una coppia di termini consecutivi xx^{-1} oppure $x^{-1}x$, con $x \in X$.
Che $\sim$ definisca effettivamente una relazione di equivalenza su S è immediato;
$\forall\ w \in S$ denotiamo con $[w]$ la sua classe di equivalenza.
Chiamiamo F l'insieme di tutte le classi di equivalenza. Vogliamo vedere che F è un gruppo. Se $w \sim w'$ e $v \sim v'$, si dimostra che $wv \sim w'v'$, quindi ha senso definire il prodotto tra $[w]$ e $[v]$ nel modo seguente:

$$[w][v] = [wv] \quad .$$

Allora $[w][1] = [w] = [1][w]$ e $[w][w^{-1}] = [ww^{-1}] = [1]$. Inoltre il prodotto è associativo: poiché è vero che $(wv)u = w(vu)$, ne segue che $([w][v]) \cdot [u] = [w] \cdot ([v][u])$.

Allora F è un gruppo con questa operazione binaria: l'elemento neutro è [1] e l'inverso di $[w]$ è $[w^{-1}]$.
Definiamo una funzione σ: $X \longrightarrow F$ con $\sigma(x) = [x]$.
Proviamo che (F, σ) è libero su X. Consideriamo α: $X \longrightarrow G$, funzione da X ad un gruppo G. Creiamo una funzione $\overline{\beta}$ che va dall'insieme di tutte le parole in X a G associando a $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ l'elemento $g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r}$ dove $g_i = \alpha(x_i)$. Ora $w \sim v$ implica che $\overline{\beta}(w) = \overline{\beta}(v)$ perché nel gruppo G i prodotti come gg^{-1} o $g^{-1}g$ sono uguali a 1_G. Allora è possibile definire una funzione β: $F \longrightarrow G$ con $\beta([w]) = \overline{\beta}([w])$. Allora $\beta([w][v]) = \beta([wv]) = \overline{\beta}(wv) = \overline{\beta}(w)\overline{\beta}(v)$ per definizione di $\overline{\beta}$. Da qui $\beta([w][v]) = \beta([w])\beta([v])$ e β: $F \longrightarrow G$ è un omomorfismo di gruppi. Inoltre $\beta(\sigma(x)) = \beta([x]) = \overline{\beta}(x) = \alpha(x)$ per $x \in X$. Infine se γ: $F \longrightarrow G$ è un altro omomorfismo tale che $\gamma \circ \sigma = \alpha$, allora $\gamma \circ \sigma = \beta \circ \sigma$ e γ e β coincidono su Im σ; ma chiaramente $F = \langle \text{Im } \sigma \rangle$ e quindi $\gamma = \beta$. □

Esaminiamo la costruzione appena descritta al fine di ottenere un'adeguata descrizione degli elementi del gruppo libero F.

Definizione 2.2. Una parola $w \in X$ è detta *ridotta* se non contiene coppie di simboli consecutivi della forma xx^{-1} o $x^{-1}x$, $x \in X$. Per convenzione la parola vuota è ridotta.

Se w è una parola arbitraria, possiamo cancellare da w tutte le coppie xx^{-1} o $x^{-1}x$ per ottenere una parola equivalente. Ripetendo questa procedura un numero finito di volte otterremo alla fine una parola ridotta equivalente a w. Quindi ogni classe di equivalenza di parole contiene una parola ridotta.

Osservazione 2.1. Spesso è possibile operare le cancellazioni in più modi. È consuetudine scegliere un verso, da sinistra a destra o viceversa, e ridurre le parole equivalenti procedendo sempre nel verso scelto.
per esempio, partendo da $w = babb^{-1}a^{-1}c^{-1}ca$ nell'alfabeto $\{a, b, c\}$, possiamo seguire due vie:

$$
\begin{array}{c}
ba\ \not{b}\ \not{b}^{-1}a^{-1}c^{-1}ca \\
\downarrow \\
b\ \not{a}\ \not{a}^{-1}c^{-1}ca \\
\downarrow \\
b\ \not{c}^{-1}\ \not{c}a \\
\downarrow \\
ba
\end{array}
$$

oppure

$$
\begin{array}{c}
bab b^{-1}a^{-1}\ \not{c}^{-1}\ \not{c}a \\
\downarrow \\
bab b^{-1}\ \not{a}^{-1}\ \not{a} \\
\downarrow \\
ba\ \not{b}\ \not{b}^{-1} \\
\downarrow \\
ba
\end{array}
$$

La parola ridotta è la stessa, nonostante le lettere provengano da posti diversi nella parola originaria.

Proposizione 2.2. *Ogni classe di equivalenza di parole in X contiene una sola parola ridotta.*

Definizione 2.3. Segue dalla Proposizione 2.2 che ogni elemento del gruppo libero F può essere scritto in modo unico nella forma $[w]$ con w parola ridotta, $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$, dove $\varepsilon_i = \pm 1$, $r \geqslant 0$ e in w non compaiono coppie del tipo xx^{-1} o $x^{-1}x$ con $x \in X$. Per definizione di moltiplicazione in F abbiamo $[w] = [x_1]^{\varepsilon_1} \cdots [x_r]^{\varepsilon_r}$. Sommando gli eventuali esponenti relativi agli stessi elementi consecutivi si ottiene:

$$[w] = [x_1]^{l_1} \cdots [x_s]^{l_s},$$

dove $s \geq 0$, l_i interi diversi da 0, e $x_i \neq x_{i+1}$. Notiamo che la parola ridotta iniziale può essere riottenuta da questa, quindi l'espressione è unica. Per semplificare la notazione identifichiamo w con $[w]$. Da ciò, ogni elemento di F può essere scritto in modo unico nella forma:

$$w = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s}$$

dove $s \geq 0$, $l_i \neq 0$ e $x_i \neq x_{i+1}$. Questa è detta *forma normale* di w.

L'esistenza di una forma normale è caratteristica dei gruppi liberi, come mostra il risultato seguente.

Proposizione 2.3. *Sia G un gruppo, ed X un sottoinsieme di G. Supponiamo che ogni elemento $g \in G$ si possa scrivere in modo unico nella forma $g = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s}$ dove $x_i \in X$, $s \geq 0$, $l_i \neq 0$, e $x_i \neq x_{i+1}$. Allora G è libero su X.*

Proposizione 2.4. *Se F_1 è libero su X_1, F_2 è libero su X_2 e $\mid X_1 \mid = \mid X_2 \mid$, allora $F_1 \simeq F_2$.*

Invece, se $F_1 \simeq F_2$, allora $|X_1| = |X_2|$.

Questo discorso rende possibile definire il *rango* di un gruppo libero come la cardinalità dell'insieme sul quale tale gruppo è libero. Osserviamo che dalla Proposizione 2.4 un gruppo libero su un insieme X è isomorfo al gruppo libero su X i cui elementi sono le parole ridotte di X. Dalle Proposizioni 2.4 e 2.1 segue che se (F, σ) è libero su un insieme X, allora Im σ genera F.

Proposizione 2.5. *Sia G un gruppo generato da un sottoinsieme X, e sia F un gruppo libero su un insieme Y. Se α: $Y \longrightarrow X$ è una funzione suriettiva, allora α è estendibile ad un epimorfismo da F a G.*

2.2 Presentazioni di Gruppi

Abbiamo visto che ogni gruppo è immagine omomorfa di un gruppo libero. Una vera e propria descrizione di un gruppo come immagine è chiamata *presentazione*. Più precisamente una presentazione di un gruppo G è un epimorfismo π da un gruppo libero F a G. Quindi se $R = Ker\ \pi$, abbiamo che $R \lhd F$ e $F/R \simeq G$. Gli elementi di R sono detti relatori della presentazione.

Per esempio sia F il gruppo libero su un insieme $Y = \{y_g \mid 1 \neq g \in G\}$ e sia π: $F \longrightarrow G$ l'omomorfismo definito da $\pi(y_g) = g$. Allora π è detta presentazione standard di G.
Supponiamo sia data una presentazione π: $F \longrightarrow G$ del gruppo G. Scegliamo un sistema libero di generatori per F, sia Y, e un sottoinsieme S di F tale che $S = Ker\ \pi$. Se X è l'immagine di Y tramite π, allora certamente X è un sistema di generatori per G. Di conseguenza $r \in F$ è un relatore di π se e solo se può essere scritto nella forma $(s_1)^{\varepsilon_1} \cdots (s_k)^{\varepsilon_k}$ dove $s_i \in S$, $\varepsilon_i = \pm 1$. La presentazione π, insieme con la scelta di Y e S, determina un *insieme di generatori e relazioni* per G, in simboli:

$$G = \langle Y|S\rangle \quad .$$

Nella pratica spesso è più conveniente elencare i generatori di G e le relazioni $\pi(s) = 1$, $s \in S$, cioè:

$$G = \langle X|\pi(s) = 1, s \in S\rangle \quad .$$

Esempio 2.1. Possiamo scrivere una presentazione di un gruppo G nei seguenti modi equivalenti:

$$G = \langle a, b|a^3 = 1, b^3 = 1, ab = ba\rangle \text{ oppure } G = \langle a, b|a^3, b^3, a^{-1}b^{-1}ab\rangle$$

dove nel primo caso,dopo i generatori di G, compaiono le relazioni, mentre nel secondo caso sono elencati i relatori.

Si tratta di due modi equivalenti di esprimere una presentazione di G.
Al contrario è facile,in linea di principio, costruire un gruppo avendo una presentazione con un dato insieme di generatori e relatori. Siano Y un qualsiasi insieme non vuoto e S un sottoinsieme del gruppo libero su Y. Sia S^F la chiusura normale di S in F (ovvero il più piccolo sottogruppo normale in F che contiene S) e poniamo $G = F/S^F$. Allora l'omomorfismo naturale π: $F \longrightarrow G$ è una presentazione di G e G ha l'insieme di generatori e relazioni $\langle Y|S\rangle$.
Il seguente risultato è spesso utile nello studio di gruppi con presentazioni simili.

Teorema 2.1. ***(di von Dyck)***
Siano G e H due gruppi con presentazioni $G = \langle X|R\rangle$ e $H = \langle X|S\rangle$. Se $R \subseteq S$ allora esiste un epimorfismo ϕ: $G \longrightarrow H$ (ovvero H è isomorfo ad un quoziente di G).

Dimostrazione. Sia F il gruppo libero su X e siano φ: $F \longrightarrow G$ e ψ: $F \longrightarrow H$ gli omomorfismi sottesi dalle due presentazioni nell'enunciato.

Allora $Ker(\varphi) = R^F \subseteq S^F = Ker(\psi)$ perché per il II teorema di isomorfismo per i gruppi $H \simeq F/S^F \simeq \frac{F/R^F}{S^F/R^F}$ e $F/R^F \simeq G$, e dunque H è isomorfo ad $F/Ker(\psi)$ che è isomorfo ad un quoziente di $F/Ker(\varphi) \simeq G$. □

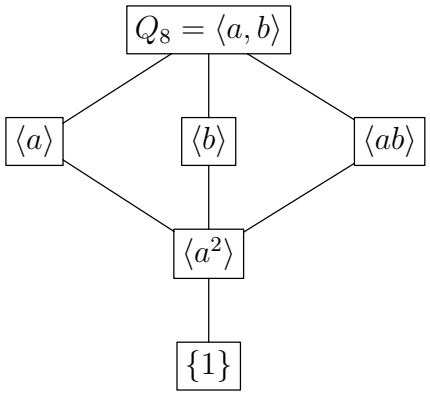
Esempio 2.2. Vediamo una presentazione del gruppo dei quaternioni, denotato con Q_8. Si tratta di un gruppo molto particolare, ha ordine 8 ed è il più piccolo gruppo non abeliano in cui tutti i sottogruppi sono normali e il cui ordine è la potenza di un primo. Una sua presentazione è la seguente:

$$Q_8 = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3 b \rangle$$

Ogni elemento può essere scritto in più modi: $a^3 = a^2 = a^2$. Inoltre,

$b^4 = (b^2)^2 = (a^2)^2 = a^4 = 1$, $(ab)^2 = abab = a(a^3b)b = a^4b^2 = b^2$

Ne segue che i sei elementi $a, a^3, b, b^3, ab, a^3b = ab^3 = (ab)^3$ hanno periodo 4. Infine, l'elemento $x = a^2 = b^2 = (ab)^2$ commuta con tutti gli altri ed è il quadrato dei sei precedenti. Allora, $Q_8 = \{id, a, a^2, a^3, b, b^3, ab, a^3b\}$
Riportiamo il diagramma di Hasse dei sei sottogruppi di Q_8, ordinati per inclusione.



Esempio 2.3. Consideriamo un gruppo con presentazione $\langle a, b | a^2, b^n, abab \rangle$. 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 più 1 e potenze di b con esponente al più $n-1$. Poi, se abbiamo una sequenza ba, la terza relazione dà, moltiplicando 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 $1, b, \ldots, b^{n-1}, a, ab, \ldots, ab^{n-1}$. Il gruppo ha quindi $2n$ elementi. Tale gruppo è noto come gruppo diedrale ed è il gruppo di simmetrie di un poligono regolare con n lati. L'elemento a di ordine 2 è una simmetria, l'elemento b una rotazione di angolo di $2\pi/n$ radianti. Le tre relazioni assumono un significato geometrico evidente. Si osservi che ogni elemento ab^k ha ordine 2. Infatti $ab^k \cdot ab^k = a^2 b^{-k} b^k = 1 \cdot 1 = 1$, ricordando la $b^{n-1} = b^{-1}$ e quindi $b^{n-k} = b^{-k}$.

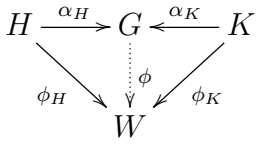
Capitolo 3

Prodotti liberi

Il *prodotto libero* di gruppi è una generalizzazione dell'idea di gruppo libero. Tratteremo il caso del prodotto libero di due gruppi: l'estensione al prodotto di famiglia arbitraria di gruppi è analogo.

Proprietà universale dei prodotti liberi. Siano H e K gruppi; una terna $(G,\ \alpha_H,\ \alpha_K\ )$, dove G è un terzo gruppo e $\alpha_H\colon\ H \longrightarrow G$, $\alpha_K\colon\ K \longrightarrow G$ sono omomorfismi, si dice *prodotto libero* di H e K se è soddisfatta la seguente proprietà universale:

Per ogni gruppo W ed omomorfismi $\alpha_H\colon\ H \longrightarrow W$, $\alpha_K\colon\ K \longrightarrow W$, esiste uno ed un unico omomorfismo $\phi\colon\ G \longrightarrow W$ tale che $\phi_H = \phi \circ \alpha_H$ e $\phi_K = \phi \circ \alpha_K$. Ovvero risulta commutativo il diagramma:



Prima di dimostrare l'esistenza dei prodotti liberi, facciamo alcune osservazioni che si deducono direttamente dalla proprietà universale.

Proposizione 3.1. *Siano H e K gruppi:*
(1) se $(G,\ \alpha_H,\ \alpha_K\ )$ è prodotto libero di H e K allora α_H e α_K sono iniettive;
(2) se G e G' sono prodotti liberi dei gruppi H e K, allora $G \simeq G'$.

Dunque, se esiste, il prodotto libero di H e K è unico (a meno di isomorfismi) e lo si denota con

$$H * K.$$

Osservazione 3.1. Analogamente al risultato trovato per i gruppi liberi, una conseguenza quasi immediata della proprietà universale è che se H e K sono gruppi, allora per ogni gruppo G che sia generato da due sottogruppi isomorfi rispettivamente ad H e a K, esiste un epimorfismo $H * K \longrightarrow G$, dunque G è isomorfo ad un quoziente del prodotto libero $H * K$.

Proviamo ora l'esistenza del prodotto libero $H * K$. Siano H e K due gruppi dati mediante presentazioni, diciamo $H = \langle X|R\rangle$ e $K = \langle Y|S\rangle$, con $X \cap Y = \emptyset$. Mostriamo che il gruppo

$$G = \langle X \cup Y|R \cup S\rangle$$

è prodotto libero di H e K. Per prima cosa definiamo gli omomorfismi α_H e α_K: per il primo si pone α_H: $H \longrightarrow G$ l'omomorfismo ottenuto componendo l'immersione $H \longrightarrow \langle X \cup Y|R\rangle$ con la proiezione $\langle X \cup Y|R\rangle \longrightarrow G$ (quindi $\alpha_H(x) = x\ \forall x \in X$); osserviamo che ponendo η: $G \longrightarrow H$ l'omomorfismo tale che $\eta(x) = x\ \forall x \in X$ e $\eta(y) = 1$ per $y \in Y$ allora $\eta \circ \alpha_H$ è l'identità su H e quindi α_H è iniettiva; allo stesso modo si definisce α_K: $K \longrightarrow G$.
Proviamo adesso la proprietà universale. Siano W un gruppo, ϕ_H: $H \longrightarrow W$ e ϕ_K: $K \longrightarrow W$ omomorfismi; definiamo ϕ: $G \longrightarrow W$ ponendo $\phi(x) = \phi_H(x)\ \forall x \in X$, e $\phi(y) = \phi_K(y)\ \forall y \in Y$ ed estendendo ad un omomorfismo: allora $\phi_H = \phi \circ \alpha_H$, $\phi_K = \phi \circ \alpha_K$, come richiesto dalla proprietà universale, e ϕ è unico per tale condizione.

Proposizione 3.2. *Sia G un gruppo e H, K sottogruppi di G tali che $G = \langle H, K\rangle$; allora $G = H * K$ se e solo se ogni elemento $g \in G$ si scrive in modo unico nella forma*

$$g = a_1 b_1 \dots a_n b_n$$

con $a_1, \dots, a_n \in H$, $b_1, \dots, b_n \in K$, $a_i \neq 1 \neq b_j$ per $i = 2, \dots, n$ e $j = 1, \dots, n-1$.

Esempio 3.1. Supponiamo di avere due gruppi G_1 e G_2 con rispettive presentazioni $\langle X|R\rangle$ e $\langle Y|S\rangle$. Il loro prodotto libero $G_1 * G_2$ ha come detto presentazione $\langle X \cup Y|R \cup S\rangle$. Una presentazione per il prodotto diretto $G_1 \times G_2$ si ottiene invece prendendo come insieme di generatori $X \cup Y$ e come relazioni tutte quelle di $R \cup S$ e in più 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 $x_1 \cdots x_n y_1 \cdots y_n$ con $x_i \in G_1$ e $y_i \in G_2$, e definire così una applicazione in $G_1 \times G_2$ mandando tale parola in (x_{1n}, y_{1n}).

Diamo un esempio: consideriamo $\mathbb{Z}_2 = \langle x|x^2\rangle$. Il prodotto cartesiano $\mathbb{Z}_2 \times Z_2$ ammette la presentazione $\langle x, y|x^2, y^2, xyx^{-1}y^{-1}\rangle$: abbiamo infatti aggiunto il relatore $xyx^{-1}y^{-1}$ poiché $\mathbb{Z}_2 \times Z_2$. Dalla definizione, invece, il prodotto libero $\mathbb{Z}_2 * \mathbb{Z}_2$ ammette la presentazione $\langle x, y|x^2, y^2\rangle$: esso è dunque costituito dal numero infinito di parole della forma $1, x, y, xy, yx, xyx, yxy, xyxy, yxyx, \ldots$

Esempio 3.2. Consideriamo il prodotto libero di due gruppi ciclici di ordine 2. Siano $H = \langle x|x^2 = 1\rangle$, $K = \langle y|y^2 = 1\rangle$, allora
$H * K = \langle x, y|x^2 = 1, y^2 = 1\rangle = D_\infty$ che è il gruppo diedrale infinito. Le uniche parole possibili sono: $1, x, y, xy, yx, xyx, yxy, xyxy, \ldots$ Posto $a = xy$ si vede che a ha ordine infinito (poichè non vale la proprietà commutativa). Inoltre $y = xa$ implica che il gruppo sia generato da a e da x, quindi possiamo scrivere anche $D_\infty = \langle a, x|x^2 = 1, xa = a^{-1}x\rangle$. Si ha in definitiva che $D_\infty = C_2 * C_2$, e i gruppi diedrali finiti sono i suoi quozienti.
Questo esempio mostra inoltre come uno stesso gruppo possa avere presentazioni molto diverse e può non essere possibile riconoscere se si tratti oppure no dello stesso gruppo.

Esempio 3.3. Consideriamo ora il prodotto libero tra il gruppo ciclico di ordine 2 e quello di ordine 3. Si ha $C_2 * C_3 = \langle x, y|x^2, y^3\rangle$. Costruiamo un epimorfismo tra questo ed S_3:

$$\begin{cases} parola\ vuota \mapsto id \\ x \mapsto (12) \\ y \mapsto (123) \\ y^2 \mapsto (132) \\ xy \mapsto (23) \\ xy^2 \mapsto (13) \end{cases}$$

Allora S_3 è isomorfo ad un quoziente del prodotto libero $C_2 * C_3$,
$S_3 \simeq \langle x, y|x^2, x^3, x^{-1}yxy^{-2}\rangle$.

Capitolo 4

Il problema della parola

Sia G un gruppo finitamente generato con generatori $x_1, \ldots, x_n$ e relatori $r_1, \ldots, r_k$. Il *problema della parola* è detto risolubile per una presentazione se esiste un algoritmo che, data una parola w nelle x_i, permetta di stabilire se questa sia o no la parola vuota $w = 1$. Questo problema è equivalente a quello dell'*uguaglianza*: date due parole $w_1, w_2 \in G$, esiste un algoritmo che permetta di stabilire se $w_1 = w_2$, ovvero se $w_1 w_2^{-1} = 1$.
Tale problema è indipendente dalla presentazione finita considerata, e riguarda invece il gruppo G. Possiamo dire che per un gruppo G il problema della parola è risolubile se lo è per una certa presentazione finita di G (e quindi per tutte le sue presentazioni).
Ricordiamo alcune definizioni della teoria della ricorsività. Un insieme S di elementi si dice *ricorsivo* se esiste un algoritmo capace di stabilire se un elemento appartiene o no all'insieme. Si dice *ricorsivamente enumerabile* se esiste un algoritmo che permetta di disporre in una lista gli oggetti di S. Ogni insieme S ricorsivo è ricorsivamente enumerabile, e S è ricorsivo se sia S che il suo complementare sono ricorsivamente enumerabili. Per un insieme ricorsivo non c'è quindi mai un'attesa infinita: facendo girare contemporaneamente i due algoritmi che danno le liste degli elementi di S e del suo complementare S', un dato elemento apparirà, prima o poi, in una delle due liste. Si dimostra però che esistono insiemi di interi positivi ricorsivamente enumerabili ma non ricorsivi, e questo fatto è, in un certo senso, la fonte di tutti i problemi di indecidibilità in matematica.
Si può fare una lista delle parole su un alfabeto finito $X \cup X^{-1}$ come si fa per un dizionario: la parola vuota 1 ha lunghezza 0; le parole di lunghezza 1 sono gli elementi x o x^{-1} ordinate per esempio come

$$x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_n, x_n^{-1},$$

quelle di lunghezza 2 nell'ordine lessicografico

$$x_1x_1, x_1x_1^{-1}, x_1x_2, \ldots, x_n^{-1}x_n^{-1},$$

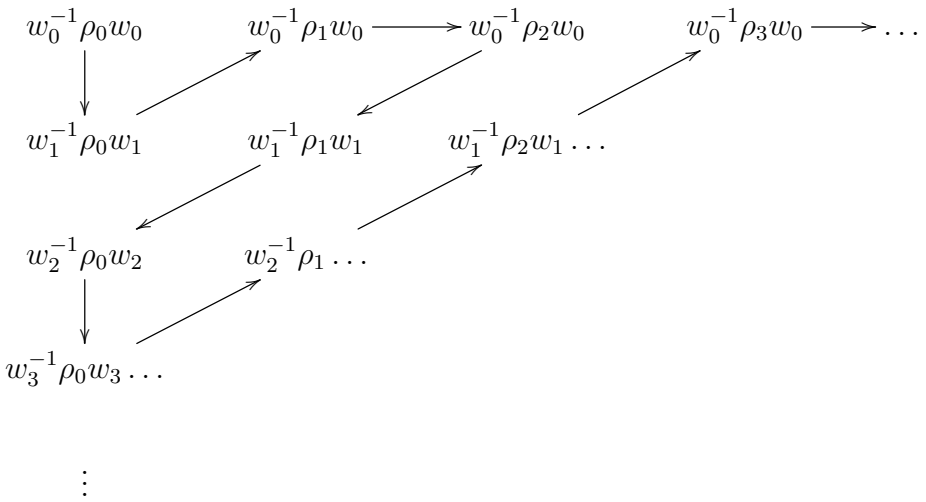
ecc. Usando la lista $w_0, w_1, w_2, \ldots$ possiamo formare una lista delle parole uguali a 1 in G.

Teorema 4.1. *Se G è finitamente presentato, $G = \langle X|R\rangle$ e Ω è l'insieme delle parole su X, allora l'insieme*

$$W = \{w \in \Omega | w = 1 \in G\}$$

è ricorsivamente enumerabile.

Dimostrazione. Usando la lista $w_0, w_1, w_2, \ldots$ delle parole nelle x_i, disponiamo in una lista $\rho_0, \rho_1, \rho_2, \ldots$ le parole nelle r_i, cioè le parole di W, nello stesso modo in cui si ottiene una enumerazione dei numeri razionali:



□

Allora, poiché per un gruppo finitamente presentato G l'insieme W è ricorsivamente enumerabile, il problema della parola per G è risolubile se anche $\{w \in \Omega | w \neq 1\}$ è ricorsivamente enumerabile.

Nota. Un gruppo finitamente generato si dice *ricorsivamente presentato* se l'insieme delle relazioni è ricorsivamente enumerabile. Il problema della parola si definisce per questi gruppi come nel caso dei gruppi finitamente presentati, ed è anch'esso un problema ricorsivamente enumerabile.

È chiaro che per il gruppo libero il problema della parola è risolubile: data una parola w l'algoritmo richiesto consiste nel procedimento di riduzione. Una parola nelle x_i è una parola $w = 1$ nel gruppo libero se dopo la cancellazione di lettere adiacenti della forma $x_i x_i^{-1}$ o $x_i^{-1} x_i$ si arriva alla parola vuota; altrimenti $w \neq 1$. Consideriamo ora la nozione di gruppo semplice nel contesto dei gruppi dati con generatori e relazioni.

Definizione 4.1. Un gruppo G si dice semplice se $N \lhd G \Rightarrow N = \{1\}$ oppure $N = G$.

Si dimostra il seguente:

Teorema 4.2. *Sia $G = \langle X|R\rangle$ un gruppo dato con generatori e relazioni. Allora G è un gruppo semplice $\Leftrightarrow$ ogniqualvolta si aggiunge a R una parola w che non è uguale a* 1 *in G si ottiene il gruppo identico:*

$$G_1 = \langle X|R, w\rangle = \{1\}.$$

Teorema 4.3. *Per un gruppo semplice $G = \langle X|R\rangle$ finitamente presentato il problema della parola è risolubile.*

Dimostrazione. Sia $w \in G$. Se $G = 1$ non c'è niente da dimostrare. Sia allora $G \neq 1$, $x \neq 1$ un fissato elemento di G, e $G_w = \langle X|R, w\rangle$. Se $w = 1 \in G$, allora ovviamente $G \simeq G_w$. Se $w \neq 1$ allora, essendo G semplice, per il Teor. 3.2 si ha $G_w = \{1\}$. Ne segue $x = 1$ in G_w se e solo se $w \neq 1$ in G. Il gruppo G_w è anch'esso finitamente presentato. Data la parola w di G, possiamo allora formare simultaneamente due liste:

- parole uguali a 1 in G; - parole uguali a 1 in G_w.

Allora:

- se $w = 1$ in G, w compare nella prima lista; - se $w \neq 1$ in G, x compare nella seconda lista.

Basta allora aspettare e vedere quale dei due fatti si verifica. □

Definizione 4.2. Sia G un gruppo, ρ una relazione tra elementi e sottoinsiemi definita su G e sulle sue immagini omomorfe, e sia P una proprietà di gruppi (ovvero tale che se $G_1 \simeq G$ e G ha la proprietà P, allora anche G_1 ha la proprietà P). Si dice allora che G ha *residualmente* la proprietà P *rispetto a* ρ, o che G è *residualmente* P, se per ogni coppia di elementi x, y che non sono tra loro nella relazione ρ esiste un omomorfismo suriettivo ϕ di G in un gruppo K che ha la proprietà P e tale che $\phi(x) \neq \phi(y)$.

Esempio 4.1. Sia ρ la relazione di uguaglianza. Allora G è residualmente P se per ogni coppia di elementi distinti x e y esiste un omomorfismo di G in un gruppo K che ha la proprietà P e tale che le immagini sono anch'esse distinte. Poiché $x = y$ è equivalente a $xy^{-1} \neq 1$, quanto detto è equivalente ad affermare che un elemento di G diverso da 1 resta diverso da 1 in un gruppo che ha la proprietà P. La cosa si può esprimere dicendo che G è residualmente P se, per ogni $g \neq 1$, esiste $N \trianglelefteq G$, dove N dipende da x, tale che $g \notin N$ e G/N ha la proprietà P (la proprietà è dunque "residua" nel senso che di essa gode il gruppo che resta quando si "toglie" il sottogruppo N).

Esempio 4.2. Gli interi sono un gruppo residualmente finito (se non si specifica la relazione ρ si intende la relazione di uguaglianza). Infatti, dati due interi n e m, con m che non divide n, n non appartiene ad $\langle m \rangle$, e il quoziente $\mathbb{Z}/\langle m \rangle$ è finito. Questo fatto vale in generale per tutti i gruppi liberi.

Teorema 4.4. *Un gruppo libero è residualmente finito.*

Teorema 4.5. *Per un gruppo G finitamente presentato e residualmente finito il problema della parola è risolubile.*

Dimostrazione. Sia F libero di rango n, R finitamente generato e $G = F/R$. Sia w una parola di F; dobbiamo decidere se $w \in R$ o no. Cominciamo allora due procedure: con la prima enumeriamo effettivamente gli elementi di R; con la seconda facciamo una lista delle tavole di moltiplicazione dei quozienti finiti di F/R. Allora basta aspettare perché necessariamente o w compare nella prima enumerazione, e quindi $w \in R$, oppure, se $w \notin R$ è $wR \neq R$, e dunque, essendo F/R residualmente finito, esiste $H/R \trianglelefteq F/R$ tale che $(F/R)/(H/R)$ è finito e $wR \notin H/R$, e pertanto wR comparirà nella lista dei quozienti finiti di F/R. $\square$

Conclusione

Un gioco con lettere "come pedine" e con regole di formaione, che ci ha consentito di costruire semplici esempi di monoidi o gruppi finiti, si è rapidamente rivelato come la "punta di un iceberg" di una parte essenziale della teoria dei gruppi, con complicazioni insospettabili che riguardano sia aspetti tecnici (trovare una presentazione "minimale" in qualche senso di un gruppo finito, oppure data una presentazione elencare gli elementi del gruppo con algoritmi opportuni) sia aspetti logigi, come la decidibilità o meno del problema della parola o dell'isomorfismo per classi di gruppi.

Bibliografia

[V] L.Verardi, *Dispense del corso di Algebra da un Punto di Vista Superiore*, a.a. 2013-2014

[A] M.Artin, *Algebra*, Bollati-Boringhieri,1997

[R] D.J.S.Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York,1996

[M] A.Machì, *Gruppi: Una introduzione a idee e metodi della Teoria dei Gruppi*, Springer-Verlag, Milano, 2007