3

Gruppi liberi

Sia X un sistema di generatori del gruppo G; dato $g \in G$, luna scrittura di g nella forma

$$g = x_1 x_2 \cdots x_n \tag{3.1}$$

con $x_1, \ldots, x_n \in X \cup X^{-1}$ si dice *ridotta* se $x_{i+1} \neq x_i^{-1}$ $(i = 1, \ldots, n-1)$. 'E facile trovare esempi nei quali lo stesso elemento di un gruppo $G = \langle X \rangle$ si può rappresentare mediante come diverse parole ridotte in $X \cup X^{-1}$: ad esempio, nel gruppo diedrale $\langle y, x \rangle$ (con $x^2 = 1$ e $y^x = y^{-1}$), $y = xyxyy$.

3.1. Gruppi liberi

Definizione. Un sistema di generatori X del gruppo G si dice *libero* se $X \cap X^{-1} = \emptyset$ e per ogni $x_1, \ldots, x_n \in X \cup X^{-1}$, con $x_i^{-1} \neq x_{i+1}$ (per $i = 1, \ldots, n-1$) si ha

$$x_1 x_2 \cdots x_n \neq 1. \tag{3.2}$$

Ciò equivale a richiedere che $X \cap X^{-1} = \emptyset$ ed ogni elemento $1 \neq g \in G$ si scrive on modo unico come in (3.1) mediante una parola ridotta in $X \cup X^{-1}$.

La definizione di partenza di gruppo libero che diamo in queste note è direttamente riferita a questo tipo di generazione.

Definizione 1. Un gruppo F è un *gruppo libero* se ammette un sistema libero di generatori. Più in generale, dato un insieme astratto X, diremo che il gruppo F è libero su X se esiste una applicazione iniettiva $\tau : X \to G$ tale che $\tau(X)$ è un sistema libero di generatori di F.

Una definizione equivalente (come proveremo) enfatizza una importante "proprietà universale" dei gruppi liberi; tanto importante che in molti testi è questa la definizione di riferimento.

Definizione 2. Un gruppo F è *libero sull'insieme* X se esiste $\tau : X \to F$, con la proprietà che per ogni gruppo G ed ogni applicazione $f : X \to G$, *esiste un unico omomorfismo* $\alpha : F \to G$ tale che $\alpha\tau = f$; in altri termini, esiste uno ed un solo omomorfismo α che rende commutativo il diagramma:

$$\begin{array}{ccc} X & \xrightarrow{\tau} & F \\ {\scriptstyle f}\downarrow & \swarrow & \nearrow {\scriptstyle \alpha} \\ G & & \end{array} \tag{3.3}$$

La proprietà universale descritta della seconda Definizione trova in questo senso corrispettivi in teorie che riguardano altri tipi di strutture algebriche. Questa definizione è più adatta (come si vedrà immediatamente) a svelare la proprietà dei gruppi liberi, mentre la definizione mediante parole con cui abbiamo iniziato, suggerisce meglio - almeno a me - la natura dei gruppi liberi; sarà ovviamente il contesto a suggerire di volta in volta quella più idonea alla comprensione.

Rinviando la dimostrazione dell'equivalenza delle due definizioni a dopo la costruzione, formale ma esplicita, di gruppi liberi su qualsiasi insieme, vediamo subito un'importantissima conseguenza della Definizione 2.

Teorema 3.1. *Siano F e G gruppi liberi su, rispettivamente, gli insiemi X e Y. Se $|X| = |Y|$, allora F e G sono isomorfi.*

Dimostrazione. Sia $g : X \to Y$ una biezione; siano F e G gruppi liberi, rispettivamente su X e su Y, con $\tau : X \to F$ e $\sigma : Y \to G$ le immersioni dei generatori. Applicando la (3.3) a $f = \sigma g$ si deduce l'esistenza di un omomorfismo $\alpha : F \to G$ tale che $\alpha\tau = \sigma g$; applicandola a $f' = \tau g^{-1}$, quella di un omomorfismo $\beta : G \to F$ tale che $\tau g^{-1} = \beta\sigma$. Dunque

$$\alpha\beta\sigma = \alpha\tau g^{-1} = \sigma g g^{-1} = \sigma. \tag{3.4}$$

Ora, la proprietà universale per il gruppo G stabilisce che la funzione identica $h = 1_G$ è *l'unico* omomorfismo $G \to G$ tale che tale che $h\sigma = \sigma$. Da (3.4) segue quindi $\alpha\beta = 1_G$. Allo stesso modo si prova $\beta\alpha = 1_F$. Dunque α è un isomorfismo. ∎

Quindi, dato un insieme X, si parla *del* gruppo libero su X, la cui esistenza proveremo tra poco e che denoteremo con $F(X)$. Anzi, poiché il tipo di isomorfismo di $F(X)$ dipende solo dalla cardinalità di X, se $|X| = \lambda$, diremo che $F(X)$ è il *gruppo libero di rango* λ. Nel caso particolare in cui $n < \infty$, denoteremo con F_n il gruppo libero di rango n. Di fatto poi, la Proposizione 3.1 ammette una formulazione inversa, nel senso che gruppi liberi di rango diverso (non necessariamente finito) non sono isomorfi (si veda anche l'esercizio 3.5).

Il nostro prossimo compito sarà la costruzione di gruppi liberi; prima, qualche esercizio.

Esercizio 3.1. Si provi che $X \subseteq G$ è un sistema libero di generatori per il gruppo G se e soltanto se ogni $1 \neq g \in G$ si scrive in modo unico nella forma $g = x_1^{\beta_1} \dots x_n^{\beta_n}$ con $x_1, \dots x_n \in X$, $x_i \neq x_{i+1}$ e $\beta_1, \dots, \beta_n \in \mathbb{Z} \setminus \{0\}$.

Esercizio 3.2. Usando la proprietà universale si provi che il gruppo $\mathbb{Z} \times \mathbb{Z}$ non è libero.

Esercizio 3.3. (Proprietà Proiettiva dei gruppi liberi) Siano G, H gruppi ed F un gruppo libero. Si provi che se $\phi : G \to H$, $\alpha : F \to H$ sono omomorfismi tali che $Im(\alpha) \leq Im(\phi)$, allora esiste un omomorfismo $\beta : F \to G$ tale che $\alpha = \phi\beta$.

Esercizio 3.4. Sia G un gruppo e sia $N \trianglelefteq G$ tale che G/N è un gruppo libero. Si provi che esiste un complemento H di N in G.

Esercizio 3.5. Sia F un gruppo libero sull'insieme finito X, e sia S un sistema di generatori per F; si provi che $|X| \leq |S|$.

Costruzione (esistenza) di gruppi liberi. Un gruppo ciclico infinito $\langle x \rangle$ è libero nel sistema di generatori $X = \{x\}$ (immediatamente secondo la Definizione 1, ma anche - perché? - secondo la definizione mediante la proprietà universale). A parte questo

immediato esempio, le due definizioni non garantiscono di per se stesse l'esistenza di gruppi con un sistema libero di generatori con due o più elementi. In questa sezione, per ogni insieme non-vuoto X, costruiremo formalmente un gruppo libero su X secondo la Definizione 1, mentre in una prossima (sezione 3.4) forniremo alcuni esempi "in natura".

Sia X un insieme non vuoto. Si considera un insieme X^{-1}, disgiunto da X e della sua stessa cardinalità, assieme ad una biezione $X \to X^{-1}$, per cui denotiamo con x^{-1} l'immagine di ciascun elemento $x \in X$.
Sia W l'insieme di tutte le *parole* nell'alfabeto $X \cup X^{-1}$, ovvero di tutte le stringhe finite

$$w = x_1 x_2 \dots x_n \tag{3.5}$$

con $x_i \in X \cup X^{-1}$, alle quali si aggiunge la parola vuota, che denotiamo col simbolo 1. Se $w \in W$ è come in (3.5) diciamo che $n = \ell(w)$ è la lunghezza di w (e $\ell(1) = 0$).
L'insieme W è in modo naturale un semigruppo, dove il prodotto di due parole consiste nelle loro giustapposizione: se $w_1 = x_1 x_2 \dots x_n$ e $w_2 = x'_1 x'_2 \dots x'_m$ sono elementi di W (quindi $x_1, \dots, x_n, x'_1, \dots, x'_m \in X \cup X^{-1}$), allora

$$w_1 \cdot w_2 = x_1 x_2 \dots x_n x'_1 x'_2 \dots x'_m. \tag{3.6}$$

Inoltre, la parola vuota 1 può essere aggregata come elemento neutro, ottenendo quindi che W è un monoide.

Sugli elementi w di W definiamo i seguenti due tipi di operazioni:

(R1) inserimento in w di una coppia di termini consecutivi del tipo xx^{-1} oppure $x^{-1}x$, con $x \in X$;
(R2) cancellazione in w di una coppia di termini consecutivi del tipo xx^{-1} oppure $x^{-1}x$, con $x \in X$

(dove si intende che l'inserimento o la cancellazione possono avvenire anche all'inizio o alla fine della parola). Una parola w si dice *ridotta* se $w = 1$ oppure w non include alcuna coppia consecutiva del tipo xx^{-1} oppure $x^{-1}x$, con $x \in X$. Diciamo poi che due parole $w_1, w_2 \in W$ sono *equivalenti*, e scriviamo $w_1 \sim w_2$, se w_2 si ottiene da w_1 mediante una successione finita di operazioni del tipo (R1) o (R2). Che $\sim$ definisca effettivamente un'equivalenza su W è immediato; per ogni $w \in W$ denotiamo con $[w]$ la sua classe di equivalenza. Ad esempio, se x, y sono elementi distinti di X allora $[xx^{-1}] = [yy^{-1}] = [1]$; un altro esempio è $1 \sim w = xyx^{-1}xy^{-1}yy^{-1}x^{-1}$, infatti una successione di operazioni del tipo (2) dà:

$$w = xy(x^{-1}x)y^{-1}yy^{-1}x^{-1} \sim x(yy^{-1})yy^{-1}x^{-1} \sim x(yy^{-1})x^{-1} \sim xx^{-1} \sim 1 \tag{3.7}$$

dove abbiamo indicato con parentesi le coppie che via via sono cancellate. Osserviamo che quella descritta da (3.7) non è l'unica serie di riduzioni che è possibile condurre a partire da w; ad esempio, un 'altra è la seguente:

$$w = xyx^{-1}xy^{-1}(yy^{-1})x^{-1} \sim xy(x^{-1}x)y^{-1}x^{-1} \sim x(yy^{-1})x^{-1} \sim xx^{-1} \sim 1 \tag{3.8}$$

Si osservi che però la parola di arrivo (in questo caso la parola vuota 1) è la stessa, ed è una parola ridotta. Questo vale in generale: si ha infatti,

Lemma 3.2. *Ogni classe di equivalenza in W modulo $\sim$ contiene una ed una sola parola ridotta.*

Dimostrazione. 1) Che ogni classe $[w]$ contenga una parola ridotta è facile: se w è ridotta siamo già arrivati; altrimenti è possibile cancellare da w una coppia xx^{-1} con $x \in X \cup X^{-1}$, ottenendo una parola $w_1 \in [w]$ tale che $\ell(w_1) = \ell(w) - 2$. Si prosegue allo stesso modo mediante cancellazioni, cioè operazioni (R2), arrivando infine ad una parola ridotta in $[w]$.
2) Proviamo ora che ogni classe contiene una sola parola ridotta. Supponiamo, per assurdo, esistano due diverse parole ridotte w, v che appartengono alla stessa classe; allora esistono $u_1, \dots, u_n \in W$, con $n \geq 1$, tali che

$$w = u_0 \sim u_1 \sim \cdots \sim u_{n-1} \sim u_n = v. \tag{3.9}$$

Scegliamo una tale coppia w, v e la catena (3.9) in modo che la somma $\sum_{i=0}^{n} \ell(u_i)$ sia minima possibile. Poiché w è ridotta, il primo passaggio, da w a u_1, è necessariamente un inserimento di tipo $(R1)$; similmente, il passaggio da u_n a v è una cancellazione di tipo $(R2)$. Esiste quindi un indice $1 \leq k \leq n-1$ tale che

$$\ell(w) < \ell(u_1) < \ldots < \ell(u_k) > \ell(u_{k+1}).$$

Per come abbiamo scelto la coppia w, v, si ha $u_{k-1} \neq u_{k+1}$. Allora esistono $s, t \in W$ e $x \in X \cup X^{-1}$ tali che $st = u_{k-1}$ e $sxx^{-1}t = u_k$; sia $y \in X \cup X^{-1}$ tale che u_{k+1} è il risultato della cancellazione di yy^{-1} da u_k. Se tale cancellazione occorre in s o in t, può essere effettuata su u_{k-1}, ottenendo una parola $u^* \sim u_{k+1}$, fornendo una catena $w = u_0 \sim \cdots \sim u_{k-1} \sim u^* \sim u_{k+1} \ldots \sim u_n = v$, la somma delle lunghezze degli elementi della qualle è inferiore a quella di (3.9), contro la scelta di quest'ultima. Pertanto la cancellazione di yy^{-1} da u deve coinvolgere una tra x o x^{-1} tra s e t; ma allora, come si vede subito, $u_{k-1} = u_{k+1}$ che ancora contraddice la scelta di u. Questa contraddizione conclude la dimostrazione. ∎

Se $w \in W$, denotiamo con $\overline{w}$ l'unica parola ridotta tale che $w \sim \overline{w}$.

Sia $F = W/\sim$ l'insieme quoziente. Su F definiamo quindi un prodotto ponendo, per ogni $w_1, w_2 \in W$,

$$[w_1] \cdot [w_2] = [w_1 w_2]. \tag{3.10}$$

Che si tratti di una buona definizione è piuttosto immediato, e lo lascio comunque per esercizio.

Proposizione 3.3. *Con l'operazione definita in (3.10), F è un gruppo, ed è libero nel sistema di generatori $\{[x] \mid x \in X\}$.*

Dimostrazione. Che l'operazione in (3.10) sia associativa discende immediatamente dal fatto che tale è l'operazione nel monoide delle parole W. Per la stessa ragione si riconosce subito che $[1]$ (dove 1 rappresenta la parola vuota) è l'elemento neutro in F, che denoteremo ancora con 1.
Ora, per ogni $x \in X$, $xx^{-1} \sim 1 \sim x^{-1}x$, e quindi, in F, $[x^{-1}] = [x]^{-1}$. Infine, sia $w = x_1^{\epsilon_1} \ldots x_n^{\epsilon_n} \in W$, con $x_1, \dots, x_n \in X$ e $\epsilon_1, \dots, \epsilon_n \in \{1, -1\}$ (dove, ovviamente, per $x \in X$, si intende $x^1 = x$); allora

$$[w]^{-1} = [x_n^{-\epsilon_n} \ldots x_1^{-\epsilon_1}].$$

Pertanto, F è un gruppo, e chiaramente $X\tau = \{[x] \mid x \in X\}$ è un suo sistema di generatori (qui $\tau : X \to F$ è la proiezione $x \mapsto [x]$, che, per il Lemma 3.2 è un'applicazione

iniettiva). Infine, tale sistema di generatori è libero per costruzione, si potrebbe dire. Infatti se se $x_1, \dots x_n \in X$, $\epsilon_1, \epsilon_2, \dots, \epsilon_n \in \{1, -1\}$, e in F,

$$[x_1]^{\epsilon_1}[x_2]^{\epsilon_2} \dots [x_n]^{\epsilon_n} = [1], \tag{3.11}$$

allora, in W, $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} \sim 1$, che significa che la parola $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$ non è ridotta., e dunque il prodotto a sinistra in (3.11) non è ridotto.
Questo prova che $\{[x] \mid x \in X\}$ è un sistema libero di generatori di F (la cui cardinalità coincide con quella di X). ∎

A questo punto, possiamo finalmente e abbastanza agevolmente provare l'equivalenza delle definizioni.

Proposizione 3.4. *Le definizioni 1 e 2 di gruppo libero sono equivalenti.*

Dimostrazione. Sia F un gruppo libero su X secondo la Definizione 1, e sia $\tau : X \to F$ tale che $\tau(X)$ è un sistema libero di generatori di F. Ogni elemento $g \neq 1$ di F si scrive allora in maniera unica come una parola ridotta $g = \tau(x_1)^{\epsilon_1} \dots \tau(x_n)^{\epsilon_n}$, con $x_i \in X$ e $\epsilon_i \in \{-1, 1\}$. Sia G un gruppo e $f : X \to G$ un'applicazione; ponendo, per $g \in F$ come sopra,

$$\alpha(g) = f(x_1)^{\epsilon_1} \dots f(x_n)^{\epsilon_n} \tag{3.12}$$

si definisce un omomorfismo $\alpha : F \to G$. Poiché F è generato da $\tau(X)$ e per ogni $x \in X$, per definizione, $\alpha\tau(x) = f(x)$, si conclude che $\alpha\tau = f$. Che un tale omomorfismo α sia unico discende anche immediatamente dal fatto che, per ogni $x \in X$, $\alpha\tau(x) = f(x)$ e $\tau(X)$ genera F.

Viceversa, supponiamo che F sia un gruppo e che sia data $\tau : X \to F$ tali che sussiste la proprietà universale della Definizione 2. Sia $F(X)$ il gruppo libero definito a partire da X come nella costruzione di sopra; per cui possiamo interpretare univocamente gli elementi di $F(X)$ come le parola ridotte in $X \cup X^{-1}$. Per la proprietà universale assunta su F, esiste un omomorfismo $\alpha : F \to F(X)$ tale che $\alpha\tau = \iota$, dove ι è l'inclusione di X in $F(X)$. D'altra parte, per quanto provato sopra, esiste un omomorfismo $\beta : F(X) \to F$ tale che $\beta\iota = \tau$. Dunque, per ogni $x \in X \subseteq F(X)$,

$$\alpha\beta(x) = \alpha(\beta\iota(x)) = \alpha\tau(x) = \iota(x) = x.$$

Poiché $F(X)$ è generato da X e $\alpha\beta$ è un omomorfismo, si conclude che $\alpha\beta$ è l'identità su $F(X)$. Allo stesso modo, $\beta\alpha$ risulta un omomorfismo $F \to F$ che fissa ogni $\tau(x)$. Per l'unicità dell'applicazione che completa il diagramma (3.3) quando $G = F$ e $f = \tau$, si deduce che $\beta\alpha$ è l'identità su F. Quindi $\alpha : F \to F(X)$ è una biezione e dunque un isomorfismo. ∎

Esercizio 3.6. Sia F un gruppo libero su X. Per ogni $g \in F$ e $x \in X$ sia $\delta_x(g)$ la somma degli esponenti con cui compare il generatore x nell'espressione di g come parola (ridotta o no è lo stesso, perché?).

(a) Si provi che per ogni $g, h \in F$, $\delta_x(gh) = \delta_x(g) + \delta_x(h)$.

(b) Si provi che $F' = \{g \in F \mid \delta_x(g) = 0 \ \forall x \in X\}$.

Esercizio 3.7. Sia F un gruppo libero di rango 2; si provi che $F/F' \simeq \mathbb{Z} \times \mathbb{Z}$. Più in generale, si provi che se $F = F_n$ con n finito, allora $F/F' \simeq \mathbb{Z}^n$.

ESERCIZIO 3.8. Sia F un gruppo libero su $\{x, y\}$. Si provi che esiste un unico automorfismo ϕ di F tale che $\phi(x) = x$ e $\phi(y) = yx$; si provi quindi che ϕ non è un automorfismo interno.

ESERCIZIO 3.9. Sia X un insieme, $\emptyset \neq Y \subseteq X$, e sia $F = F(X)$ il gruppo libero su X. Si provi che F/Y^F è libero su $X \setminus Y$.

3.2. Sottogruppi di gruppi liberi

In questa sezione dimostreremo il fondamentale teorema (di Nielsen e Schreier) che afferma che ogni sottogruppo di un gruppo libero è un gruppo libero.

Proposizione 3.5. *Sia G un gruppo e sia $\emptyset \neq X \subseteq G$. Sono equivalenti:*

(1) *X è un sistema libero di generatori di G;*

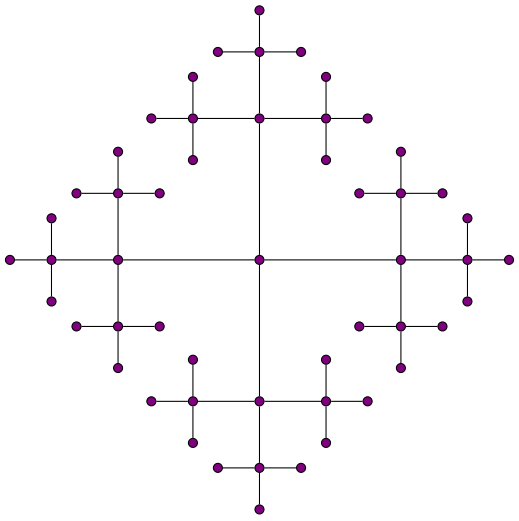
(2) *$X \cap X^{-1} = \emptyset$ e $\Gamma[G, X]$ è un albero.*

Dimostrazione. (1) $\Rightarrow$ (2). Sia G libero su X e $\Gamma = \Gamma[G, X]$. Poiché $G = \langle X \rangle$, Γ è connesso per il Lemma 2.7. Supponiamo, per assurdo, che Γ non sia un albero, e siano $g_1, g_2, \ldots, g_{n-1}, g_n = g_1$ i vertici di un circuito non banale $\mathcal{C}$ di Γ . Scegliendo $\mathcal{C}$ di lunghezza minima possiamo assumere $x_i \neq x_j$ per ogni $i \neq j$, $i, j \in \{1, \ldots, n-1\}$. Per ogni tale indice i, esiste $x_i \in X \cup X^{-1}$ tale che $g_{i+1} = g_i x_i$. Allora

$$g_1 = g_n = g_1 x_1 x_2 \ldots x_{n-1}$$

q quindi $x_1 x_2 \ldots x_{n-1} = 1$. Poiché X è un sistema libero di generatori deve esistere $i = 1, \ldots, n-2$ tale che $x_{i+1} = x_i^{-1}$. Ma allora $g_{i+1} = g_{i-1}$, una contraddizione.

(2) $\Rightarrow$ (1). Sia $X \cap X^{-1} = \emptyset$ e $\Gamma = \Gamma[G, X]$ un albero. Poiché Γ è connesso, X è un sistema di generatori di G. Supponiamo esistano $x_1, \ldots, x_n \in X \cup X^{-1}$ tali che $x_i x_{i+1} \neq 1$, per ogni $i = 1, \ldots n-1$, e $x_1 x_2 \cdots x_n = 1$. Ponendo, per ogni $1 \leq i \leq n$, $g_i = x_1 \cdots x_i$, si osserva che $1, g_1, g_2, \ldots g_n = 1$ sono i vertici di un circuito non banale in Γ, ul che è assurdo. Dunque X è un sistema libero di generatori di G. ∎



un pezzo del grafo di Cayley di F_2

Abbiamo ora una fondamentale caratterizzazione dei gruppi liberi.

Teorema 3.6. *Sia G un gruppo. Sono equivalenti*

1. *G è un gruppo libero:*
2. *G agisce liberamente e senza inversioni su un albero.*

Dimostrazione. [$1 \Rightarrow 2$]. Sia G gruppo libero sul sistema libero di generatori X. Allora, per la Proposizione 3.5, il grafo di Cayley $\Gamma = \Gamma[G, X]$ è un albero. Per la Proposizione 2.8 la moltiplicazione a sinistra descrive un'azione di G su Γ, che chiaramente non ha vertici fissi. Sia $e = \{u, v\}$ un arco di Γ, allora $v = ux$ con $x \in X \cup X^{-1}$. Supponiamo, per assurdo, che esista $1 \neq g \in G$ tale che $e = g \cdot e$; allora $gu = ux$ e $gux = u$, da cui $u = gux = ux^2$ da cui l'assurdo $x^2 = 1$. Quindi G opera liberamente e senza inversioni su Γ.

[$2 \Rightarrow 1$]. Supponiamo che il gruppo G operi liberamente sull'albero Γ. Sia T un sottoalbero delle orbite come nella Proposizione 2.5; quindi T contiene esattamente un vertice in ognuna delle orbite di G su $V(\Gamma)$. Sia Γ_T il grafo associato, l'insieme dei cui vertici è l'insieme $\{gT \mid g \in G\}$ - vedi (2.2). Per la Proposizione 2.6, Γ_T è un albero, e l'azione di G su Γ induce un'azione su Γ_T che è libera, senza inversioni, e transitiva sui vertici. Per la Proposizione 2.9, Γ_T è isomorfo ad un grafo di Cayley su G ed infine, per la Proposizione 3.5, G è un gruppo libero. ∎

Sia F un gruppo libero. Allora, per il Teorema 3.6, F opera liberamente su un albero Γ; ne segue che ogni sottogruppo di F opera liberamente su Γ e dunque è libero. Si ha quindi il seguente importante risultato.

Teorema 3.7. *Ogni sottogruppo di un gruppo libero è libero.*

Nel caso di gruppi liberi di rango finito, è possibile raffinare quantitativamente la dimostrazione per ottenere il seguente risultato.

Teorema 3.8. (Nielsen–Schreier) *Sia F un gruppo libero di rango finito n, e sia $H \leq F$ un sottogruppo di indice finito $|F : H| = m$. Allora H è un gruppo libero ed il suo rango è $nm + 1 - m$.*

Dimostrazione. Sia $F = F_n$ il gruppo libero di rango (finito) n e sia Γ l'albero regolare di grado $2n$ che è il grafo di Cayley per F_n rispetto ad un sistema libero di generatori. Sia $H \leq F_n$, allora H agisce (per restrizione) in modo libero e senza inversioni su Γ. Elementi $g, g' \in F_n = V(\Gamma$ appartengono ad orbite distinte per l'azione di H se e solo se $Hg \neq Hg'$, le orbite di H sono quindi in corrispondenza biunivoca con le classi laterali destre di F_n modulo H. Sia $[F_n : H] = m < \infty$, e sia T un sottoalbero delle orbite per H su Γ e Γ_T il grafo associato. Come nella dimostrazione del Teorema precedente, Γ_T è un albero regolare e H è un gruppo libero il cui rango è uguale alla metà del grado di un qualsiasi vertice (ad esempio, T) di Γ_T. Ora, tale grado è uguale al numero di archi in Γ che hanno un vertice in T e l'altro fuori di T, che è quindi

$$d = \sum_{x \in V(T)} 2n - 2|E(T)|.$$

Ma, per quanto detto prima, T ha m vertici e dunque, per la Proposizione 2.2 , $m - 1$ archi; si ha allora

$$d = 2n|V(T)| - 2|E(T)| = 2nm - 2(m + 1).$$

Quindi H è un gruppo libero di rango $nm - m + 1$. ∎

Esercizio 3.10. Sia F_2 il gruppo libero di rango due. Si trovino tre elementi di F_2 tali che il sottogruppo da essi generato sia libero di rango 3.

Esercizio 3.11. Sia F un gruppo libero e sia $1 \neq a \in F$.

1. Si provi che $C_F(a) = \{g \in F \mid ga = ag\}$ è un gruppo ciclico. Dedurre che se $rk(F) \geq 2$ allora $Z(F) = 1$.
2. Si provi che esiste $n \geq 1$ tale che per ogni $m > n$ non esiste alcun $b \in F$ tale che $b^m = a$.

Esercizio 3.12. Si trovi una dimostrazione del Teorema 1.9 utilizzando il Teorema 3.8.

Esercizio 3.13. Si descriva un sottogruppo del gruppo libero F_2 che abbia rango infinito.

Esercizio 3.14. Sia F un gruppo libero di rango almeno 2. Si provi che il sottogruppo derivato F' ha rango infinito, e che il gruppo abeliano F/F' è torsion-free.

Esercizio 3.15. Siano F, F' gruppi liberi di rango finito; si provi che F, F' hanno lo stesso rango se e solo se esistono sistemi di generatori S di F e S' di F' tali che $\Gamma[F, S] \simeq \Gamma[F', S']$.

3.3. Presentazioni di gruppi

Sia G un gruppo; siano X un sistema di generatori di G, e $F(X)$ il gruppo libero su X. Applicando la proprietà universale di $F(X)$, con $f : X \to G$ l'immersione di X in G, si conclude che esiste un unico omomorfismo

$$\phi : F(X) \to G \quad \text{tale che} \quad \phi(\tau(x)) = x \text{ per ogni } x \in X, \tag{3.13}$$

dove, al solito, τ è l'immersione $X \to F(X)$. Poiché G è generato da X, ϕ è suriettivo e, per il Teorema di omomorfismo,

$$G \simeq F(X)/\ker(\phi). \tag{3.14}$$

Quindi, in particolare: *ogni gruppo è immagine omomorfa di un gruppo libero.* Un isomorfismo come in (3.14) è ciò che si chiama una *presentazione* del gruppo G, e gli elementi di $\ker(\phi)$ sono dette le *relazioni* della presentazione.

Illustriamo ora il modo con cui viene in genere definita una presentazione. Sia ϕ come in (3.13) e sia R un sottoinsieme di $\ker(\phi)$ tale che $\langle R \rangle^{F(X)} = \ker(\phi)$, allora la presentazione (3.14) si descrive come

$$G = \langle \tau(X) \mid R \rangle. \tag{3.15}$$

Nella pratica, spesso - e noi così faremo - si identifica x con $\tau(x)$ (per ogni $x \in X$) e si specificano gli elementi di R in quanto inducenti relazioni nel gruppo G, ovvero invece di (3.15), si preferisce scrivere la presentazione come

$$G = \langle X \mid \phi(r) = 1,\ r \in R \rangle. \tag{3.16}$$

Ad esempio, per ogni $n \geq 1$, $\langle x \mid x^n = 1 \rangle$ è una presentazione del gruppo ciclico di ordine n, mentre $\langle x, y \mid xy = yx \rangle = \langle x, y \mid xyx^{-1}y^{-1} = 1 \rangle$ è una presentazione del prodotto diretto $\mathbb{Z} \times \mathbb{Z}$.

Teorema 3.9. (von Dyck) *Siano G e H due gruppi con presentazioni $G = \langle X \mid R\rangle$ e $H = \langle X \mid S\rangle$. Se $R \subseteq S$ allora H è isomorfo ad un quoziente di G.*

Dimostrazione. Sia $F = F(X)$ e siano $\phi : F \to G$ e $\psi : F \to H$ gli omomorfismi sottesi dalle due presentazioni nell'enunciato. Allora $\ker(\phi) = R^F \leq S^F = \ker(\psi)$ e dunque H è isomorfo $F/\ker(\psi)$ che è isomorfo ad un quoziente di $F/\ker(\phi) \simeq G$. ∎

Esempio 3.1. Il gruppo $D_\infty = \langle x, y \mid x^2 = 1,\ y^2 = 1\rangle$ è il gruppo diedrale infinito. Infatti, ponendo $a = yx$, si ha $D_\infty = \langle a, x\rangle$ e $a^x = xyxx^{-1} = xy = a^{-1} = a^y$. Quindi $\langle a\rangle \trianglelefteq D_\infty$, e possiamo identificare D_∞ con il prodotto semidiretto $\langle a\rangle \rtimes \langle x\rangle$, con $|a| = \infty$, $|x| = 2$, e $a^x = a^{-1}$. In effetti, un'altra presentazione per il gruppo D_∞ è $\langle x, y \mid x^2 = 1,\ y^x = y^{-1}\rangle$.
Sia $n \geq 2$ un intero; allora (lo si provi per esercizio) $\langle x, y \mid x^2 = 1,\ y^2 = 1,\ (xy)^n = 1\rangle$ e $\langle x, y \mid x^2 = 1,\ y^n = 1,\ y^x = y^{-1}\rangle$, sono due presentazioni del gruppo diedrale D_{2n}. □

Esempio 3.2. Siano $a, b \in \mathbb{N}$ diversi da 0 e coprimi, e sia

$$G = \langle x, y \mid xy^{-1}x^{-1}y^{a+1} = 1,\ yx^{-1}y^{-1}x^{b+1} = 1\rangle.$$

Dalle relazioni segue $(y^{-1})^x = xy^{-1}x^{-1} = (y^{a+1})^{-1}$ e quindi $y^x = y^{a+1}$; similmente si trova $x^y = x^{b+1}$; quindi

$$z := x^b = x^y x^{-1} = y(y^{-1})^x = y^{-a};$$

in particolare, z commuta con y. Allora,

$$z = z^y = (x^b)^y = (x^y)^b = (x^{b+1})^b = (x^b)^{b+1} = z^{b+1} = z^b z,$$

da cui $z^b = 1$. Allo stesso modo $z^a = 1$. Poiché $(a, b) = 1$, risulta $z = 1$. Quindi

$$x^b = 1 = y^a,\quad x^y = x,\quad y^x = y.$$

Dunque $[x, y] = 1$, e pertanto $G = \langle x\rangle \times \langle y\rangle \simeq C_b \times C_a$. □

Dato un gruppo non è in genere facile trovare una sua presentazione; viceversa, non è facile dedurre le proprietà di un gruppo a partire da una sua presentazione. Il ricorso al Teorema 3.9 è efficace quando, data una presentazione $G = \langle X \mid R\rangle$ si riesce a trovare un gruppo H ed un suo sistema di generatori in modo che le relazioni R siano soddisfatte; allora si deduce che H è (isomorfo a) un quoziente di G.

Esempio 3.3. Consideriamo il gruppo $G = \langle x, y \mid y^x = y^2\rangle$. Sia $Q = H \rtimes \langle\alpha\rangle$ dove H è il gruppo dei numeri razionali il cui denominatore è una potenza di 2 e α la moltiplicazione per 2; allora Q soddisfa la presentazione con $y = 1 \in \mathbb{Z} \leq H$, $x = \alpha$ (e messo in notazione moltiplicativa); quindi Q è un quoziente di G; detto meglio, esiste un omomorfismo suriettivo $\pi : G \to Q$ tale che $\pi(y) = 1$ e $\pi(x) = \alpha$; in particolare $|x| = |y| = \infty$. Ora, per ogni $n \in \mathbb{N}$ si ha $y^{x^n} = 2^n y$, quindi, per ogni $n, m \in \mathbb{Z}$, con $n \geq m$,

$$[y^{x^n}, y^{x^m}] = [y^{x^{n-m}}, y]^{x^m} = [2^{n-m}y, y]^{x^m} = 1,$$

e quindi $N = \langle y\rangle^G = \langle y^{x^z} \mid z \in \mathbb{Z}\rangle = \langle 2^z y \mid z \in \mathbb{Z}\rangle$ è abeliano, e $G = N \rtimes \langle x\rangle$. Ogni numero razionale in H si scrive in modo unico nella forma $z2^i$ con $z, i \in \mathbb{Z}$ e z dispari; per tali numeri si pone $z2^i \mapsto (y^z)^{x^i}$ e si verifica senza difficoltà che ciò stabilisce un omomorfismo $\phi : H \to N$, la cui immagine $\phi(H)$ contiene y ed è normalizzata da x. Quindi, $N = \phi(H)$, e ϕ si estende ad un omomorfismo suriettivo $Q \to G$ con $\phi(x) = \alpha$. A questo punto si trova che ϕ e π sono uno inverso dell'altro, e che dunque $G \simeq Q$. □

Presentazione del gruppo simmetrico. Nei casi in cui, data una presentazione di un gruppo G, si riesce a provare che $|G| \leq n$, e quindi si trova un gruppo H che soddisfa le stesse relazioni ed è tale che $|H| = n$, si deve concludere che $H \simeq G$. Questa procedura è applicata nella seguente proposizione, che fornisce una presentazione dei gruppi simmetrici finiti.

Proposizione 3.10. *Sia $n \geq 2$. Allora*

$$S_n = \langle x_1, \dots, x_{n-1} \mid x_i^2 = (x_j x_{j+1})^3 = (x_k x_\ell)^2 = 1 \rangle. \tag{3.17}$$

dove $1 \leq i \leq n-1,\ 1 \leq j \leq n-2$ e $1 \leq \ell < k-1 < n-1$.

Dimostrazione. Sia G il gruppo la cui presentazione è il termine a destra di (3.17). Proviamo, per induzione su n, che $|G| \leq n!$.
Per $n = 2$ si ha che $G = \langle x_1, x_2 \mid x_1^2 = x_2^2 = (x_1 x_2)^3 = 1 \rangle$ è il gruppo diedrale di ordine 6, ovvero S_3. Sia $n \geq 3$ e sia H il sottogruppo di G generato da $\{x_1, \dots, x_{n-2}\}$. Per ipotesi induttiva, $|H| \leq (n-1)!$. È dunque sufficiente provare che $|G : H| \leq n$. Consideriamo l'azione di G per moltiplicazione a destra sull'insieme della classi laterali destre di H in G. Siano $i, j \in \{1, \dots, n-1\}$.
- Se $j < i-1$ allora $(x_s x_j)^2 = 1$, dunque $x_s x_j = x_j x_s$ per ogni $s \geq i$, e quindi (poiché $j < n-1$ e dunque $x_j \in H$),

$$(H x_{n-1} \dots x_i) x_j = H x_j x_{n-1} \dots x_i = H x_{n-1} \dots x_i.$$

- Se $j > i$, allora $x_k x_j = x_j x_k$ per $|j-k| > 1$, inoltre $(x_{j-1} x_j)^3 = 1$ da cui segue subito $x_{j-1} x_j x_{j-1} = x_j x_{j-1} x_j$; quindi

$$\begin{aligned} (H x_{n-1} \dots x_i) x_j &= H x_{n-1} \dots x_{j+1} (x_j x_{j-1} x_j) x_{j-2} \dots x_i = \\ &= H x_{n-1} \dots x_{j+1} (x_{j-1} x_j x_{j-1}) x_{j-2} \dots x_i \\ &= H x_{j-1} x_{n-1} \dots x_i = H x_{n-1} \dots x_i. \end{aligned}$$

- Infine, nei casi $j = i$ e $j = i-1$ si ha, rispettivamente,

$$(H x_{n-1} \dots x_i) x_j = H x_{n-1} \dots x_{i+1} \quad \text{e}$$
$$(H x_{n-1} \dots x_i) x_j = H x_{n-1} \dots x_i x_{i-1}.$$

Tenendo conto che gli elementi x_j (con $j = 1, \dots, n-1$) generano G, si conclude che l'insieme di classi laterali $\Omega = \{H, H x_{n-1}, H x_{n-1} x_{n-2}, \dots, H x_{n-1} x_{n-2} \dots x_1\}$ è invariante per l'azione di G; siccome tale azione è transitiva, si conclude che Ω è l'insieme di tutte le classi laterali destre di H in G. Quindi $|G : H| = |\Omega| \leq n$, che è quel che si voleva. Dunque, $|G| \leq n!$.
A questo punto si osserva che, posto per ogni $i = 1, \dots, n-1$, $x_i = (i\ i+1)$, allora $S_n = \langle x_1, \dots, x_{n-1} \rangle$ e gli elementi x_i soddisfano le relazioni che definiscono G. Per il Teorema 3.9, si deduce che S_n è isomorfo ad un quoziente di G. Poiché $|S_n| = n! \geq |G|$, si conclude che $|G| = n!$ e $G \simeq S_n$. ∎

Esercizio 3.16. Sia p un primo, si provi che il gruppo con presentazione

$$\langle x, y \mid x^p = y^p = x^{-2} y^{-1} x y = 1 \rangle$$

è il gruppo ciclico di ordine p.

Esercizio 3.17. Sia $p \geq 3$ un primo. Si provi che il gruppo

$$G = \langle x, y \mid x^p = y^p = (xy)^p = 1 \rangle$$

è infinito (mentre, per $p = 2$, il gruppo è abeliano di ordine 4). [sugg. Detta $\omega = 2^{\frac{2\pi i}{p}}$ una radice primitiva p-esima dell'unità, si considerino le trasformazioni del piano complesso f, g definite da, per ogni $z \in \mathbb{C}$, $f : z \mapsto \omega z$ e $g : z \mapsto \omega z + 1$ e sia $H = \langle f, g \rangle$. Si provi che $f^p = g^p = (fg)^p = 1$, quindi $H \dots$]

Esercizio 3.18. Si provi che il gruppo dato dalla presentazione

$$\langle x_1, x_2, x_3, \dots \mid x_{n+1}^{n+1} = x_n, \forall n \geq 1 \rangle$$

è il gruppo additivo $(\mathbb{Q}, +)$.

Esercizio 3.19. Sia $G = \langle X \mid R \rangle$ con $|X| = n < \infty$; si provi che se $|R| < n$ allora G è infinito. [sugg.: se $F = F(X)$ e K è il nucleo dell'omomorfismo $F(X) \to G$ allora $K = \langle R \rangle (K \cap F')$, quindi $d(K/(K \cap F')) \leq |R|$, mentre se G è finito ...]

Esercizio 3.20. Sia F un gruppo libero di rango finito. Si provi che F non è isomorfo ad un suo quoziente proprio.

Gruppi finitamente presentati. Un caso particolarmente interessante di presentazioni è costituito da quelle finite; dove una presentazione $G = \langle X \mid R \rangle$ si dice finita se sia X che R sono finiti, Un gruppo che ammette una presentazione finita si dice *finitamente presentato*. Per dire una delle ragioni di interesse di cui sopra, il gruppo fondamentale di ogni varietà topologica compatta è finitamente presentato.
Ogni gruppo finito è (ovviamente) finitamente presentato: la tavola di moltiplicazione di un gruppo finito fornisce infatti relazioni sufficienti a presentarlo (un'altra dimostrazione viene applicando il Teorema 1.9); ed è finitamente presentato ogni gruppo libero finitamente generato. L'esempio 3.3 mostra come sottogruppi normali di gruppi finitamente presentati non siano necessariamente finitamente generati. In effetti, quasi tutti gli esempi di presentazione di gruppi finitamente generati che abbiamo esaminato sin qui hanno riguardato presentazioni finite; un'eccezione la presentazione del gruppo del Lampionaio L_2 nell'esercizio 3.21; in effetti, i gruppi del lampionaio sono esempi di gruppi finitamente generati non finitamente presentati.
Per la dimostrazione ci serviremo al passo iniziale della seguente osservazione, della quale tralasciamo la dimostrazione (che non è difficile).

Proposizione 3.11. *Sia G un gruppo finitamente presentato. Per ogni sistema di generatori X di G esiste un sottoinsieme finito $Y \subseteq X$ tale che G ha un presentazione finita nei generatori Y.*

Proviamo ora che il gruppo del Lampionaio $L_2 = \mathbb{Z}_2 \wr \mathbb{Z}$ (sezione 2.7) non è finitamente presentato. Per l'esercizio 3.21 L_2 ha la seguente presentazione

$$L_2 = \langle a, x \mid a^2 = 1,\ a^{x^n} a = a^{x^n} a\ \forall n \in \mathbb{Z} \rangle, \tag{3.18}$$

dove $\langle x \rangle = \mathbb{Z}$ è il complemento e $a \neq 0$ un elemento della base. Supponiamo, per assurdo, che L_2 sia finitamente presentato. Esisterebbe allora, per la Proposizione 3.11, una presentazione finita, con relazioni, diciamo $r_1, \dots, r_n$, negli stessi generatori a, x. Ogni relazione r_j è una conseguenza delle relazioni in (3.18), cioè un prodotto di un numero finito di tali relazioni o loro coniugati nel gruppo libero generato da a ed x; poiché il numero delle r_j è finito, è possibile selezionare un insieme finito S di relazioni in (3.18) tale che ogni r_j è conseguenza di relazioni in S. Allora, esiste $t \in \mathbb{N}$, tale che $S \subseteq \{a^2\} \cup \{a^{x^i} a (a a^{x^i})^{-1} \mid -t \leq i \leq t\}$. Per il Lemma di von Dyck, L_2 ammette un quoziente isomorfo al gruppo

$$H = \langle a, x \mid a^2 = 1,\ a^{x^i} a = a^{x^i} a\ (-t \leq i \leq t) \rangle. \tag{3.19}$$

Deriveremo un assurdo, provando che L_2 non può avere un tale quoziente.

Sia $n = 2t + 3$ e, nel gruppo simmetrico S_n, consideriamo i due elementi $a = (1\,2)$ e $x = (1\ 3 \dots n-2\ n\ 2\ 4 \dots n-1)$. Si ha $a^2 = 1$ e, con facile induzione,

$$a^x = (3\,4),\ a^{x^2} = (5\,6), \dots, a^{x^t} = (2t+1\ 2t+2) = (n-2\ n-1).$$

Quindi, per ogni $1 \leq i \leq t$, a^{x^i} commuta con a, dunque sono soddisfatte le relazioni in (3.19) e $\langle a, x\rangle$ è isomorfo ad un quoziente di H. Ma $a^{x^{t+1}} = (n\,1)$, $a^{x^{t+12}} = (2\,3), \dots$ e non è difficile provare che $\langle a, x\rangle = S_n$, che non può essere isomorfo ad un quoziente di L_2 perché (dato che $n \geq 3$) il derivato di S_n non è un 2-gruppo abeliano. A maggior ragione H in (3.19) non è isomorfo ad un queoziente di L_2, e dunque L_2 non è finitamente presentato.

Esercizio 3.21. Si provi che

$$\langle a, x \mid a^2 = 1,\ a^{x^n} a = a^{x^n} a\ \forall n \geq 1\rangle$$

è una presentazione del gruppo del Lampionaio L_2.

Esercizio 3.22. Sia G un gruppo e H un sottogruppo di indice finito di G. Si provi che G è finitamente presentato se e solo se H è finitamente presentato.

Esercizio 3.23. Siano G un gruppo finitamente presentato e $N \trianglelefteq G$; si provi che se N è finitamente generato allora G/N è finitamente presentato.

3.4. Esempi. Lemma del Ping-Pong

Per ogni insieme X abbiamo costruito in modo astratto un gruppo libero su X. Vediamo ora, mediante alcuni esempi, come i gruppi liberi non ciclici si trovino (e anche con una certa frequenza) "in natura". Per provare che un certo gruppo è libero, un criterio semplice ma molto efficace è il *Lemma del Ping–Pong*, che fu sostanzialmente applicato già da Felix Klein. Quella che vediamo è la sua versione basica.

Lemma 3.12. *Sia G un gruppo che agisce sull'insieme Ω, e siano $x, y \in G$. Supponiamo esistano sottoinsiemi non vuoti Ω_1, Ω_2 di Ω tali che $\Omega_1 \not\subseteq \Omega_2$, e*

$$x^z \cdot \Omega_1 \subseteq \Omega_2, \qquad y^z \cdot \Omega_2 \subseteq \Omega_1,$$

per ogni $0 \neq z \in \mathbb{Z}$. Allora $\langle x, y\rangle$ è un gruppo libero su $\{x, y\}$.

Dimostrazione. Nel gruppo $\langle x, y\rangle$ consideriamo un prodotto del tipo (1.12), dove quindi, per ogni indice $i = 1, \dots, n$, $x_i \in \{x, y\}$. Distinguiamo vari casi, cominciando da quello in cui il primo e l'ultimo generatore che compaiono nel prodotto sia x; ovvero, $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_{n-1}} y^{\beta_{n-1}} x^{\alpha_n}$, con $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{n-1} \in \mathbb{Z} \setminus \{0\}$. Allora

$$w \cdot \Omega_1 = x^{\alpha_1} y^{\beta_1} \dots y^{\beta_{n-1}} \cdot (x^{\alpha_1} \cdot \Omega_1) \subseteq x^{\alpha_1} \dots (y^{\beta_{n-1}} \cdot \Omega_2) \subseteq \dots \subseteq x^{\alpha_1} \cdot \Omega_1 \subseteq \Omega_2$$

e poiché $\Omega_1 \not\subseteq \Omega_2$, si conclude che w non agisce come l'identità, e quindi $w \neq 1$.
Supponiamo ora $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_n} y^{\beta_n}$; allora scelto un intero $0 \neq z \neq alpha_1$, si ha che $w^{x^z} = x^z w x^{-z}$ è un elemento del tipo analizzato sopra. Quindi $w^{x^z} \neq 1$ e dunque $w \neq 1$. Nei casi rimanenti, ovvero, $w = y^{\beta_1} \dots y^{\beta_{n-1}} x^{\alpha_n}$ e $w = y^{\beta_1} \dots x^{\alpha_n} y^{\beta_n}$ si procede in modo analogo. ∎

Esempio 3.4. Il gruppo $G = GL(2,\mathbb{R})$ opera in modo naturale sull'insieme dei punti di $\mathbb{R}^2$; se $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ e $(\alpha,\beta) \in \mathbb{R}^2$,

$$A \cdot (\alpha,\beta) = A\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = (a\alpha + b\beta, c\alpha + d\beta). \tag{3.20}$$

In G consideriamo gli elementi

$$x = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Si verifica facilmente che, per ogni $z \in \mathbb{Z}$,

$$x^z = \begin{pmatrix} 1 & 2z \\ 0 & 1 \end{pmatrix} \qquad \text{e} \qquad y^z = \begin{pmatrix} 1 & 0 \\ 2z & 1 \end{pmatrix}.$$

Posto $\Omega_1 = \{(\alpha,\beta) \in \mathbb{R}^2 \mid |\alpha| < |\beta|\}$ e $\Omega_2 = \{(\alpha,\beta) \in \mathbb{R}^2 \mid |\alpha| > |\beta|\}$, sia $(\alpha,\beta) \in \Omega_1$ e $0 \neq z \in \mathbb{Z}$. Allora, per (3.20), $x^z(\alpha,\beta) = (\alpha + 2z\beta, \beta)$, e si ha

$$|\alpha + 2z\beta| > \big||2z\beta| - |\alpha|\big| = 2|z||\beta| - |\alpha| > (2|z| - 1)|\alpha| > |\beta|,$$

e dunque $(\alpha + 2z\beta, \beta) \in \Omega_2$. Quindi $x^z\Omega_1 \subseteq \Omega_2$. In maniera analoga si prova che, per ogni $0 \neq z \in \mathbb{Z}$, $y^z\Omega_2 \subseteq \Omega_1$. Per il Lemma del Ping–Pong si conclude che il gruppo $\langle x, y\rangle$ è libero nei generatori x e y.
Osserviamo che questo gruppo $G = \langle x, y\rangle$ è un sottogruppo di $SL(2,\mathbb{Z})$. Non è difficile provare (vedi esercizio 3.27) che l'indice $[SL(2,\mathbb{Z}) : G]$ è finito, quindi $SL(2,\mathbb{Z})$ è virtualmente un gruppo libero (cioè ha un sottogruppo libero di indice finito, vedi anche l'esercizio 3.29). □

In questo ambito citiamo, senza dimostrazione, un importante risultato generale dovuto a J. Tits (ricordo che un gruppo G è *risolubile* se esiste una catena finita di sottogruppi $1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$ con G_{i-1}/G_i abeliano per ogni $i = 1, \ldots n$).

Teorema 3.13 (Tits alternative)**.** *Siano F un campo, $1 \leq n \in \mathbb{N}$ e G un sottogruppo di $GL(n,F)$. Allora G contiene un sottogruppo libero di rango almeno due oppure un sottogruppo risolublie di indice finito.*

Il nostro prossimo esemplare è un sottogruppo del gruppo degli omeomorfismi della retta reale o, anche, del gruppo degli automorfismi $Aut(\mathbb{R},\leq)$ dell'insieme ordinato dei reali, ed è tratto da un articolo di C. Bennett [1].

Esempio 3.5. Si consideri la funzione lineare a tratti $\phi : [0,1] \to [0,1]$, definita da

$$\phi(x) = \begin{cases} 4x & \text{se} \quad 0 \leq x \leq 1/5 \\ x/4 + 3/4 & \text{se} \quad 1/5 \leq x \leq 1 \end{cases}$$

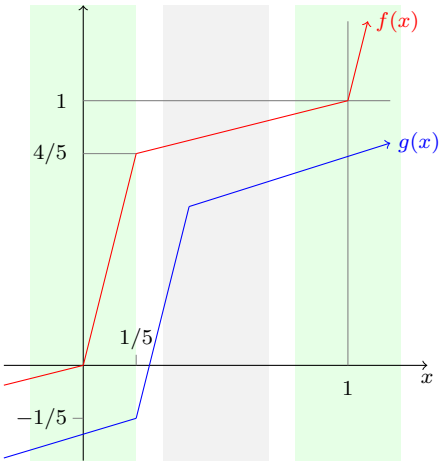
Sia quindi $f : \mathbb{R} \to \mathbb{R}$ definita da, per ogni $x \in \mathbb{R}$,

$$f(x) = [x] + \phi(x - [x]),$$

dove $[x]$ è la parte intera di x. Infine sia $g = \tau^{-1} f \tau$ dove τ è la traslazione, $x \mapsto x - 1/2$ (per ogni $x \in \mathbb{R}$); cioè

$$g(x) = f(x - 1/2) + 1/2.$$

Allora $\{f, g\} \subseteq Aut(\mathbb{R},\leq)$.



Siano

$$\Omega_1 = \bigcup_{u\in\mathbb{Z}} \left(u + \frac{3}{10}, u + \frac{7}{10}\right) \quad \text{e} \quad \Omega_2 = \bigcup_{u\in\mathbb{Z}} \left(u - \frac{1}{5}, u + \frac{1}{5}\right).$$

Allora, per ogni $0 \neq z \in \mathbb{Z}$ si ha

$$f^z(\Omega_1) \subseteq \Omega_2 \qquad \text{e} \qquad g^z(\Omega_2) \subseteq \Omega_1$$

(nella figura, Ω_1 sono le ascisse delle zone grigie, Ω_2 quelle delle zone verdi; lascerei poi al lettore che lo desideri svolgere le verifiche, non difficili, oppure consultare [1]). Per il Lemma del Ping–Pong si conclude quindi che $\langle f, g\rangle$ è un gruppo liberamente generato da f e g. □

Esercizio 3.24. Si provi che il sottogruppo di $SL(2,\mathbb{R})$,

$$G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$$

non è un gruppo libero.

Esercizio 3.25. Sia Z il gruppo delle matrici scalari non nulle di $SL(2,\mathbb{C})$. Allora, il gruppo $G = PSL(2,\mathbb{C}) = SL(2,\mathbb{C})/Z$ opera sulla sfera $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, mediante

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az + b}{cz + d}.$$

Applicando il Lemma del Ping–Pong a tale azione, si trovi un sottogruppo di G che è un gruppo libero di rango 2.

Esercizio 3.26. Generalizzando in modo opportuno il Lemma del Ping–Pong, si trovi un sottogruppo di $PSL(2,\mathbb{C})$ che sia libero di rango 3.

Esercizio 3.27. Sia $\pi_2 : SL(2,\mathbb{Z}) \to SL(2,\mathbb{Z}/2\mathbb{Z})$ l'omomorfismo di riduzione modulo 2, cioè:

$$\pi_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + 2\mathbb{Z} & b + 2\mathbb{Z} \\ c + 2\mathbb{Z} & d + 2\mathbb{Z} \end{pmatrix}.$$

e sia $G_2 = \ker(\pi_2)$. Siano quindi $x, y \in SL(2,\mathbb{Z})$ come nell'esempio 3.4 e $G = \langle x, y\rangle$.

(1) Si provi che $[SL(2,\mathbb{Z}) : G_2] = 6$.

(2) Sia $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_2 \middle| a \equiv 1 (\mathrm{mod}\ 4) \right\}$; si provi che H è un sottogruppo di G_2 e che $[G_2 : H] = 2$.

(3) Si provi che $H = G$ (questo è impegnativo ed un po' laborioso), concludendo che $[SL(2,\mathbb{Z}) : G] = 12$.

Esercizio 3.28. Si provi che il gruppo G_2 dell'esercizio precedente non è libero.

Esercizio 3.29. Si provi che $SL(3,\mathbb{Z})$ non è virtualmente libero [sugg.: si assuma che esista un sottogruppo libero F di $G = SL(3,\mathbb{Z})$ tale che $[G : F]$ è finito. Per il Teorema 3.7 si può supporre $F \trianglelefteq G$ e dedurre che esiste $n \geq 1$ tale che

$$A = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

appartiene a F; si studi quindi il centralizzante di A in G e si arrivi ad una contraddizione – vedi punto 1 dell'esercizio 3.11].

3.5. $SL(2,\mathbb{Z})$ e il grafo di Farey

Continuiamo ad occuparci di sottogruppi di $SL(2,\mathbb{Z})$. Per ogni intero $m \geq 2$, sia $SL(2,\mathbb{Z})[m]$ il nucleo dell'omomorfismo di riduzione modulo m,

$$\pi_m : SL(2,\mathbb{Z}) \to SL(2,\mathbb{Z}/m\mathbb{Z}).$$

Proveremo che, per $m \geq 3$, $SL(2,\mathbb{Z})[m]$ è un gruppo libero (dagli esercizi 3.27 e 3.28 segue che $SL(2,\mathbb{Z})[2]$ non è libero ma ha un sottogruppo libero di indice 2). Questa volta, lo faremo applicando il Teorema 3.6; per prima cosa, dunque, ci procuriamo un albero opportuno, l'*albero di Farey*, un oggetto, oltre che bello, ubiquo in matematica.

Una coppia ordinata di numeri interi (p,q) è *primitiva* se p e q sono coprimi, cioè se $mcd(p,q) = 1$. Sull'insieme delle coppie primitive in $\mathbb{Z}^2$ si definisce un'equivalenza stabilendo che (p,q) è in relazione con $\pm(p,q)$. L'insieme quoziente

$$\mathbb{V} = \frac{\{(p,q) \in \mathbb{Z}^2 \mid (p,q) \text{ primitiva}\}}{\pm},$$

i cui elementi denotiamo con $\frac{p}{q}$, è l'insieme dei vertici del grafo di Farey $\mathcal{F}$. Si osservi che, poiché per ogni intero n si ha $mcd(n,0) = |n|$, $\frac{0}{1} = \frac{0}{-1}$ e $\frac{1}{0} = \frac{-1}{0}$ sono i due soli vertici in cui una componente è uguale a 0; in effetti, $\mathbb{V}$ si può identificare con l'insieme $\mathbb{Q} \cup \{\infty\}$, dove ∞ è rappresentato dalla classe $\frac{1}{0} = \frac{-1}{0}$ e il numero 0 da $\frac{0}{1} = \frac{0}{-1}$.
Due vertici $\frac{p}{q}$, $\frac{r}{s}$ sono adiacenti in $\mathcal{F}$ se $|ps - qr| = 1$, ovvero se

$$\det \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \pm 1$$

(è chiaro che questa è una buona definizione).

Prima di descrivere geometricamente il grafo $\mathcal{F}$, definiamo l'azione del gruppo $SL(2,\mathbb{Z})$ su di esso, che è quella, naturale, indotta dall'azione su $\mathbb{V} = \mathbb{Q} \cup \{\infty\}$ mediante *trasformazioni di Möbius* (esercizio 3.25): se $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ e $\frac{p}{q} \in \mathbb{V}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{p}{q} = \frac{ap + bq}{cp + dq} = \frac{a(p/q) + b}{c(p/q) + d}.$$

Il nucleo Z di tale azione è l'insieme delle matrici scalari in $SL(2,\mathbb{Z})$, quindi[1]

$$Z = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Questa azione è un'azione sul grafo $\mathcal{F}$. Infatti se $\frac{p}{q}, \frac{r}{s}$ sono vertici adiacenti allora, per definizione, $|ps - qr| = 1$; quindi per ogni $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$,

$$\det \begin{pmatrix} ap + bq & ar + bs \\ ccp + dq & cr + ds \end{pmatrix} = \det \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} \right) = \det \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \pm 1,$$

dunque $A \cdot \frac{p}{q}$ è adiacente in $\mathcal{F}$ ad $A \cdot \frac{r}{s}$.

L'azione è transitiva sui vertici. Se (p, q) è una coppia primitiva di interi esistono $b, d \in \mathbb{Z}$ tali che $pd - qb = 1$, e allora

$$\begin{pmatrix} p & b \\ q & d \end{pmatrix} \cdot \frac{1}{0} = \frac{p}{q};$$

dunque l'orbita di $\frac{1}{0}$ è tutto l'insieme $\mathbb{V}$ e quindi l'azione è transitiva.

Stabilizzatori dei vertici. Poiché l'azione su $\mathbb{V}$ è transitiva, gli stabilizzatori sono coniugati dello stabilizzatore del punto $\frac{1}{0}$, che è

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \,\middle|\, a = \pm 1, b \in \mathbb{Z} \right\}. \tag{3.21}$$

L'azione è transitiva sugli archi. SI osservi che i vertici adiacenti in $\mathcal{F}$ a $\infty = \frac{1}{0}$ sono tutte e sole le frazioni $\frac{n}{1}$ con $n \in \mathbb{Z}$. Ora, per ogni $n, m \in \mathbb{Z}$, $\begin{pmatrix} 1 & n - m \\ 0 & 1 \end{pmatrix} \in H$ e

$$\frac{n}{1} = \begin{pmatrix} 1 & n - m \\ 0 & 1 \end{pmatrix} \cdot \frac{m}{1}.$$

Quindi H, lo stabilizzatore di $\frac{1}{0}$, è transitivo sull'insieme dei vertici adiacenti a $\frac{1}{0}$, dunque è transitivo sull'insieme degli archi incidenti $\frac{0}{1}$. Per la transitività dell'azione di $SL(2,\mathbb{Z})$ su $\mathbb{V}$ si deduce che $SL(2,\mathbb{Z})$ è transitivo sull'insieme degli archi di $\mathcal{F}$. A questo punto, gli stabilizzatori degli archi sono i coniugati dello stabilizzatore dell'arco $\{\frac{1}{0}, \frac{0}{1}\}$, che semplici calcoli di matrici mostrano essere il sottogruppo (di ordine 4)

$$\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle. \tag{3.22}$$

Torniamo al grafo di Farey $\mathcal{F}$. Una maniera elementare per descriverlo è basata sulla semplice nozione di *mediante*[2] di due frazioni $\frac{p}{q}, \frac{r}{s}$, che è definita come

$$\frac{p}{q} \boxplus \frac{r}{s} = \frac{p + r}{q + s}. \tag{3.23}$$

[1] Il gruppo quoziente $SL(2,\mathbb{Z})/Z$, che dunque opera fedelmente su $\mathcal{F}$, si denota con $PSL(2,\mathbb{Z})$ e si chiama *gruppo modulare*.

[2] Credo il termine venga dalla teoria musicale: la *mediante* è il terzo grado di una scala diatonica.

Si osservi che la mediante dipende dalle rappresentazioni $\frac{p}{q}$ e $\frac{r}{s}$ delle due frazioni, ed in genere non è una coppia primitiva, anche se $\frac{p}{q}$ e $\frac{r}{s}$ lo sono. Tuttavia, si constata immediatamente che se $\frac{p}{q}$ e $\frac{r}{s}$ sono adiacenti nel grafo di Farey, allora $\frac{p+r}{q+s}$ è primitiva ed è adiacente sia a $\frac{p}{q}$ che a $\frac{r}{s}$. In altri termini, se $\left\{\frac{p}{q}, \frac{r}{s}\right\}$ è un arco in $\mathcal{F}$, allora

$$\frac{p}{q} \qquad \frac{r}{s} \qquad \frac{p}{q} \boxplus \frac{r}{s}$$

sono i vertici di un triangolo in $\mathcal{F}$. Anche in questo caso, la mediante dipende dalla rappresentazione per i due vertici iniziali; ad esempio

$$\frac{1}{1} \boxplus \frac{3}{2} = \frac{4}{3} \neq \frac{2}{1} = \frac{-1}{-1} \boxplus \frac{3}{2}.$$

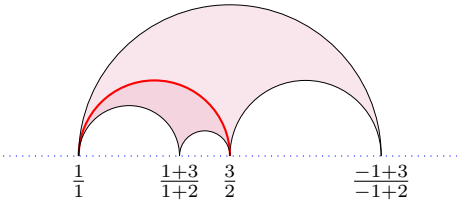
In generale, due distinte frazioni primitive $x = \frac{p}{q}$ e $y = \frac{r}{s}$ hanno due medianti:

$$\frac{p+r}{q+s} \qquad \text{e} \qquad \frac{-p+r}{-q+s}; \tag{3.24}$$

se poi x, y sono adiacenti in $\mathcal{F}$, allora i due vertici dati dalle due medianti, diversi tra loro e da x e y, sono i vertici di due triangoli che hanno in comune l'arco $\{x, y\}$. Non è difficile (ed è lasciato per esercizio) provare che sono i soli.

Lemma 3.14. *Siano $\frac{p}{q}, \frac{r}{s}$ vertici adiacenti di $\mathcal{F}$. Allora esistono esattamente due altri vertici che sono adiacenti ad entrambi, e sono dati dalle medianti (3.24). In particolare, ogni arco di $\mathcal{F}$ appartiene ad esattamente due triangoli di $\mathcal{F}$.*

La figura di sotto (in cui l'arco iniziale $\left\{\frac{1}{1}, \frac{3}{2}\right\}$ è tracciato in rosso) illustra questo fatto nel caso dell'esempio di sopra (la ragione per cui gli archi sono disegnati come semicirconferenze verrà chiarita tra poco).



Possiamo ora procedere alla costruzione ricorsiva del grafo di Farey. Ne indichiamo di fatto una realizzazione geometrica, in cui i vertici razionali di $\mathcal{F}$ sono disposti come i punti razionali di una retta orizzontale mentre il vertice $\infty = \frac{1}{0}$ non è disegnato ma inteso localizzarsi 'fuori'; gli archi che incidono al punto $\frac{1}{0}$ sono tracciati come semirette verticali, gli altri come semicirconferenze centrate sulla retta e disposte nel semipiano superiore (come nella figura precedente).
Si comincia dai vertici $\frac{0}{1}$ e $\frac{1}{0}$, che costituiscono un primo arco. Si aggiungono quindi i due vertici medianti

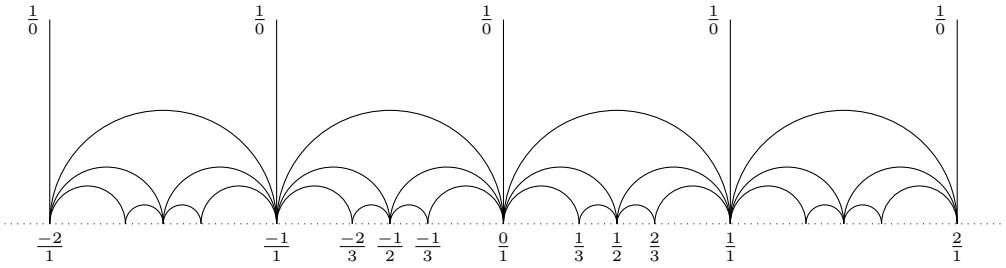
$$\frac{0+1}{1+0} = \frac{1}{1} \quad \text{e} \quad \frac{0+1}{-1+0} = \frac{-1}{1}$$

ed i nuovi archi che si generano $\left\{\frac{0}{1}, \frac{1}{1}\right\}, \left\{\frac{0}{1}, \frac{-1}{1}\right\}, \left\{\frac{1}{0}, \frac{1}{1}\right\}$ e $\left\{\frac{1}{0}, \frac{-1}{1}\right\}$. Quindi, si determinano le medianti, diverse dai due punti precedenti, relative a questi nuovi archi; si

avranno quattro nuovi vertici:

$$\frac{0+1}{1+1}=\frac{1}{2}\quad \frac{0-1}{1+1}=\frac{-1}{2}\quad \frac{1+1}{0+1}=\frac{2}{1}\quad \frac{1+1}{0-1}=\frac{2}{-1}$$

e gli archi che si generano. E così via. Ad ogni stadio, si aggiungono le frazioni medianti degli archi aggiunti allo stadio precedente (una per ciascun nuovo arco, perché l'altra è già presente tra i vertici del passo precedente) ed i nuovi archi che si determinano. La figura che segue mostra una parte di quel che si ottiene dopo alcuni passi.



Due fatti sono a questo punto da osservare.

1) In questo modo, si costruiscono tutte le frazioni $\frac{p}{q}\in\mathbb{Q}\cup\{\infty\}$, e quindi tutti gli archi che le collegano.

2) Gli archi nella realizzazione geometrica descritta si intersecano solo negli estremi (cioè nei vertici del grafo).

Per il punto (1), sia $x=\frac{p}{q}\in\mathbb{Q}\cup\{\infty\}$ con (p,q) primitiva; osserviamo che se $|p|+|q|=1$ allora x è uno dei due vertici iniziali, mentre se $|p|+|q|>1$, possiamo supporre $x=\frac{p}{q}$ oppure $x=\frac{-p}{q}$ con $p,q\geq 1$; ora

$$\frac{p}{q}=\frac{p-1}{1}\boxplus\frac{1}{q-1},\qquad \frac{-p}{q}=\frac{-p+1}{1}\boxplus\frac{-1}{q-1},$$

e $\frac{p-1}{1}$, $\frac{1}{q-1}$, $\frac{-p+1}{1}$ e $\frac{-1}{q-1}$ sono costruite per ipotesi induttiva; quindi $\frac{p}{q}$ e $\frac{-p}{q}$ sono costruite dato che, nella procedura descritta, ad ogni stadio si aggiungono tutte le mediane ancora mancanti tra frazioni dello stadio precedente.

Anche per il punto (2) è possibile riferirsi al processo ricorsivo, provando che i nuovi archi che si tracciano intersecano gli archi dello stadio precedente solo nei loro estremi; oppure si può procedere con qualche calcolo, mostrando che se $\frac{p}{q}<\frac{m}{n}<\frac{r}{s}$ con $\frac{p}{q}$ e $\frac{r}{s}$ adiacenti, allora per ogni vertice $\frac{t}{u}$ adiacente a $\frac{m}{n}$ si ha $\frac{p}{q}<\frac{t}{u}<\frac{r}{s}$, quindi il semicerchio che rappresenta l'arco tra $\frac{m}{n}$ e $\frac{t}{u}$ non interseca il semicerchio (o la semiretta) che rappresenta l'arco tra $\frac{p}{q}$ e $\frac{r}{s}$. Vediamo invece più in dettaglio il metodo che coinvolge l'azione di $SL(2,\mathbb{Z})$; poiché infatti questa è transitiva sia sui vertici che sugli archi, è sufficiente provare che nessun altro arco interseca al di fuori dei due estremi l'arco i cui estremi sono $\frac{1}{0}$ e $\frac{0}{1}$, cioè la semiretta passante per 0; e questo si mostra mediante la facile osservazione che vertici adiacenti in $\mathbb{Q}\setminus\{0\}$ sono entrambi positivi o entrambi negativi.

NOTA. A questo punto, e prima di proseguire a definire l'albero di Farey, tiriamo in ballo il piano iperbolico; anche se per gli scopi attuali non è strettamente necessario, è

utile per attingere a una comprensione più profonda di quello che stiamo facendo (chi non lo conosce può saltare questa nota, sapendo però che prima o poi di spazi iperbolici dovremo parlare in modo sostanziale). La realizzazione geometrica data del grafo $\mathcal{F}$ si colloca naturalmente in $\mathbb{H} \cup (\mathbb{R} \cup \{\infty\})$, dove

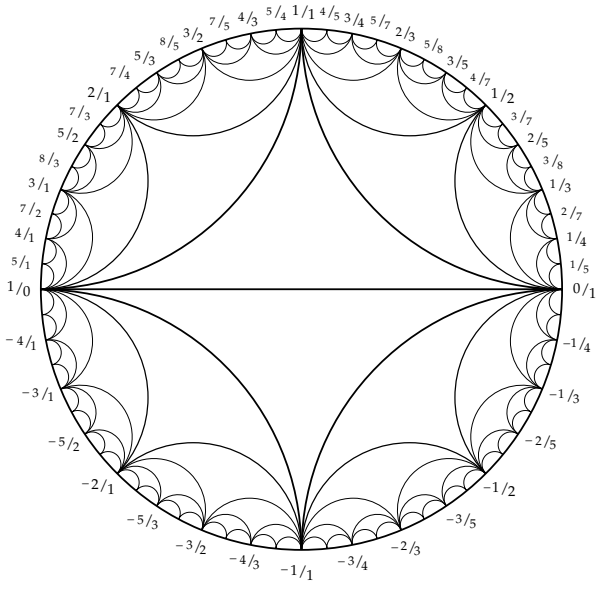
$$\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$$

è il piano iperbolico. Com'è noto, le rette di $\mathbb{H}$ sono le semirette verticali e le semicirconferenze centrate in $\mathbb{R}$, quindi gli archi di $\mathcal{F}$ sono rette in $\mathbb{H}$. Questa interpretazione è vantaggiosa perché singnifica che gli elementi di $SL(2,\mathbb{Z})$, agendo come trasformazioni di Möbius su $\mathbb{H}$, preservano gli archi di $\mathcal{F}$, così come i triangoli, come sottoinsiemi di $\mathbb{H}$. I triangoli di $\mathcal{F}$, per le cose viste, costituiscono una tassellazione di $\mathbb{H}$, sui termini della quale $SL(2,\mathbb{Z})$ agisce (transitivamente).

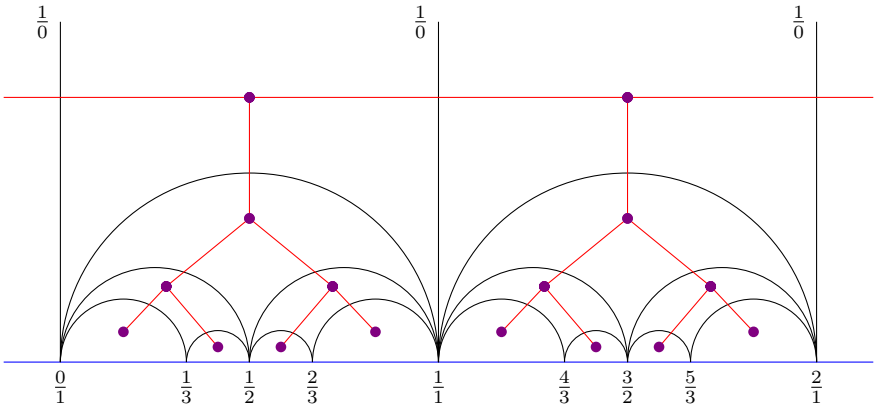
Si ha poi che la mappa di Cayley

$$z \mapsto \frac{z-1}{z+i}$$

(per ogni $z \in \mathbb{C}$) trasforma $\mathbb{H}$ nel disco di Poincarè $\mathbb{E} = \{z \in \mathbb{C} \mid |z| < 1\}$ (un altro modello del piano iperbolico) e $\mathbb{R} \cup \{\infty\}$ nel toro complesso $S = \{z \in \mathbb{C} \mid |z| = 1\}$. Applicata al grafo $\mathcal{F}$ disegnato in $\mathbb{H}$ dà luogo al bel diagramma che, scaricatolo dal web, riportiamo qui di seguito,



Definiamo ora l'*albero di Farey* $T\mathcal{F}$. I vertici di $T\mathcal{F}$ sono i triangoli di $\mathcal{F}$ (se si preferisce, le tessere della tassellazione di $\mathbb{H}$), e due vertici sono adiacenti se hanno un lato (un arco di $\mathcal{F}$) in comune. Poichè, come abbiamo visto, ogni arco di $\mathcal{F}$ appartiene esattamente a due triangoli, $T\mathcal{F}$ è un grafo 3-regolare. La figura seguente visualizza un pezzo di $T\mathcal{F}$.



Si verificano quindi i seguenti fatti.

Proposizione 3.15. *Sia $T\mathcal{F}$ il grafo definito sopra. Allora*

(1) *$T\mathcal{F}$ è un albero;*

(2) *$SL(2,\mathbb{Z})$ agisce transitivamente su $T\mathcal{F}$;*

(3) *lo stabilizzatore in $SL(2,\mathbb{Z})$ di un vertice di $T\mathcal{F}$ ha ordine 6 ed è un coniugato del sottogruppo*

$$P = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\rangle.$$

Dimostrazione. (1) Esercizio 3.32.

(2) Poiché $SL(2,\mathbb{Z})$ è transitivo sugli archi di $\mathcal{F}$ è sufficiente provare che i due triangoli che hanno in comune l'arco $\left\{\frac{1}{0}, \frac{0}{1}\right\}$ appartengono alla stessa orbita, e per questo basta osservare che

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \frac{1}{0} = \frac{0}{1}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \frac{0}{1} = \frac{-1}{0} = \frac{1}{0} \quad \text{e} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \frac{1}{1} = \frac{-1}{1}.$$

(3) Per il punto (2), gli stabilizzatori in $SL(2,\mathbb{Z})$ dei vertici di $T\mathcal{F}$ sono coniugati allo stabilizzatore P del triangolo $\Delta = \left\{\frac{1}{0}, \frac{0}{1}, \frac{1}{1}\right\}$. Si verifica con semplici considerazioni, che un elemento in P fissa tutti e tre vertici di Δ (quindi appartiene a Z) oppure li permuta ciclicamente; con facili calcoli di matrici si trova che P è il sottogruppo generato da $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, e che questo ha effettivamente ordine 6. □

Finalmente, il risultato annunciato all'inizio.

Teorema 3.16. *Per ogni $m \geq 3$, il gruppo $SL(2,\mathbb{Z})[m]$ è libero.*

Dimostrazione. Sia $m \geq 3$ e $G = SL(2,\mathbb{Z})[m]$, e consideriamo l'azione di G sull'albero $T\mathcal{F}$ indotta da quella di $SL(2,\mathbb{Z})$. Sia P come al punto (3) della Proposizione 3.15; allora $G \cap P = \{1\}$, inoltre, per ogni vertice v di $T\mathcal{F}$ esiste $A \in SL(2,\mathbb{Z})$ tale che lo stabilizzatore G_v è $G \cap APA^{-1}$. Poiché G è normale in $SL(2,\mathbb{Z})$,

$$G_v = G \cap APA^{-1} = A(G \cap P)A^{-1} = \{1\};$$

quindi G agisce liberamente su $T\mathcal{F}$. Ora, se un elemento A di $SL(2,\mathbb{Z})$ inverte un arco di $T\mathcal{F}$, allora fissa l'arco di $\mathcal{F}$ comune ai due triangoli che costituiscono gli estremi dell'arco in $T\mathcal{F}$, e dunque, per quanto visto in precedenza, A appartiene ad un coniugato di $Q = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$. Ma $G \cap Q = \{1\}$ e quindi, come prima, $A \notin G$.
In conclusione, G agisce liberamente e senza inversioni su $T\mathcal{F}$ e dunque è un gruppo libero per il Teorema 3.6. □

Si osservi che $P \cap SL(2,\mathbb{Z})[2] = Z \neq \{1\}$; quindi $SL(2,\mathbb{Z})[2]$ non agisce liberamente sull'albero $T\mathcal{F}$.

Esercizio 3.30. Sia H il sottogruppo di $SL(2,\mathbb{Z})$ definito in (3.21). Si provi che due distinti coniugati di H si intersecano in Z. Quindi l'azione del gruppo $PSL(2,\mathbb{Z}) = SL(2,\mathbb{Z})/Z$ sull'insieme dei vertici di $\mathcal{F}$ è fedele, transitiva e tale che *l'identità è il solo elemento del gruppo che fissa due vertici distinti*[3].

Esercizio 3.31. Si dimostri il Lemma 3.14.

Esercizio 3.32. Si dimostri che il grafo $T\mathcal{F}$ è un albero [si provi che per ogni coppia di vertici distinti di $T\mathcal{F}$ esiste uno ed un solo cammino ridotto dall'uno all'altro].

Esercizio 3.33. Si provi che $|SL(2,3)| = 24$; si provi quindi che il numero di orbite di $SL(2,\mathbb{Z})[3]$ sull'insieme dei vertici dell'albero di Farey $T\mathcal{F}$ è 4. Si determini infine il rango del gruppo libero $SL(2,\mathbb{Z})[3]$. Si faccia lo stesso per $SL(2,\mathbb{Z})[5]$.

3.6. Prodotti liberi

Il *prodotto libero* di gruppi è una generalizzazione dell'idea di gruppo libero. Noi tratteremo il caso del prodotto libero di due gruppi: l'estensione al prodotto di famiglia arbitraria di gruppi dovrebbe riuscire comunque abbastanza naturale (ed è lasciata per esercitazione al lettore laborioso). Iniziamo con la proprietà universale che caratterizza il prodotto libero.

Definizione. Siano H e K gruppi; un gruppo G si dice un *prodotto libero* di H e K se esistono omomorfismi $\alpha_H : H \to G$, $\alpha_K : K \to G$, tali che è soddisfatta la seguente proprietà universale. *Per ogni gruppo W ed omomorfismi $\phi_H : H \to W$, $\phi_K : K \to W$, esiste uno ed un unico omomorfismo $\phi : G \to W$ tale che $\phi_H = \phi\alpha_H$ e $\phi_K = \phi\alpha_K$; ovvero risulta commutativo il diagramma*

$$\begin{array}{ccccc} H & \xrightarrow{\alpha_H} & G & \xleftarrow{\alpha_K} & K \\ & \searrow^{\phi_H} & \downarrow \phi & \swarrow_{\phi_K} & \\ & & W & & \end{array} \tag{3.25}$$

Prima di dimostrare l'esistenza dei prodotti liberi, facciamo alcune osservazioni che si deducono direttamente e facilmente dalla proprietà universale, e dunque proviamo l'unicità (a meno di isomorfismi) del prodotto libero.

Lemma 3.17. *Sia G un prodotto libero dei gruppi H e K; allora gli omomorfismi α_H e α_K nella definizione (e in (3.25)) sono iniettivi; inoltre $G = \langle \alpha_H(H), \alpha_K(K) \rangle$.*

[3] Un gruppo di permutazioni G, transitivo e con tale proprietà si dice gruppo di Frobenius; nel caso in cui G è finito si tratta di una condizione che implica grosse restrizioni alla struttura di G.

Dimostrazione. Applicando la proprietà universale (3.25) quando $W = H$, $\phi_H = i_H$, l'identità su H, e ϕ_K l'omomorfismo banale ($\phi_K(x) = 1_H$ per ogni $x \in K$), si ottiene un omomorfismo $\phi : G \to H$ tale che $\phi\alpha_H = i_H$, provando così che α_H è iniettiva; similmente si prova che α_K è iniettiva.
Posto $W = \langle \alpha_H(H), \alpha_K(K) \rangle$, $\phi_H = \alpha_H$ e $\phi_K = \alpha_K$, la proprietà universale stabilisce che c'è un omomorfismo (chiaramente suriettivo) $\phi : G \to W$ tale che $\phi\alpha_H = \alpha_H$ e $\phi\alpha_K = \alpha_K$, e che la funzione identica i_G è l'unico omomorfismo $G \to G$ con $i_G\alpha_H = \alpha_H$ e $i_G\alpha_K = \alpha_K$. Da ciò segue che se $\eta : W \to G$ è l'immersione identica, allora $i_G = \eta\phi$; quindi $\phi = i_G$. □

Proposizione 3.18. *Se G e G' sono prodotti liberi dei gruppi H e K, allora $G \simeq G'$.*

Dimostrazione. Siano $\alpha_H : H \to G$, $\alpha_K : K \to G$ le immersioni di H e K in G come in (3.25), e $\beta_H : H \to G'$, $\beta_K : K \to G'$ le analoghe immersioni per il prodotto libero G'. Per la proprietà universale esistono degli unici omomorfismi $\phi : G \to G'$ e $\psi : G' \to G$ tali che

$$\beta_H = \phi\alpha_H, \quad \beta_K = \phi\alpha_K, \quad \psi\beta_H = \alpha_H \quad \psi\beta_K = \alpha_K.$$

Quindi, $\alpha_H = \psi\phi\alpha_H$ e $\alpha_K = \psi\phi\alpha_K$. Come nel caso dei gruppi liberi l'unicità nella proprietà universale (applicata a $W = G$, $\phi_H = \alpha_H$, $\phi_k = \alpha_K$) implica $\psi\phi = id_G$. Analogamente, si prova $\phi\psi = id_{G'}$.Quindi, $\phi = \psi^{-1}$ è un isomorfismo. □

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

$$H * K.$$

Dalla proprietà universale e dalla Proposizione 3.18 discende anche che se H, K e T sono gruppi allora

$$(H * K) * T \simeq H * (K * T); \tag{3.26}$$

per cui si scrive senza ambiguità $H * K * T$; e $H_1 * H_2 * \cdots * H_n$ per una famiglia finita $H_1, H_2, \ldots, H_n$ di gruppi.

Dalle proprietà universali segue anche facilmente la seguente osservazione, che rende conto dell'affermazione che il prodotto libero è una generalizzazione del concetto di gruppo libero.

Lemma 3.19. *Siano F_n e F_m due gruppi liberi di rango n e m rispettivamente; allora*

$$F_n * F_m = F_{n+m}.$$

In particolare, per ogni $n \geq 1$, $F_n \simeq \mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}$ (n volte).

Vediamo un esempio meno immediato, e sul quale torneremo più avanti.

Esempio 3.6. Siano $H = \langle a \rangle$ e $K = \langle b \rangle$ gruppi ciclici di ordine 2 e D_∞ il gruppo diedrale infinito. D_∞ è generato da due involuzioni a', b' con $|a'b'| = \infty$; definiamo α_H e α_K ponendo $\alpha_H(a) = a'$ e $\alpha_K(b) = b'$. Se ϕ_H, ϕ_K sono omomorfismi, rispettivamente, di H e di K in un gruppo G allora $x = \phi_H(a)$ e $y = \phi_K(b)$ sono involuzioni di G (il caso in cui ϕ_H e ϕ_K non sono entrambi iniettivi è facile e lo lascio al lettore), dunque (esempio 1.5) $\langle x, y \rangle$ e un gruppo diedrale ed esiste un omomorfsmo $\phi : D_\infty \to G$ (la cui immagine è $\langle x, y \rangle$) tale che $\phi(a') = x$ e $\phi(b') = y$. Allora $\phi\alpha_H = \phi_H$, $\phi\alpha_K = \phi_K$, e $D_\infty = H * K$. □

Osservazione. Analogamente a quello che vale per i gruppi liberi, una conseguenza pressoché immediata della proprietà universale è ce 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 omomorfismo suriettivo $H * K \to G$ (dunque G è isomorfo ad un quoziente del prodotto libero $H * K$).

Costruzione del prodotto libero. Proviamo ora l'esistenza del prodotto libero $H*K$ dei gruppi H e K. Siano H e K dati mediante presentazioni, diciamo $H = \langle X \mid R \rangle$ e $K = \langle Y \mid S \rangle$, con $X \cap Y = \emptyset$ (si può, ad esempio, prendere $H = \langle H \mid T_H \rangle$ dove T_H è l'insieme delle relazioni dato dalla tavola di moltiplicazione di H e fare lo stesso per K); mostreremo che il gruppo

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

è prodotto libero di H e K. Innanzi tutto definiamo α_H e α_K. Per il primo, si pone $\alpha_H : H \to G$ l'omomorfismo ottenuto componendo l'immersione $H \to \langle X \cup Y \mid R \rangle$ con la proiezione $\langle X \cup Y \mid R \rangle \to G$ (quindi $\alpha_H(x) = x$ per ogni $x \in X$); osserviamo che ponendo $\eta : G \to H$ l'omomorfismo tale che $\eta(x) = x$ per ogni $x \in X$ e $\eta(y) = 1$ per $y \in Y$ (l'unico omomorfismo da $F(X \cup Y) \to H$ dato da $x \mapsto x$ per $x \in X$, e $y \mapsto 1$ per $y \in Y$, contiene $R \cup S$ nel suo nucleo e dunque induce un'omomorfismo - η appunto - da G in H), allora $\eta\alpha_H$ è l'identità su H e pertanto α_H è iniettiva; similmente si definisce e si ragiona per $\alpha_K : K \to G$.

Passiamo quindi a provare la proprietà universale. Siano W un gruppo, $\phi_H : H \to W$ e $\phi_K : K \to W$ omomorfismi; definiamo $\phi : G \to W$ ponendo $\phi(x) = \phi_H(x)$ per ogni $x \in X$, e $\phi(y) = \phi_K(y)$ per ogni $y \in Y$, ed estendendo ad un omomorfismo; allora $\phi_H = \phi\alpha_H$, $\phi_K = \phi\alpha_K$, come vuole la proprietà universale, e ϕ è chiaramente unico per tale condizione. Questo completa la dimostrazione dell'esistenza del prodotto $H * K$.

L'esempio 3.6 illustra quanto appena detto: in quel caso $H = \langle x \mid x^2 \rangle$, $K = \langle y \mid y^2 \rangle$, ed infatti $D_\infty = \langle x, y \mid x^2, y^2 \rangle$; quindi $D_\infty = C_2 * C_2$. In generale, se C_n, C_m sono gruppi ciclici di ordine, rispettivamente n e m, allora $C_n * C_m = \langle x, y \mid x^n, y^m \rangle$. Più avanti dimostreremo il classico risultato di Felix Klein e Robert Fricke (1890) per cui

$$PSL(2, \mathbb{Z}) = C_2 * C_3.$$

Prima, la seguente e naturale caratterizzazione "interna" di un prodotto libero.

Proposizione 3.20. *Siano H, K sottogruppi del gruppo 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*

$$g = a_1 b_1 \cdots a_n b_n \tag{3.27}$$

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

Dimostrazione. Siano $H, K \leq G$ e $G = \langle H, K \rangle$. Allora esiste un omomorfismo suriettivo $\phi : H * K \to G$ tale che $x = \phi\alpha_H(x)$ per ogni $x \in H$ e $y = \phi\alpha_K(y)$ per ogni $y \in K$ (α_H e α_K sono, rispettivamente, le immersioni di H e di K in $H * K$). Se per ogni $1 \neq g \in G$ è soddisfatta la richiesta (3.27) allora $\ker(\phi) = 1$ e dunque ϕ è un isomorfismo.

Viceversa, sia $G = H * K$ e, per ogni $x \in H$ ed ogni $y \in K$, identifichiamo x con $\alpha_H(x)$ e y con $\alpha_K(y)$. È facile convincersi che, per provare che la (3.27) vale per ogni $g \in G$, è sufficiente dimostrare che per ogni $n \geq 1$, $a_1, \ldots, a_n \in H \setminus \{1\}$, $b_1, \ldots, b_n \in K \setminus \{1\}$

$$a_1 b_1 \cdots a_n b_n \neq 1 \tag{3.28}$$

(mediante coniugio per elementi di H o di K, ci si riconduce ad una forma del genere). Sia Ω l'insieme di tutte le sequenze finite $(u_1, u_2, \dots, u_n)$ con $u_i \in K \cup H \setminus \{1\}$, e

$$\begin{cases} u_i \in H \Rightarrow u_{i+1} \in K \\ u_i \in K \Rightarrow u_{i+1} \in H, \end{cases}$$

insieme alla sequenza vuota. Ora, il porre, per ogni $\mathbf{u} = (u_1, \dots, u_n) \in \Omega$ e $1 \neq a \in H$,

$$a \cdot \mathbf{u} = \begin{cases} (a, u_1, \dots, u_n) & \text{se} \quad u_1 \in K \\ (u_2, \dots, u_n) & \text{se} \quad u_1 = a^{-1} \\ (au_1, \dots, u_n) & \text{se} \quad a^{-1} \neq u_1 \in A \end{cases}$$

definisce, come si vede facilmente, un'azione di H su Ω. In modo analogo si definisce un'azione di K su Ω. Tali azioni sono fedeli, dunque possiamo vedere H e K come sottogruppi di $Sym(\Omega)$. Per la proprietà universale esiste un omomorfismo suriettivo da $H * K$ nel sottogruppo $S = \langle H, K \rangle$ di $Sym(\Omega)$; e questo solleva l'azione su Ω da S a $H * K$. Sia $g \in H * K$ il membro di sinistra di (3.28), ed $\mathbf{e} \in \Omega$ la parola vuota; allora (come si dimostra subito per induzione sulla lunghezza n di g),

$$g \cdot \mathbf{e} = (a_1, b_1, \dots, a_n, b_n) \neq \mathbf{e}$$

e dunque $g \neq 1$. ∎

La scrittura, per $g \in H * K$, $g = a_1 b_1 \dots a_n b_n$ come in (3.27) si dice *forma normale* dell'elemento g. Alcune immediate ma basilari conseguenze della Proposizione 3.20 sono descritte negli esercizi 3.35 e 3.36. Va da sé che, da qui in avanti (ad esempio negli esercizi) adotteremo, come nella seconda parte della dimostrazione precedente, la convenzione di identificare, in un prodotto libero (interno o esterno) $G = H * K$, gli elementi di H e di K con le loro immagini in G (cioè, per $h \in H$, scriveremo h per $\alpha_H(h)$, etc.)

Esercizio 3.34. Si enunci e si dimostri un Lemma del Ping–Pong (del tipo del lemma 3.12) per il prodotto libero di due gruppi.

Esercizio 3.35. Siano H, K gruppi e sia $g \in H * K$; si provi che $H \cap H^g \neq 1$ se e solo se $g \in H$. Si provi che se $H \neq 1 \neq K$ allora $Z(H * K) = 1$.

Esercizio 3.36. Sia $G = H * K$. Si provi che ogni elemento periodico di G è coniugato ad un elemento di $H \cup K$. Si deduca che se H e K sono senza torsione allora $H * K$ è senza torsione.

Esercizio 3.37. Si provi che se H e K sono gruppi residualmente finiti allora anche $H * K$ è residualmente finito. Si deduca che un gruppo libero di rango finito è residualmente finito.

Esercizio 3.38. Siano H, K gruppi e $G = H * K$; si provi che $G/G' \simeq H/H \times K/K'$.

Esercizio 3.39. Siano H e K gruppi non banali e $G = H * K$; si provi che il sottogruppo $[H, K]$ di G è un gruppo libero nel sistema di generatori $\{[x, y] \mid x \in H,\ y \in K\}$.

Prodotti liberi amalgamati. Siano G_1, G_2, H gruppi e $\phi_i : H \to G_i$ $(i = 1, 2)$ omomorfismi iniettivi; il *prodotto amalgamato* $G_1 *_H G_2$ è il massimo quoziente del prodotto libero $G_1 * G_2$ nel quale i sottogruppi $\phi_1(H)$ e $\phi_2(H)$ sono identificati (elemento per elemento). Quindi

$$G_1 *_H G_2 = \frac{G_1 * G_2}{N} \tag{3.29}$$

dove N è il sottogruppo normale di $G_1 * G_2$ generato da tutti i coniugati degli elementi del tipo $\phi_1(x)\phi_2(x)^{-1}$ $(x \in H)$.
Se $\langle X \mid R \rangle$, $\langle Y \mid S \rangle$ sono presentazioni, rispettivamente di G_1 e di G_2, allora

$$G_1 *_H G_2 = \langle X \cup Y \mid R, S,\ \phi_1(x)\phi_2(x)^{-1}\ (x \in H)\rangle. \tag{3.30}$$

Il prodotto amalgamato svolge un ruolo naturale in topologia: il Teorema di Seifert–Van Kampen dice il gruppo fondamentale dell'unione di due spazi topologici lungo un sottospazio (dove tutto quanto è connesso per archi) è il prodotto amalgamato dei gruppi fondamentali dei due spazi rispetto al gruppo fondamentale dell'intersezione.

Esempio 3.7. Siano $G_1 = \langle a\rangle$, $G_2 = \langle b\rangle$ gruppi ciclici infiniti e $H = \mathbb{Z}$; fissiamo gli omomorfismi $\phi_1 : \mathbb{Z} \to G_1$, $\phi_2 : \mathbb{Z} \to G_2$ ponendo $\phi_1(z) = a^{2z}$, $\phi_2(z) = b^{2z}$ (per ogni $z \in \mathbb{Z}$). Una presentazione del prodotto amalgamato su H è

$$G_1 *_H G_2 = \langle a, b \mid a^2 = b^2\rangle.$$

Si verifichi per esercizio che tale gruppo è (isomorfo a) il prodotto semidiretto $\langle x\rangle \rtimes \langle y\rangle$, con $|x| = |y| = \infty$ e l'azione data da $x^y = x^{-1}$ [sugg.: porre $a = x,\ b = yx$] □

Esempio 3.8. Non è sempre così agevole determinare la forma di un prodotto amalgamato; consideriamo ad esempio il prodotto $PSL(2,\mathbb{Q}) *_{\mathbb{Z}} \mathbb{Z}$ dove ϕ_1 e ϕ_2 è una qualsiasi coppia di omomorfismi iniettivi da $\mathbb{Z}$ in $PSL(2,\mathbb{Q})$ e in $\mathbb{Z}$, rispettivamente. Osserviamo che le immagini $x = 1\phi_1$ e $y = 1\phi_2$ sono elementi di ordine infinito. Se N è il sottogruppo normale del prodotto amalgamato $PSL(2,\mathbb{Q})*\mathbb{Z}$ come in (3.29) allora per ogni $z \in \mathbb{Z}$ (come sottogruppo del prodotto) si ha

$$N \ni (y^{-1}x)^{-1}(y^{-1}x)^z = x^{-1}x^z$$

(questo esempio è tratto da un esercizio nel libro *Trees* di J.P. Serre). □

Anche il prodotto amalgamato, come è facile prevedere, soddisfa una proprietà universale, la cui dimostrazione omettiamo.

Proposizione 3.21. *Siano H e K sottogruppi isomorfi dei gruppi G_1, G_2, e $f : H \to K$ un fissato isomorfismo. Allora per ogni gruppo G ed omomorfismi $\alpha_i : G_i \to G$ $(i = 1, 2)$ tali che $\alpha_2 f(x) = \alpha_1(x)$ per ogni $x \in H$, esiste un'unico omomorfismo $\phi : G_1 *_H G_2 \to G$ tale che ristretto a G_i coincide con α_i (per $i = 1, 2$).*

Dove, per non sovraccaricare di notazione l'enunciato, i gruppi G_i sono visti nel modo ovvio come sottogruppi del prodotto $G_1 *_H G_2$, e $H = G_1 \cap G_2$. Con queste identificazioni, descriviamo la *forma normale* degli elementi del prodotto $G = G_1 *_H G_2$ (la cui dimostrazione lasciamo per esercizio): siano $\mathcal{T}_1$ un sistema di rappresentanti delle classi laterali $\{gH \mid g \in G_1\} \setminus \{H\}$ e $\mathcal{T}_2$ un sistema di rappresentanti delle classi laterali $\{gH \mid g \in G_2\} \setminus \{H\}$; allora ogni elemento $g \in G$ si scrive in modo *unico* nella forma,

$$g = x_1 x_2 \cdots x_n a \tag{3.31}$$

con $a \in H$, $x_1, x_2, \ldots, x_n \in \mathcal{T}_1 \cup \mathcal{T}_2$, e con $x_i \in \mathcal{T}_1 \Rightarrow x_{i+1} \in \mathcal{T}_2$, $x_i \in \mathcal{T}_2 \Rightarrow x_{i+1} \in \mathcal{T}_1$, per ogni $1 \le i \le n-1$.

Esercizio 3.40. Si provi la correttezza della (3.31).

Esercizio 3.41. Il gruppo fondamentale $G = \pi_1(X)$ di una superficie chiusa orientabile X di genere 2 ha presentazione

$$G = \langle x, x_1, y, y_1 \mid [x, y] = [x_1, y_1]\rangle$$

si provi che $G = F_2 *_{\mathbb{Z}} F_2$ (dove F_2 è il gruppo libero di rango 2).

ESERCIZIO 3.42. Si provi che il gruppo $\langle x, y \mid xyx = yxy\rangle$ (si tratta di un cosiddetto *Braid group*) è un prodotto amalgamato di due gruppi ciclici infiniti.

ESERCIZIO 3.43. Per $i = 1, 2$, sia $G_i = \langle x_i, y_i \mid x_i^2 = y_i^4 = 1,\ y_i^{x_i} = y_i^{-1}\rangle$ gruppo diedrale di ordine 8, Sia $H = \langle a\rangle \times \langle b\rangle$ un gruppo abeliano elementare di ordine 4. Si considerino gli omomorfismi iniettivi $\phi_1 : H \to G_1$, $\psi_1 : H \to G_1$, $\phi_2 : H \to G_2$, dati da

$$\begin{array}{lll} \phi_1(a) = x_1 & \psi_1(a) = x_1 & \phi_2(a) = x_2 \\ \phi_1(b) = y_1^2 & \psi_1(b) = x_1 y_1^2 & \phi_1(b) = y_2^2 \end{array}$$

Si provi che i prodotti liberi amalgamati $G_1 *_H G_2$ definiti dalle coppie di omomorfismi (ϕ_1, ϕ_2) e (ψ_1, ϕ_2) non sono isomorfi.

3.7. Azioni su alberi

È possibile caratterizzare i prodotti liberi con amalgama in modo analogo a quanto fatto con il Teorema 3.6 per i gruppi liberi.

Proposizione 3.22. *Esiste un albero T sul quale il prodotto amalgamato $G = G_1 *_A G_2$ agisce senza inversioni e transitivamente sull'insieme degli archi, ed esiste in T un arco $e = \{x_1, x_2\}$ con $G_1 = Stab_G(x_1)$, $G_2 = Stab_G(x_2)$ e $A = Stab_G(e)$.*

Dimostrazione. Siano $\mathcal{C}_1, \mathcal{C}_2$, rispettivamente, l'insieme delle classi laterali sinistre di G modulo G_1 e modulo G_2. Sia T il grafo il cui insieme dei vertici è $V = \mathcal{C}_1 \cup \mathcal{C}_2$, e due elementi di V sono adiacenti se hanno intersezione non vuota. Questo significa che gli archi di T sono tutte e sole le coppie $\{gG_1, gG_2\}$ con $g \in G$. L'azione di G su T è quella, naturale, per moltiplicazione a sinistra: $g \cdot xG_i = (gx)G_i$ per ogni $g \in G$ e ogni $xG_i \in V$ $(i = 1, 2)$. Tale azione è chiaramente transitiva sugli archi e, poiché $G_1 \neq G_2$, è senza inversioni; inoltre, ponendo $x_1 = G_1, x_2 = G_2$ si ha che $e = \{G_1, G_2\}$ è un arco in T, e chiaramente, $G_1 = Stab_G(x_1), G_2 = Stab_G(x_2), H = G_1 \cap G_2 = Stab_G(e)$.
Resta da provare che T è un albero. Se $G \ni g = x_1 y_1 \cdots x_n y_n$ con $x_1, \ldots, x_n \in G_1$ e $y_1, \ldots, y_n \in G_2$, allora

$$\begin{aligned} x_1 y_1 \cdots x_n y_n G_1 &\sim_T x_1 y_1 \cdots x_n y_n G_2 = x_1 y_1 \cdots x_n G_2 \\ &\sim_T x_1 y_1 \cdots x_n G_1 = x_1 y_1 \cdots x_{n-1} y_{n-1} G_2 \end{aligned}$$

quindi, con una ovvia induzione, T è connesso. Il fatto che T non contenga circuiti non banali viene dalla unicità della forma normale (3.31) per gli elementi di G. ∎

Vediamo quindi la caratterizzazione inversa.

Teorema 3.23. *Supponiamo che il gruppo G agisca su un albero $T = (V, E)$, senza inversioni, transitivamente sull'insieme degli archi e con due orbite sull'insieme dei vertici. Sia $e = \{x_1, x_2\}$ un arco di T, e siano $G_1 = Stab_G(x_1)$, $G_2 = Stab_G(x_2)$ e $A = Stab_G(e)$; allora*

$$G \simeq G_1 *_A G_2.$$

In particolare, se G agisce liberamente sull'insieme degli archi di T, allora G è un prodotto libero.

Dimostrazione. Siano G, T, G_1, G_2 come nelle ipotesi; a partire dalle specifiche di queste, in sostanza, si ricostruisce il prodotto amalgamato. Si osservi innanzi tuto che le ipotesi implicano che vertici adiacenti in T appartengono ciascuno ad una delle due

diverse G-orbite. Sia $\{x_1, y\} \in E$, allora esiste $g \in G$ tale che $g \cdot \{x_1, x_2\} = \{x_1, y\}$ e poiché x_1 e y appartengono a G-orbite diverse deve risultare $g \cdot x_1 = x_1$, $g \cdot x_2 = y$. Quindi G_1 permuta transitivamente i vertici adiacenti a x_1 (e i corrispondenti archi), e lo stabilizzatore di uno di questi è $G_1 \cap G_2 = A$. Dunque, se $\mathcal{T}_1$ è un sistema di rappresentanti delle classi laterali sinistre di G_1 modulo A (contenente, per comodità, 1) allora l'insieme dei vertici adiacenti a x_1 è $\{a \cdot x_2 \mid a \in \mathcal{T}_1\}$. Similmente G_2 permuta transitivamente i vertici adiacenti a x_2 e, posto $\mathcal{T}_2$ un sistema di rappresentanti delle classi laterali sinistre di G_2 modulo A (contenente 1), l'insieme dei vertici adiacenti a x_2 è $\{b \cdot x_1 \mid a \in \mathcal{T}_2\}$. Constatato ciò, è semplice, procedendo per induzione sulla distanza da x_1, provare che per ogni vertice $y \neq x_1$ appartenente alla G-orbita di x_1 esistono $n \geq 1$, $a_1, \ldots, a_n \in \mathcal{T}_1$, $b_1, \ldots, b_n \in \mathcal{T}_2$, tali che

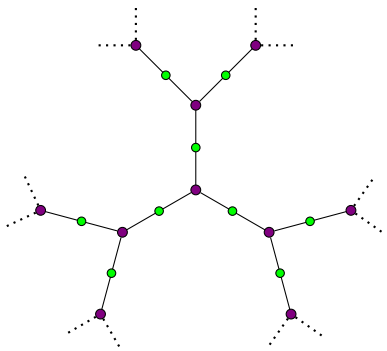
$$y = (b_1 a_1 \cdots b_{n-1} a_{n-1} b_n) \cdot x_1, \tag{3.32}$$

e similmente per i vertici nell'orbita di x_2 (scambiando $\mathcal{T}_1$ e $\mathcal{T}_2$). Questo prova in particolare che $\langle G_1, G_2 \rangle = G$.
Sia $W = G_1 *_A G_2$. Per la Proposizione 3.21, l'applicazione $\phi(g) = g$ per ogni $g \in G_1 \cup G_2$ si estende ad un omomorfismo suriettivo $W \to G$. Se $w \in \ker(\phi)$, per la forma normale (3.31) $w = a_1 b_1 \cdots a_n b_n h$ con $h \in A$, $a_1, \ldots, a_n \in \mathcal{T}_1$ e $b_1, \ldots, b_n \in \mathcal{T}_2$ (o viceversa), ma allora (con x_2 eventualmente al posto di x_1)

$$x_1 = (a_1 b_1 \cdots a_n b_n h) \cdot x_1.$$

Se $n \geq 1$, per la discussione vista sopra, questo implica che nel grafo T esiste un circuito ridotto non-banale passante per x_1, il che è assurdo. Dunque $w = h \in A \cap \ker(\phi) = 1$. Pertanto, ϕ è un isomorfismo. ∎

Applichiamo il Teorema 3.23 al caso del gruppo $G = SL(2, \mathbb{Z})$, a partire dall'azione di G sull'albero di Farey $T\mathcal{F}$ studiata nella sezione 3.5. L'azione di G su $T\mathcal{F}$ non rispetta le ipotesi del Teorema, perché è transitiva sull'insieme dei vertici di $T\mathcal{F}$ (Proposizione 3.15); ma questo si aggira passando alla suddivisione baricentrica di $T\mathcal{F}$ (figura di sotto, vedi esercizio 2.16), che denotiamo semplicemente con T.



suddivisione baricentrica di $T\mathcal{F}$

L'albero T è composto quindi da vertici di grado 3 (i vertici originari di $T\mathcal{F}$) e da vertici di grado 2 (corrispondendi agli archi di $T\mathcal{F}$). Per le cose viste nella sezione 3.5, questi due insiemi di vertici costituiscono due orbite per l'azione di G; inoltre (esercizio 2.16), G agisce senza inversioni su T, ed è transitivo sugli archi (quest'ultima affermazione discende da quanto osservato nella dimostrazione del punto (2) della Proposizione 3.15:

per ogni arco di $\mathcal{F}$ esiste un elemento di G che scambia i due triangoli (nel grafo $\mathcal{F}$) che lo contengono). Siano quindi x, y vertici adiacenti in T, di grado, rispettivamente, 3 e 2, e sia $e = \{x, y\}$. Per il punto (3) della e l'osservazione in (3.22),

$$Stab_G(x) \simeq C_6 \qquad Stab_G(y) \simeq C_4;$$

inoltre $Stab_G(e) = Stab_G(x) \cap Stab_G(y) = Z = \{\pm I\}$ ha ordine 2. Le caso del gruppo modulare $\overline{G} = PSL(2, \mathbb{Z}_= SL(2, \mathbb{Z})/Z$, gli stabilizzatori sono gli stessi quozientati modulo Z, ovvero $Stab_{\overline{G}}(x) \simeq C_3$, $Stab_{\overline{G}}(y) \simeq C_2$, $Stab_{\overline{G}}(e) = \{1\}$. Applicando il Teorema 3.23 si giunge quindi il seguente classico risultato.

Teorema 3.24 (Klein e Fricke)**.** $PSL(2, \mathbb{Z}) = C_2 * C_3$ *e* $SL(2, \mathbb{Z}) = C_4 *_{C_2} C_6$.

In particolare, otteniamo le presentazioni

$$PSL(2, \mathbb{Z}) = \langle a, b \mid a^2 = b^3 = 1 \rangle, \quad SL(2, \mathbb{Z}) = \langle a, b \mid a^4 = b^6 = 1, a^2 = b^3 \rangle.$$

Citiamo a questo punto, senza dimostrarlo, il seguente risultato di J.P. Serre:

Teorema 3.25. *Se $n \geq 3$, $SL(3, \mathbb{Z})$ non è esprimibile come un prodotto libero amalgamato non-banale.*

Esercizio 3.44. Si completino nei dettagli le dimostrazioni della Proposizione 3.22 e del Teorema 3.23.

Esercizio 3.45. Si provi che $GL(2, \mathbb{Z}) \simeq D_8 *_{D_4} D_{12}$ (dove, per ogni $n \geq 1$, D_{2n} è il gruppo diedrale di ordine $2n$).

Esercizio 3.46. Sia S un sottogruppo del prodotto libero amalgamato $G = H *_A K$. Si provi che se $S \cap (H \cup K)^x = \{1\}$ per ogni $x \in G$, S è un gruppo libero.

Esercizio 3.47. Sia $G = G_1 *_H G_2$; si provi che ogni sottogruppo finito di G è coniugato ad un sottogruppo di G_1 oppure ad un sottogruppo di G_2. [Questo generalizza l'esercizio 3.36; dato H un sottogruppo finito di G, si consideri l'azione di H sull'albero nella Proposizione 3.22, si applichi il Lemma 2.4, quindi . . .]

3.8. Estensioni HNN

Nelle estensioni HNN (acronimo dei nomi degli tre studiosi che le introdussero e studiarono sistematicamente: Graham Higman, Bernhard Neumann e Hanna Neumann), un gruppo G è esteso in modo che un isomorfismo tra due sottogruppi sia indotto da un coniugio (automorfismo interno). La loro definizione è in sostanza contenuta nella dimostrazione della possibilità di far questo.

Teorema 3.26. (G. Higman, B. Neumann, H. Neumann) *Siano H, K sottogruppi isomorfi di uno stesso gruppo G, e $\alpha : H \to K$ un fissato isomorfismo. Allora G può essere immerso in un gruppo $\overline{G}$ nel quale α è indotto da un automorfismo interno.*

Dimostrazione. Siano G, H, K e α come nelle ipotesi. Poniamo $U = G * \langle u \rangle$, $V = G * \langle v \rangle$, con $\langle u \rangle$ e $\langle v \rangle$ gruppi ciclici infiniti. Nel gruppo U si vede che $R = \langle G, H^u \rangle = G * H^u$, similmente in V, $S = \langle G, H^u \rangle = G * K^v$. Ora, esiste un omomorfismo $\phi : R \to S$ tale che $\phi(g) = g$ per ogni $g \in G$ e $\phi(h^u) = \alpha(h)^v$ per ogni $h \in H$. È immediato verificare

che ϕ è un isomorfismo. A questo punto, si considera il prodotto libero amalgamato $\overline{G} = U *_\phi V$ in cui R è amalgamato a S tramite ϕ. Sia ha $G \leq \overline{G}$, e per ogni $h \in H \leq G$,

$$h^u = \phi(h^u) = \alpha(h)^v,$$

quindi $\alpha(h) = h^{uv^{-1}}$, e questo mostra che α è indotto dal coniugio per uv^{-1}. ∎

Si osservi che se il gruppo G è senza torsione, allora, per l'esercizio 3.36, anche U e V lo sono, e per ragioni simili, anche $\overline{G}$ è senza torsione.

DEFINIZIONE. Sia $\phi : A \to B$ un isomorfismo tra A e B, sottogruppi di un gruppo G. Sia $\langle t \rangle$ un gruppo ciclico infinito; la *estensione HNN di G associata a ϕ*, che denotiamo con $G*_\phi$ è il gruppo quoziente di $G * \langle t \rangle$ modulo il sottogruppo normale generato dall'insieme di elementi $\{tat^{-1}\phi(a)^{-1} \mid a \in A\}$.
Quindi, se $G = \langle X, R \rangle$ è una presentazione di G, e t una nuova lettera:

$$G*_\phi = \langle X, t \mid R \cup \{tat^{-1}\phi(a)^{-1} \mid a \in A\} \rangle. \tag{3.33}$$

G si chiama *base* di $G*_\phi$ e t *stable letter*.

Nella dimostrazione del Teorema 3.26, ponendo $t = uv^{-1}$, il gruppo (sottogruppo di $\overline{G}$) $\langle G, t \rangle$ è la HNN-estensione di G associata a ϕ con stable letter t. In generale, alcune delle caratteristiche di base della struttura di una HNN-estensione, come appena definita, si ricavano dalla esistenza di una *forma normale* per i suoi elementi, che ora descriviamo, tralasciando la dimostrazione.

Lemma 3.27. *Sia $G*_\phi$ la HNN-estensione di G associata a $\phi : A \to B$ con stable letter t, e siano $\mathcal{T}_A$ e $\mathcal{T}_B$ insiemi di rappresentanti delle classi laterali sinistre in G, rispettivamente modulo A e modulo B, contenenti 1. Ogni elemento di $G*_\phi$ si scrive in modo unico nella forma*

$$g_1 t^{\epsilon_1} g_2 t^{\epsilon_2} \cdots g_n t^{\epsilon_n} g^*, \tag{3.34}$$

con $g^* \in G$, $\epsilon_i \in \{1, -1\}$, per ogni $i = 1, \ldots, n$, e

- *$g_i \in \mathcal{T}_A$ se $\epsilon_i = 1$, $\quad g_i \in \mathcal{T}_B$ se $\epsilon_i = -1$;*
- *non ci sono sequenze consecutive del tipo $t^\epsilon 1 t^{-\epsilon}$.*

Corollario 3.28. *Sia $G*_\phi$ la HNN-estensione di G associata a $\phi : A \to \phi(A)$ con stable letter t. Allora*

(1) *$G \subseteq G*_\phi$ e $G*_\phi = \langle G, t \rangle$;*

(2) *$\phi(A) = tAt^{-1} = A^t$ e $G \cap G^t = A^t$.*

Vediamo due notevoli applicazioni.

Teorema 3.29. (Higman, Neumann e Neumann) *Ogni gruppo numerabile è isomorfo ad un sottogruppo di un gruppo 2-generato.*

Dimostrazione. Sia $H = \{1 = x_0, x_1, x_2, \ldots\}$ un gruppo numerabile e $F = F_2$ il gruppo libero generato da $\{a, b\}$. Si considerino i due sottogruppo del prodotto libero $G = H * F$,

$$A = \langle a, a^b, a^{b^2}, \ldots \rangle \qquad \text{e} \qquad B = \langle bx_0, b^a x_1, b^{a^2} x_2, \ldots \rangle$$

Allora $\{a, a^b, a^{b^2}, \dots\}$ è un sistema libero di generatori per A, e $\{bx_0, b^a x_1, b^{a^2} x_2, \dots\}$ un sistema libero di generatori per B (si provino queste affermazioni per esercizio). Porre, per ogni $i \in \mathbb{N}$, $a^{b^i} \mapsto b^{a^i} x_i$, individua un isomorfismo $\alpha : A \to B$, e un'applicazione del Teorema 3.26 assicura l'esistenza di una HNN-estensione $\overline{G} = \langle G, t\rangle$ in cui $(a^{b^i})^t = b^{a^i} x_i$, per ogni $i \in \mathbb{N}$. Ora, il sottogruppo $\langle a, t\rangle$ contiene $a^t = b$ e quindi contiene $(a^{b^i})^t = b^{a^i} x_i$. Dunque $\langle a, t\rangle$ contiene x_i, per ogni $i \in \mathbb{N}$, e pertanto $H \leq \langle a, t\rangle$. ∎

Teorema 3.30. (H.N.N.) *Sia G un gruppo numerabile torsion-free. Esiste un'estensione numerabile W di G in cui ogni tutti gli elementi non banali sono tra loro coniugati.*

Dimostrazione. Sia $G \setminus \{1\} = \{g_0, g_1, g_2, \dots\}$. Per quanto detto sinora, esiste una HNN-estensione G_1 di G tale che g_0, g_1 sono coniugati in G_1, inoltre G_1 è numerabile e torsion-free. Un semplice argomento induttivo stabilisce che esiste una catena di gruppi numerabili torsion-free $G = G_0 \leq G_1 \leq \dots \leq G_n \leq G_{n+1} \leq \dots$ tale che $g_0, g_1, \dots, g_n$ sono coniugati in G_n, per ogni $n \geq 1$. Sia $G^\sharp = \bigcup_{n\geq 0} G_n$; per costruzione, $G^\sharp$ è numerabile torsion-free, contiene G, e tutti glie elementi non-banali di G sono coniugati in $G^\sharp$. A questo punto, si pone $W_0 = G$, e $W_{n+1} = W_n^\sharp$ per ogni $n \geq 0$. Quindi si considera

$$W = \bigcup_{n\in\mathbb{N}} W_n,$$

che è un gruppo numerabile torsion-free in cui tutti gli elementi non banali sono tra loro coniugati. □

NOTA. Questo Teorema vale senza l'ipotesi di numerabilità; in quel caso la dimostrazione (per il resto del tutto analoga a quella nel caso numerabile) parte dalla possibilità di definire un buon ordinamento su G (un Teorema di base in Logica, ma forse non familiare a tutti); ho preferito limitare enunciato e dimostrazione al caso numerabile, visto la natura dimostrativa che questo risultato ha nel piano del corso.

HNN e alberi. Anche le estensioni HNN possono essere caratterizzate da un'azione su un albero.

Proposizione 3.31. *Sia $G = \langle H, t\rangle$ la HNN-estensione del gruppo H associata all'isomorfismo $\phi : A \to \phi(A) = A^t$. Esiste un'azione di G su un albero $T = (V, E)$, senza inversioni e transitiva sia su V che su E. Inoltre, esiste un arco $e = \{x, y\}$ di T tale che $Stab_G(x) = H$, $Stab_G(y) = H^t$ e $Stab_G(e) = A$.*

Dimostrazione. Sia $G = \langle H, t\rangle$ come nelle ipotesi. Definiamo il grafo T ponendo come insieme di vertici l'insieme $V = \{gH \mid g \in G\}$, e stabilendo che ogni vertice gH è adiacente a tutti i vertici $(ht^\epsilon g)H$ con $h \in H$ e $\epsilon \in \{1, -1\}$ (è chiaramente una buona definizione). L'azione di G è quella per moltiplicazione a sinistra, che per definizione è transitiva su V. Ora, gli archi di T incidenti in H sono del tipo $\{H, ht^\epsilon H\}$ con $h \in H$; e si ha $h \cdot \{H, tH\} = \{H, htH\}$, $ht^{-1} \cdot \{H, tH\} = \{ht^{-1}H, H\}$. Quindi, tutti gli archi incidenti a H appartengono alla stessa G-orbita; poiché G è transitivo sui vertici, si conclude che G è transitivo sugli archi di T.
Sia $x = H, y = tH$ allora $e = \{x, y\}$ è un arco, $Stab_G(x) = H$, $Stab_G(y) = H^t$ e, per il Corollario 3.28, $Stab_G(e) = H \cap H^t = A$.
Rimane da provare che T è un albero. Fissati i trasversali di G modulo A e A^t, sia $g \in G$ scritto nella forma normale 3.34. Procedendo per induzione su n (se $n = 0$, $g \in H$ e $gH = H$) si prova abbastanza facilmente che in T esiste un unico cammino

ridotto da H a gH; per la transitività dell'azione di G sui vertici, si conclude che T è un albero. □

Teorema 3.32. *Sia G un gruppo che agisce su un albero $T = (V, E)$, senza inversioni e transitivamente sia su V che su E. Siano $e = \{x, y\} \in E$, $H = Stab_G(x)$, $g \in G$ tale che $g \cdot x = y$, e $A = Stab_G(e)$; allora G è isomorfo alla HNN-estensione con base H associata all'isomorfismo $A \to A^g$ indotto dal coniugio per g in G.*

Dimostrazione. Non è molto diversa da quella del Teorema 3.23. □

Le evidenti affinità tra la caratterizzazioni dei gruppi liberi, dei prodotti amalgamanti e delle HNN-estensioni viste nei teoremi e 3.6, 3.23 e 3.32, suggeriscono la possibilità di un tipo più generale di costruzione, che è infatti prodotta dalla teoria dei *Grafi di Gruppi*, sviluppata da H. Bass e J.-P. Serre. Sarebbe certo interessante parlarne, ma richiederebbe tempo che per ora vogliamo destinare ad altro; una introduzione accessibile si trova nella seconda parte del testo di Bogopolski [2].

Esercizio 3.48. Si dimostri il Teorema 3.32.

Esercizio 3.49. Si provi che esiste un gruppo 2-generato che contiene come sottogruppo una copia isomorfa di qualsiasi gruppo abeliano numerabile.

Esercizio 3.50. Una HNN-estensione $G*_\alpha$ con $\alpha : G \to G$ un omomorfismo iniettivo si dice una estensione HNN ascendente.

(1) Si provi che se $\alpha \in Aut(G)$ allora $G*_\alpha \simeq G \rtimes \langle t \rangle$ dove $|t| = \infty$ e l'azione di t su G è quella di α (cioè $t \cdot g = \alpha(g)$ per ogni $g \in G$).

(2) Sia $\alpha : \mathbb{Z} \to \mathbb{Z}$ la moltiplicazione per $n \geq 1$; si provi che il gruppo $\mathbb{Z}*_\alpha$ ha un sottogruppo normale abeliano il quoziente rispetto al quale è ciclico.

Gruppi di Baumslag–Solitar. Un importante classe di gruppi finitamente presentati è costituita dai *gruppi di Baumslag-Solitar*; ce n'è uno per ogni coppia $m, n \in \mathbb{Z} \setminus \{0\}$, definito nel modo seguente:

$$BS(m, n) = \langle a, b \mid ab^m = b^n a \rangle.$$

$BS(1, 1) = \mathbb{Z} \times \mathbb{Z}$, mentre $BS(1, -1)$ è il gruppo dell'esempio 3.7 [infatti, in $B(1, -1)$ si ha $(ba)^2 = b(ab)a = b(b^{-1}a)a = a^2$]. Anche il gruppo $BS(1, 2)$ lo abbiamo già incontrato, e più volte: è infatti il gruppo dell'esempio 3.3, e quindi, come là dimostrato, quello dell'esempio 1.9. In particolare, il gruppo $BS(1, 2)$ è l'estensione di un sottogruppo dei razionali per un gruppo ciclico infinito. Questo vale in generale per i gruppi $BS(1, n)$: procedendo come nell'esempio 3.3 si dimostra che, per $n \geq 1$,

$$BS(1, n) \simeq \mathbb{Z}[1/n] \rtimes \langle \alpha \rangle,$$

dove $\mathbb{Z}[1/n]$ è il gruppo additivo dei numeri razionali il cui denominatore è (divide, se la rappresentazione è primitiva) una potenza di n, e α l'automorfismo di $\mathbb{Z}[1/n]$ definito da $a(x) = nx$ per ogni $x \in \mathbb{Z}[1/n]$. Come per $BS(1, 2)$ nell'esercizio 1.25 si dimostra che $BS(1, n)$ è isomorfo al sottogruppo di $Aut(\mathbb{R}, \geq)$ generato da f, g con

$$f(x) = nx, \quad g(x) = x + 1$$

per ogni $x \in \mathbb{R}$. Una rappresentazione di $BS(1, n)$ come gruppo lineare è suggerita nell'esercizio 3.51.

Il gruppo $BS(1,n)$ compare anche nel punto (2) dell'esercizio 3.50 come estensione HNN. E in generale, i gruppi di Baumslag–Solitar sono estensioni HNN: sia $\langle b\rangle$ un gruppo ciclico infinito e $\phi : \langle g^m\rangle \to \langle g^n\rangle$ l'isomorfismo determinato da $\phi(b^m) = b^n$, allora la HNN-estensione di $\langle b\rangle$ associata a ϕ con stable letter a è, per (3.33)

$$\langle b\rangle *_\phi = \langle a, b \mid ab^m a^{-1}\phi(b^m)^{-1} = \langle a, b \mid ab^m a^{-1}b^{-n} = 1\rangle = BS(m,n).$$

DEFINIZIONE. Un gruppo G si dice *hopfiano* se non è isomorfo ad alcun suo quoziente proprio (cioè $G \not\cong G/N$ per ogni $1 \neq N \trianglelefteq G$), ovvero se ogni omomorfismo suriettivo da G in se stesso è un isomorfismo.

Sono hopfiani i gruppi finiti, i gruppi semplici e i gruppi liberi di rango finito (vedi esercizio 3.20 oppure la prossima proposizione), ed anche il gruppo additivo $\mathbb{Q}$ dei razionali. Di contro, non è difficile trovare gruppi non-hopfiani tra quelli non finitamente generati: ad esempio sono non-hopfiani, i gruppi di Prüfer C_∞ e i gruppi liberi di rango infinito. Più difficile è reperire gruppi finitamente generati non-hopfiani (questa era la domanda originalmente posta da H. Hopf (1894–1971)). Ad esempio, vale il seguente risultato

Proposizione 3.33. *Ogni gruppo finitamente generato e residualmente finito è hopfiano.*

Dimostrazione. Sia G un gruppo finitamente generato e residualmente finito e sia $\phi : G \to G$ un omomorfismo suriettivo. Supponiamo per assurdo che esista $1 \neq x \in K = \ker\phi$. Allora esiste un sottogruppo normale N di indice finito in G tale che $x \notin N$. Poiché G è finitamente generato il numero di sottogruppi normali di G il cui indice è al più $k = |G/N|$ è finito (Proposizione 1.11); siano $M_1, \ldots, M_n$ tali sottogruppi. Allora le immagini inverse $\phi^{-1}(M_1), \ldots, \phi^{-1}(M_n)$ sono n sottogruppi normali e distinti di G di indice al più k, quindi tra di loro c'è anche il sottogruppo N, il che è una contraddizione dato che $N \not\geq K$. ∎

Gruppi finitamente generati non-hopfiani esistono, e ne parliamo qui perché molti dei gruppi di Baumslag-Solitar sono esempi di gruppi finitamente presentati e non-hopfiani (un diverso esempio, che è anche un gruppo risolubile, è descritto nell'esercizio 3.52.

Proposizione 3.34. *Siano nm interi coprimi e diversi da $0, 1, -1$; allora il gruppo di Baumslag–Solitar $BS(m,n)$ è non-hopfiano.*

Dimostrazione. Siano m, n come nelle ipotesi, sia $G = BS(m,n) = \langle a, b \mid ab^m = b^n a\rangle$, e sia $H = \langle a, b^m\rangle$. Poiché m, n sono coprimi, esistono interi $u, v \in \mathbb{Z}$ tali che $1 = mu + nv$; quindi

$$H \ni ab^{mv}a^{-1}b^{mu} = b^{nv}b^{mu} = b^{nv+mu} = b,$$

quindi $H = G$. Ora, $a(b^m)^m a^{-1} = (ab^m a^{-1})^m = (b^n)^m = (b^m)^n$, da cui $a(b^m)^m = (b^m)^n a$. Quindi, per il Teorema di von Dyck, esiste un omomorfismo suriettivo $\phi : G \to G$ tale che $\phi(a) = a$ e $\phi(b) = b^m$. Proviamo che ϕ non è iniettivo, utilizzando l'interpretazione di G come HNN-estensione in cui a è la stable letter. Così, abbiamo

$$\phi(aba^{-1}b^{-1}) = ab^m a^{-1}b^{-m} = b^{n-m} = \phi(b^{-1}aba^{-1}),$$

mentre, in G, $aba^{-1}b^{-1} \neq b^{-1}aba^{-1}$ per il Lemma 3.27. Dunque ϕ non è iniettivo, il che mostra che G non è hopfiano. ∎

Esercizio 3.51. Si provi che per ogni $n \geq 1$ il gruppo $BS(1,n)$ è isomorfo al sottogruppo di $GL(2,\mathbb{R})$

$$\left\langle \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

Esercizio 3.52. (P. Hall: un gruppo risolubile f.g. non hopfiano). Sia $\mathbb{Z}[1/2]$ l'anello dei razionali della forma $m2^z$ con $m, z \in \mathbb{Z}$, e sia $U = UT(3,\mathbb{Z}[1/2])$ il gruppo delle matrici unitriangolari superiori di ordine 3 su $\mathbb{Z}[1/2]$; siano

$$g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \zeta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

e $G = \langle U, g\rangle$. Poiché g normalizza U sia ha $G = U \rtimes \langle g\rangle$ (con $\langle g\rangle$ gruppo ciclico infinito); inoltre $\zeta \in Z(G)$. Si provi che G è finitamente generato, e che porre $g \mapsto g$ e, per ogni $a, b, c \in \mathbb{Z}[1/2]$,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & a & 2b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

definisce un automorfismo di G. A questo punto si provi che $H = G/\langle\zeta\rangle$ non è hopfiano

Esercizio 3.53. Si provi che il gruppo del Lampionaio è hopfiano.

Esercizio 3.54. È vero che ogni quoziente di un gruppo hopfiano è hopfiano?

Esercizio 3.55. Diciamo che un gruppo G soddisfa la condizione di massimo sui sottogruppi normali (*Max*-n) se ogni catena $N_1 \leq N_2 \leq \dots$ di sottogruppi normali N_1 di G è finita. Si provi che *Max*-n implica hopfiano.

4

Quasi-isometrie

Se uno degli obiettivi generali, inarrivabile certo ma, almeno, dicibile, della Teoria dei gruppi finiti è la loro classificazione a meno di isomorfismo, questa prospettiva, per gruppi infiniti (e finitamente generati) costituirebbe una ambizione assolutamente smodata. Si è quindi giunti a elaborare, per gruppi finitamente generati, una diversa nozione di equivalenza, la *quasi-isometria*, molto più debole dell'isomorfismo, e tuttavia in grado di discernere tra diverse tipologie (e di descriverne alcune) che, secondo un'espressione ricorrente, riguardano proprietà su "larga scala" di un gruppo. Questo capitolo è una prima introduzione a tale concetto, che è uno degli strumenti fondamentali della Teoria geometrica dei gruppi.

4.1. Isometrie e quasi-isometrie

Cominciamo ricordando la definizione di spazio metrico.

DEFINIZIONE. Uno *spazio metrico* è una coppia (X, d) consistente in un insieme X e una applicazione $d : X \times X \to \mathbb{R}_{\geq 0}$ che soddisfa le proprietà seguenti:

- per ogni $x, y \in X$, $d(x, y) = 0 \Leftrightarrow x = t$;
- per ogni $x, y \in X$, $d(x, y) = d(y, x)$;
- (diseguaglianza triangolare) per ogni $x, y, z \in X$,

$$d(x, y) + d(y, z) \leq d(x, z).$$

Diversi spazi metrici importanti sono certamente già noti a chi legge, alcuni dei quali saranno richiamati in esempi o esercizi a seguire. E certamente è familiare come ad uno spazio metrico (X, d) sia canonicamente associato un spazio topologico (X, τ_d) dove la topologia τ_d è quella una cui base di aperti è costituita dalla *palle aperte*

$$\mathcal{B}(x_0, r) = \{x \in X \mid d(x_0, x) < r\}$$

al variare di $x_o \in X$ e $0 < r \in \mathbb{R}$.

Metrica di grafo. Ogni grafo connesso Γ ammette una distanza naturale d_Γ (sezione 2.1) definita, per ogni coppia (u, v) di vertici, come la lunghezza minima di un cammino da u a v, ed è quindi uno spazio metrico. In questo caso la topologia associata è quella discreta, ma più avanti tratteremo realizzazioni geometriche di grafi e la metrica sarà quella indotta da quella dello spazio che contiene la realizzazione.

Word metric. Se G è un gruppo ed S un suo sistema di generatori non contenente 1_G, la *word metric* di G rispetto a S è la distanza d_S nel grafo di Cayley $\Gamma[G, S]$; quindi, per ogni $g, h \in G$,

$$d_S(g, h) = \ell_S(g^{-1}h)$$

dove $\ell_S(x)$ è la lunghezza di x in S (vedi sezione 2.4).

DEFINIZIONI. Siano (X, d_X) e (Y, d_Y) spazi metrici; una applicazione $f : X \to Y$ si dice *inclusione isometrica* se, per ogni $x, x' \in X$,

$$d_Y(f(x), f(x')) = d_X(x, x')$$

Una *isometria* è un'inclusione isometrica invertibile. Se $f : X \to Y$ è un'isometria, allora evidentemente anche la funzione inversa $f^{-1} : Y \to X$ è un'isometria. Gli spazi (X, d_X) e (Y, d_Y) si dicono *isometrici* se esiste un'isometria dall'uno nell'altro.

Si osservi che ogni inclusione isometrica è iniettiva. Ancora, se (X, d_X), (Y, d_Y), (Z, d_Z) sono spazi metrici e $f : X \to Y$, $g : Y \to Z$ sono inclusioni isometriche (isometrie), allora la composizione $g \circ f : X \to Z$ è un'inclusione isometrica (isometria). In particolare, l'insieme delle isometrie di un spazio (X, d) in se stesso

$$\mathrm{Isom(X)} = \{\mathrm{f : X \to X \mid f \text{ isometria}}\},$$

è un gruppo rispetto alla composizione. Un'azione *per isometrie* di un gruppo G sullo spazio (X, d) è un omomorfismo $G \to \mathrm{Isom(X)}$. Se G è un gruppo e S un suo sistema di generatori non contenente 1, l'azione per moltiplicazione a sinistra di G sulla spazio (G, d_S) è un'azione per isometrie.

Quando associata a gruppi (finitamente generati), la relazione di isometria è troppo restrittiva e inadatta: due diverse word-metrics sullo stesso gruppo G sono in genere non isometriche, dunque la nozione di isometria non può essere trasferita dai singoli spazi (G, d_S) ai gruppi in se stessi. Affidiamo ad un semplice esempio il compito di introdurre una prima nozione più lasca di equivalenza tra spazi metrici.

Esempio 4.1. Sull'insieme $\mathbb{R}^2$ denotiamo con d l'usuale metrica euclidea (o "standard") e con d_1 la metrica definita da, per ogni $(x, y), (x', y') \in \mathbb{R}^2$,

$$d_1((x, y), (x', y')) = |x - x'| + |y - y'|.$$

Gli spazi $(\mathbb{R}^2, d)$ e $(\mathbb{R}^2, d)$ non sono isometrici, tuttavia, per ogni $a = (x, y), b = (x', y') \in \mathbb{R}^2$,

$$\frac{1}{2}d(a, b) \leq d_1(a, b) \leq 2d(a, b);$$

e questo basta a far sì, ad esempio, che d e d_1 definiscano la stessa topologia su $\mathbb{R}^2$. □

L'esempio che precede suggerisce la seguente

DEFINIZIONE. Siano (X, d_X) e (Y, d_Y) spazi metrici. Un'applicazione $f : X \to Y$ si dice *equivalenza bi-lipschitziana* se è biettiva[1] ed esiste una costante $1 \leq C \in \mathbb{R}$ tale che

$$C^{-1}d_X(x, x') \leq d_Y(f(x), f(x')) \leq Cd_X(x, x'),$$

per ogni $x, x' \in X$.

È chiaro che inverse e composizioni di equivalenze bi-lipschitziane sono equivalenze bi-lipschitziane, e dunque questa relazione stabilisce un'equivalenza nella classe degli spazi metrici. Quello che poi ci interessa è la seguente facile osservazione.

[1] Naturalmente, si definiscono anche le inclusioni bi-lipschitziane per le quali non è richiesta la biettivitá; vedi esercizio 4.4.

Proposizione 4.1. *Sia G un gruppo finitamente generato, e siano X, Y insiemi finiti di generatori di G, non contenenti 1. Allora la funzione identica su G è una equivalenza bi-lipschitziana tra gli spazi (G, d_X) e (G, d_Y).*

Dimostrazione. Poiché X e Y sono finiti esiste un intero $M \geq 1$ tale che $\ell_X(y) \leq M$ per ogni $y \in Y$ e $\ell_Y(x) \leq M$ per ogni $x \in X$. Ne segue che, per ogni $g, h \in G$,

$$d_Y(g,h) = \ell_Y(g^{-1}h) \leq M\ell_X(g^{-1}h) = Md_X(g,h)$$

e, simmetricamente, $d_X(g,h) \leq Md_Y(g,h)$. Dunque

$$M^{-1}d_X(g,h) \leq d_Y(g,h) \leq Md_X(g,h),$$

provando che l'identità è un'equivalenza bi-lipschitziana tra (G, d_X) e (G, d_Y). □

È dunque possibile trasferire ai gruppi la relazione: diciamo che due gruppi finitamente generati G e H sono bi-lipschitz equivalenti se per qualche (quindi, per qualsiasi) coppia S, T di sistemi finiti di generatori di G e H rispettivamente, esiste un'equivalenza bi-lipschitziana tra gli spazi (G, d_S) e (H, d_T).

Sembra che ci siamo. Ma anche l'equivalenza bi-lipschitziana si rivela operativamente non del tutto funzionale, e concettualmente ancora un poco ristretta. Un tratto di questa rigidità è, mi pare, la biettività; ad esempio, spazi di cardinalità diversa non possono essere bi-lipschitz equivalenti, mentre, per utilizzare l'immagine normalmente evocata a questo punto, vorremo comprendere nella stessa tipologia spazi che tendono a confondersi se "visti da molto molto lontano", come ad esempio gli spazi standard $\mathbb{Z}$ e $\mathbb{R}$ (che tendono entrambi a sembrare una retta), oppure due spazi finiti qualsiasi.

Quasi-isometrie. La nozione, più debole, di quasi-isometria, oltre ad essere, come vedremo nelle dimostrazioni, uno strumento più duttile, è quella che meglio espleta il compito di accomunare spazi che non si distinguono quando "visti da lontano".

Definizioni. Siano $(X, d_X), (Y, d_Y)$ spazi metrici.

(1) Un'applicazione $f : X \to Y$ si dice *inclusione quasi-isometrica* se esistono costanti $\lambda \geq 1, C \geq 0$ tali che

$$\lambda^{-1}d_X(x,x') - C \leq d_Y(f(x), f(x')) \leq \lambda d_X(x,x') + C, \tag{4.1}$$

per ogni $x, x' \in X$. Con maggiore precisione diremo che una tale f è un'inclusione (λ, C)-quasi-isometrica.

(2) Un'applicazione $g : Y \to X$ si dice una *quasi-inversa* dell'inclusione (λ, C)-quasi-isometrica $f : X \to Y$ se g è un'inclusione (λ, C)-quasi-isometrica ed esiste una costante $K \geq 0$ tale che, per ogni $x \in X$ e $y \in Y$,

$$d_X(gf(x), x) \leq K \quad \text{e} \quad d_Y(fg(y), y) \leq K. \tag{4.2}$$

(3) Un'inclusione (λ, C)-quasi-isometrica che ammette una quasi-inversa[2] si dice una *quasi-isometria* (se si desidera essere precisi sui parametri, si parlerà di (λ, C)-quasi-isometria). Due spazi metrici (X, d_X) e (Y, d_Y) si diranno *quasi-isometrici* se esiste una quasi-isometria $f : X \to Y$. In tal caso, scriveremo $X \sim_{QI} Y$.

[2]Si veda l'esercizio 4.1 per un criterio di esistenza di una quasi-inversa.

Se $f : X_1 \to X_2$, $g : X_2 \to X_3$ sono, rispettivamente, inclusioni (λ, C) e (μ, D) quasi-isometriche tra gli spazi X_1, X_2, X_3, allora l'applicazione composta $g \circ f : X_1 \to X_3$ è un'inclusione $(\lambda\mu, \mu C + D)$-quasi-isometrica. In particolare, la relazione di quasi-isometria tra spazi metrici è transitiva (oltre che riflessiva e simmetrica).

ESEMPI E OSSERVAZIONI. 1) Per ogni $x \in \mathbb{R}$, sia $\lfloor x \rfloor \in \mathbb{Z}$ la "parte intera" di x (il massimo numero intero non superiore a x). Si verifica facilmente che, per ogni $x, y \in \mathbb{R}$,

$$|x - y| - 1 < |\lfloor x \rfloor - \lfloor y \rfloor| < |x - y| + 1.$$

Dunque la funzione parte intera $\lfloor \cdot \rfloor$ è un'inclusione $(1, 1)$-quasi-isometrica di $\mathbb{R}$ in $\mathbb{Z}$, intesi con le usuali distanza sulla retta: $d(x, y) = |x - y|$. L'immersione identica $\mathbb{Z} \to \mathbb{R}$ preserva la distanza, dunque è un'inclusione $(1, 0)$-quasi-isometrica (a maggior ragione $(1, 1)$-quasi-isometrica), ed è una quasi-inversa di $\lfloor \cdot \rfloor$ (la (4.2) è verificata con $K = 1$). Pertanto, la parte intera è una quasi isometria da $\mathbb{R}$ in $\mathbb{Z}$; questo esempio mostra, in particolare, che, diversamente dalle inclusioni ismotriche, una quasi-isometria non è necessariamente iniettiva, né continua.
In generale, per ogni $n \geq 1$, gli spazi metrici $(\mathbb{Z}^n, d), (\mathbb{R}^n, d)$ (dove d è la distanza euclidea) sono quasi-isometrici; più precisamente, l'immersone identica $Z^n \to \mathbb{R}^n$ è una quasi-isometria.

2) Per ogni coppia di interi $n, m \geq 1$, $\mathbb{R}^n \sim_{\mathrm{QI}} \mathbb{R}^m$ se e solo se $n = m$ (questo lo dimostreremo più avanti, vedi Proposizione 4.15).

3) Sia X uno spazio metrico di diametro finito D, e $Y = \{y\}$ lo spazio costituito da un unico punto; la sola funzione f da X in Y ($f(x) = y$ per ogni $x \in X$) è una $(1, D)$-quasi-isometria (qualsiasi funzione $Y \to X$ è una sua quasi-inversa). Viceversa, sia (X, d) uno spazio metrico quasi-isometrico ad un punto, allora, in particolare esistono costanti $\lambda \geq 1, C \geq 0$ tali che, per ogni coppia $x, x' \in G$,

$$\lambda^{-1} d(x, x') - C \leq 0,$$

e dunque $d(x, x') \leq \lambda C$. Quindi, uno spazio metrico è quasi-isometrico ad un punto se e soltanto se ha diametro finito.
In particolare, la retta euclidea $\mathbb{R}$ non è quasi-isometrica all'intervallo limitato $[0, 1]$; questo si può vedere anche direttamente, osservando che per ogni $\lambda \geq 1$ e $C \geq 0$ esistono $x, y \in \mathbb{R}$ tali che $\lambda^{-1}|x - y| - C > 1$; dunque non esiste alcuna inclusione quasi-isometrica da $\mathbb{R}$ in $[0, 1]$.

Poiché le equivalenze bi-lipschitziane sono quasi-isometrie, dalla Proposizione 4.1, segue il segunet fatto fondamentale.

Proposizione 4.2. *Sia G un gruppo finitamente generato, e siano X, Y insiemi finiti di generatori di G, non contenenti 1. Allora la funzione identica su G è una quasi-isometria tra i grafi di Cayley $\Gamma[G, X]$ e $\Gamma[G, Y]$. Ovvero, gli spazi (G, d_X) e (G, d_Y) sono quasi-isometrici.*

DEFINIZIONE. Due gruppi finitamente generati G e H sono *quasi–isometrici*, e scriveremo $G \sim_{\mathrm{QI}} H$, se per qualche (quindi, per qualsiasi) coppia S, T si sistemi finiti di generatori di G e H rispettivamente, gli spazi (G, d_X) e (G, d_Y) sono quasi-isometrici[3].

[3]In generale, se G è un gruppo e (X, d) uno spazio metrico, scriviamo $G \sim_{\mathrm{QI}} X$ se X è quasi-isometrico ad un grafo di Cayley per un sistema finito di generatori di G.

Ad esempio, $\mathbb{Z} \sim_{QI} D_\infty$ (abbiamo visto che tali gruppi ammettono grafi di Cayley isomorfi); inoltre il grafo di Cayley di D_∞ nell'esempio 2.7 è anche un grafo di Cayley per il prodotto diretto $\mathbb{Z} \times C_2$. Sono quindi tra loro quasi isometrici i tre gruppi (non-isomorfi), $\mathbb{Z}$, $\mathbb{Z} \times C_2$, D_∞; questa semplice osservazione sarà generalizzata più avanti, nel senso che tutti i gruppi che hanno un sottogruppo di indice finito isomorfo a $\mathbb{Z}$ sono quasi-isometrici a $\mathbb{Z}$.

Per l'osservazione 3) di sopra, un gruppo finitamente generato è quasi-isometrico allo spazio costituito da un unico punto se e solo se, per ogni sistema finito S di generatori di G il diametro del grafo di Cayley $\Gamma[G, S]$ è finito; ovvero se e solo se esiste $D \geq 0$ tale che $\ell_S(x) \leq D$ per ogni $x \in G$; il che, essendo S finito, equivale a dire che G è un gruppo finito.

Concludiamo la sezione con due osservazioni che ci saranno diverse volte utili. La prima è nell'ambito, appunto, dei gruppi finitamente generati: abbiamo detto fin da subito che una quasi-isometria f non è necessariamente iniettiva, tuttavia, se il dominio di f è uno spazio di tipo (G, d_S) allora f è quasi-iniettiva, nel senso dell'enunciato che segue.

Lemma 4.3. *Siano G un gruppo finitamente generato, S un sistema finito di generatori di G e $f : G \to X$ un'inclusione isometrica da (G, d_S) in uno spazio metrico (X, d). Allora, per ogni sottoinsieme finito B di X, $f^{-1}(B)$ è finita.*

Dimostrazione. Sia $f : G \to X$ una (λ, C)-inclusione isometrica; è sufficiente provare che $f^{-1}(\{b\})$ è finito per ogni $b \in X$. Supponiamo $f^{-1}(\{b\}) \neq \emptyset$ e siano $x, x' \in f^{-1}(\{b\})$. Allora, $\lambda^{-1} d_S(x, x') \leq d(f(x), f(x')) + C = C$, quindi $x' \in B_S(x, \lambda C)$. Poiché S è finito, la palla chiusa $B_S(x, \lambda C)$ è finita, e questo finisce anche la dimostrazione. □

La seconda osservazione è un criterio di quasi-invertibilità, la cui dimostrazione (che usa l'assioma della scelta) è lasciata per esercizio.

Lemma 4.4. *Siano (X, d_X) e (Y, d_Y) spazi metrici e $f : X \to Y$ un'inclusione quasi-isometrica; allora f è una quasi-isometria se e solo se esiste una costante $D > 0$ tale che per ogni $y \in Y$ esiste un punto $x \in X$ per cui $d_Y(f(x), y) \leq D$. In particolare, un'inclusione quasi-isometrica suriettiva è una quasi-isometria.*

Esercizio 4.1. Si provi il Lemma 4.4.

Esercizio 4.2. Sia $\mathbb{R}$ la retta reale con la metrica standard, e siano $f, g : \mathbb{R} \to \mathbb{R}$ definite nel modo seguente:

$$f(x) = \begin{cases} x + 2 & \text{se } x \in \mathbb{Z} \setminus \{0\} \\ x & \text{altrimenti} \end{cases}$$

$$g(x) = \begin{cases} 2x & \text{se } x \in \mathbb{Z} \setminus \{0\} \\ x & \text{altrimenti} \end{cases}$$

Si provi che f è una quasi-isometria, mentre g non lo è.

Esercizio 4.3. Si dimostri nei dettagli che per ogni $n \geq 1$ gli spazi $\mathbb{Z}^n$ e $\mathbb{R}^n$ (con la metrica euclidea standard) sono quasi-isometrici. Si provi quindi che lo stesso vale se si dota $\mathbb{Z}^n$ della metrica d_1 definita da

$$d_1((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i=1}^{n} |x_i - y_i|,$$

per ogni $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{Z}^n$ (in $\mathbb{R}^n$ tale metrica si chiama di solito metrica ℓ^1).

ESERCIZIO 4.4. Se (X, d_X) e (Y, d_Y) sono spazi metrici, un'applicazione $f : X \to Y$ si dice *inclusione bi-lipschitziana* se esiste una costante $1 \leq C \in \mathbb{R}$ tale che, per ogni $x, x' \in X$,

$$C^{-1} d_X(x, x') \leq d_Y(f(x), f(x')) \leq C d_X(x, x'),$$

(un'inclusione bi-lipschitziana è chiaramente una funzione iniettva, se è suriettiva è un'equivalenza bi-lipschitziana). Siano G, H due gruppi finitamente generati quasi-isometrici ed S, T sistemi finiti di generatori di G e, rispettivamente, di H; si provi che esistono inclusioni bi-lipschitziane $f : (G, d_S) \to (H, d_T)$ e $g : (H, d_T) \to (G, d_S)$ che sono quasi-inverse una dell'altra, ma che G non è necessariamente bi-lipschitz equivalente ad H.

ESERCIZIO 4.5. Sia (X, d) uno spazio metrico; si dice che due applicazioni $f, g : X \to X$ hanno *distanza finita* se

$$\sup_{x \in X} d(f(x), g(x)) < \infty.$$

1) Si provi che se $f, g : X \to X$ hanno distanza finita e f è una quasi-isometria allora g è una quasi-isometria.
2) Si provi che l'avere distanza finita definisce una relazione di equivalenza nell'insieme $\Omega = X^X$ di tutte le applicazioni da X in se stesso.
3) Denotando, per ogni $f \in \Omega$, con $[f]$ la classe di equivalenza di f si provi che porre $[f][g] = [f \circ g]$ definisce un'operazione nell'insieme

$$\mathcal{QI}(X) = \{[f] \mid f \in \Omega,\ f \text{ quasi-isometria}\},$$

rispetto alla quale $\mathcal{QI}(X)$ è un gruppo, detto *gruppo di quasi-isometria* di X.

ESERCIZIO 4.6. Si provi che se X e Y sono spazi quasi–isometrici allora $\mathcal{QI}(X) \simeq \mathcal{QI}(Y)$.

ESERCIZIO 4.7. Si provi che il gruppo moltiplicativo $\mathbb{R}^*$ è un sottogruppo del qruppo $\mathcal{QI}(\mathbb{Z})$ delle quasi-isometrie dello spazio $\mathbb{Z}$. [sugg. per ogni $0 \neq r \in \mathbb{R}$ si consideri la quasi-isometria di $\mathbb{Z}$ definita da $x \mapsto \lfloor rx \rfloor$ per ogni $x \in \mathbb{Z}$]

4.2. Spazi geodetici e realizzazione geometrica

DEFINIZIONE. Sia (X, d) uno spazio metrico; un *segmento geodetico* in X è un'inclusione isometrica $\gamma : [0, r] \to X$, dove $0 \leq r \in \mathbb{R}$ e la metrica dell'intervallo reale $[0, r]$ è quella standard ereditata da $\mathbb{R}$. Il numero reale r è detto lunghezza del segmento geodetico γ, mentre i punti $\gamma(0)$ e $\gamma(r)$ di X si dicono punto iniziale e punto terminale del segmento. Una *retta geodetica* è un'immersione isometrica $\mathbb{R} \to X$.

OSSERVAZIONE. Sia γ un segmento geodetico nello spazio (X, d), con punto iniziale x, punto terminale y, e lunghezza r; allora, poiché γ è isometrica, $r = d_X(x, y)$.

DEFINIZIONE. Uno spazio metrico (X, d) è detto uno spazio *geodetico* se per ogni coppia $x, y \in X$ esiste un segmento geodetico in X con punto iniziale x e punto terminale y (in genere si tende a identificare un segmento geodetico Γ con la sua immagine in X).

Ad esempio, per ogni $n \geq 1$, lo spazio euclideo $\mathbb{R}^n$ è geodetico, ed i segmenti geodetici non sono altro che i segmenti standard di retta; mentre lo stesso spazio privato di un punto non è geodetico (ad esempio, in $\mathbb{R}^n \setminus \{0\}$ non esiste alcun segmento geodetico tra un punto $P \neq 0$ e il punto $-P$).
Un altro esempio di spazio geodetico è il piano iperbolico $\mathbb{H}^2$, al quale abbiamo accennato nella sezione 3.5; in tal caso i segmenti geodetici sono tratti di rette verticali o di semicirconferenze centrate sull'asse delle x.

Un grafo connesso localmente finito (e non banale) $\Gamma = (V, E)$ con la metrica di grafo non è uno spazio geodetico, ma può essere reso tale mediante la cosiddetta *realizzazione geometrica* $|\Gamma|$; si tratta essenzialmente dello spazio ottenuto dotando ogni arco di Γ della natura di intervallo reale $[0, 1]$, e definendo la metrica "sovrapponendo" alla metrica del grafo la metrica standard di $[0, 1]$ su ogni arco. Ad esempio, la realizzazione geometrica del grafo di Cayley $\Gamma[\mathbb{Z}, 1]$ è la retta reale $\mathbb{R}$.

La descrizione formale è abbastanza naturale anche se tecnicamente richiede qualche attenzione. Se Γ consiste di un solo punto isolato allora $|\Gamma| = \Gamma$. Assumiamo di qui in avanti che questo non sia il caso ovvero, essendo Γ connesso, $E \neq \emptyset$. Si comincia fissando un 'verso' per ogni arco di Γ; una maniera per farlo è di fissare un ordinamento totale $\leq$ su V (questo è sempre possibile farlo), quindi ad ogni arco $\{x, y\} \in E$ si associa la coppia ordinata (x, y) se $x \leq y$. Posto $\overline{E} = \{(x, y) \mid \{x, y\} \in E,\ x \leq y\}$, sull'insieme $\overline{E} \times [0, 1]$ si definisce la relazione $\sim$ ponendo, per $(x, y), (x', y') \in \overline{E}$ e $t, t' \in [0, 1]$,

$$((x, y), t) \sim ((x', y'), t')$$

se $((x, y), t) = ((x', y'), t')$, oppure

- $x = x'$ e $t = t' = 0$;
- $y = y'$ e $t = t' = 1$;
- $x = y'$, $t = 0$ e $t' = 1$;
- $y = x'$, $t = 1$ e $t' = 0$.

(si verifica facilmente che si tratta di una equivalenza). Poniamo ora

$$|\Gamma| = (\overline{E} \times [0, 1])/\sim$$

e su di esso definiamo la distanza $d_{|\Gamma|}$. Dati due punti $[(x, y), t], [(x', y'), t'] \in |\Gamma|$ (le parentesi quadre indicano che stiamo considerando classi di equivalenza), definiamo $D = d_{|\Gamma|}([(x, y), t], [(x', y'), t'])$ nel modo che segue:

$$D = |t' - t| \text{ se } (x, y) = (x', y'),$$

mentre, se $(x, y) \neq (x', y')$,

$$D = \min\{t + d_\Gamma(x, x') + t',\ t + d_\Gamma(x, y') + 1 - t',\ 1 - t + d_\Gamma(y, x') + t',\ 1 - t + d_\Gamma(y, y') + 1 - t'\}.$$

Calcoli magari un po' laboriosi ma semplici, mostrano che $d_{|\Gamma|}$ è ben definita ed è una metrica su $|\Gamma|$. Lo spazio $(|\Gamma|, d_{|\Gamma|})$ è la *realizzazione geometrica* del grafo Γ. Si prova anche che la realizzazione geometrica non dipende dalla scelta dell'orientazione scelta su Γ per definirla.

Si dimostra quindi che $(|\Gamma|, d_{|\Gamma|})$ è uno spazio geodetico. Anche questa è una dimostrazione tediosa ma non difficile. Siano $u = [(x, y), t], u' = [(x', y'), t']$ due punti di $|\Gamma|$ e supponiamo, ad esempio, che $R = d_{|\Gamma|}(u, u') = t + d_\Gamma(x, x') + t'$ (gli altri casi sono del tutto analoghi); allora esiste in Γ un cammino $x, x_1, \ldots x_{m-1}, x_m = x'$ di lunghezza minima $m = d_X(x, x')$ da x a x', i cui vertici sono tutti diversi da y e y'; si definisce allora il segmento geodetico $\gamma : [0, R] \to |\Gamma|$, da u a u', ponendo

$$\gamma(r) = \begin{cases} [(x, y), t - r] \text{ per } r \in [0, t] \\ [(x', y'), r - R + t'] \text{ per } r \in [R - t', R], \end{cases}$$

e "stendendo" isometricamente l'intervallo $[t, R-t'] = [t, t+1] \cup \ldots \cup [t+m-1, t+m]$ a tratti lungo gli archi del cammino dato.

Osserviamo che, se Γ non è un albero, allora, diversamente ad esempio dagli spazi euclidei $\mathbb{R}^n$, tra due punti distinti di $|\Gamma|$ può distendersi più di un segmento geodetico. Omettiamo ulteriori dettagli, che costituirebbero la dimostrazione del punto (1) della seguente Proposizione; la dimostrazione del punto (2), che consiste in una verifica, e quella del punto (3), poco più che una constatazione, sono lasciate per esercizio.

Proposizione 4.5. *Sia $\Gamma = (V, E)$ un grafo connesso. Allora*

(1) *la realizzazione geometrica $(|\Gamma|, d_{|\Gamma|})$ è uno spazio metrico geodetico;*

(2) *l'immersione identica $V \to |\Gamma|$ è un'immersione isometrica ed una quasi-isometria di (V, d_Γ) in $(|\Gamma|, d_{|\Gamma|})$;*

(3) *ogni automorfismo del grafo Γ si estende canonicamente ad un'isometria dello spazio metrico $|\Gamma|$.*

Il caso che ci riguarda maggiormente è quello di un grafo di Cayley Γ per un gruppo finitamente generato G; dove l'azione per moltiplicazione a sinistra di G su Γ, che è un'azione per isometrie, si estende canonicamente ad un'azione di G, sempre per isometrie (lineari a tratti), sulla spazio geodetico $|\Gamma|$ (e si osservi che, in tali casi, G agisce liberamente su $|\Gamma|$). Nel seguito, è possibile che non faremo troppe distinzioni fra le due cose.

Esercizio 4.8. Si completi la dimostrazione della Proposizione 4.5.

Esercizio 4.9. Posto $S = \{(1,0), (0,1)\}$, si provi che la realizzazione geometrica di $\Gamma[\mathbb{Z}^2, S]$ è isometrica al sottospazio di $\mathbb{R}^2$,

$$X = \{(x, y) \in \mathbb{R}^2 \mid x \in \mathbb{Z} \text{ o } y \in \mathbb{Z}\}$$

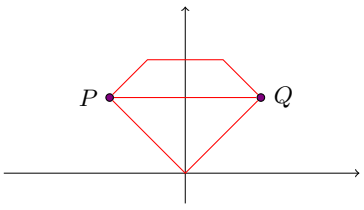
con la metrica indotta dalla metrica d_1 su $\mathbb{R}^2$ (vedi esercizio 4.3).

Esercizio 4.10. Sia $\Gamma = (V, E)$ un grafo e sia Γ^o la sua suddivisione baricetrica. Si provi che le realizzazioni geometriche di Γ e Γ^0 sono quasi-isometriche.

Esercizio 4.11. Sull'insieme $\mathbb{R}^2$ si consideri la metrica d_∞ definita da

$$d_\infty((x, y), (x', y')) = \max\{|x - x'|, |y - y'|\}.$$

1) Si provi che $(\mathbb{R}^2, d_\infty)$ è uno spazio geodetico ma non *univocamente geodetico* (nel senso che non è necessariamente unico il segmento geodetico tra due diversi punti).



geodetiche in $(\mathbb{R}^2, d_\infty)$

2) Si dica se lo spazio $(\mathbb{R}^2 \setminus \{(0,0)\}, d_\infty)$ è uno spazio geodetico.

4.3. Il Lemma di Milnor-Švarc

Il risultato principale dimostrato in questa sezione, il Lemma di Milnor-Švarc, è normalmente celebrato dagli intenditori come *l'osservazione fondamentale della Teoria Geometrica dei Gruppi*. Esso stabilisce una connessione diretta tra due delle prospettive principali di questa teoria: lo studio delle azioni (come isometrie) di gruppi su spazi metrici e l'indagine delle proprietà dei gruppi finitamente generati in quanto spazi metrici essi stessi; in soldoni, dice che se un gruppo opera con 'buone' proprietà su uno spazio metrico ben fatto, allora il gruppo è fintamente generato e quasi-isometrico allo spazio stesso; o, viceversa, che un gruppo finitamente generato G può agire con 'buone' proprietà su un unico spazio metrico ben fatto, a meno di quasi-isometria.

Per rendere pienamente intellegibile l'enunciato è necessario farlo precedere da alcune definizioni di natura topologica.

Definizione. Uno spazio metrico (X, d) si dice *proprio* se per ogni $x \in X$ e $0 < R \in \mathbb{R}$ la palla chiusa $B(x, R) = \{y \in X \mid d(x, y) \leq R\}$ è un insieme compatto nella topologia indotta dalla metrica d.

Definizione. Un'azione $G \times X \to X$ di un gruppo G su uno spazio metrico X si dice

- *propriamente discontinua* se per ogni insieme compatto B di X l'insieme

$$\{g \in G \mid g \cdot B \cap B \neq \emptyset\}$$

  è finito;

- *co-compatta* se per ogni $x_0 \in X$ esiste un raggio $R > 0$ tale X è contenuto nell'unione dei G-traslati della palla chiusa $B(x_0, R)$, ovvero

$$X \subseteq \bigcup_{g \in G} B(g \cdot x_0, R).$$

Esempio 4.2. Nella nostra prospettiva, l'esempio fondamentale di un'azione propriamente discontinua e co-compatta su uno spazio metrico proprio è quella di un gruppo finitamente generato G per moltiplicazione sinistra su un suo grafo di Cayely $\Gamma = \Gamma[G, S]$, ovvero sullo spazio (G, d_S), con S un sistema di generatori finito di G (in questo caso, lo spazio è discreto, quindi i sottoinsiemi compatti sono i sottoinsiemi finiti).
Tale azione si estende ad un'azione di G sulla realizzazione geometrica $|\Gamma|$; in questo caso, la spazio $|\Gamma|$ oltre che proprio è *geodetico*, e l'azione è ancora totalmente discontinua (ogni sottoinsieme compatto di $|\Gamma|$ contiene un numero finito di vertici di Γ) e co-compatta (i G-traslati di una palla chiusa di raggio 1 coprono $|\Gamma|$). □

Esempio 4.3. L'azione del gruppo $G = \mathbb{Z}^2$ sullo spazio euclideo $\mathbb{R}^2$ per traslazione,

$$(z, z') \cdot (x, y) = (x + z, y + z') \quad \forall z, z' \in \mathbb{Z}, (x, y) \in \mathbb{R}^2,$$

è propriamente discontinua e co-compatta; mentre l'azione di $\mathbb{Z}$ su $\mathbb{R}^2$ per traslazione orizzontale,

$$z \cdot (x, y) = (x + z, y) \quad \forall z \in \mathbb{Z}, (x, y) \in \mathbb{R}^2,$$

è propriamente discontinua ma non co-compatta. □

Esempio 4.4. Sia R un numero reale non razionale e sia $\alpha \in Isom(\mathbb{R}^2)$ la rotazione di angolo $2\pi/R$ centrata nell'origine; allora $G = \langle\alpha\rangle \simeq \mathbb{Z}$. L'azione naturale di G sulla palla $B = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ è co-compatta ma non propriamente discontinua. □

Possiamo ora enunciare e provare il Lemma di Milnor–Švarc; si osservi che nessuna ipotesi viene fatta sul gruppo G, ma solo sullo spazio X e sull'azione.

Teorema 4.6 (Lemma di Milnor–Švarc)**.** *Sia G un gruppo che agisce per isometrie su uno spazio metrico non vuoto, proprio e geodetico (X, d). Se tale azione è propriamente discontinua e co-compatta, allora G è finitamente generato e per ogni $x \in X$ l'applicazione*

$$\begin{aligned} G &\to X \\ g &\mapsto g \cdot x \end{aligned}$$

è una quasi-isometria (dove la metrica su G è la word-metric per un sistema finito di generatori).

Dimostrazione. Dato un punto $x_0 \in X$, sia $0 < R \in \mathbb{R}$ tale che X è contenuto nell'unione dei G-traslati della palla chiusa $B := B(x_0, R)$. Per ipotesi, B è un sottoinsieme compatto di X e l'insieme

$$S = \{g \in G \mid g \neq 1,\ B \cap g \cdot B \neq \emptyset\}$$

è finito (si osservi anche che $S = S^{-1}$). Poniamo

$$r := \inf\{d(B, g \cdot B) \mid g \in G \setminus (S \cup \{1\})\},$$

e mostriamo che $r > 0$. Per questo, si osservi che per ogni $0 < \rho \in \mathbb{R}$, $g \in G$ si ha

$$d(B, g \cdot B) \leq \rho \quad \Rightarrow \quad B(x_0, R + \rho) \cap g \cdot B(x_0, R + \rho) \neq \emptyset;$$

dunque, per la discontinuità propria dell'azione, esiste al più un numero finito di elementi $g \in G$ per cui $d(B, g \cdot B) \leq \rho$. Preso un qualsiasi $g_0 \in G \setminus (S \cup \{1\})$, ed osservato che, per la compattezza di B, $d(B, g_0 \cdot B) = \inf\{d(x, g_0 \cdot y) \mid x, y \in B\} > 0$, si conclude che solo un numero finito di traslati $g \cdot B$, disgiunti da B, hanno distanza minore (e positiva) da B. Quindi, banalmente, r esiste ed è positivo.

Proviamo ora che S è un sistema di generatori di G, e che per ogni $g \in G$,

$$\ell_S(g) \leq d(x_0, g \cdot x_0)/r + 1. \tag{4.3}$$

Se $g \in S \cup \{1\}$ la cosa è ovvia. Sia $1 \neq g \in G \setminus S$ e sia $L = d(x_0, g \cdot x_0)$; allora $L \geq 2R + r \geq R + r$, quindi esiste un minimo intero $m \geq 2$ tale che

$$R + (m - 1)r \leq L < R + mr. \tag{4.4}$$

Sia $\gamma : [0, L] \to X$ un segmento geodetico da x_0 a $g \cdot x_0$. Posto $\varepsilon = \frac{R+mr-L}{m}$, siano

$$x_1 = \gamma(R), \quad x_{m+1} = g \cdot x_0$$

e, per per $k = 1, \cdots, m - 1$,

$$x_{k+1} = \gamma(R + k(r - \varepsilon))$$

Abbiamo quindi $m+1$ punti, $x_1, x_2, \ldots, x_{m+1} = g \cdot x_0$, distribuiti lungo (l'immagine di) γ tali che

$$d(x_0, x_1) = R \quad \text{e} \quad d(x_i, x_{i+1}) < r \text{ per } i = 1, \ldots, m.$$

Esistono quindi elementi $1 = g_0, g_1, \ldots, g_m = g$ tali che $x_{i+1} \in g_i \cdot B$, per $i = 0, \ldots, m$. Per $1 \leq i \leq k$ poniamo $s_i = g_{i-1}^{-1} g_i$; allora

$$d(B, s_i \cdot B) = d(g_{i-1} \cdot B, g_i \cdot B) \leq d(x_i, x_{i+1}) < c,$$

quindi $s_i \in S$. Ora, tenendo conto che $g_0 = 1$,

$$g = g_m = (g_0^{-1} g_1)(g_1^{-1} g_2) \cdots (g_{m-1}^{-1} g_m) = s_1 s_2 \cdots s_m \in \langle S \rangle,$$

e, dalla (4.4), $\ell_S(g) \leq m \leq d(x_0, g \cdot x_0)/r + 1$, che è quello che si voleva dimostrare.

Sia ora d_S la metrica su G associata a S, e sia $f : G \to X$ la funzione definita da $f(g) = g \cdot x_0$, per ogni $g \in G$. Per ogni $h, g \in G$, poiché G agisce per isometrie su X,

$$d(f(g), f(h)) = d(g \cdot x_0, h \cdot x_0) = d(x_0, (g^{-1} h) \cdot x_0);$$

quindi, per quanto provato sopra:

$$d(f(g), f(h)) \geq r \ell_S(g^{-1} h) - r = r d_S(g, h) - r. \tag{4.5}$$

Ora, per definizione di S, $d(x_0, s \cdot x_0) \leq 2R$ per ogni $s \in S$. Se $g \in G$, per la diseguaglianza triangolare,

$$d(x_0, sg \cdot x_0) \leq d(x_0, s \cdot x_0) + d(s \cdot x_0, sg \cdot x_0) \leq 2R + d(x_0, g \cdot x_0).$$

Un'ovvia induzione conduce a $d(x_0, g \cdot x_0) \leq 2R \ell_S(g)$, per ogni $g \in G$. Quindi

$$d(f(g), f(h)) = d(x_0, (g^{-1} h) \cdot x_0) \leq 2R \ell_S(g^{-1} h) = 2R \cdot d_S(g, h),$$

per ogni $g, h \in G$. In congiunzione con (4.5) questo prova che f è un'inclusione quasi-isometrica. Che infine f sia quasi-invertibile, e quindi una quasi-isometria, deriva, per il Lemma 4.4, dal fatto che per ogni $x \in X$ esiste un $g \in G$ tale che $d(x, g \cdot x_0) \leq R$. Questo completa la dimostrazione. □

Esempio 4.5. L'azione del gruppo $SL(2, \mathbb{Z})$ sulla realizzazione geometrica $|T\mathcal{F}|$ dell'albero di Farey è totalente discontinua e co-compatta, quindi $SL(2, \mathbb{Z})$ è quasi-isometrico a $|T\mathcal{F}|$ (e $T\mathcal{F}$). □

Commensurabilità. Come prima applicazione del Lemma di Milnor–Švarc vediamo un criterio generale, ancora relativamente semplice ma molto utile, di quasi-isometria.

Definizione. Due gruppi G e G' si dicono *commensurabili* se esistono sottogruppi $H \leq G$ e $H' \leq G'$ di indice finito e tali che $H \simeq H'$. I gruppi G e G' si dicono *quasi-commensurabili* se esistono sottogruppi $N \trianglelefteq H \leq G$, $N' \trianglelefteq H' \leq G'$, con N, N' finiti, $|G : H|, |G' : H'|$ finiti e $H/N \simeq H'/N'$.

Proposizione 4.7. *Se G e G' sono gruppi finitamente generati e quasi-commensurabili allora $G \sim_{QI} G'$.*

Dimostrazione. Sarà sufficiente provare le seguenti due affermazioni, per un gruppo finitamente generato G:

(i) se H è un sottogruppo di indice finito di G, allora $H \sim_{\mathrm{Q}I} G$;

(ii) se N è un sottogruppo normale e finito di G, allora $G/N \sim_{\mathrm{Q}I} G$.

Nel caso (i), sia S un sistema finito di generatori di G e sia X la realizzazione geometrica del grafo di Cayley $\Gamma[G, S]$. X è uno spazio proprio e geodetico, e l'azione di G su X soddisfa le ipotesi del Lemma di Milnor–Švarc. In particolare anche l'azione di H su X ereditata da quella di G è propriamente discontinua. Inoltre, se T è un sistema di rappresentati delle classi laterali destre di G modulo H, allora T è finito ed esiste $R > 0$ tale che $T \subseteq B(1, R)$, e poichè $HT = G$ si ha

$$\bigcup_{h \in H} h \cdot B(1, R) = X,$$

dunque l'azione di H su X è co-compatta. Per Milnor–Švarc, $H \sim_{\mathrm{Q}I} X \sim_{\mathrm{Q}I} G$.
Nel caso (ii) si considera la realizzazione geometrica X di un grafo di Cayley $\Gamma = \Gamma[G/N, S]$. Mediante la proiezione $G \to G/N$ è definita una azione di G per moltiplicazione a sinistra su Γ, il cui nucleo è N, e quindi una azione su X che è chiaramente co-compatta. Tale azione è anche completamente discontinua perché tale è quella di G/N e N è finito. Per Milnor–Švarc, $G \sim_{\mathrm{Q}I} X \sim_{\mathrm{Q}I} G/N$. □

Esempio 4.6. Il gruppo modulare $M = PSL(2, \mathbb{Z}) \simeq C_2 * C_3$ è il quoziente, modulo un sottogruppo di ordine 2, del gruppo $SL(2, \mathbb{Z})$ che, a sua volta, contiene un sottogruppo di indice finito isomorfo al gruppo libero F_2. Quindi, M è quasi-commensurabile, e dunque quasi-isometrico, a F_2. □

Esempio 4.7. È piuttosto ben noto che, poiché $\mathbb{Q}$ è un campo di ordine almeno 4, i sottogruppi normali propri del gruppo $G = SL(2, \mathbb{Q})$ sono $\{1\}$ e $Z = \{1, -1\}$; in particolare, G non ammette sottogruppi di indice finito. Ne segue che G e $PSL(2, \mathbb{Q}) = G/Z$ sono quasi-commensurabli ma non commensurabili. □

Nell'esempio di sopra, il gruppo $G = SL(2, \mathbb{Q})$ non è finitamente generato; esempi di gruppi finitamente generati che sono quasi-commensurabili ma non commensurabili esistono, ma sono più complicati.
Esistono poi molte coppie di gruppi quasi-isometrici ma non quasi-commensurabili; un metodo per trovarne è descritto nell'esercizio 4.17.

Esercizio 4.12. Si provi che non è possibile, nelle conclusioni del Lemma di Milnor–Švarc, rimpiazzare "quasi–isometria" con "equivalenza bi-lipschitziana". [sugg.: considerare l'azione del gruppo $\mathbb{Z}$ sullo spazio $\mathbb{R}$.]

Esercizio 4.13. Si provi che $\mathbb{R}$ (con la metrica standard) non è quasi isometrico a $[0, +\infty)$.

Esercizio 4.14. Siano A, B gruppi finiti non-banali. Si provi che il prodotto libero $A * B$ è quasi-isometrico a $\mathbb{Z}$ oppure a F_2. [sugg.: ricordarsi dell'esercizio 3.39.]

Esercizio 4.15. Siano $2 \leq m, n \in \mathbb{N}$. Si provi che i gruppi di Baumslag-Solitar $BS(1, m)$ e $BS(1, n)$ (vedi sezione 3.8) sono quasi–isometrici.

Esercizio 4.16. Sia H il gruppo di isometrie dello spazio euclideo $\mathbb{R}^2$ generato da tre riflessioni lungo i lati di un triangolo equilatero. Si provi che H agisce in modo totalmente discontinuo e co-compatto su $\mathbb{R}^2$. Si deduca che H contiene un sottogruppo finito isomorfo a $\mathbb{Z}^2$.

4.4. Invarianti per quasi–isometria

Questa breve sezione, in cui citeremo senza dimostrazioni una serie di risultati di natura omogenea, serve principalmente da motivazione per il seguito del corso. Se un'ipotetica classificazione dei gruppi finitamente generati a meno di quasi-isometria è, come si può indovinare, assolutamente fuori portata, sussistono importanti e forse inaspettati legami tra la geometria del tipo di quasi-isometria di un gruppo finitamente generato e alcune proprietà che definiremo piuttosto come algebriche.
Al fine di evidenziare questi legami, diciamo che una classe (o una proprietà[4]) di gruppi $\mathfrak{X}$ è *geometrica* se per ogni coppia di gruppi finitamente generati G, H, se G è in $\mathfrak{X}$ e $H \sim_{\mathrm{QI}} G$ allora anche H è in $\mathfrak{X}$.

Teorema 4.8. *Sono geometriche le seguenti classi di gruppi:*

1) *Finiti;*

2) *Virtualmente ciclici infiniti;*

3) *Virtualmente abeliani;*

4) *Virtualmente nilpotenti;*

5) *Virtualmente liberi;*

6) *Finitamente presentati;*

7) *Iperbolici;*

8) *Amenabili.*

Ricordo (sezione 1.4) che un gruppo G è virtualmente-$\mathfrak{X}$ se G ha un sottogruppo di indice finito appartenente a $\mathfrak{X}$. A parte per la 1), che abbiamo già osservato verso la fine della sezione 4.1, le dimostrazioni delle affermazioni in questo enunciato sono tutt'altro che ovvie[5]; nella sezione 4.6 dimostreremo la 2) che è relativamente accessibile. Le classi ai punti 7) e 8), che non sono ancora state definite, costituiranno l'argomento della prossima parte del corso.

Ancora, supponiamo che ad ogni gruppo finitamente generato G in una data classe $\mathfrak{X}$ sia associato un elemento $\nu(G)$ di un certo insieme V (spesso $V = \mathbb{N}$) in modo che $\nu(G) = \nu(H)$ se $G \simeq H$; si dice allora che $\nu(G)$ è un invariante di G nella classe[6] $\mathfrak{X}$ (ad esempio, la cardinalità minima $d(G)$ di un sistema di generatori di G è un invariante nella classe di tutti i gruppi finitamente generati); un invariante si dice quindi *invariante geometrico* se per ogni coppia G, H di gruppi finitamente generati nella classe $\mathfrak{X}$,

$$G \sim_{\mathrm{QI}} H \;\Rightarrow\; \nu(G) = \nu(H).$$

Esempio 4.8. Sia $\mathfrak{F}$ la classe dei gruppi liberi di rango finito. Vediamo che il rango non è un invariante geometrico nella classe $\mathfrak{F}$. Sia F_2 il gruppo libero di rango 2 e, dato $m \geq 2$ sia H un sottogruppo di indice m in F_2 (esiste: perché?); allora, per il Teorema 3.8, H è un gruppo libero di rango $2m - m + 1 = m + 1$. Questo mostra che per ogni

[4] Una classe, o proprietà, di gruppi è una famiglia di gruppi chiusa per isomorfismo.

[5] A complemento di questa affermazione, e da confrontare con il punto 4) del Teorema, si veda, più avanti, il Teorema 4.10.

[6] Una classe è essa stessa un invariante a valori $0, 1$ nella famiglia di tutti i gruppi finitamente generati.

$n \geq 3$, F_2 ammette un sottogruppo di indice finito isomorfo a F_n. Per la Proposizione 4.7, F_2 e F_n sono quasi-isometrici; di conseguenza, per ogni coppia di interi $n, m \geq 2$, $F_n \sim_{QI} F_m$, mostrando che il rango non è un invariante geometrico nella classe $\mathfrak{F}$. Questa osservazione ha come corollario che per ogni coppia di interi $n, m \geq 2$, l'albero n-regolare T_n è quasi isometrico (con la metrica di grafo) all'albero regolare T_m. □

Esempi di invarianti geometrici sono individuati nel seguente enunciato (e definiti subito dopo)[7].

Proposizione 4.9. *Il* numero di ends $e(G)$ *e il* tipo di crescita $\gamma(G)$ *sono invarianti geometrici nella classe di tutti i gruppi finitamente generati.*

Per quanto riguarda il numero di ends, vedremo la dimostrazione nella sezione 4.6. Il concetto di *tipo di crescita* di un gruppo finitamente generato è invece uno di quelli fondamentali; prendiamo l'occasione di definirlo nella prossima sezione, con l'intenzione, anche in questo caso, di riprenderlo più avanti per studiarlo in modo un po' approfondito.

Concludiamo questa sezione dimostrando un risultato di A. Dyubina, che va in direzione contraria rispetto all'enunciato in 4.8.

Teorema 4.10. *La classe dei gruppi virtualmente risolubili non è geometrica.*

La dimostrazione discende abbastanza agevolmente dalla seguente osservazione.

Proposizione 4.11. *Siano A e B gruppi finiti. Se $|A| = |B|$ allora il prodotto intrecciato $A \wr \mathbb{Z}$ è quasi-isometrico a $B \wr \mathbb{Z}$.*

Dimostrazione. Sia $A^\omega = \{f \mid a : \mathbb{Z} \to A,\ |supp(f)| < \infty\}$ la base del prodotto $A \wr \mathbb{Z}$ e, similmente, B^ω quella di $B \wr \mathbb{Z}$. Quindi, $A \wr \mathbb{Z} = A^\omega \rtimes \mathbb{Z}$ dove l'azione di $\mathbb{Z}$ su A^ω è quella di "shift", ovvero, per ogni $f \in A^\omega, z, t \in \mathbb{Z}$,

$$f^z(t) = f(z - t)$$

e similmente per $B \wr \mathbb{Z}$. Sia quindi $\phi : A \to B$ una biezione tale che $\phi(1_A) = 1_B$, e consideriamo poi la funzione $\overline{\phi} : A \wr \mathbb{Z} \to B \wr \mathbb{Z}$, definita da

$$\overline{\phi}(f, t) = (\phi \circ f, t),$$

per ogni $(f, t) \in A \wr \mathbb{Z}$. $\overline{\phi}$ è abbastanza chiaramente una biezione.
Per ogni $a \in A$ e $b \in B$ definiamo $\overline{a} \in A^\omega$, $\overline{b} \in B^\omega$ nel modo solito,

$$\overline{a}(z) = \begin{cases} a & \text{se } z = 0, \\ 1_A & \text{se } z \neq 0 \end{cases} \qquad \overline{b}(z) = \begin{cases} b & \text{se } z = 0, \\ 1_B & \text{se } z \neq 0 \end{cases}$$

Si ha quindi che $S_A = \{\overline{a}, 0) \mid 1 \neq a \in A\} \cup \{(\overline{1}, 1)\}$ e $S_B = \{\overline{b}, 0) \mid 1 \neq b \in B\} \cup \{(\overline{1}, 1)\}$ sono sistemi di generatori, rispettivamente, di $A \wr \mathbb{Z}$ e $B \wr \mathbb{Z}$ (si osservi anche che $|S_A| = |S_B|$).

Proviamo che $\overline{\phi}$ è un isomorfismo tra i grafi di Cayley $\Gamma_A = \Gamma[A \wr \mathbb{Z}, S_A]$ e $\Gamma_B = \Gamma[B \wr \mathbb{Z}, S_B]$; da questo l'asserzione di quasi-isometria segue ovviamente.

Abbiamo già osservato che $\overline{\phi}$ è una biezione; verifichiamo che conserva la relazione di adiacenza. Siano $(f, t), (g, t')$ adiacenti in Γ_A; si verificano due casi:

(1) $(g, t') = (f, t)(\overline{1}, \pm 1) = (f, t \pm 1)$,
(2) $(g, t') = (f, t)(\overline{a}, 0) = (f\overline{a}^t, t)$, per qualche $a \in A \setminus \{1_A\}$.

[7] Per un altro esempio si veda più avanti la Proposizione 4.15.

Nel caso (1) si ha

$$\overline{\phi}(g,t') = (\phi \circ f, t \pm 1) = (\phi \circ f, t)(\overline{1}, \pm 1) = \overline{\phi}(f,t)(\overline{1}, \pm 1),$$

che è adiacente a $\overline{\phi}(f,t)$ in Γ_B.
Nel caso (2) si ha

$$\overline{\phi}(g,t') = (\phi \circ (f\bar{a}^t), t).$$

Poniamo $b = \phi(f(t))^{-1}\phi(f(t)a)$, osservando che, poiché $a \neq 1_A$ e ϕ è un biezione, risulta $b \neq 1_B$. Allora, per ogni $z \in \mathbb{Z}$,

$$(\phi \circ (f\bar{a}^t))(z) = \phi(f\bar{a}^t(z)) = \begin{cases} \phi(f(z)) & \text{se } z \neq t, \\ \phi(f(t)a) = \phi(f(t))b & \text{se } z = t \end{cases}$$

quindi, $\phi \circ (f\bar{a}^t) = (\phi \circ f)\overline{b}^t$, e dunque

$$\overline{\phi}(g,t') = ((\phi \circ f)\overline{b}^t, t) = (\phi \circ f, t)(\overline{b}, 0) = \overline{\phi}(f,t)(\overline{b}, 0),$$

che è adiacente a $\overline{\phi}(f,t)$ in Γ_B. Poiché $\overline{\phi}$ è una biezione tra gli insiemi dei vertici di Γ_A e Γ_B, e questi sono grafi regolari con lo stesso grado, si conclude che ϕ è un isomorfismo di grafi. □

Dimostrazione del Teorema 4.10. Sia A un gruppo abeliano di ordine 60 (ad esempio il gruppo ciclico) e sia $B = A_5$ (il gruppo alterno su 5 oggetti; si ricordi che A_5 è semplice e $|A_5| = 60$). Per la Proposizione 4.11, $A \wr \mathbb{Z}$ e $B \wr \mathbb{Z}$ sono quasi–isometrici. Tuttavia, $A \wr \mathbb{Z}$ è risolubile (cone le notazioni della dimostrazione precedente, A^ω e $(A \wr \mathbb{Z})/A^\omega \simeq \mathbb{Z}$ sono abeliani), mentre $B \wr \mathbb{Z}$ non è virtualmente risolubile. Sia, infatti, H un sottogruppo di indice finito di $B \wr \mathbb{Z}$, che possiamo assumere essere un sottogruppo normale; allora (ancora con le notazioni della dimostrazione precedente) $N = H \cap B^\omega$ è un sottogruppo normale di indice finito in $B^\omega = Dir_{z\in\mathbb{Z}} B_z$ (con $B_z \simeq A_5$ per ogni $z \in \mathbb{Z}$), in particolare $N \neq \{1\}$. Poiché, chiaramente, $Z(B^\omega) = \{1\}$, esiste $z \in \mathbb{Z}$ con $[B_z, N] \neq \{1\}$, e siccome anche B_z è normale in B^ω, $[B_z, N] \trianglelefteq B_z$, dunque, per la semplicità di B_z,

$$B_z = [B_z, N] \leq N,$$

qundi N, e di conseguenza H, non può essere risolubile. □

Esercizio 4.17. Sia A un gruppo non-banale; si provi che il prodotto intrecciato $W = A \wr \mathbb{Z}$ non ammette sottogruppi normali finiti diversi da $\{1\}$. Applicando il Teorema 4.10 si trovino due gruppi finitamente generati quasi-isometrici ma non quasi-commensurabili.

4.5. Crescita (definizioni ed esempi)

Sia G un gruppo finitamente generato, S un suo sistema finito di generatori e, per $g \in G$, $\ell_S(g)$ la lunghezza di g in S (ricordo che $\ell_S(g)$ è la distanza del vertice g dal vertice 1 nel grafo di Cayley $\Gamma[G,S]$). Per ogni $n \in \mathbb{N}$ è definita la palla chiusa di raggio n centrata in 1,

$$B_G^S(n) = \mathcal{B}_S(1, n+1) = \{g \in G \mid \ell_S(g) \leq n\}. \tag{4.6}$$

Poiché S è finito, per ogni $n \geq 0$,

$$\gamma_G^S(n) = |B_G^S(n)| \tag{4.7}$$

è un intero positivo. La funzione $\gamma_G^S : \mathbb{N} \to \mathbb{N}$ si chiama *funzione di crescita* del gruppo G rispetto al sistema di generatori S.

È chiaro che, fissato il gruppo G, la funzione di crescita dipende dal sistema di generatori scelto; ad esempio, nel gruppo $\mathbb{Z}$ la funzione di crescita rispetto al sistema di generatori

$\{1\}$ è data da $\gamma_{\mathbb{Z}}^{\{1\}}(n) = 2n+1$, per ogni $n \in \mathbb{N}$, mentre la funzione di crescita rispetto al sistema $\{2,3\}$ vale: $\gamma_{\mathbb{Z}}^{\{2,3\}}(0) = 1$, $\gamma_{\mathbb{Z}}^{\{2,3\}}(1) = 5$ e

$$\gamma_{\mathbb{Z}}^{\{2,3\}}(n) = 6n+1 \tag{4.8}$$

per ogni $n \geq 2$. Tuttavia, funzioni di crescita in uno stesso gruppo definite da sistemi diversi (finiti) di generatori, sono strettamente correlate nel senso che ora descriviamo.

Date due funzioni crescenti $\gamma, \mu : \mathbb{N} \to \mathbb{R}_{\geq 0}$, scriviamo $\gamma \preccurlyeq \mu$, se esistono due costanti positive C, D ed un $n_0 \in \mathbb{N}$ tali che

$$\gamma(n) \leq D\mu(Cn)$$

per ogni $n \geq n_0$. Diciamo quindi che γ e μ sono *(asintoticamente) equivalenti*, scrivendo $\gamma \sim \mu$, se $\gamma \preccurlyeq \mu$ e $\mu \preccurlyeq \gamma$.
È immediato verificare che la relazione $\preccurlyeq$ definisce un pre-ordine sull'insieme delle funzioni $\mathbb{N} \to \mathbb{R}$; quindi, $\sim$ è un'equivalenza e $\preccurlyeq$ induce una relazione d'ordine sulle classi, ovvero

$$[\gamma]_\sim \leq [\mu]_\sim \quad \text{se} \quad \gamma \preccurlyeq \mu.$$

Proposizione 4.12. *Siano G, H gruppi finitamente generati quasi-isometrici. Allora per ogni coppia di sistemi finiti di generatori S di G e T di H, si ha $\gamma_G^S \sim \gamma_H^T$.*

Dimostrazione. Poniamo $X = \Gamma[G,S]$ e $Y = \Gamma[H,T]$. Sia $f : X \to Y$ una (λ, C)-quasi-isometria, e sia $d = d_Y(f(1),1)$.
Sia $n \geq C + d$, allora per ogni $g \in B_G^S(n)$,

$$d_Y(f(g),1) \leq d_Y(f(g),f(1)) + d_Y(f(1),1) \leq \lambda d_X(g,1) + C + d \leq (\lambda+1)n;$$

quindi

$$f(B_G^S(n)) \subseteq B_H^T((\lambda+1)n). \tag{4.9}$$

Inoltre, se $x, x' \in G$ sono tali che $f(x) = f(x')$, allora $\lambda^{-1} d_X(x,x') - C \leq 0$ e dunque $d_X(x^{-1}x',1) = d_X(x,x') \leq \lambda C$; in particolare, se $D = \gamma_G^S([\lambda C])$, allora il numero di elementi di G la cui immagine coincide con $f(x)$ non supera D. In congiunzione con (4.9) si ottiene, per ogni $n \geq C + d$,

$$\gamma_G^S(n) = |B_G^S(n)| \leq D|f(B_G^S(n))| \leq D|B_H^T((\lambda+1)n)| = D\gamma_H^T((\lambda+1)n);$$

dunque $\gamma_G^S \preccurlyeq \gamma_H^T$. La relazione inversa si ottiene per simmetria, e pertanto $\gamma_G^S \sim \gamma_H^T$. □

Corollario 4.13. *Siano S e U sistemi finiti di generatori del gruppo G; allora le funzioni di crescita γ_G^S e γ_G^U sono equivalenti.*

DEFINIZIONE. Se S è un sistema finito di generatori del gruppo G, la classe d'equivalenza $\gamma_G := [\gamma_G^S]_\sim$ è detto *tipo di crescita* di G.

La Proposizione 4.12 può essere dunque riformulata nel modo seguente.

Proposizione 4.14. *Il tipo di crescita è un invariante geometrico nella classe di tutti i gruppi finitamente generati.*

Crescita polinomiale. Osserviamo ora che se f e g sono polinomi reali, allora le funzioni $f(n)$ e $g(n)$ sono equivalenti se e soltanto se $\deg f = \deg g$; quindi, al variare di $1 \leq d \in \mathbb{N}$, le funzioni $n \mapsto n^d$ costituiscono un sistema di rappresentanti modulo $\sim$ per le funzioni polinomiali. Più in generale, per ogni $0 < \alpha, \beta \in \mathbb{R}$, $n^\alpha \sim n^\beta$ se e solo se $\alpha = \beta$.

DEFINIZIONE. Si dice che un gruppo finitamente generato G ha *crescita polinomiale* se esiste un intero $d > 0$ tale che $\gamma_G = [n^d]$.

Esempio 4.9. Sia $A \simeq \mathbb{Z}^r$ e $\mathcal{X} = \{x_1, \dots, x_r\}$ un suo sistema indipendente di generatori. Allora ogni elemento $a \in A$ si scrive in modo unico come $a = x_1^{\beta_1(g)} \cdots x_r^{\beta_r(g)}$ con $(\beta_1(g), \dots, \beta_r(g)) \in \mathbb{Z}^r$. Quindi $\ell_{\mathcal{X}}(a) = \sum_{i=1}^r |\beta_i(g)|$ e, per ogni $n \geq 1$,

$$\gamma_A^{\mathcal{X}}(n) = |\{(\beta_1, \dots, \beta_r) \in \mathbb{Z}^r \mid |\beta_1| + \cdots + |\beta_r| \leq n\}|.$$

Mediante una minorazione ed una maggiorazione abbastanza immediate, ma sufficienti ai nostri fini, si può affermare che, per ogni $n \geq 1$,

$$\left(\frac{n}{r} - 1\right)^r \leq \left\lfloor \frac{n}{r} \right\rfloor^r \leq \gamma_A^{\mathcal{X}}(n) \leq (2n+1)^r$$

(per $r = 2$, facendo i conti esatti, si trova $\gamma_{\mathbb{Z}^2}(n) = n^2 + (n+1)^2$, mentre per il valore esatto in generale si veda l'esercizio 4.20). Quindi il tipo di crescita di $A = \mathbb{Z}^r$ è $[n^r]$. □

Dal Teorema di struttura dei gruppi abeliani finitamente generati (Teorema 1.8), segue che per ogni tal gruppo G è univocamente determinato il numero $r = r_0(G)$ di fattori infiniti in una decomposizione come prodotto diretto di gruppi ciclici (quindi $r = 0$ se e solo se G è finito). Ora, a partire dalle considerazioni nell'esempio 4.9, tenendo presente le Proposizioni 4.7 e 4.12, possiamo quindi ricavare le seguenti osservazioni.

Proposizione 4.15. 1) *Ogni gruppo abeliano finitamente generato ha crescita polinomiale.*

2) *Il rango r_0 è un invariante geometrico nella classe dei gruppi abeliani finitamente generati; ancor meglio, due gruppi abeliani A e B sono quasi-isometrici se e solo se $r_0(A) = r_0(B)$.*

Il punto 2) rende anche conto dell'affermazione fatta nella sezione 4.1, che per ogni coppia di interi $n, m \geq 1$, gli spazi $\mathbb{R}^n$ e $\mathbb{R}^m$ sono quasi-isometrici se e solo se $n = m$.

Crescita esponenziale. All'altra estremità dei possibili tipi di crescita si colloca la *crescita esponenziale*. Partiamo dalla constatazione che tutte le funzioni esponenziali, cioè del tipo a^n, con $1 < a \in \mathbb{R}$, sono equivalenti; dunque equivalenti alla funzione 2^n. Si dice che un gruppo finitamente generato G ha *crescita esponenziale* se $\gamma_G = [2^n]$. L'esempio principale di gruppi a crescita esponenziale è costituito dai gruppi liberi (di rango finito).

Esempio 4.10. Sia $r \geq 1$ e sia X un sistema libero di generatori del gruppo libero F_r. Denotiamo con $\sigma_r(n)$ il numero di elementi di F_r la cui X-lunghezza è esattamente n; poiché il grafo di Cayley di F_n rispetto a X è un albero regolare di grado $2r$ (Proposizione 3.5), si vede che $\sigma_r(0) = 1$, $\sigma_r(1) = 2r$ e, per $n \geq 2$,

$$\sigma_r(n) = (2r-1)\sigma_r(n-1) = 2r(2r-1)^{n-1},$$

quindi per $n \geq 1$,

$$\gamma^X_{F_r}(n) = \sum_{i=o}^{n} \sigma_r(i) = 1 + 2r \sum_{j=0}^{n-1} (2r-1)^j = 1 + 2r \frac{(2r-1)^n - 1}{(2r-1) - 1} \geq (2r-1)^n.$$

In particolare, per $r = 2$ si ha $\gamma_{F_2}(n) = 2 \cdot 3^n - 1$. A questo punto, non è difficile provare (lo si faccia per esercizio) che, per ogni r, $\gamma_{F_r}(n) \sim 2^n$. □

L'esempio di sopra mostra quindi che ogni gruppo libero di rango finito $r \geq 2$ ha crescita esponenziale. È chiaro che, rispetto alla relazione d'ordine definita prima, quella esponenziale è la massima crescita possibile per gruppi finitamente generati. La crescita esponenziale non implica tuttavia, come forse si sarebbe portati a credere, che il sistema di generatori in questione sia prossimo ad essere libero. Ad esempio, vediamo come il gruppo del Lampionaio, che è abeliano per ciclico, abbia crescita esponenziale.

Esempio 4.11. Il gruppo del lampionaio L_2 è il prodotto intrecciato $C_2 \wr \mathbb{Z}$; che a sua volta vediamo come il prodotto demidiretto $L_2 = B \rtimes \langle x \rangle$ dove B è l'insieme delle funzioni $\mathbb{Z} \to \{0, 1\}$ a supporto finito e x la traslazione $z \mapsto z + 1$. Seguendo le notazioni introdotte nella sezione 2.7, posto $\mathbf{a} = (\delta_{0z})_{z \in \mathbb{Z}}$ (δ_{ij} il delta di Kronecker) allora $X = \{\mathbf{a}, x\}$ è un sistema di generatori di L_2. Per ogni $\mathbf{b} \in B$, come osservato nella sezione 2.7, formula (2.6), se il supporto di $\mathbf{b}$ è contenuto in $[-n, n]$, allora

$$\ell_X(\mathbf{b}) \leq 6n + 1. \tag{4.10}$$

Ora, il numero di funzioni $\mathbb{Z} \to \{0, 1\}$ il cui supporto è contenuto in $[-n, n]$ è chiaramente 2^{2n+1}. Da (2.6) segue pertanto, per $m \geq 4$,

$$\gamma^X_{L_2}(m) \geq 2^{\frac{m-1}{3}+1} = 2 \cdot 2^{\frac{m}{4}};$$

quindi $2^n \preccurlyeq \gamma^X_{L_2}$, e dunque $\gamma_{L_2} = [2^n]$. □

Come detto, lo studio della crescita di gruppi finitamente generati è un argomento centrale in teoria geometrica dei gruppi, ricco di problemi e risultati di grande interesse, e ci torneremo più avanti.

Esercizio 4.18. Si dimostri la correttezza della formula (4.8).

Esercizio 4.19. Siano G un gruppo finitamente generato e S un suo sistema finito di generatori. Si provi che la funzione di crescita γ^S_G è submoltiplicativa; ovvero

$$\gamma^S_G(n + m) \leq \gamma^S_G(n)\gamma^S_G(m),$$

per ogni $n, m \in \mathbb{N}$.

Esercizio 4.20. Dato $r \geq 1$, sia $A = Z^r$, e $X = \{x_1, \ldots, x_r\}$ un suo sistema di generatori indipendenti. Si provi che, per ogni $n \geq 1$,

$$\gamma^X_A(n) = \sum_{i=0}^{r} 2^i \binom{r}{i} \binom{n}{i}.$$

Esercizio 4.21. Siano G, H gruppi finitamente generati e X, Y sistemi di generatori finiti, rispettivamente, di G e di H. Posto $D = (X \cup \{1\}) \times (Y \cup \{1\})$, si provi che

$$\gamma^D_{G \times H} \sim \gamma^X_G \cdot \gamma^Y_H.$$

Esercizio 4.22. Il gruppo di Heisenberg discreto è il gruppo:

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \Big| a, b, c \in \mathbb{Z} \right\}.$$

In H, siano

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

1) Si provi che $H = \langle a, b \rangle$, che $\langle c \rangle = Z(H)$ e che $H/Z(H) \simeq \mathbb{Z} \times \mathbb{Z}$. Questo, in particolare, dice che H è un gruppo nilpotente.
2) Si provi che ogni $g \in H$ si scrive in modo unico nella forma $g = a^m b^n c^t$ con $m, n, t \in \mathbb{Z}$.
3) Utilizzando il sistema di generatori $S = \{a, b, c\}$ si provi che H ha crescita polinomiale.

4.6. Ends e gruppi virtualmente ciclici

In questa sezione dimostriamo un paio di risultati enunciati nelle sezioni precedenti. Il primo è che il numero di ends $e(G)$ di un gruppo finitamente generato è un invariante geometrico.

Teorema 4.16. *Siano G, H gruppi finitamente generati; se G e H sono quasi-isometrici allora $e(G) = e(H)$.*

Dimostrazione. Siano G e H gruppi finitamente generati. Proviamo che se esiste una quasi-isometria $G \to H$ allora $e(H) \leq e(G)$. Da questo discende chiaramente il Teorema. Siano dunque S e T sistemi finiti di generatori, rispettivamente, di G e H, e sia

$$f : (G, d_S) \to (H, d_T)$$

una (λ, C)-quasi isometria, con $\lambda \geq 1, C \geq 0$. A meno di traslazione per un elemento di H possiamo supporre $f(1_G) = 1_H$. Per ogni $n \geq 1$, poniamo $M = M(n) = \lambda(n+\lambda+2C)$. Sia X l'insieme dei vertici di una componente connessa infinita di $G \setminus B_S(1, M)$. Quindi, per ogni $g \in X$, $\ell_S(g) > M$ e

$$\ell_T(f(g)) = d_T(1, f(g)) \geq \lambda^{-1} d_S(1, g) - C = \lambda^{-1} \ell_S(g_i) - C > \lambda^{-1} M + C,$$

e quindi $f(X) \subseteq H \setminus B_T(1, \lambda^{-1}M - C) = H \setminus B_T(1, n + \lambda - C)$. Inoltre, se $g, g' \in X$ sono adiacenti (cioè $d_S(g, g') = 1$) allora

$$d_T(f(g), f(g')) \leq \lambda d_S(g, g') + C = \lambda + C;$$

ed esiste quindi in H un cammino da $f(g)$ a $f(g')$ di lunghezza al più $\lambda + C$, cui vertici hanno quindi, per la diseguaglianza triangolare, lunghezza maggiore di

$$\min\{\ell_T(f(g)), \ell_T(f(g'))\} - (\lambda + C) > n + \lambda + C - (\lambda + C) = n;$$

dunque $f(g), f(g')$ sono connessi da un cammino in H che giace interamente fuori dalla palla $B_T(1, n)$. Questo prova che $f(X)$ è contenuta in una unica componente connessa $f(X)^o$ di $H \setminus B_T(1, n)$. Poiché X è infinito, dal Lemma 4.3, segue che $f(X)^o$ è infinita. Dal Lemma 4.4 segue poi piuttosto facilmente che questa associazione è suriettiva. Quindi, se indichiamo con $\mathfrak{c}$ il numero di componenti connesse infinite di un grafo:

$$\mathfrak{c}(H \setminus B_T(1, n)) \leq \mathfrak{c}(G \setminus B_S(1, M(n))).$$

Da ciò segue $e(H) \leq e(G)$ e dunque il Teorema. □

* * *

Il secondo risultato che proviamo è la caratterizzazione dei gruppi quasi-isometrici a $\mathbb{Z}$.

Teorema 4.17. *Un gruppo finitamente generato G è quasi-isometrico al gruppo ciclico $\mathbb{Z}$ se e solo se G ammette un sottogruppo di indice finito che è isomorfo a $\mathbb{Z}$.*

Dimostrazione. Se G ha un sottogruppo di indice finito isomorfo a $\mathbb{Z}$ allora $G \sim_{QI} \mathbb{Z}$ per la Proposizione 4.7. Il grosso del Teorema è il viceversa.

Sia dunque G un gruppo finitamente generato e quasi-isometrico a $\mathbb{Z}$. Fissato un sistema finito S di generatori di G, sia $d = d_S$ la corrispondente word metric su G, e sia $f : G \to \mathbb{Z}$ una quasi-isometria con costanti (λ, C); quindi

$$\lambda^{-1} d(x,y) - C \leq |f(x) - f(y)| \leq \lambda d(x,y) + C, \tag{4.11}$$

per ogni $x, y \in G$. Senza perdere in generalità possiamo inoltre assumere $f(1) = 0$. Ricordiamo che, per il Lemma 4.3, la controimmagine di ogni sottoinsieme finito di $\mathbb{Z}$ è un sottoinsieme finito di G.

1) *G possiede un elemento a di ordine infinito.*

Per il teorema 4.16, il numero di ends di G è uguale a quello di $\mathbb{Z}$, cioè $e(G) = 2$ (vedi sezione 2.6). Ciò significa che possiamo trovare $L \geq \lambda + C$, tale che, posto $B = f^{-1}([-L/2, L/2])$, il grafo $\Gamma \setminus B$, ottenuto da $\Gamma = \Gamma[G, S]$ rimuovendo tutti i vertici in B e gli archi ad essi incidenti, ha esattamente due componenti connesse infinite. Osserviamo che, siccome B è finito, $\Gamma \setminus B$ ha un numero finito di componenti connesse, e dunque un numero finito di componenti connesse finite; possiamo quindi espandere il nostro insieme finito B in modo da contenere anche i vertici di tali componenti. Fatto questo, $\Gamma \setminus B$ ha esattamente due componenti connesse, entrambe infinite. Mostriamo che queste componenti sono

$$A_- = \{x \in G \setminus B \mid f(x) < -L/2\} \quad \text{e} \quad A_+ = \{x \in G \setminus B \mid f(x) > L/2\}.$$

Osservato che A_- e A_+ sono entrambe non vuote, siano $x \in A_-$, $y \in A_+$, e siano $x = g_0, g_1, \ldots, g_n = y$ i vertici di un cammino che congiunge x a y nel grafo Γ; dalla (4.11) segue che, per ogni $i = 0, \ldots, n-1$,

$$|f(g_{i+1}) - f(g_i)| \leq \lambda \cdot 1 + C \leq L.$$

Poiché $f(g_0) = f(x) < -L/2$ e $f(g_n) = f(y) > -L/2$, da ciò segue che per almeno un indice i si deve avere $-L/2 \leq f(g_i) \leq L/2$, e dunque $g_i \in B$. Quindi elementi di A_- ed elementi di A_+ appartengono a componenti connesse distinte di $\Gamma \setminus B$; siccome $\Gamma \setminus B$ ha due componenti connesse, si conclude che queste devono essere A_- ed A_+.

Proviamo ora che G contiene un elemento di ordine infinito. Siano $g \in A_+$ e $h \in A_-$ tali che $d(1, g) > 2diam(B)$ e $d(1, h) > 2diam(B)$; mostriamo che esiste $a \in \{g, h, gh\}$ tale che aA_+ è un sottoinsieme proprio di A_+, oppure aA_- è un sottoinsieme proprio di A_-. Questo implica $|a| = \infty$ (se $a^n = 1$ allora $A_+ = a^n A_+ \subseteq aA_+ \subset A_+$, che è assurdo).
Sia $x \in B$; allora $d(gx, g) = d(x, 1)$, e dunque, per la scelta di g, $gx \in A_+$ (se $y \in B \cup A_-$ ogni cammino da g a y passa per un punto di B, quindi $d(y, g) > diam(B)$). Pertanto, $gB \subseteq A_+$, e similmente $hB \subseteq A_-$. Se $gA_+ \subseteq A_+$ allora $gA_+ \subseteq A_+ \setminus gB$ che è un sottoinsieme proprio di A_+ ed abbiamo finito. Possiamo quindi assumere $gA_+ \not\subseteq A_+$

e, simmetricamente, $hA_- \not\subseteq A_-$. Poiché gA_+ e gA_- sono le componenti connesse di $\Gamma \setminus gB$, abbiamo allora $gA_- \subseteq A_+$ e, dall'altra parte, $hA_+ \subseteq A_-$. Ma allora,

$$ghA_+ = g(hA_+) \subseteq g(A_- \setminus hB)$$

è un sottoinsieme proprio di A_+. Questo completa la dimostrazione che esiste $a \in G$ di ordine infinito.

2) $\langle a \rangle$ *ha indice finito in* G.

Poiché le potenze intere a^z di a sono tutte distinte mentre l'insieme S è finito, si ha che $d(1, a^n)$ tende a infinito quando $n \to \infty$. Poiché f è una quasi-isometria, di conclude che, eventualmente sostituendo a con a^{-1}, la successione $\{f(a^n)\}_{n\geq 0}$ tende a $+\infty$ e la successione $\{f(a^n)\}_{n\leq 0}$ tende a $-\infty$. Ora, per ogni $z \in \mathbb{Z}$,

$$|f(a^{z+1}) - f(a^z)| \leq \lambda d(a^{z+1}, a^z) + C = \lambda d(a, 1) + C = M,$$

con M una costante che non dipende da z. Questo significa che per ogni $w \in \mathbb{Z}$ esiste $n \in \mathbb{Z}$ tale che

$$|f(a^n) - w| \leq M/2.$$

In particolare, posto $K = \lambda(M/2 + C)$, si ha che per ogni $x \in G$ esiste $n \in \mathbb{Z}$ tale che

$$d(1, ga^n) = d(g^{-1}, a^n) \leq \lambda(|f(g) - f(a^n)| + C) \leq \lambda(M/2 + C) = K.$$

Quindi $G = B_S(1, K)\langle a \rangle$; poiché la palla $B_S(1, K)$ è finita, si conclude che $\langle a \rangle$ ha indice finito in G. □

Esercizio 4.23. Un conseguenza della Proposizione 4.17 è che un gruppo quasi-commensurabile al gruppo ciclico $\mathbb{Z}$ ammette un sottogruppo di indice finito isomorfo a $\mathbb{Z}$. Si dia una dimostrazione di questo fatto che non faccia ricorso a tale Proposizione.

Esercizio 4.24. Si provi che i gruppi $\mathbb{Z}$ e D_∞ sono bi-lipschitz equivalenti (si ricordi che una corrispondenza bi-lipschitziana è una biezione).

Esercizio 4.25. (A. Dyubina) Siano A e B gruppi finitamente generati e bi-lipschitz equivalenti; si provi che $A \wr \mathbb{Z}$ e $B \wr \mathbb{Z}$ sono bi-lipschitz equivalenti (questo esercizio generalizza, in modo non proprio immediato, il Teorema 4.10).

Esercizio 4.26. (A. Dyubina) Utilizzando i due esercizi precedenti si provi che la classe dei gruppi (finitamente generati) virtualmente torsion–free non è geometrica.