Corso di Laurea magistrale in Matematica

ALGEBRA SUPERIORE

anno 2020

Testi suggeriti per la consultazione

- Oleg Bogopolski, *Introduction to Group Theory*,
European Mathematical Society Textbooks in Mathematics, 2008.

- Clara Löh, *Geometric Group Theory: an Introduction*,
Springer, 2017.

- Francesco Matucci, *Topics in Geometric Group Theory.*
University of Virginia, 2011.

- John Meier, *Groups, Graphs and Trees*,
London Mathematical Society Student Texts 73. Cambridge University Press, 2008.

Indice

1

Richiami di Teoria dei Gruppi

In questo primo capitolo ricordiamo rapidamente (e per fissare le notazioni) alcuni aspetti di base della teoria dei gruppi. Non ripeteremo le definizioni e i risultati veramente iniziali (sottogruppi, classi laterali, quozienti, Teorema di Lagrange, gruppi ciclici, etc.), e per altri rimandiamo alle dispense di Algebra II [3] o testi elementari del genere, per esempi e dimostrazioni. Ma già partire dalla sezione 1.3, il cui materiale potrebbe risultare nuovo a qualcuno, le dimostrazioni ritorneranno. Sottolineiamo che, in tutte queste dispense, la notazione per le funzioni è sulla sinistra.

1.1. Quozienti, isomorfismi, sottogruppi normali

Siano G e G' gruppi; un'*omomorfismo* da G a G' è un'applicazione $\phi : G \to G'$ tale che

$$\phi(xy) = \phi(x)\phi(y),$$

per ogni $x, y \in G$. Se $\phi : G \longrightarrow G'$ è un omomorfismo, allora $\phi(1_G) = 1_{G'}$ e, per ogni $g \in G$, $z \in \mathbb{Z}$, $\phi(g^z) = (\phi(g))^z$ (in particolare $\phi(g^{-1}) = (\phi(g))^{-1}$). Un *isomorfismo* dal gruppo G nel gruppo G' è un omomorfismo biettivo $\phi : G \longrightarrow G'$ (e si verifica facilmente che ϕ^{-1} è allora un omomorfismo).

Proposizione 1.1 (di omomorfismo)**.** *Sia $\phi : G \to H$ un omomorfismo di gruppi; allora il nucleo $\ker(\phi) = \{g \in G \mid \phi(g) = 1_{G'}\}$ è un sottogruppo normale di G, e la posizione $g\ker(\phi) \mapsto \phi(g)$ definisce un isomorfismo da $G/\ker(\phi)$ in $\phi(G)$ (in particolare, se ϕ è suriettivo, $G/\ker(\phi) \simeq H$).*

Proposizione 1.2. *Siano G un gruppo e $N \trianglelefteq G$.*

- (secondo teorema di omomorfismo) *Per ogni $H \leq G$, $H \cap N \trianglelefteq H$ e*

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}.$$

- (terzo teorema di omomorfismo) *Per ogni $M \trianglelefteq G$ con $N \subseteq M$, $\frac{M}{N} \trianglelefteq \frac{G}{N}$ e*

$$\frac{G}{M} \simeq \frac{G/N}{M/N}.$$

Un isomorfismo di G in se stesso si dice *automorfismo* di G. Per ogni gruppo G, l'applicazione identica ι_G è un automorfismo; inoltre se ϕ, ψ sono automorfismi di G, allora

ϕ^{-1} e $\phi \circ \psi$ sono automorfismi di G. Quindi, l'insieme $Aut(G)$ di tutti gli automorfismi del gruppo G è un gruppo rispetto all'operazione di composizione, detto *Gruppo degli automorfismi* di G.

Coniugio. Importanti automorfismi del gruppo G sono quelli di *coniugio*: per ogni $g \in G$, infatti, l'applicazione

$$\begin{aligned} \sigma_g : G &\to G \\ x &\mapsto x^g = gxg^{-1} \end{aligned}$$

è un automorfismo di G. L'elemento gxg^{-1} si chiama coniugato di x tramite g. Per ogni $g, h \in G$, $\sigma_g \circ \sigma_h = \sigma_{gh}$ (e $\sigma_{g^{-1}} = \sigma_g^{-1}$), il che mostra che la posizione $g \mapsto \sigma_g$ definisce un omomorfismo $G \to Aut(G)$, il cui nucleo è il centro $Z(G)$ di G, e la cui immagine

$$Inn(G) = \{\sigma_g \mid g \in G\}$$

è detta gruppo degli *automorfismi interni* di G. Per il Teorema di omomorfismo si ha

$$Inn(G) \simeq \frac{G}{Z(G)}.$$

Si verifica subito che per ogni $\phi \in Aut(G)$ ed ogni $g \in G$, $\phi\sigma_g = \sigma_{\phi(g)}\phi$, quindi $Inn(G)$ è un sottogruppo normale di $Aut(G)$; il gruppo quoziente

$$Out(G) := \frac{Aut(G)}{Inn(G)}$$

si chiama *gruppo degli automorfismi esterni* di G.

La notazione esponenziale x^g per il coniugato di un elemento si estende nel modo che ci si aspetta all'immagine di un qualsiasi sottoinsieme: se $X \subseteq G$, ovvero

$$X^g = \sigma_g(X) = \{x^g \mid x \in X\}$$

che si chiamerà, ancora, coniugato di X tramite g. In particolare, se $H \leq G$ e $g \in G$ allora $H^g \leq G$, e che la restrizione del coniuguio σ_g ad H determina un isomorfismo $H \to H^g$. Inoltre, un sottogruppo H di G è normale se e solo se

$$H^g = H \text{ per ogni } g \in G,$$

condizione che si riconosce subito essere equivalente a $x^g \in H$ per ogni $x \in H,\ g \in G$.

Centralizzanti e normalizzanti. Sia G un gruppo e $X \subseteq G$. Il *centralizzante* di X in G è

$$C_G(X) := \{g \in G \mid xg = gx \text{ per ogni } x \in X\}.$$

(quindi, ad esempio, $C_G(G) = Z(G)$). Si verifica agevolmente che per ogni $X \subseteq G$, $C_G(X) \leq G$; se inoltre $X \subseteq Y \subseteq G$, allora $C_G(Y) \leq C_G(X)$.
Se H è un sottogruppo del gruppo G, il *normalizzante* di H in G è

$$\mathcal{N}_G(H) = \{g \in G \mid H^g = H\}.$$

Quindi, un sottogruppo H di G è normale se (e solo se) $\mathcal{N}_G(H) = G$. Più compiutamente, per ogni $H \leq G$ sussistono le proprietà seguenti:

- $H \trianglelefteq \mathcal{N}_G(H) \leq G$;
- $C_G(H) \trianglelefteq \mathcal{N}_G(H)$;
- $\mathcal{N}_G(H)/C_G(H)$ è isomorfo ad un sottogruppo di $Aut(H)$.

Solo la verifica dell'ultimo punto richiede, forse, un commento: poiché H è un sottogruppo normale di $\mathcal{N}_G(H)$, ogni elemento $b \in \mathcal{N}_G(H)$ induce per coniugio (ristretto ad H) un automorfismo di H, e gli elementi di b tali che $\sigma_b|_H$ è l'identità sono precisamente quelli che appartengono a $C_H(H)$.
I concetti e le notazioni per centralizzanti e normalizzanti si relativizzano a sottogruppi; così, se H e T sono sottogruppi di G, il normalizzante di H in T è

$$\mathcal{N}_T(H) = \{x \in T \mid H^x = H\} = T \cap \mathcal{N}_G(H);$$

e similmente, se $X \subseteq G$, il centralizzante di X in T è $C_T(X) = C_G(X) \cap T$.

L'intersezione di tutti i sottogruppi normali di G che contengono un dato sottogruppo H, è un sottogruppo normale di G che si denota con H^G e si chiama *chiusura normale* di H in G. Quindi, H^G è il minimo sottogruppo normale di G contenente H e $H \trianglelefteq G \Leftrightarrow H^G = H$. Si vede facilmente che H^G coincide con il sottogruppo generato da tutti i coniugati di H. Dualmente, si definisce il *cuore* H_G di $H \leq G$ come il massimo sottogruppo normale di G che è contenuto in H. Quindi , $H \trianglelefteq G \Leftrightarrow H_G = H$, e, ancora, si vede facilmente che H_G coincide l'intersezione di tutti i coniugati di H, cioè

$$H_G = \bigcap_{g \in G} H^g. \tag{1.1}$$

Prodotti diretti. Se, per $1 \leq n \in \mathbb{N}$, $H_1, \ldots, H_n$ sono gruppi, il loro *prodotto diretto* è l'insieme $H_1 \times H_2 \times \cdots \times H_n$ dotato dell'operazione per componenti:

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n),$$

per ogni $x_i, y_i \in H_i$ $(i = 1, \ldots, n)$. Talvolta, questo, che si denota semplicemente con $H_1 \times H_2 \times \ldots \times H_n$, è denominato prodotto diretto 'esterno', distinguendolo da quello 'interno', che richiamiamo nel caso $n = 2$, lasciando per esercizio la formulazione e la dimostrazione della estensione ad un arbitrario intero positivo n.

Proposizione 1.3. *Se A, B sono sottogruppi normali del gruppo G, ed inoltre $G = AB$ e $A \cap B = 1$, allora $G \simeq A \times B$.*

Gruppi simmetrici. Esempi fondamentali di gruppi (non commutativi) sono i gruppi simmetrici. Sia X un insieme; una *permutazione* di X è un'applicazione biettiva da X in se stesso. L'insieme $(Sym(X), \circ)$ di tutte le permutazioni di X), con l'operazione di composizione è un gruppo, detto il *gruppo simmetrico* su X. È facile vedere che, per ogni coppia di insiemi X, Y, $Sym(X) \simeq Sym(Y)$ se e solo se $|X| = |Y|$. Il gruppo simmetrico sull'insieme $I_n = \{1, 2, \ldots, n\}$ si denota abitualmente con S_n e si chiama *gruppo simmetrico di grado n*. Ogni elemento di S_n si scrive in modo uncio (a meno cioè dell'ordine dei fattori) come un prodotto di *cicli* disgiunti.
Normalmente, ometteremo il simbolo $\circ$ nella composizione di due permutazioni (e spesso, se il contesto lo permette, anche per la composizione di funzioni in genere), ricordando però che la composizione (circoletto e non circoletto) e sempre intesa su funzioni scritte 'a sinistra'. Ad esempio, nel gruppo S_7,

$$(1\,3\,5\,2\,4)(3\,7\,2) = (1\,3\,7\,4)(2\,5).$$

ESERCIZIO 1.1. Sia G un gruppo, e poniamo $A = Aut(G)$ e $I = Inn(G)$. Si provi che se $Z(G) = 1$ allora $C_A(I) = 1$.

ESERCIZIO 1.2. Siano $\mathbb{F}$ un campo, $n \geq 1$ e $G = GL(n, \mathbb{F})$ (il gruppo delle matrici invertibili $n \times n$ a coefficienti in $\mathbb{F}$). Allora l'applicazione "inversa della trasposta" $A \mapsto (A^{\mathrm{T}})^{-1}$ $(\forall A \in G)$ è un automorfismo di G. Si provi che non è un automorfismo interno.

ESERCIZIO 1.3. Un sottogruppo C del gruppo G si dice *caratteristico* in G (e si scrive $C\, char\, G$) se $\phi(C) = C$ per ogni $\phi \in Aut(G)$. Si provi che se C, N sono sottogruppi di G tali che $C\, char\, N \trianglelefteq G$ allora $C \trianglelefteq G$. Sia quindi M il gruppo additivo di uno spazio vettoriale (su qualche campo); si provi che $\{0\}$ e M sono i soli sottogruppi caratteristici di M.

1.2. Azioni

Il concetto di azione di un gruppo è fondamentale, ed è quello che, si potrebbe ben dire, garantisce l'importanza del ruolo dei gruppi nell'intera matematica.
Iniziamo col fissare le notazioni; in particolare stabilendo che, in queste note, azioni di gruppi saranno sulla sinistra.

DEFINIZIONE. Un'*azione* di un gruppo G su un insieme non vuoto S è un'applicazione

$$\begin{array}{ccc} G \times S & \to & S \\ (g, s) & \mapsto & g \cdot s \end{array}$$

tale che sono soddisfatte le seguenti condizioni: per ogni $g, h \in G$ ed ogni $s \in S$:

$$1_G \cdot s = s, \quad (gh) \cdot s = g \cdot (h \cdot s). \tag{1.2}$$

Data una tale azione, per ogni $g \in G$ la funzione $\phi(g) : S \to S$, definita da $\phi(g)(s) = g \cdot s$, è una permutazione di S (cioè un elemento di $Sym(S)$), e le proprietà in (1.2) implicano l'omomorfismo di gruppi

$$\begin{array}{ccc} G & \to & Sym(S) \\ g & \mapsto & \phi(g) \end{array} \tag{1.3}$$

Viceversa, ogni omomorfismo come in (1.3) induce naturalmente un'azione di G su S.

Un'azione di un gruppo G su un insieme S si dice *fedele* se per ogni $1 \neq g \in G$ esiste $s \in S$ tale che $g \cdot s \neq s$; questo equivale a richiedere che l'omomorfismo (1.3) sia iniettivo; in tal caso l'immagine $\phi(G)$ è un sottogruppo di $Sym(S)$ isomorfo a G, e si dice (identificando G con $\phi(G)$) che G è un *gruppo di permutazioni* su S.

Data un'azione del gruppo G su S, per ogni $x \in S$ si definiscono

- l'*orbita* di x: $\mathcal{O}(x) = \{g \cdot x \mid g \in G\}$;
- lo *stabilizzatore* in G di x: $G_x = \{g \in G \mid g \cdot x = x\}$.

Si verifica agevolmente (vedi Algebra II) che G_x è un sottogruppo di G, e che la posizione $gG_x \mapsto g \cdot x$ definisce una biezione dall'insieme delle classi laterali sinistre $\{gG_x \mid g \in G\}$ in $\mathcal{O}(x)$. In particolare

$$|G : G_x| = |\mathcal{O}(x)|.$$

L'azione è *transitiva* se per ogni $(x, y) \in S \times S$ esiste $g \in G$ tale che $g \cdot x = y$ (ovvero $\mathcal{O}(x) = S$ per ogni $x \in S$.

Un'utile osservazione è la seguente.

Lemma 1.4. *Data un'azione del gruppo G su S siano $x \in S$, $g \in G$ e $y = g \cdot y$; allora $Gy = G_x^g$. In particolare, se l'azione è transitiva gli stabilizzatori dei punti sono tra loro coniugati in G.*

Dimostrazione. Esercizio. □

Esempio 1.1. Un esempio significativo di azione transitiva è quello del gruppo speciale lineare n-dimensionale sullo spazio proiettivo $(n-1)$-dimensionale. Vediamo il caso $n = 2$. Sia quindi $\mathbb{K}$ un campo e $G = SL(2, \mathbb{K})$.
La moltiplicazione a sinistra, (per $A \in G$ e $\mathbf{v} = (a, b) \in \mathbb{K}^2$, $A \cdot \mathbf{v} = A\mathbf{v}^T$) definisce l'azione naturale di G sullo spazio $V = \mathbb{K}^2$. Questa, a sua volta, induce un'azione di G sulla *retta proiettiva*

$$P(1, \mathbb{K}) = \{\mathbb{K}\mathbf{u} \mid 0 \neq \mathbf{u} \in V\}$$

(l'insieme dei sottospazi 1-dimensionali di V), mediante la posizione

$$(g, \mathbb{K}\mathbf{u}) \mapsto \mathbb{K}g(\mathbf{u}).$$

Il nucleo K di questa azione è l'insieme della matrici scalari in G, dunque $K = \{\pm I\}$ (dove I è la matrice identica). Tale azione è 2-*transitiva*, nel senso che date due qualsiasi coppie ordinete $(\mathbb{K}\mathbf{u}_1, \mathbb{K}\mathbf{u}_2)$ $(\mathbb{K}\mathbf{u}'_1, \mathbb{K}\mathbf{u}'_2)$, di punti in $P(1, \mathbb{K})$, tali che $\mathbb{K}\mathbf{u}_1 \neq \mathbb{K}\mathbf{u}_2$ e $\mathbb{K}\mathbf{u}'_1 \neq \mathbb{K}\mathbf{u}'_2$, esiste un elemento $gK \in G/K$ tale che

$$g(\mathbb{K}\mathbf{u}_1) = \mathbb{K}\mathbf{u}'_1, \quad g(\mathbb{K}\mathbf{u}_2) = \mathbb{K}\mathbf{u}'_2. \tag{1.4}$$

L'analoga azione si può descrivere interpretando la retta proiettiva $P(1, \mathbb{K})$ come l'insieme ottenuto aggiungendo a $\mathbb{K}$ un elemento (detto *infinito*), ovvero $P(1, \mathbb{K}) = \mathbb{K} \cup \{\infty\}$; l'azione di $G = SL(2, \mathbb{K})$ è definita associando ad ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ la *trasformazione di Möbius*

$$x \mapsto \frac{ax + b}{cx + d} \qquad (x \in P(1, \mathbb{K}))$$

(con le operazioni ovvie riguardo ∞). □

Esempio 1.2. Sia H un sottogruppo del gruppo G, e sia $X = \{xH \mid x \in G\}$ l'insieme delle classi laterali sinistre di G modulo H. L'applicazione

$$\begin{array}{ccc} G \times X & \to & X \\ (g, xH) & \mapsto & (gx)H \end{array}$$

definisce un'azione transitiva di G su X. Per ogni $xH \in X$, il suo stabilizzatore in G è

$$\{g \in G \mid gxH = xH\} = \{g \in G \mid x^{-1}gxH = H\} = \{g \in G \mid x^{-1}gx \in H\} = xHx^{-1}.$$

Dunque il nucleo dell'azione è l'intersezione dei coniugati in G di H,

$$H_G := \bigcap_{x \in G} xHx^{-1},$$

che è il più grande sottogruppo normale di G contenuto in H. Quando $H = \{1\}$ tale azione non è che quella per moltiplicazione a sinistra di G su se stesso.

Si osservi, in particolare, che se $[G : H] = n$ è finito allora G/H_G è isomorfo ad un sottogruppo di S_n; dunque H_G è un sottogruppo normale di G il cui indice divide $n!$. □

ESERCIZIO 1.4. Si dimostrino per bene le affermazioni nell'esempio 1.1 riguardo l'azione di $SL_2(\mathbb{K})$ sulla retta proiettiva. Si provi inoltre che nessun elemento $g \neq \pm I$ fissa più di due diversi punti di $P(1, \mathbb{K})$.

ESERCIZIO 1.5. Due azioni di un gruppo G sugli insiemi S e S' si dicono *equivalenti* se esiste una biezione $\alpha : S \to S'$ tale che $g \cdot \alpha(x) = \alpha(g \cdot x)$ per ogni $g \in G$ e $x \in S$. Si provi che ogni azione transitiva del gruppo G è equivalente ad un'azione sulle classi laterali di un sottogruppo, come descritta nell'esempio 1.2 (considerare lo stabilizzatore di un punto).

ESERCIZIO 1.6. (Lemma detto "di Burnside") Data un'azione del gruppo G sull'insieme S, per ogni $g \in G$ denotiamo con S^x l'insieme dei punti fissi per g, $S^g = \{x \in S \mid g \cdot x = x\}$. Calcolando in due maniere l'ordine dell'insieme $\{(g, x) \in G \times S \mid g \cdot x = x\}$, si provi che se S è finito allora

$$t|G| = \sum_{g \in G} |S^g|,$$

dove t è il numero di orbite distinte di G su S.

1.3. Costruzioni di gruppi

Vogliamo estendere l'idea di prodotto diretto di un numero finito di gruppi in modo da arrivare al prodotto di famiglie anche infinite di gruppi. Gli elementi di un prodotto $G_1 \times \ldots \times G_n$ sono in modo naturale n-uple; e se l'insieme dei gruppi è indicizzato da $\mathbb{N}$ (cioè, è numerabile) non è difficile immaginare gli elementi di un prodotto come sequenze $(g_0, g_1, g_2, \ldots)$. Questa sorta di visualizzazione rimane un'utile guida, ma diventa per così dire 'interiore' quando la famiglia di gruppi di cui si vuole un prodotto non è già ordinata come i numeri naturali.
La maniera più semplice per estendere l'idea di n-upla ad una famiglia $\mathcal{G}$ qualsiasi di gruppi (o, in generale, di insiemi) è quella di considerare le funzioni $f : \mathcal{G} \to \bigcup_{H \in \mathcal{G}} H$ tali che $f(H) \in H$ per ogni $H \in \mathcal{G}$. Nel seguito consideriamo, per comodità, famiglie di gruppi indicizzate su un insieme (è la stessa cosa: in quello detto prima, la famiglia $\mathcal{G}$ è indicizzata da se stessa).

Prodotto cartesiano. Sia $(G_n)_{n \in I}$ una famiglia di gruppi, per qualche opportuno insieme di indici I. Sia W l'insieme di tutte le applicazioni

$$f : I \to \bigcup_{n \in I} G_n$$

tali che $f(n) \in G_n$ per ogni $n \in I$.
Su W si definisce l'operazione $\cdot$ di prodotto 'puntuale': ossia, date $f, g \in W$, si pone

$$(f \cdot g)(n) = f(n)g(n) \in G_n \quad \text{per ogni } n \in I.$$

Si prova immediatamente che $(W, \cdot)$ è un gruppo, che è il *prodotto cartesiano* della famiglia $(G_n)_{n \in I}$, e che denoteremo con $Car_{n \in I} G_n$. È una facile evidenza che, se $I = \{1, \ldots, n\}$ allora $Car_{n \in I} G_n = G_1 \times \ldots G_n$.

Una fondamentale utilizzo del prodotto cartesiano è conseguenza dal seguente risultato.

Proposizione 1.5. *Sia $\mathcal{R}$ una famiglia di sottogruppi normali del gruppo G. Allora l'applicazione*

$$G \to W = Car_{N \in \mathcal{R}} G/N$$

che ad ogni $g \in G$ associa l'applicazione data da

$$N \mapsto Ng, \quad \text{per ogni } N \in \mathcal{R}$$

è un omomorfismo di gruppi il cui nucleo è $\bigcap_{N\in\mathcal{R}} N$. In particolare, se $\bigcap_{N\in\mathcal{R}} N = 1$, allora G è isomorfo ad un sottogruppo di $Car_{N\in\mathcal{R}} G/N$.

Dimostrazione. L'enunciato indica in modo abbastanza chiaro la sua dimostrazione. Questa proprietà si può descrivere in modo più astratto e generale come una qualità universale del prodotto cartesiano (vedi esercizio 1.7). ∎

Sia, come sopra, $(G_i)_{i\in I}$ una famiglia di gruppi e $W = Car_{i\in I} G_i$. Per ogni $i \in I$ si definisce la proiezione $\pi_i : W \to G_i$ ponendo $f \mapsto f(i)$ per ogni $f \in W$. Per definizione di operazione in W, π_i è un omomorfismo suriettivo; il suo nucleo, non è altro che il prodotto cartesiano

$$\ker \pi_i = Car_{i\neq n\in I} G_n. \tag{1.5}$$

Corrispondentemente, si definisce il sottogruppo

$$G_i^* = \{f \in W \mid f(j) = 1_{G_j} \text{ per } j \neq i\}. \tag{1.6}$$

La restrizione a G_i^* della proiezione π_i è un isomorfismo $G_i^* \to G_i$, ed è immediato verificare che $G_i^* \trianglelefteq W$; segue quindi che

$$W \simeq G_i^* \times (\ker \pi_i) \tag{1.7}$$

Prodotto diretto. Il prodotto diretto è un sottogruppo del prodotto cartesiano (ed è proprio se la famiglia dei gruppi è infinita). Sia, come sopra, $(G_n)_{n\in I}$ una famiglia di gruppi; per ogni $f \in W = Car_{n\in I} G_n$ si definisce il *supporto* di f:

$$supp(f) = \{n \in I \mid f(n) \neq 1_{G_n}\}. \tag{1.8}$$

Si prova facilmente che l'insieme delle funzioni a supporto finito,

$$\{f \in W \mid |supp(f)| < \infty\},$$

è un sottogruppo normale di W; questo sottogruppo, che denotiamo con $Dir_{n\in I} G_n$ è, per definizione, il *prodotto diretto* della famiglia $(G_n)_{n\in I}$.

Va da sé che se I è finito ($I = \{1, \ldots, n\}$) il prodotto diretto coincide con quello cartesiano che a sua volta coincide con la definizione di prodotto diretto $G_1 \times \cdots \times G_n$ data nel corso di Algebra.

Prodotti semidiretti. Sia N un sottogruppo normale del gruppo G, e supponiamo esista un sottogruppo H di G che ne sia un complemento, cioè si abbia:

$$\begin{cases} G = NH \\ N \cap H = 1 \end{cases}$$

Essendo normale, N è invariante per ogni coniugio mediante elementi di H. Segue quindi facilmente che l'applicazione

$$\begin{array}{rcl} \phi : H & \to & Aut(N) \\ h & \mapsto & \sigma_h|_N \end{array}$$

è un omomorfismo, il cui nucleo è $C_H(N) = \{h \in H \mid hx = xh \ \forall x \in N\}$. Si dice che il gruppo G è il *prodotto semidiretto* (interno) di N per H, con ϕ omomorfismo associato.

Descriviamo la corrispondente costruzione "esterna". Siano N, H gruppi e sia dato un omomorfismo $\phi : H \to Aut(N)$. Per ogni $x \in H$ e $a \in N$ scriviamo $a^{\phi(x)}$ per $\phi(x)(a)$. Sull'insieme $N \times H$ si definisce un'operazione ponendo, per ogni $(a, x), (b, y) \in N \times H$,

$$(a, x)(b, y) = (ab^{\phi(x)}, xy), \tag{1.9}$$

Si verifica che con tale operazione $G = N \times H$ è un gruppo, che si chiama il *prodotto semidiretto* (esterno) di N per H associato all'omomorfismo ϕ, che noi denoteremo con

$$G = N \rtimes_\phi H$$

(semplicemente $N \rtimes H$ quando non ci saranno ambiguità riguardo all'omomorfismo ϕ, o quando ci riferiremo ad un generico prodotto semidiretto dei due gruppi N e H). Si vede facendo direttamente i conti che $1_G = (1_N, 1_H)$, e

$$(a, x)^{-1} = ((a^{-1})^{\phi(x^{-1})}, x^{-1}) \tag{1.10}$$

per ogni $a \in N$, $x \in H$. Osserviamo poi che se ϕ è l'omomorfismo banale (cioè $\phi(x) = \iota_N$ per ogni $x \in H$), allora $N \rtimes_\phi H$ non è altro che il prodotto diretto $N \times H$.

L'identità tra i concetti interno ed esterno di prodotto semidiretto è data dalla seguente Proposizione, la cui dimostrazione è lasciata per esercizio.

Proposizione 1.6. *Siano H, N gruppi, $\phi : H \to Aut(N)$ un omomorfismo. Nel prodotto semidiretto $G = N \rtimes_\phi H$ siano $N^* = \{(a, 1_H) \mid a \in N\}$ e $H^* = \{(1_N, x) \mid x \in H\}$. Allora $N^* \trianglelefteq G$ e H^* è un suo complemento.*

Con le stesse notazioni osserviamo che, se $a^* = (a, 1) \in N^*$ e $x^* = (1, x) \in H^*$, allora

$$(a^*)^{x^*} = (1, x)(a, 1)(1, x^{-1}) = (a^{\phi(x)}, 1) = (a^{\phi(x)})^*,$$

Quindi, l'automorfismo indotto per coniugio da $x^* \in H^*$ su N^* coincide - via isomorfismo $*$ - con $\phi(x)$. Nella prassi, in un prodotto semidiretto esterno G come nella Proposizione 1.6, si identificano N con N^* e H con H^*, e si vede a G come il prodotto NH.

Esempio 1.3. Sia $\mathbb{F}$ un campo. Allora, per ogni $0 \neq a \in \mathbb{F}$ la proprietà distributiva assicura che moltiplicazione per a definisce un automorfismo del gruppo additivo $(\mathbb{F}, +)$ che denotiamo con $\phi(a)$ (quindi, $\phi(a)(x) = xa$ per ogni $x \in \mathbb{F}$. Posto $\mathbb{F}^* = \mathbb{F} \setminus \{1\}$ il gruppo moltiplicativo di $\mathbb{F}$, si ha (lo si verifichi) che l'applicazione $\phi : \mathbb{F}^* \to Aut(\mathbb{F})$ è un omomorfismo. Questo consente di definire un prodotto semidiretto $\mathbb{F} \rtimes_\phi \mathbb{F}^*$. □

Esempio importante: isometrie di $\mathbb{R}^n$. Sia $n \geq 2$ un intero e sia $V = \mathbb{R}^n$ lo *spazio euclideo* delle n-uple di numeri reali, provvisto della *distanza euclidea* d definita nel modo corrente: se $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ e $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ sono elementi di $\mathbb{R}^n$, allora la

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}.$$

Una *isometria* di V è un'applicazione $\phi : V \to V$ che conserva le distanze, ovvero tale che, per ogni $\mathbf{x}, \mathbf{y} \in V$:

$$d(\phi(\mathbf{x}), \phi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}).$$

Indichiamo con M_n l'insieme di tutte le isometrie di $V = \mathbb{R}^n$. È chiaro che la composizione di due isometrie è un'isometria. Inoltre, si prova (esercizio) che

(∗) *Ogni isometria è una biezione, e la sua inversa è un'isometria.*

Si deduce quindi che $M = M_n$, con l'operazione di composizione, è un gruppo, detto *Gruppo delle isometrie* di $\mathbb{R}^n$. Un rilievo particolare rivestono due tipi di simmetrie: traslazioni e rotazioni. Per ogni $\mathbf{v} \in V$ definiamo la *traslazione* $t_\mathbf{v}$ modulo $\mathbf{v}$ come l'applicazione di V in se stesso definita da $t_\mathbf{v}(\mathbf{x}) = \mathbf{x} + \mathbf{v}$, per ogni $\mathbf{x} \in V$. Si verifica immediatamente che, per ogni $\mathbf{v} \in V$, $t_\mathbf{v}$ è una isometria. Chiaramente, $t_\mathbf{0}$ è l'applicazione identica; inoltre, per ogni $\mathbf{v}, \mathbf{w} \in V$

$$t_\mathbf{v} \circ t_\mathbf{v} = t_{\mathbf{v}+\mathbf{w}} \qquad \text{e} \qquad t_\mathbf{v}^{-1} = t_{-\mathbf{v}}$$

In particolare, il sottoinsieme di tutte le traslazioni di V, $T = \{t_\mathbf{v} \mid \mathbf{v} \in V\}$, è un sottogruppo di M, detto il *gruppo delle traslazioni* di V, e l'applicazione

$$\begin{array}{ccc} \mathbb{R}^n & \to & T \\ \mathbf{v} & \mapsto & t_\mathbf{v} \end{array}$$

è un isomorfismo del gruppo additivo $(\mathbb{R}^n, +)$ in T. Consideriamo ora l'insieme di tutte le isometrie di V che fissano l'origine, cioè

$$R = \{\rho \in M \mid \rho(\mathbf{0}) = \mathbf{0})\} \ .$$

Chiaramente R è un sottogruppo di M, detto *gruppo delle rotazioni* di V. Inoltre non è difficile provare che ogni elemento di R è un'applicazione lineare (invertibile) di $\mathbb{R}^n$ (di fatto, R coincide con l'insieme delle isometrie che sono lineari). Si conclude con il seguente fatto:

(∗∗) *M è il prodotto semidiretto $M = T \rtimes R$; in particolare, ogni isometria di V si scrive in modo unico come il prodotto di una traslazione per una rotazione.*

Sia infatti $f \in M$, e scriviamo $\mathbf{v} = f(\mathbf{0})$. Allora, posto $\rho = t_{-\mathbf{v}} \circ f$, si ha

$$\rho(\mathbf{0}) = (t_{-\mathbf{v}} \circ f)(\mathbf{0}) = t_{-\mathbf{v}}(f(\mathbf{0})) = f(\mathbf{0}) - \mathbf{v} = \mathbf{v} - \mathbf{v} = \mathbf{0}$$

quindi ρ è una rotazione, e $f = t_{-\mathbf{v}}^{-1} \circ \rho = t_\mathbf{v} \circ \rho$. Dunque, $M = TR$. Inoltre è ovvio che $T \cap R = \{\iota\}$. Rimane da provare che $T \trianglelefteq M$; e per questo basta osservare che ogni rotazione ρ normalizza T. Siano dunque $t_\mathbf{v} \in T$ e $x \in \mathbb{R}^n$; allora , tenendo conto che ρ è lineare:

$$\rho t_\mathbf{v} \rho^{-1}(x) = \rho(\rho^{-1}(x) + \mathbf{v}) = x + \rho(\mathbf{v}).$$

Quindi $\rho t_\mathbf{v} \rho^{-1} = t_{\rho(\mathbf{v})} \in T$. □

Gruppi diedrali. Un'importante famiglia di prodotti semidiretti (definiti da un'azione non banale) è quella dei gruppi diedrali. Sia A un gruppo ciclico (finito o infinito) e sia $H = \langle x \rangle$ un gruppo ciclico di ordine due che opera come l'inversione su A, ovvero si associa ad x l'automorfismo di A definito dall'inversione ($u^x = u^{-1}$ per ogni $u \in A$). Il prodotto semidiretto $A \rtimes H$ si chiama *gruppo diedrale*: se A è ciclico infinito si denota con D_∞ (e si chiama gruppo diedrale infinito); mentre se $|A| = n$ è finito, si denota con D_{2n}. Notiamo che in questo ultimo caso si ha $|D_{2n}| = |A||H| = 2n$, e quindi D_{2n} si chiama gruppo diedrale di ordine $2n$.
Osserviamo che, secondo la definizione, $D_4 \simeq C_2 \times C_2$, $D_6 \simeq S_3$, mentre per $n \geq 2$, D_{2n}, così come D_∞, non è abeliano. (Non è difficile provare che, per $n \geq 3$, il gruppo diedrale D_{2n} è isomorfo al gruppo delle simmetrie di un n-agono regolare sul piano, cioè il gruppo delle isometrie di $\mathbb{R}^2$ che lasciano fisso un n-agono regolare centrato nell'origine.)

ESERCIZIO 1.7. (Proprietà universale del prodotto cartesiano) Sia $(G_i)_{i\in I}$ una famiglia di gruppi, e $C = Car_{i\in I}G_i$ il suo prodotto cartesiano. Per ogni $i \in I$ si denoti con π_i la proiezione $C \to G_i$. Sia H un gruppo e per ogni $i \in I$ sia assegnato un omomorfismo $\phi_i : H \to G_i$. Si provi che esiste un unico omomorfismo $\phi : H \to C$ tale che $\phi\pi_i = \phi_i$ per ogni $i \in I$.

ESERCIZIO 1.8. Sia $n \geq 2$ e D_{2n} il gruppo diedrale di ordine $2n$. Si provi che le seguenti condizioni sono equivalenti:

(1) n è dispari;

(2) le involuzioni (cioè gli elementi di ordine 2) di D_{2n} sono a due a due coniugate.

ESERCIZIO 1.9. Sia G un gruppo infinito tale che esiste $A \trianglelefteq G$ con A ciclico e $|G : A| = 2$. Si provi che G è isomorfo ad uno dei seguenti gruppi: $\mathbb{Z}$, $\mathbb{Z} \times C_2$, D_∞.

1.4. Tipi di gruppi

Richiamiamo ora - con il principale intento di fissare la nomenclatura e le notazioni - alcune importanti classi di gruppi. Se g è un elemento di un gruppo, denotiamo con $|g|$ il suo ordine, ricordando che l'ordine di un elemento coincide con quello del sottogruppo ciclico da esso generato.

DEFINIZIONI. Sia G un gruppo.

(1) G si dice *commutativo* (o *abeliano*) se $xy = yx$ per ogni $x, y \in G$.

(2) G si dice *periodico* se ogni suo elemento ha ordine finito; se p è un numero primo, G si dice un *p-gruppo* se ogni suo elemento ha ordine una potenza di p.

(3) G si dice *torsion-free* se ogni suo elemento $g \neq 1$ ha ordine infinito.

Una classe $\mathfrak{X}$ di gruppi è chiusa per sottogruppi se $H \in \mathfrak{X}$ per ogni $G \in \mathfrak{X}$ e $H \leq G$. La classe $\mathfrak{X}$ è chiusa per quozienti (o, per omomorfismi) se $G/N \in \mathfrak{X}$ per ogni $G \in \mathfrak{X}$ e $N \trianglelefteq G$ (che chiaramente equivale a dire che per ogni $G \in \mathfrak{X}$ ed ogni omomorfismo $\phi : G \to G'$ l'immagine $\phi(G)$ appartiene a $\mathfrak{X}$).
La classe $\mathfrak{X}$ è chiusa per estensioni se dati un gruppo G e $N \trianglelefteq G$, da $N, G/N \in \mathfrak{X}$ segue $G \in \mathfrak{X}$: condizione che può essere anche formulata dicendo che per ogni $N, H \in \mathfrak{X}$ ed ogni sequenza esatta di omomorfismi $1 \to N \to G \to H \to 1$, si ha $G \in \mathfrak{X}$.
Tutte le classi della definizione precedente sono chiuse per sottogruppi. Le classi ai punti (1) e (2) sono chiuse per quozienti, mentre così non è per il caso (3): il gruppo additivo $\mathbb{Z}$ è torsion-free ma ammette come immagini omomorfe i gruppi finiti $\mathbb{Z}/n\mathbb{Z}$. Sono chiuse per estensioni la classi ai punti (2) e (3) (lo si dimostri per esercizio), ma non quella dei gruppi commutativi: gli esempi più semplici sono i gruppi diedrali (vedi sezione 1.3), infatti per ogni $n \geq 1$ si ha la sequenza esatta

$$1 \to C_n \to D_{2n} \to C_2 \to 1$$

dove C_2 e C_n (gruppi ciclici di ordine, rispettivamente, 2 e n) sono commutativi ma D_{2n} non lo è (se $n \geq 3$).

Vediamo alcune altre importanti classi le cui definizioni sono un poco meno dirette.

DEFINIZIONI. Sia G un gruppo e sia $\mathfrak{X}$ una classe di gruppi.

(1) G si dice *localmente–$\mathfrak{X}$* se ogni sottoinsieme finito di G è contenuto in un sottogruppo che appartiene alla classe $\mathfrak{X}$.

(2) G si dice *residualmente–*$\mathfrak{X}$ se l'intersezione di tutti i sottogruppi $N \trianglelefteq G$ tali che $G/N \in \mathfrak{X}$ è il sottogruppo banale.

Osserviamo che la proprietà in (2) equivale a richiedere che per ogni $1 \neq x \in G$ esistano un gruppo $H \in \mathfrak{X}$ ed un omomorfismo suriettivo $\phi : G \to H$ tale che $\phi(x) \neq 1$.

Di particolare interesse il caso in cui $\mathfrak{X}$ è la classe di tutti i gruppi finiti; si hanno allora i gruppi *localmente finiti*, in cui ogni sottoinsieme finito è contenuto in un sottogruppo finito, ed i gruppi *residualmente finiti*, in cui l'intersezione dei sottogruppi normali di indice finito è il gruppo identico.

La classe dei gruppi localmente finiti è chiusa per sottogruppi e per quozienti, e questo è facile, mentre la non immediata dimostrazione che è chiusa per estensioni la vedremo più avanti (esercizio 1.27). Chiaramente, ogni gruppo localmente finito è periodico; la prima costruzione di gruppi periodici (ed infatti, p-gruppi) non localmente finiti fu fornita da Golod nel 1964, rispondendo così ad un famoso problema formulato da Burnside nel 1902. Nel seguito, vedremo delle costruzioni più recenti di gruppi di questo tipo.

La classe dei gruppi residualmente finiti è chiusa per sottogruppi, ed anche questo è banale, ma non per quozienti, né per estensioni, cose delle quali ancora rinviamo le non ovvie dimostrazioni. Facciamo invece la seguente osservazione; sia G un gruppo residualmente–$\mathfrak{X}$, per una data classe $\mathfrak{X}$, e sia $\mathcal{M}$ una famiglia di sottogruppi normali di G tale che $G/N \in \mathfrak{X}$ per ogni $N \in \mathcal{M}$ e $\bigcap_{N\in\mathcal{M}} N = 1$; allora, per la Proposizione 1.5, G è isomorfo ad un sottogruppo di $Car_{N\in\mathcal{M}} G/N$, un prodotto cartesiano di gruppi appartenenti a $\mathfrak{X}$.

Un'importante classe di gruppi, quasi certamente già nota a chi legge, ovvero quella dei gruppi finitamente generati, particolarmente importante e centrale per gli argomenti di questo corso, sarà introdotto nella prossima sezione.

Infine, un'altra definizione che è abbastanza frequente incontrare nello studio dei gruppi infiniti, è quella per cui, data una classe di gruppi $\mathfrak{X}$, un gruppo G si dice *virtualmente-*$\mathfrak{X}$ se esiste un $H \leq G$ con $H \in \mathfrak{X}$ e $[G : H]$ finito. Ovviamente, si tratta di una nozione che acquista senso non banale solo per gruppi infiniti; ad esempio, il gruppo diedrale infinito D_∞ è virtualmente abeliano (ed, infatti, virtualmente ciclico), così come ogni prodotto semidiretto $A \rtimes F$ con A abeliano e F finito.

Esercizio 1.10. Le classi di gruppi nella prima definizione di sopra sono chiuse per prodotti diretti, ma non tutte lo sono per prodotti cartesiani. Perché? Si trovi una condizione necessaria e sufficiente sulla famiglia dei fattori affinché il loro prodotto cartesiano sia un gruppo periodico.

Esercizio 1.11. Sia p un numero primo e, per ogni $n \geq 1$, sia $H_n = C_{p^n}$ un gruppo ciclico di ordine p^n. Siano

$$G = Car_{n\geq 1} H_n,\ D = Dir_{n\geq 1} H_n,\ \text{e } T = \{x \in G \mid |x| < \infty\}.$$

Si provi che $D \leq T \leq G$, che T è un p-gruppo, e che T/D è radicabile (un gruppo W è radicabile se per ogni $x \in W$ ed ogni intero positivo n esiste una 'radice n-esima' in W, cioè esiste $y \in W$ tale che $y^n = x$).

Esercizio 1.12. Si provi che il prodotto cartesiano di gruppi finiti è residualmente finito; si deduca quindi che un gruppo G è residualmente finito se e solo se è isomorfo ad un sottogruppo di un prodotto cartesiano di gruppi finiti.

Esercizio 1.13. Si provi che il gruppo diedrale infinito D_∞ è residualmente finito.

ESERCIZIO 1.14. Sia $N = \mathbb{Z} \times \mathbb{Z}$ il prodotto diretto di due gruppi ciclici infiniti, e sia $\langle g \rangle$ un gruppo ciclico infinito. Sia $\phi : \langle g \rangle \to Aut(N)$ l'omomorfismo che associa a g l'automorfismo $\tau \in Aut(T)$ con $\tau(x, y) = (y, x)$ per ogni $x, y \in \mathbb{Z}$. Si provi che il prodotto semidiretto $N \rtimes_\phi \langle g \rangle$ è un gruppo virtualmente abeliano e residualmente finito.

ESERCIZIO 1.15. Sia $\mathfrak{X}$ una classe di gruppi chiusa per sottogruppi, e sia G un gruppo virtualmente $\mathfrak{X}$. Si provi che G ha un sottogruppo normale N di indice finito con $N \in \mathfrak{X}$.

Gruppi di matrici (gruppi lineari). Per A anello commutativo e $n \geq 1$ sia $M_n(A)$ l'anello delle matrici quadrate di ordine n a coefficienti in A. Il gruppo degli elementi invertibili di $M_n(A)$ si denota con $GL(n, A)$ e si chiama il gruppo *Generale Lineare* di ordine n su A. Se A^* è l'insieme degli elementi invertibili di A, allora

$$GL(n, A) = \{A \in M_n(A) \mid \det A \in A^*\}.$$

Il determinante definisce un omomorfismo suriettivo $GL(n, A) \to A^*$ (A^* è un gruppo moltiplicativo). Il nucleo di questo omomorfismo

$$SL(n, A) = \{A \in M_n(A) \mid \det A = 1\}$$

è un sottogruppo normale di $GL(n, A)$ chiamato gruppo *Speciale Lineare* di ordine n su A. Per il Teorema di omomorfismo:

$$GL(n, A)/SL(n, A) \simeq A^*.$$

Se $\mathbb{K}$ è un campo e V uno spazio vettoriale su $\mathbb{K}$, si denota con $GL(V)$ il gruppo degli automorfismi (applicazioni lineari invertibili) di V. Un gruppo G si dice *lineare* se esiste uno spazio vettoriale di dimensione finita V su un campo $\mathbb{K}$ tale che G è isomorfo ad un sottogruppo[1] di $GL(V)$. Se V ha dimensione n allora ad ogni base di V è associato un isomorfismo $GL(n, \mathbb{K}) \to GL(V)$; quindi i gruppi lineari sono (isomorfi a) gruppi di matrici quadrate di ordine finito su un campo $\mathbb{K}$.

Così, si ha a disposizione anche un apparato geometrico per i gruppi di matrici dal quale spesso si può trarre profitto. Ad esempio per determinare quale sia il centro del gruppo $GL(n, \mathbb{K})$ (limitiamoci al caso di coefficienti su un campo $\mathbb{K}$) con $n \geq 1$, si possono fare considerazioni di calcolo matriciale, ma si può anche osservare che un elemento A in $G = GL(n, \mathbb{K})$ appartiene al centro di G se e soltanto se $P^{-1}AP = A$ per ogni $P \in G$; ciò significa che l'isomorfisimo $\mathbb{K}^n \to \mathbb{K}^n$ associato ad A non dipende dalla scelta della base su $\mathbb{K}^n$. Si deduce in modo abbastanza ovvio che V deve risultare un autospazio per A relativo ad un unico autovalore, e quindi che A deve essere una matrice scalare (cioè del tipo $A = \lambda I_n$, dove $0 \neq \lambda \in \mathbb{K}$ e I_n la matrice identica). Abbiamo quindi (la dimostrazione relativa al caso del gruppo speciale è lasciata per esercizio) la seguente:

Proposizione 1.7. *Sia $\mathbb{F}$ un campo e $n \geq 1$; allora*

- $Z(GL(n, \mathbb{K})) = \{\lambda I_n \mid 0 \neq \lambda \in \mathbb{K}\}$ *è isomorfo al gruppo moltiplicativo $\mathbb{K}^*$;*
- $Z(SL(n, \mathbb{K})) = \{\lambda I_n \mid \lambda \in \mathbb{K}, \lambda^n = 1\}$ *è isomorfo al gruppo delle radici n-esime dell'unità in $\mathbb{K}^*$.*

I gruppi quoziente di $GL(n, \mathbb{F})$ e $SL(n, \mathbb{F})$ modulo il loro centro si denotano con $PGL(n, \mathbb{F})$ e $PSL(n, \mathbb{F})$, e si chiamano, rispettivamente, il gruppo *generale proiettivo* e il gruppo *speciale proiettivo* di dimensione $n - 1$ sul campo $\mathbb{F}$.

[1] In generale, un omomorfismo $G \to GL(V)$, per G un gruppo e V uno spazio vettoriale di dimensione finita, si chiama una *rappresentazione lineare* di G.

Esercizio 1.16. Sia B l'insieme delle matrici triangolari superiori in $G = SL(n, A)$, dove A è un anello commutativo; cioè l'insieme di tutte le matrici del tipo

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

con $a_{ij} \in A$ e $a_{11}a_{22}\cdots a_{nn} = 1$ ($B = B(n, A)$ è detto un *sottogruppo di Borel* di $SL(n, A)$). Sia $U = UT(n, A)$ l'insieme delle matrici *unitriangolari superiori*, cioè il sottoinsieme di B costituito dalle matrici i cui elementi diagonali $a_{11}, a_{22}, \ldots, a_{nn}$ sono tutti uguali a $1 = 1_A$; e sia H l'insieme delle matrici diagonali, cioè del tipo

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \cdot & \cdot & \cdots & 0 \\ 0 & 0 & \cdots & a_n \end{pmatrix}$$

con $a_1a_2\cdots a_n = 1$. Si provi che B è il prodotto semidiretto $U \rtimes H$.

Esercizio 1.17. Si provi che se $\mathbb{K}$ è un campo di caratteristica diversa da 2 allora $SL(2, \mathbb{K})$ contiene un unico elemento di ordine 2.

Esercizio 1.18. Sia $T(2, \mathbb{Z})$ il gruppo delle matrici triangolari superiori invertibili su $\mathbb{Z}$; si provi che $T(2, \mathbb{Z}) \simeq D_\infty \times C_2$.

Esercizio 1.19. Sia $G = UT(3, \mathbb{Q})$. Si provi che per ogni $x \in G$ e $n \geq 1$ esiste $y \in G$ tale che $y^n = x$.

1.5. Gruppi finitamente generati

Se X è un sottoinsieme di un gruppo G si denota con $\langle X \rangle$ il *sottogruppo generato* da X, ovvero il minimo[2] sottogruppo di G contenente X (l'intersezione di tutti i sottogruppi di G che contengono X). In particolare, $\langle \emptyset \rangle = \{1\}$, mentre se X non è vuoto è facile verificare che, posto $X^{-1} = \{x^{-1} \mid x \in X\}$,

$$\langle X \rangle = \{x_1 \ldots x_n \mid 1 \leq n \in \mathbb{N},\ x_1, \ldots, x_n \in X \cup X^{-1}\}. \tag{1.11}$$

X si dice un *sistema di generatori* del gruppo G se $G = \langle X \rangle$. Poiché in un prodotto del tipo $x_1 \ldots x_n$, termini consecutivi che siano uguali oppure inversi possono essere moltiplicati in modo da ottenere una potenza di quell'elemento, da (1.11) risulta che X è un sistema di generatori per G se ogni elemento $g \in G$ si può scrivere nella forma

$$g = x_1^{\beta_1} \ldots x_n^{\beta_n} \tag{1.12}$$

con $n \geq 1$, $x_i \in X$ e $\beta_i \in \mathbb{Z}$ per ogni $i = 1, \ldots, n$.

Esempio 1.4. Un gruppo è ciclico se può essere generato da un singolo elemento. Per ogni intero q, sia dato un gruppo ciclico non banale $H_q = \langle x_q \rangle$, e consideriamo il prodotto cartesiano $G = Car_{q\in\mathbb{Z}} H_q$. Identifichiamo con x_q stesso l'elemento del prodotto G che associa x_q alla componente q ed 1 alle altre. Allora, il sottogruppo $\langle \{x_q \mid q \in \mathbb{Z}\} \rangle$ coincide con il prodotto diretto $Dir_{q\in\mathbb{Z}} H_q$. □

[2] Si intende, ovviamente, rispetto alla relazione di inclusione.

Esempio 1.5. Sia G un gruppo e siano $x, y \in G$ con $|x| = 2 = |y|$. Allora il sottogruppo generato da $\{x, y\}$ è un gruppo diedrale.

Infatti, siano x e y involuzioni del gruppo G, sia $a = xy$ e $A = \langle a \rangle$. Sia quindi $\langle x, y \rangle$ il sottogruppo generato da $\{x, y\}$. Si osservi innanzi tutto che $A \leq \langle x, y \rangle$ e che $a^{-1} = yx$. Ora $a^x = x(xy)x = yx = a^{-1}$, quindi $A^x = A$. Similmente, $a^y = y(xy)y = yx = a^{-1}$ e $A^y = A$. Da cioò segue che A è un sottogruppo normale di $\langle x, y \rangle$, e si conclude facilmente che $\langle x, y \rangle = A \rtimes \langle x \rangle$, con x che induce per coniugio l'inversione su A. Dunque $\langle x, y \rangle$ è un gruppo diedrale. □

Esempio 1.6. Siano A un anello commutativo e $n \geq 2$. Per ogni $1 \leq i, j \leq n$, denotiamo con e_{ij} la matrice $n \times n$ i cui coefficienti sono tutti 0 tranne quello di posto (i, j) che è $1 = 1_A$. Per ogni $b \in A$ ed indici i, j come sopra, poniamo $t_{ij}(b) = 1 + be_{ij}$; (dove $1 = I_n$ la matrice identica di ordine n); in particolare, se $i \neq j$, $t_{ij}(b)$ è la matrice i cui coefficienti sono: 1 sulla diagonale, b nel posto (i, j), e 0 altrove. È chiaro che, se $i \neq j$, allora $\det t_{ij}(b) = 1$, e quindi $t_{ij}(b) \in SL(n, A)$.
Il prodotto di matrici del tipo e_{ij} è facilmente descritto da $e_{ij} \cdot e_{kt} = \delta_{jk} e_{it}$, dove δ_{jk} è il delta di Kronecker, da cui, per distributività, scendono la regole per la moltiplicazione per matrici del tipo $t_{ij}(b)$. Ad esempio:

$$t_{ij}(b)t_{jt}(b') = 1 + be_{ij} + b'e_{jt} + bb'e_{it}. \tag{1.13}$$

Si prova quindi che $X = \{t_{ij}(b) \mid 1 \leq i, j \leq n, i \neq j, b \in A\}$ è un sistema di generatori di $SL(n, A)$. □

Gruppi finitamente generati. Un gruppo G si dice *finitamente generato* (e scriveremo f.g.) se ammette un sistema finito di generatori. Quando sarà necessario essere più precisi, si dirà che un gruppo è n-generato se ammette un sistema di generatori X con $|X| = n$; in particolare, un gruppo è 1-generato se e soltanto se è ciclico[3].

Un sistema di generatori di un gruppo G è minimale se nessun suo sottoinsieme proprio genera G. Una cosa del genere non è detto esista in qualunque gruppo (vedi esercizio 1.21), ma, ovviamente, gruppi finitamente generati ammettono sistemi di generatori minimali; questi possono però non avere la stessa cardinalità. Ad esempio, $\mathbb{Z} = \langle 1 \rangle$, ma si osservi che se $p_1, \ldots, p_k$ sono primi distinti e, per ogni $i = 1, \ldots, k$, $n_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k$, allora $\{n_1, \ldots, n_k\}$ è un sistema minimale di generatori di $\mathbb{Z}$ (lo si dimostri per esercizio).
Chiaramente, però, se G è finitamente generato allora esiste un minimo, che denoteremo con $d(G)$, per le cardinalità dei suoi sistemi di generatori .

Ricordiamo, senza dimostrazione e nella forma meno dettagliata, la fondamentale caratterizzazione dei gruppi f.g. abeliani.

Teorema 1.8. *Un gruppo abeliano è finitamente generato se e solo se è il prodotto diretto di un numero finito di gruppi ciclici.*

Esempio 1.7. Sia $n \geq 2$; è un fatto elementare che il gruppo simmetrico S_n è generato dall'insieme delle sue trasposizioni $t_n = \{(i\ j) \mid 1 \leq i < j \leq n\}$. Per $n \geq 3$, t_n non è un sistema minimale, infatti, come si vede facilmente, gli insiemi $S = \{(1\,2), (1\,3), \ldots, (1\,n)\}$ e $\{(1\,2), (2\,3), \ldots, (n-1\,n)\}$ sono sistemi di generatori di S_n propriamente contenuti in t_n; questi sono invece minimali (togliendo un elemento, ad esempio, in S, il sottogruppo generato dall'insieme dei rimanenti è S_{n-1}). Ma S non è un sistema col minimo numero di generatori di S_n; infatti, per ogni $n \geq 2$, $\{(1\,2), (1\,2\,3 \ldots n)\}$ è un sistema di generatori per S_n (dimostrarlo per esercizio), quindi $d(S_n) = 2$. □

[3]Se $X = \{x_1, \ldots, x_n\}$ scriveremo $\langle x_1, \ldots, x_n \rangle$ per il sottogruppo generato $\langle \{x_1, \ldots, x_n\} \rangle$.

Esempio 1.8. Rimanendo nell'ambito dei gruppi abeliani, vediamo il caso di un gruppo non complicato da definire ma con interessanti proprietà. Fissato un numero primo positivo p, per ogni $n \geq 0$ sia $U_{p,n}$ il gruppo moltiplicativo delle radici complesse p^n-esime dell'unità; com'è noto $U_{p,n}$ è un gruppo ciclico di ordine p^n; sia quindi

$$C_{p^\infty} = \{u \in \mathbb{C} \mid u^{p^n} = 1 \text{ per qualche } n \geq 1\} = \bigcup_{n \geq 0} U_{p,n}.$$

C_{p^∞}, che è un sottogruppo del gruppo moltiplicativo dei numeri complessi diversi da zero, si chiama il p-gruppo di Prüfer; non è finitamente generato mentre ogni suo sottogruppo proprio è (ciclico) finito (vedi esercizio 1.24). □

Esercizio 1.20. Sia G un gruppo finitamente generato. Si provi che per ogni sistema di generatori X di G esiste un sottoinsieme finito di $Y \subseteq X$ tale che $\langle Y \rangle = G$.

Esercizio 1.21. Si provi che il gruppo (additivo) $\mathbb{Q}$ non è finitamente generato e non ammette alcun sistema di generatori minimale. Si provi che la stessa situazione si verifica per i gruppi di Prüfer C_{p^∞}.

Esercizio 1.22. Si provi che un prodotto cartesiano di gruppi non-banali è finitamente generato se e soltanto se è il prodotto diretto di un insieme finito di gruppi finitamente generati.

Esercizio 1.23. Si provi che per ogni $n \geq 1$, $SL(n, \mathbb{Z})$ è finitamente generato.

Esercizio 1.24. Sia p un numero primo fissato e $G = C_{p^\infty}$.

(1) Sia $H \leq G$; si provi che se $H \not\leq U_{p,n}$ per ogni $n \geq 0$ allora $H = G$, concludendo che ogni sottogruppo proprio di G è uno degli $U_{p,n}$.

(2) Sia H un sottogruppo proprio di G; si provi che $G/H \simeq G$.

(3) Sia $\mathbb{Q}(p) = \{n/p^i \in \mathbb{Q} \mid n \in \mathbb{Z},\ i \geq 0\}$; si provi che $G \simeq \mathbb{Q}/\mathbb{Q}(p)$.

Sottogruppi di gruppi f.g. È chiaro che ogni quoziente (quindi, ogni immagine omomorfa) di un gruppo f.g. G è finitamente generato: se $G = \langle g_1, \ldots, g_r \rangle$ e $N \trianglelefteq G$ allora $G/N = \langle Ng_1, \ldots, Ng_r \rangle$ (dunque $d(G/N) \leq d(G)$). Diversamente, come mostrano i seguente esempi, *sottogruppi di gruppi finitamente generati possono non essere finitamente generati.*

Esempio 1.9. Sia $H := \mathbb{Z}[1/2] = \{n/2^i \mid n \in \mathbb{Z},\ i \geq 0\}$ (H è un sottogruppo del gruppo additivo dei razionali) e sia α l'automorfismo di H definito da $\alpha(q) = 2q$ per ogni $q \in H$; allora il prodotto semidiretto $G = H \rtimes \langle \alpha \rangle$ è 2-generato (infatti $G = \langle 1, \alpha \rangle$) ma il suo sottogruppo H non è finitamente generato (si osservi anche che H è sottogruppo normale di G). □

Esempio 1.10. (Gruppo del lampionaio) Sia B il prodotto diretto di copie di $\mathbb{Z}/2\mathbb{Z}$ indicizzate su $\mathbb{Z}$, ovvero l'insieme delle funzioni $f : \mathbb{Z} \to \{0, 1\}$ a supporto finito (cioè tali che $f(x) = 0$ tranne per un numero finito di $x \in \mathbb{Z}$) con la somma puntuale: $(f + g)(x) = f(x) + g(x) \pmod 2$, per ogni $f, g \in B$ e $z \in Z$. Sia $\alpha : B \to B$ definita da, per ogni $f \in B$ e $x \in \mathbb{Z}$,

$$\alpha(f)(x) = f(x - 1).$$

Si vede facilmente che α è un automorfismo di B di ordine infinito; consideriamo quindi il prodotto semidiretto $G = B \rtimes \langle \alpha \rangle$. Si verifica allora che $G = \langle h, \alpha \rangle$ dove $h \in B$ è definita da $h(z) = 1 \Leftrightarrow z = 0$. Quindi G è 2-generato, mentre il suo sottogruppo normale B, prodotto diretto di infinite copie di $\mathbb{Z}/2\mathbb{Z}$, non è finitamente generato. Maggiori dettagli su questo e gruppi simili nella sezione 2.7. □

In effetti, la non-chiusura per sottogruppi della classe dei gruppi finitamente generati si manifesta in modo radicale. Ogni gruppo finitamente generato (e di conseguenza ogni suo sottogruppo) è numerabile; e, come vedremo più avanti (Teorema 3.29) ogni gruppo numerabile è isomorfo ad un sottogruppo di un gruppo 2-generato. Tuttavia, vi è anche un importante caso che sussiste in generale, che è quello dei sottogruppi di indice finito.

Teorema 1.9. *Un sottogruppo di indice finito di un gruppo finitamente generato è finitamente generato.*

Questo risultato discende immediatamente dal seguente,

Lemma 1.10. *Sia H un sottogruppo di G, $\mathcal{T}$ un sistema di rappresentanti delle classi laterali sinistre di G modulo H tale che $1 \in T$, e $\tau : G \to \mathcal{T}$ la proiezione associata a $\mathcal{T}$ (cioè $\tau(g)H = gH$, per ogni $g \in G$). Sia X un sistema di generatori del gruppo G; allora l'insieme degli elementi*

$$Y = \{\tau(xt)^{-1}(xt) \mid t \in \mathcal{T},\ x \in X \cup X^{-1}\}$$

costituisce un sistema di generatori di H.

Dimostrazione. Che per ogni $t \in \mathcal{T}$ e $x \in X \cup X^{-1}$ si abbia $\tau(xt)^{-1}(xt) \in H$ viene immediatamente dalla definizione di τ. Sia $h = x_1 x_2 \dots x_n$ un elemento di H, con $x_1, \dots, x_n \in X \cup X^{-1}$. Poniamo $t_n = \tau(x_n)$ e, per $1 \leq i \leq n-1$, $t_i = \tau(x_i t_{i+1})$. Quindi $t_n^{-1} x_n \in Y$ e $t_i^{-1} x_i t_{i+1} \in Y$ per ogni $i = 1, \dots, n-1$. Allora

$$h = t_1(t_1^{-1}x_1t_2)(t_2^{-1}x_2t_3)\dots(t_{n-1}^{-1}x_{n-1}t_n)(t_n^{-1}x_n),$$

e poiché $(t_1^{-1}x_1t_2)(t_2^{-1}x_2t_3)\dots(t_{n-1}^{-1}x_{n-1}t_n)(t_n^{-1}x_n)$ appartiene ad H, si ha $t_1 \in H$ e dunque $t_1 = 1$. Quindi

$$h = (t_1^{-1}x_1t_2)(t_2^{-1}x_2t_3)\dots(t_{n-1}^{-1}x_{n-1}t_n)(t_n^{-1}x_n),$$

è un prodotto di elementi di Y, e ciò completa la dimostrazione. ∎

Un'altra considerazione importante che riguarda i sottogruppi di indice finito di un gruppo f.g. è la seguente.

Proposizione 1.11. *Sia G un gruppo finitamente generato. Allora per ogni intero $n \geq 1$ il numero di sottogruppi di G il cui indice è al più n è finito.*

Dimostrazione. Sia G un gruppo finitamente generato e $X = \{x_1, \dots, x_d\}$ un suo sistema finito di generatori. Sia H un sottogruppo di indice al più n di G; per quanto osservato nella sezione 1.2 (esempio 1.2), H contiene un sottogruppo normale H_G il cui indice è al più $n!$. È dunque sufficiente provare che per ogni $n \geq 1$ è finito il numero di sottogruppi normali di G il cui indice è al più n.
Sia F un qualsiasi gruppo; dalla (1.12) segue che ogni omomorfismo $\phi : G \to F$ è determinato dalla d-upla delle immagini degli elementi di X. Se F è finito, per ogni x_i c'è un numero finito di possibili $\phi(x_i)$, e dunque c'è un numero finito di omomorfismi $G \to F$. Ora, per ogni $1 \leq n \in \mathbb{N}$, il numero (a meno di isomorfismo) di gruppi finiti di ordine al più n è finito; si deduce che i possibili omomorfismi da G il cui nucleo ha indice al più n sono in numero finito. Poiché ogni sottogruppo normale di G di indice al più n è il nucleo di qualche omomorfsimo da G in un gruppo di ordine al più n, la dimostrazione è finita. ∎

Sottogruppi massimali. Un sottogruppo H del gruppo G si dice *massimale* se $H \neq G$ e per ogni $H \leq K \leq G$ si ha $K = H$ o $K = G$. Non ogni gruppo ammette sottogruppi massimali; ad esempio il gruppo additivo $\mathbb{Q}$ non ne ha.

Proposizione 1.12. *Sia $G \neq 1$ un gruppo finitamente generato; allora G ha sottogruppi massimali*

Dimostrazione. Sia $G \neq 1$ un gruppo finitamente generato e sia $X = \{x_1, \ldots, x_n\}$ un insieme minimale di generatori di G. Poniamo $H = \langle x_1, \ldots, x_{n-1}\rangle$ ($H = \{1\}$ nel caso $n = 1$). Per la minimalità di X, $x_n \notin H$. Applicando il Lemma di Zorn esiste un elemento M massimale nell'insieme $\mathcal{H} = \{K \leq G \mid H \leq K, x_n \notin K\}$ ordinato per inclusione. M è un sottogruppo proprio perché non contiene x_n, ed è un sottogruppo massimale; infatti se $M \leq K \leq G$ e $M \neq K$ allora $K \notin \mathcal{H}$, dunque $x_n \in M$; pertanto

$$M \supseteq H \cup \{x_n\} \supseteq \{x_1, \ldots, x_{n-1}, x_n\}$$

e quindi $K = G$. ∎

Esercizio 1.25. In $Aut(\mathbb{R}, \leq)$ si considerino gli elementi f, g definiti da $f(x) = 2x$ e $g(x) = x + 1$, per ogni $x \in \mathbb{R}$. Si provi che $\langle f, g\rangle$ è isomorfo al gruppo G dell'esempio 1.9.

Esercizio 1.26. Si provi che ogni sottogruppo di un gruppo abeliano finitamente generato è finitamente generato.

Esercizio 1.27. Sia N un sottogruppo normale del gruppo G; si provi che se N e G/N sono gruppi localmente finiti (vedi sezione 1.4) allora G è localmente finito.

Esercizio 1.28. Sia G un gruppo finitamente generato. Si provi che ogni sottogruppo proprio di G è contenuto in un sottogruppo massimale.

Esercizio 1.29. (Condizione di massimo) Un gruppo G soddisfa la *condizione di massimo* sui sottogruppi (abbreviato: *Max*) se ogni catena $H_0 \leq H_1 \leq H_2 \leq \ldots$ di sottogruppi di G è finita (cioè esiste $n \geq 0$ tale che $H_i = H_n$ per ogni $i \geq n$). Si provi che un gruppo G soddisfa la condizione di massimo sui sottogruppi se e solo se ogni sottogruppo di G è finitamente generato.

Esercizio 1.30. Si provi che per ogni $m \geq 1$, il gruppo $\mathbb{Z}^m$ soddisfa Max. Si provi che se G è un gruppo e $N \trianglelefteq G$, allora G soddisfa Max se e solo se N e G/N soddisfano Max. Utilizzando questi due fatti, si provi che il gruppo $G = U(3, \mathbb{Z})$ delle matrici unitriangolari intere di ordine 3 (vedi Esercizio 1.16) soddisfa Max.

Esercizio 1.31. (Rango di Prüfer) Un gruppo G ha *rango di Prüfer* finito se esiste $n \geq 1$ tale che ogni sottogruppo finitamente generato di G può essere generato da un insieme di ordine al più n; in tal caso, il minimo n per cui ciò si verifica si chiama *rango* (di Prüfer) di G. L'esempio 1.10 mostra che gruppi finitamente generati non sono necessariamente di rango finito: infatti il sottogruppo abeliano B contiene gruppi finitamente generati con un numero minimo di generatori arbitrariamente grande. Viceversa, ci sono tanti gruppi non finitamente generati che hanno rango finito. Il caso più rimarchevole è quello del gruppo additivo $\mathbb{Q}$: si provi infatti che ogni sottogruppo finitamente generato di $\mathbb{Q}$ è ciclico e, quindi, che $\mathbb{Q}$ è un gruppo di rango di Prüfer 1 (lo stesso avviene per i gruppi del tipo C_{p^∞}). Si provi quindi che il gruppo dell'esempio 1.9 ha rango di Prüfer 2.

Esercizio 1.32. Si provi che il gruppo $U(3, \mathbb{Q})$ delle matrici unitriangolari di ordine 3 a coefficienti razionali (vedi ancora Esercizio 1.16) ha rango di Prüfer finito.

1.6. Gruppi risolubili e nilpotenti

Una *serie* in un gruppo G è una catena finita

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G, \tag{1.14}$$

dove $G_i \trianglelefteq G_{i+1}$ per ogni $0 \leq i \leq n-1$. I quozienti G_{i+1}/G_i sono detti i *fattori*, e l'intero n la *lunghezza*, della serie. La serie si dice *normale* se $G_i \trianglelefteq G$ per ogni $0 \leq i \leq n$.

DEFINIZIONE. Un gruppo G è *risolubile* se ammette una serie i cui fattori sono abeliani. La minima lunghezza di una tale serie si chiama *lunghezza derivata* di G.

Sono ad esempio risolubili tutti i gruppi diedrali (con lunghezza derivata 2 se il loro ordine è almeno 6, mentre D_4 è abeliano). Il gruppo simmetrico S_4 è risolubile con lunghezza derivata 3 (per $n \geq 5$, S_n ha un unica serie, $1 \leq A_n \leq S_n$, che non è a fattori abeliani). Un gruppo risolubile di lunghezza derivata al più 2 si dice *metabeliano* (quindi, G è metabeliano se e solo se esiste $N \trianglelefteq G$ con N e G/N abeliani).
Dalla definizione segue immediatamente che se $N \trianglelefteq G$ e N e G/N sono risolubili, allora il gruppo G è risolubile; in particolare un prodotto semidiretto di gruppi risolubili è risolubile. Semplici applicazioni dei Teoremi di omomorfismo provano poi che ogni sottogruppo ed ogni quoziente di un gruppo risolubile è risolubile.

Nei gruppi risolubili esiste una serie abeliana canonica, detta *serie derivata*. Per definirla si parte dall'utile concetto di *commutatore* di due elementi x, y di un gruppo G:

$$[x, y] = x^{-1}y^{-1}xy,$$

che, in un certo senso, 'misura' la deviazione dalla condizione che x e y commutino; infatti $xy = yx[x, y]$. Dati due sottoinsiemi X e Y di G con la scrittura $[X, Y]$ si intende il sottogruppo di Ggenerato dall'insieme di tutti i commutatori $[x, y]$ con $x \in X$ e $y \in Y$. Il *sottogruppo derivato* G' di G é il sottogruppo $[G, G]$.
Dal fatto che per ogni automorfismo ϕ di G e $x, y \in G$ si ha $\phi([x, y]) = [\phi(x), \phi(y)]$, segue che G' è un sottogruppo caratteristico di G (vedi esercizio 1.3). La proprietà principale del sottogruppo derivato è di carattere elementare (essenzialmente è il fatto, ovvio, che G è un gruppo abeliano se e solo se $G' = 1$), e certamente ben nota.

Lemma 1.13. *Sia N un sottogruppo normale del gruppo G; allora G/N è abeliano se e solo se $N \geq G'$.*

La *serie derivata* $(G^{(n)})_{n\in\mathbb{N}}$ del gruppo G è definita ponendo $G^{(0)} = G$, $G^{(1)} = G'$ e, per ogni $n \in \mathbb{N}$,

$$G^{(n+1)} = (G^{(n)})'.$$

Se, per qualche $n \in \mathbb{N}$, $G^{(n)} = 1$, allora, per il Lemma 1.13, $1 = G^{(n)} \leq G^{(n-1)} \leq \ldots \leq G^{(1)} \leq G$ è una serie a fattori abeliani di G; viceversa, e sempre per il Lemma 1.13 (ed un ovvia induzione) se $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ è una serie a fattori abeliani di G allora $G_i \geq G^{(n-i)}$ per ogni $i = 0, \ldots, n$. Segue quindi la seguente osservazione.

Proposizione 1.14. *Un gruppo G è risolubile se e solo se esiste un intero $n \geq 0$ tale che $G^{(n)} = 1$; in tal caso, il minimo n tale che $G^{(n)} = 1$ è la lunghezza derivata di G.*

DEFINIZIONE. Una serie (1.14) si dice *centrale* se è normale e $G_{i+1}/G_i \leq Z(G/G_i)$ per ogni $0 \leq i \leq n-1$. Un gruppo G è *nilpotente* se ammette una serie centrale; la minima lunghezza di una tale serie si chiama *classe di nilpotenza* di G.

Si osserva che la condizione $G_{i+1}/G_i \leq Z(G/G_i)$ sui termini di una serie equivale a richiedere $[G_{i+1}, G] \leq G_i$. Questo suggerisce che, come per i gruppi risolubili, anche per gruppi nilpotenti esista una serie centrale per così dire canonica. In effetti, ce ne sono almeno due, che definiamo subito. Per ogni gruppo G si definisce la *serie centrale discendente* $(\gamma_n(G))_{n\geq 1}$ ponendo $\gamma_1(G) = G$ e, per $n \geq 2$,

$$\gamma_n(G) = [\gamma_{n-1}(G), G].$$

La *serie centrale ascendente* $(Z_n(G))_{n\geq 0}$ del gruppo G è invece definita da $Z_0(G) = \{1\}$, $Z_1(G) = Z(G)$ (il centro di G) e, per $n \geq 1$,

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\Big(\frac{G}{Z_{n-1}(G)}\Big).$$

Sussistono quindi la seguentì proprietà, la cui facile dimostrazione si trovano in ogni introduzione alla Teoria dei Gruppi.

Lemma 1.15. *Sia G un gruppo nilpotente e sia $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ una serie centrale di G. Allora $\gamma_{n-i+1}(G) \leq G_i \leq Z_i(G)$ per ogni $i = 0, \ldots, n$.*

E quindi,

Proposizione 1.16. *Un gruppo G è nilpotente se e solo se esiste $n \geq 0$ tale che $Z_n(G) = G$, oppure $\gamma_{n+1}(G) = \{1\}$. In tal caso il minimo indice n per cui $Z_n(G) = G$ coincide con il minimo n per cui $\gamma_{n+1}(G) = 1$ e con la classe di nilpotenza di G.*

Mentre risulta immediato (applicando i teoremi di omomorfismo) che ogni sottogruppo ed ogni immagine omomorfadi un gruppo nilpotente di classe c è nilpotente di classe al più c, semplicissimi esempi, come i gruppi diedrali D_{2n} con n dispari (vedi l'esercizio 1.36), mostrano che estensioni di gruppi nilpotenti non sono in genere nilpotenti.

Esempio 1.11. Il più citato fra i gruppi nilpotenti non abeliani è il *gruppo di Heisenberg*

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

Di fatto, sono nilpotenti tutti i gruppi di matrici unitriangolari; per $n \geq 1$, sia (come nella sezione 1.4) $UT(n, A)$ il gruppo moltiplicativo delle matrici unitriangolari superiori $n \times n$ a coefficienti in un anello commutativo A, si prova allora che

$$UT(n, A) \text{ è nilpotente di classe } n - 1.$$

Illustriamo rapidamente questo fatto. Posto $E = M_n(A)$ l'anello di tutte le matrici $n \times n$ a coefficienti in A, sia S il sottoanello di tutte le matrici i cui elementi su e sotto la diagonale principale sono 0: queste sono somme di matrici del tipo ae_{ij}, con $a \in A$, $1 \leq i < j \leq n$, dove le e_{ij} matrici elementari come definite nell'esempio 1.6. Il gruppo $U = UT(n, A) = \{1+s \mid s \in S\}$ è quindi generato dall'insieme di tutte le trasvezioni $t_{ij}(a)$, con $a \in R$ e $1 \leq i < j \leq n$. Siano $i < j$, $r < s$ e (cosa che possiamo sempre assumere) $i \leq r$; dalla formula (1.13) segue la seguente regola di commutazione

$$[t_{ij}(a), t_{rs}(b)] = \begin{cases} t_{is}(ab) & \text{se } j = r \\ 1 & \text{se } j < r. \end{cases} \tag{1.15}$$

Applicando la quale si trova immediatamente $\gamma_2(U) = \langle t_{ij}(a) \mid a \in A,\ j \geq i + 2\rangle$, che è l'insieme delle matrici unitriangolari superiori in cui la prima diagonale sopra quella principale è composta da 0. Per $c \geq 2$, con una semplice induzione, si ottiene

$$\gamma_c(U) = \langle t_{ij}(a) \mid a \in A,\ j \geq i + c\rangle.$$

Quindi, in particolare, $\gamma_{n-1}(U) = \langle t_{1n}(a) \mid a \in A\rangle$ (un sottogruppo isomorfo al gruppo additivo $(A, +)$), e $\gamma_n(U) = 1$. Pertanto U è nilpotente di classe $n - 1$. □

Esercizio 1.33. Sia $\mathbb{F}$ un campo. Si determinino i fattori della serie derivata del gruppo delle matrici unitriangolari superiori invertibili $T(3, \mathbb{F})$.

ESERCIZIO 1.34. Si provi che un prodotto diretto (cartesiano) di una famiglia di gruppi $(H_\lambda)_{\lambda\in\Lambda}$ è risolubile (nilpotente) se e soltanto se esiste $c \in \mathbb{N}$ tale che ogni gruppo H_λ è risolubile (nilpotente) di lunghezza derivata (classe di nilpotenza) al più c.

ESERCIZIO 1.35. Si data una azione fedele e transitiva del gruppo G sull'insieme$X$.

(1) Fissato $x \in X$, sia $H = G_x$ lo stabilizzatore di x in G e sia $1 \neq A$ un sottogruppo normale abeliano di G; si provi che se $AH = G$ allora $A \cap H = 1$ (quindi $G = A \rtimes H$ ed esiste una biezione $A \to X$ [sugg.: ricordarsi del Lemma 1.4].

(2) Si provi che se $|X| = p$ è un numero primo e G è risolubile, allora G è metabeliano.

ESERCIZIO 1.36. Si provi che il gruppo diedrale D_{2n} è nilpotente se e solo se n è una potenza di 2. Si provi quindi che il gruppo diedrale infinito D_∞ è residualmente nilpotente, ma $Z(D_\infty) = 1$.

ESERCIZIO 1.37. Sia A un gruppo abeliano e x l'automorfismo di inversione su A (cioè $a \mapsto a^{-1}$ per ogni $a \in A$). Si provi che il prodotto semidiretto $A \rtimes \langle x\rangle$ è nilpotente se e soltanto se A è un 2-gruppo di esponente finito.

ESERCIZIO 1.38. Sia $H = C_{2^\infty}$ il 2-gruppo di Prüfer e x l'automorfismo di inversione su A. Si descrivano le serie centrali ascendenti e discendenti di $G = H \rtimes \langle x\rangle$.

ESERCIZIO 1.39. Sia G un gruppo tale che $Z_1(G) < Z_2(G)$. Provare che $G' < G$. [sugg.: preso $g \in Z_2(G) \setminus Z_1(G)$ considerare l'applicazione da $G \to Z_1(G)$ definita da $x \mapsto [x, g]$]

ESERCIZIO 1.40. Si provi il *Teorema di Fitting*: Siano M, N sottogruppi normali e nilpotenti del gruppo G; allora MN è un sottogruppo nilpotente di G. [se c è la classe di nilpotenza di M, provare che $Z_1(N) \leq Z_c(MN)$; quindi fare induzione sulla classe di N].

2

Grafi di Cayley

In queste note faremo uso dell'idea di grafo nella sua forma più semplice; quella che - nelle visioni più generali - si descrive come *grafo semplice, non-diretto, privo di cappi* (loops). Prima di definire i grafi di Cayley diamo una rapida rassegna dei concetti e definizioni di base della teoria dei grafi.

2.1. Grafi

Se V un insieme e $1 \leq n \in \mathbb{N}$, si denota con $V^{[n]}$ l'insieme di tutti i sottoinsiemi di V di cardinalità n.

Definizione. Un *grafo* è una coppia $\Gamma = (V(\Gamma), E(\Gamma))$, dove

- $V(\Gamma)$ è un insieme non vuoto, i cui elementi sono detti *vertici* (o nodi) del grafo;
- $E(\Gamma)$ è un sottoinsieme (anche vuoto) di $V(\Gamma)^{[2]}$, i cui elementi sono detti *archi* del grafo.

(quando ciò non darà luogo ad ambiguità, capiterà che abbrevieremo, scrivendo V per $V(\Gamma)$ ed E per $E(\Gamma)$).

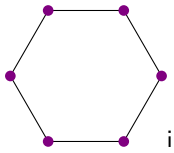
Se $e = \{x, y\} \in E(\Gamma)$ i vertici x e y sono chiamati *estremi* dell'arco e; si dice anche che il vertice x e l'arco e sono *incidenti*. Vertici x e y sono detti *adiacenti* se $\{x, y\} \in E(\Gamma)$; in tal caso scriveremo $x \sim y$ (o, se è necessario specificare a quale grafo ci riferiamo, $x \sim_\Gamma y$).

Come detto, la nozione di grafo (semplice) appena definita sarà quella che utilizzeremo di norma. Qualche volta, tuttavia, sarà conveniente utilizzare la definizione (e non molto altro) di *grafo diretto*; che è una coppia (V, A) dove V è insieme non vuoto di vertici e A (archi) è un sottoinsieme di coppie ordinate $(x, y) \in V^2$ con $x \neq y$. Quindi, la differenza con un grafo semplice è che ogni arco $e = (x, y)$ ha una 'direzione', ovvero un vertice iniziale $i(e) = x$ ed un vertice finale $t(e) = y$.

Esempi di base. 1) Sia n un intero positivo; il *cammino* P_n è il grafo il cui insieme dei vertici è $\{0, 1, \ldots, n\}$ e gli archi sono tutti e soli gli insiemi $\{j, j+1\}$ con $0 \leq j \leq n-1$ (si osservi che l'indice n denota il numero di archi - cioè la *lunghezza* - di P_n; P_0 è il grafo costituito da un unico vertice isolato).

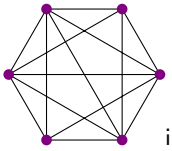
il grafo P_5

2) Sia $n \geq 3$; il *ciclo* C_n è il grafo il cui insieme dei vertici è $\{1, 2, \ldots, n\}$ e gli archi sono $\{1,2\}, \{2,3\}, \ldots, \{n-1, n\}, \{n, 1\}$.



il grafo C_6

3) Se X è un insieme non vuoto, il *grafo completo* K_X è il grafo il cui insieme dei vertici è X e quello degli archi tutto $X^{[2]}$ (cioè i vertici sono a due a due adiacenti). Chiaramente, tali grafi dipendono solo dalla cardinalità di X; se X è finito di cardinalità n, il grafo completo su X si denota con K_n.



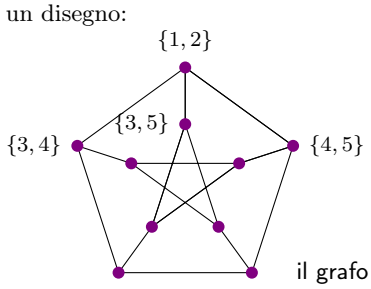
il grafo K_6

Un grafo si dice finito se tale è l'insieme dei suoi vertici[1]. Sarà importante per noi considerare anche grafi infiniti (cioè con un numero infinito di vertici) *localmente finiti*: intendendo con ciò grafi in cui ciascun vertice è incidente ad un numero finito di archi. Se v è un vertice del grafo localmente finito Γ, il *grado* $\deg_\Gamma(v)$ di v è appunto il numero di archi incidenti a v; in altri termini, $\deg_\Gamma(v)$ è il il numero di vertici di Γ che sono adiacenti a v. Poiché ogni arco contiene due vertici distinti, nel caso in cui Γ sia un grafo in cui il numero di archi è finito, si ricava la seguente utile formula:

$$2|E(\Gamma)| = \sum_{v \in V(\Gamma)} \deg_\Gamma(v). \tag{2.1}$$

Un grafo Γ si dice *regolare* se esiste $d \in \mathbb{N}$ tale che $\deg_\Gamma(v) = d$ per ogni vertice v di Γ (in modo più preciso, si dice in tal caso che Γ è d-regolare). Se Γ è un grafo d-regolare, da (2.1) segue $2|E(\Gamma)| = d|V(\Gamma)|$.

Esempio 2.1. Tra i grafi con un numero ridotto di vertici, il *grafo di Petersen*[2] P, che è un grafo 3-regolare, è uno dei più interessanti. Per le sue caratteristiche non banali, è il primo grafo che in genere si testa quando si ha in mente qualche proprietà dei grafi regolari; tuttavia, per ragioni che saranno presto svelate, questo grafo si trova appena al di fuori di quella parte del regno dei grafi che più ci riguarda. Ma è così elegante e in parte misterioso che vale la pena di darne la definizione. Ecco un disegno:



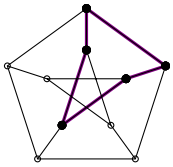
il grafo P

[1] Quindi, è finito anche il numero di archi; in accezioni più ampie del concetto di grafo, in cui sono ammessi diversi archi tra gli stessi vertici, si chiede sia finito anche l'insieme degli archi.

[2] Julius Petersen, matematico danese (1839-1910) che per primo lo descrisse nel 1898.

Si può ottenere prendendo come insieme dei vertici $V = V(P)$ l'insieme dei sottoinsiemi di cardinalità 2 di $\{1,2,3,4,5\}$, e stabilendo che due vertici $\{i,j\},\{r,s\}$ siano gli estremi di un arco in $E = E(P)$ se e solo se $\{i,j\} \cap \{r,s\} = \emptyset$. Si ha quindi $|V| = \binom{5}{2} = 10$ e , per ogni $v \in V$, $\deg_\Gamma(v) = \binom{3}{2} = 3$; P è in particolare un grafo regolare e $|E| = \frac{3|V|}{2} = 15$. □

Sottografi. Un *sottografo* di un grafo $\Gamma = (V,E)$ è semplicemente una coppia (X,E') con $\emptyset \neq X \subseteq V$ e $E' \subseteq E \cap X^{[2]}$.
Il sottografo (X,E') si dice *indotto* da X se $E' = E \cap X^{[2]}$; in maniera discorsiva, un sottografo indotto di un grafo Γ è un sottoinsieme di vertici di Γ assieme a tutti gli archi di Γ i cui estremi appartengono a tale insieme (esempio in figura).



Cammini e metrica su un grafo. Sia $n \in \mathbb{N}$; un *cammino* di lunghezza n nel grafo $\Gamma = (V(\Gamma), E(\Gamma))$ è una sequenza di vertici $v_0, v_1, \ldots, v_n$, tale che per ogni $i = 0, \ldots, n-1$, il vertice v_i è adiacente a v_{i+1}. Equivalentemente, è una sequenza di archi $e_1, e_2, \ldots, e_n$ tale che e_{i+1} è incidente a e_i per ogni $i = 1, \ldots n-1$. Questa seconda versione, oltre ad essere quella che si applica a definizioni più ampie di grafo, è forse più idonea all'intuizione, suggerendo difatti che un cammino è una concatenazione di archi, per così dire "percorribile senza salti" nell'ordine dato.

Il grafo Γ si dice *connesso* se per ogni coppia di vertici $v, w \in V(\Gamma)$ esiste un cammino il cui vertice iniziale è v e quello finale w. In generale, la relazione che associa coppie di vertici tra i quali esiste un cammino finito nel grafo Γ (incluso il cammino nullo) è una relazione di equivalenza su $V(\Gamma)$; i sottografi indotti generati dai vertici di ciascuna classe di equivalenza sono chiaramente connessi, e si chiamano le *componenti connesse* di Γ; ogni vertice ed ogni arco di Γ appartengono ad una e una sola componente connessa.

Un cammino $\mathcal{C} : v_0\ v_1 \ldots v_n$ in Γ si dice *ridotto* se $v_{i+2} \neq v_i$ per ogni $i = 0, \ldots, n-2$; ovvero se ciascuno degli archi $e_i = \{v_{i-1}, v_i\}$ è diverso dal successivo e_{i+1}, per ogni $i = 1, \ldots, n-1$. Il cammino $\mathcal{C}$ si dice *semplice* se tutti i vertici che lo compongono, eccetto eventualmente il primo e l'ultimo, sono distinti.
È quasi evidente che, dati due vertici v, w di Γ, se esiste un cammino da v a w, allora esiste un cammino ridotto da v a w.

Sia ora Γ un grafo connesso, e siano $v, w \in V = V(\Gamma)$; si definisce *distanza* tra v e w la *minima lunghezza* di un cammino che inizia in v e termina in w, e si denota $d_\Gamma(v,w)$. Si verifica immediatamente che la funzione

$$\begin{array}{rccc} d_\Gamma : & V \times V & \to & \mathbb{R} \\ & (v,w) & \mapsto & d_\Gamma(v,w) \end{array}$$

è una *metrica* su V nel senso formale del termine.
Se $\Gamma = (V,E)$ è un grafo connesso, è possibile anche definire la distanza di un vertice v da un sottoinsieme non vuoto S di V, ponendo semplicemente

$$d_\Gamma(v,S) = \min_{w \in S} d_\Gamma(v,w);$$

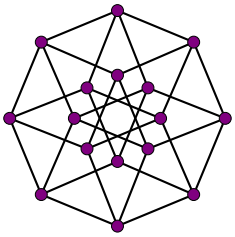
e in modo ovvio si definirà allora la distanza tra due sottoinsiemi non vuoti di V.

Cicli. Un *circuito* di lunghezza n in un grafo Γ è un cammino ridotto $v_0\ v_1\ \dots v_n$ tale che $v_0 = v_n$; si osservi che un circuito non banale (che, cioè, non consiste di un unico vertice) ha lunghezza almeno 3. Un *ciclo* è un circuito in cui tutti i vertici (tranne ovviamente il primo e l'ultimo) sono distinti.

Esempio 2.2. Il grafo Q_n, detto *n-ipercubo*, è il grafo i cui vertici sono le n-uple a coefficienti in $\{0,1\}$, ovvero

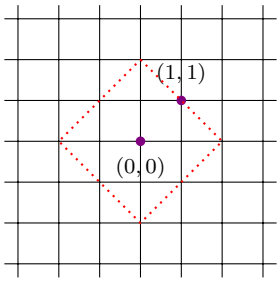
$$V(Q_n) = (\mathbb{Z}/2\mathbb{Z})^n = \{(x_1, \dots, x_n) \mid x_i \in \{0,1\}\},$$

e due n-uple sono adiacenti se e solo se differiscono esattamente per una componente. Dunque il numero di vertici di Q_n è $|(\mathbb{Z}/2\mathbb{Z})^n| = 2^n$; inoltre, Q_n è regolare di valenza n; in particolare, $2|E| = 2^n n$, e dunque $|E| = n2^{n-1}$. Q_3 non è altro che l'usuale cubo, mentre la seguente è una rappresentazione di Q_4:



Nel grafo Q_n la distanza tra due vertici $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{Z}/2\mathbb{Z}$ è il numero di componenti in cui le due n-uple differiscono (in combinatoria e nelle applicazioni nota come *distanza di Hamming*); il *diametro*, ovvero la massima distanza ra due vertici, è n.
Una proprietà importante degli ipercubi è di essere *bipartiti*; intendendo con ciò che l'insieme dei vertici ammette una bipartizione non banale $V(\Gamma) = X \cup Y$ tale che ogni arco del grafo ha un estremo in X e l'altro in Y; nel caso dell'ipercubo Q_n una tale partizione è realizzata dall'insieme X delle n-uple con un numero pari di coordinate uguali ad 1 e dall'insieme Y di quelle con un numero dispari di coordinate uguali ad 1. □

Esempio 2.3. Consideriamo il grafo il cui insieme dei vertici è l'insieme $\mathbb{Z}^2$ dei punti nel piano euclideo con coordinate intere, e due punti sono adiacenti se distano 1 secondo la metrica usuale del piano (cioè giacciono consecutivi su una stessa retta verticale o orizzontale):



È un grafo 4-regolare in cui la distanza tra due punti, $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, è

$$d_\Gamma(P, Q) = |x_2 - x_1| + |y_2 - y_1|.$$

Il tratteggio in rosso descrive la frontiera della palla di raggio 2 centrata nell'origine $B_\Gamma((0,0), 2)$, che contiene 13 punti. Per esercizio si provi che, per $n \geq 1$, si ha $|B_\Gamma((0,0), n)| = 2n^2 + 2n + 1$. Si dimostri poi che anche questo grafo (infinito) è bipartito. □

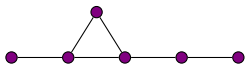
Automorfismi di grafi. Siano Γ e Δ grafi; un *isomorfismo* da Γ in Δ è una biezione

$$\phi : V(\Gamma) \to V(\Delta)$$

tale che, per ogni $x, y \in V(\Gamma)$,

$$\{x, y\} \in E(\Gamma) \quad \Leftrightarrow \quad \{\phi(x), \phi(y)\} \in E(\Delta).$$

Un *automorfismo* del grafo Γ è un isomorfismo di Γ in se stesso. È immediato osservare che l'insieme $Aut(\Gamma)$ degli automorfismi di Γ, con la composizione, costituisce un gruppo.
Per definizione, $Aut(\Gamma)$ è un sottogruppo del gruppo $Sym(V(\Gamma))$ di tutte le permutazioni dell'insieme dei vertici di Γ, che in genere può essere molto più piccolo: ad esempio il gruppo degli automorfismi del grafo



è costituito dalla sola identità sui vertici. Sulla sponda opposta, un grafo Γ si dice *vertex–transitivo* se per ogni $v, w \in V(\Gamma)$ esiste $\phi \in Aut(\Gamma)$ tale che $\phi(u) = w$ (ovvero, $Aut(\Gamma)$ opera transitivamente sull'insieme dei vertici); chiaramente, un grafo con tale proprietà è regolare (gli esempi più semplici di grafi vertex-transitivi sono i cicli ed i grafi completi). Di solito, non è facile decidere quali siano gli automorfismi di un grafo, ed ancor meno se due grafi siano isomorfi.
Osserviamo, per il momento, che un automorfismo di un grafo Γ, oltre che sull'insieme dei vertici, induce una permutazione anche sull'insieme $E(\Gamma)$ degli archi; ma su questa e altre cose torneremo più in dettaglio nella sezione 2.3.

Esercizio 2.1. Siano v, w vertici distinti di un grafo Γ; si provi che se esiste un cammino da v a w, allora esiste anche un cammino semplice (cioè, tale che tutti i vertici, tranne eventualmente v e w, sono distinti) da v a w.

Esercizio 2.2. Sia Γ un grafo finito connesso. Si provi che $|E(\Gamma)| \geq |V(\Gamma)| - 1$.

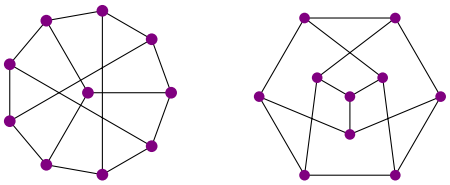
Esercizio 2.3. Si provi che un grafo connesso e 2-regolare è un singolo ciclo finito C_n oppure un cammino infinito:

Esercizio 2.4. Si provi che se un grafo ha un circuito allora ha un ciclo non banale.

Esercizio 2.5. Si provi che, per $n \geq 2$, l'ipercubo Q_n contiene cicli di lunghezza $2t$ per ogni $2 \leq t \leq 2^{n-1}$.

Esercizio 2.6. Per n un intero positivo, si dimostri che i soli grafi con n vertici il cui gruppo degli automorfismi è isomorfo all'intero gruppo simmetrico S_n sono il grafo banale (cioè quello privo di lati) ed il grafo completo K_n.

Esercizio 2.7. Si provi che i due grafi nella figura seguente sono isomorfi al grafo di Petersen (esempio 2.1).



Esercizio 2.8. Si provi che i grafi degli esempi 2.1, 2.2 e 2.3 sono vertex–transitivi. È vero che il gruppo degli automorfismi del grafo dell'esempio 2.3 è transitivo sull'insieme degli archi?

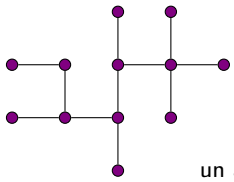
Esercizio 2.9. Sia $\Gamma = (V, E)$ un grafo connesso; il *diametro* di Γ è definito come

$$diam(\Gamma) = \sup\{d_\Gamma(u, v) \mid u, v \in V\}.$$

Si provi che un grafo connesso localmente finito ha diametro infinito se e solo se ha un numero infinito di vertici.

2.2. Alberi

Un *albero* è un grafo connesso privo di circuiti non banali.



La seguente caratterizzazione è semplice ma fondamentale.

Proposizione 2.1. *Sia Γ un grafo. Sono equivalenti*

1. *Γ è un albero;*
2. *per ogni coppia di vertici distinti x, y di Γ esiste uno ed un solo cammino in Γ che inizia in x e termina in y.*

Dimostrazione. 1. $\Rightarrow$ 2. Sia Γ un albero, e siano u, v vertici distinti di Γ. Siccome Γ è connesso, esiste un cammino $\mathcal{C} : u = v_0\, v_1 \dots v_{d-1}\, v_d = v$. Osserviamo che, poiché Γ è privo di circuiti non banali, i vertici di $\mathcal{C}$ sono tutti distinti. Supponiamo, per assurdo, che $\mathcal{C}' : u = w_0\, w_1\, w_2 \dots$ sia un altro cammino da u a v, distinto da $\mathcal{C}$. Allora esiste un minimo indice $i = 1, \dots, d$ tale che $v_i \neq w_i$, ed un minimo $j > i$ tale che $v_j \in \{w_{i+1}, w_{i+2}, \dots\}$. Ma allora G conterrebbe un ciclo non banale che inizia e termina in v_{i-1}, il che è contro l'ipotesi.
2. $\Rightarrow$ 1. Esercizio. ∎

Per grafi finiti sussiste un'ulteriore caratterizzazione degli alberi.

Proposizione 2.2. *Sia $\Gamma = (V, E)$ un grafo finito e connesso.*

(1) *Se Γ è un albero allora contiene almeno un vertice di grado 1.*

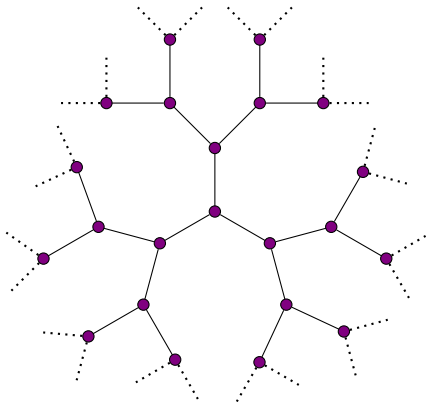
(2) *Γ è un albero se e soltanto se $|E| = |V| - 1$.*

Dimostrazione. (1) Sia $\Gamma = (V, E)$ un albero. Fissato $u \in V$ sia $w \in V$ tale che la distanza $d_\Gamma(u, w)$ è massima possibile; allora w ha grado 1.
(2) Sia $\Gamma = (V, E)$ un albero e procediamo per induzione su $|E|$. Se $|E| = 0$, Γ è costituito da un unico vertice e la formula nell'enunciato sussiste. Se $|E| \geq 1$, sia $u \in V$ un vertice di grado 1 e sia $e \in E$ l'unico arco incidente a u; allora $(V \setminus \{u\}, E \setminus \{e\})$ è, come si vede facilmente, un albero, quindi, per ipotesi induttiva

$$|E| - 1 = |E \setminus \{e\}| = |V \setminus \{u\}| - 1 = |V| - 2$$

da cui la formula per Γ.
Viceversa, sia $\Gamma = (V, E)$ un grafo finito e connesso, tale che $|E| = |V| - 1$. Procedendo per induzione su $|V|$, ed essendo il caso $|V| = 1$ ovvio, possiamo assumere $|V| \geq 2$. Dall'uguaglianza (2.1) si deduce che esiste $u \in V$ con $\deg_\Gamma(u) = 1$; sia $e \in E$ è l'unico arco incidente a u; allora $\Gamma_1 = (V \setminus \{u\}, E \setminus \{e\}$ è un sottografo connesso di Γ e $|E \setminus \{e\}| = |E| - 1 = |V| - 2 = |V \setminus \{u\}| - 1$, quindi, per ipotesi induttiva, Γ_1 è un albero, per cui immediatamente si ha che Γ è un albero. □

Un semplice corollario della Proposizione precedente è che non ci sono alberi finiti regolari[3]. Quelli infiniti rivestiranno per noi particolare interesse.



un albero 3-regolare

Spanning-tree. Sia $\Gamma = (V, E)$ un grafo; uno *spanning-tree* di Γ è un suo sottografo T che è un albero ed il cui insieme dei vertici è tutto l'insieme V. È evidente che un grafo che ammette uno spanning-tree è connesso.

Proposizione 2.3. *Ogni grafo connesso ammette uno spanning-tree.*

Dimostrazione. Sia $\Gamma = (V, E)$ un grafo connesso, e sia $T = (S, E')$ un sottoalbero massimale di Γ, cioè un sottografo la cui esistenza è ottenuta applicando il Lemma di Zorn all'insieme dei sottoalberi di Γ ordinato per inclusione nel modo naturale: $(S_1, E_1) \subseteq (S_2, E_2) \Leftrightarrow S_1 \subseteq S_2$ e $E_1 \subseteq E_2$. Proviamo che $S = V$ e dunque che T è uno spanning-tree di Γ. Sia, per assurdo, $S \neq V$, e sia $v \in V \setminus S$ tale che v ha distanza minima d da S; sia $w \in S$ tale che $d_\Gamma(v, w) = d$; considerando un cammino in Γ da v, w, la scelta di v implica $d = 1$, ovvero $e = \{v, w\} \in E$. Ma allora il sottografo $(S \cup \{v\}, E' \cup \{e\})$ è un sottoalbero di Γ, e questo contraddice la scelta di T come sottoalbero massimale. ■

È abbastanza chiaro che un grafo connesso ammette molti diversi spanning-trees, che non sono in genere tra loro isomorfi (vedi esercizio 2.12).

Esercizio 2.10. Sia $\Gamma = (V, E)$ un grafo connesso. Si provi che Γ è un albero se e solo se per ogni $e \in E$ il grafo $(V, E \setminus \{e\})$ non è connesso.

Esercizio 2.11. Sia T un albero finito, e denotiamo con κ la lunghezza massima di un cammino (semplice) di T. Sia quindi $\mathcal{C} : v_0\ v_1\ v_2\ \ldots\ v_{\kappa-1}\ v_\kappa$ un cammino di lunghezza massima in T. Si provi che v_0 e v_κ sono vertici di grado 1. Supposto che $\kappa = 2t$ sia pari, sia $v = v_t$ il vertice "centrale" del cammino dato; si provi che ogni altro cammino di lunghezza κ di T contiene v.

[3] A parte, per essere del tutto precisi, il grafo costituito da un unico vertice.

Esercizio 2.12. Provare che ogni albero con n vertici è isomorfo ad uno spanning-tree del grafo completo K_n.

Esercizio 2.13. Supponiamo di aver colorato ogni lato di un grafo completo K_n con uno di due colori dati (diciamo: rosso o verde). Si provi che esiste uno spanning-tree di K_n monocromo.

Esercizio 2.14. Sia T un albero infinito e localmente finito. Si provi che T ammette un cammino semplice infinito.

Esercizio 2.15. Sia T un albero localmente finito e sia $A = Aut(T)$. Fissato un vertice $v \in V(T)$, sia $S_A(v) = \{\phi \in A \mid \phi(v) = v\}$. Si provi che $S_A(v)$ è un gruppo residualmente finito.

2.3. Azioni di gruppi su grafi

Definizioni. (1) Un'azione di un gruppo G sul grafo Γ è un'azione di G su $V(\Gamma)$ tale che

$$\{x, y\} \in E(\Gamma) \Leftrightarrow \{g \cdot x, g \cdot y\} \in E(\Gamma),$$

per ogni $x, y \in V(\Gamma)$ e ogni $g \in G$. In altri termini c'è un omomorfismo $G \to Aut(\Gamma)$. È chiaro che un'azione di G su Γ induce un'azione di G su $E(\Gamma)$ che denoteremo allo stesso modo, $(g, e) \mapsto g \cdot e$, per $g \in G$ e $e \in E(\Gamma)$.

(2) Un'azione di un gruppo G sul grafo Γ si dice:

- *libera* se $g \cdot x \neq x$ per ogni $x \in V(\Gamma)$ ed ogni $1 \neq g \in G$;
- *senza inversioni* se per ogni $e = \{x, y\} \in E(\Gamma)$ e $g \in G$,

$$g \cdot e = e \Leftrightarrow \begin{cases} g \cdot x = x \\ g \cdot y = y \end{cases}$$

ovvero non esiste alcun elemento di g che scambia gli estremi di un arco.

Azioni libere e senza inversioni su grafi in generale non sono inusitate: ad esempio il gruppo ciclico di ordine n opera naturalmente in modo libero sul grafo n-ciclo.
Azioni libere e/o senza inversioni su alberi sono invece molto restrittive. Vediamo una prima osservazione in questo senso.

Lemma 2.4. *Sia G un gruppo finito che agisce su un albero $T = (V, E)$; esiste allora un vertice o un arco di T che è fissato da tutti gli elementi di G. In particolare, un gruppo che opera liberamente e senza inversioni su un albero è torsion-free.*

Dimostrazione. Proviamo prima il caso in cui anche T è finito, procedendo per induzione sul numero $|V|$ di vertici di T. Se $|V| = 1$, ovviamente il solo vertice è un punto fisso per G.; se $|V| = 2$, T è composto da un solo arco che dunque è fissato da G. Sia quindi $|V| \geq 3$ e sia v un vertice di grado 1 (Proposizione 2.2); se $g \cdot v = v$ per ogni $g \in G$ abbiamo finito; altrimenti sia $V_0 = \mathcal{O}_G(v)$ l'orbita di v tramite G; ogni elemento $w \in V_0$ ha grado 1 ed è incidente ad un solo arco e_w; l'insieme $E_0 = \{e_w \mid w \in V_0\}$ è un'orbita per l'azione di G su E. La restrizione degli elementi di G a $V \setminus V_0$ (poiché $|V| \geq 3$, $V \setminus V_0$ non è vuoto) definisce quindi un'azione di G sul grafo $T_0 = (V \setminus V_0, E \setminus E_0)$. Ora, T_0 è connesso ed è quindi un albero; per ipotesi induttiva, G fissa un vertice o un arco di T_0, ed abbiamo concluso.

Nel caso generale, in cui non si assume che T sia finito, prendiamo un vertice $v \in V$; se v è fissato da G abbiamo finito; altrimenti consideriamo l'orbita $\mathcal{O}_G(v)$ di v (è un insieme finito di vertici), e per ogni coppia di vertici in $\mathcal{O}_G(v)$ l'insieme dei vertici nel cammino ridotto che li congiunge; poiché tale cammino è unico, si vede subito che l'insieme W di tutti i vertici che costituiscono tali cammini è invariante per l'azione di G. Ora, il sottografo T_0 indotto da W è un albero finito, e dunque, per la discussione precedente, G fissa almeno un vertice o un arco di T_0. ∎

Albero delle orbite. Più avanti (Teorema 3.6) proveremo una fondamentale caratterizzazione dei gruppi che agiscono liberamente e senza inversioni su un albero. Per il momento, torniamo alle azioni su grafi in genere, provando l'esistenza, per azioni di gruppi su grafi connessi, dell'equivalente di un *dominio fondamentale*. Se G agisce su Γ e $\Delta = (V_1, E_1)$ è un sottografo di Γ, per $g \in G$ scriviamo ovviamente $g\Delta = (g(V_1), g(E_1))$ (è chiaro che $g\Delta$ è anche un sottografo di Γ).

Proposizione 2.5. *Sia data un'azione del gruppo G sul grafo connesso $\Gamma = (V, E)$; allora esiste un sottoalbero T di Γ che contiene esattamente un vertice per ogni orbita di G su V. Se inoltre l'azione è libera allora $gT \cap T = \emptyset$ per ogni $1 \neq g \in G$.*

Dimostrazione. La dimostrazione è simile a quella dell'esistenza degli spanning-tree (che ne è anzi un caso particolare). Si considera la relazione di inclusione sull'insieme $\mathcal{T}_G$ di tutti i sottoalberi di Γ i cui vertici appartengono tutti a G-orbite distinte. Questo insieme ordinato soddisfa i requisiti per applicare il Lemma di Zorn. Sia quindi T un elemento massimale di $\mathcal{T}_G$ e proviamo che T è l'oggetto cercato. Supponiamo per assurdo che esistano orbite di G su V tali che nessun vertice di esse appartiene a $V(T)$, cioè supponiamo che l'insieme $K = \{x \in V \mid g \cdot x \notin V(T) \text{ per ogni } g \in G\}$ non sia vuoto. Sia $x \in K$ tale che $d = d_\Gamma(x, V(T))$ è minima e sia $u \in V(T)$ con $d_\Gamma(u, x) = d$. Se $d \geq 2$, un cammino di lunghezza d da u a x include almeno un vertice w diverso dagli estremi. Per la scelta di x si ha $w \notin K$, dunque esiste $g \in G$ tale che $g \cdot w \in V(T)$ e di conseguenza, poiché $g \cdot x \notin V(T)$, l'assurdo

$$d \leq d_\Gamma(g \cdot w, g \cdot x) = d_\Gamma(w, x) \leq d - 1.$$

Quindi $d = 1$ e $\{u, x\} \in E$. Ma allora il sottografo ottenuto da T aggiungendo il vertice x e l'arco $\{u, x\}$ è un albero in cui ogni vertice appartiene ad un'orbita distinta, e che contiene propriamente T, ancora un assurdo.
Proviamo ora l'ultima affermazione e supponiamo dunque che l'azione di G su Γ sia libera. Sia T come sopra e $1 \neq g \in G$. Se $gT \cap T \neq \emptyset$ allora esistono vertici $v, v_1 \in V(T)$ tali che $g \cdot v = v_1$. Poiché vertici distinti di T appartengono a G-orbite distinte, si ha allora $v_1 = v$, quindi $g \cdot v = v$ contraddicendo la libertà dell'azione di G su Γ. ∎

Continuando in questa direzione, sia data un'azione libera del gruppo G sul grafo connesso $\Gamma = (V, E)$, e sia T un albero delle orbite come nella Proposizione 2.5; sia V^* l'insieme dei vertici di T, allora, per la seconda parte della proposizione, V è l'unione disgiunta

$$V = \bigcup_{g \in G} g \cdot V^*.$$

Possiamo ora definire un grafo Γ_T che ha come insieme dei vertici l'insieme

$$V(\Gamma_T) = \{gT \mid g \in G\} \tag{2.2}$$

dei G-traslati di T, e stabilendo che, per ogni $g, h \in G$ con $g \neq h$, $\{gT, hT\}$ è un arco di Γ_T se esistono $x, y \in V^*$ tali che $\{g \cdot x, h \cdot y\}$ è un arco in Γ. Si verifica subito che Γ_T è connesso.
Per definizione (azione a sinistra) G agisce transitivamente (e liberamente) sull'insieme dei vertici di Γ_T, ed è immediato vedere che tale azione conserva la relazione di adiacenza appena definita. Si ha insomma la prima parte della seguente Proposizione.

Proposizione 2.6. *Data un'azione libera del gruppo G sul grafo connesso $\Gamma = (V, E)$, sia T un albero delle orbite per tale azione. Sia quindi Γ_T il grafo definito sopra.*

(1) *L'azione di G indotta su Γ_T è libera e transitiva sui vertici.*

(2) *Se Γ è un albero, Γ_T è un albero; in tal caso l'azione di G su Γ_T è senza inversioni se tale è l'azione di G su Γ.*

Dimostrazione. Dopo quanto già detto, la dimostrazione di (1) è già fatta.
(2) Sia $\Gamma = (V, E)$ un albero. Osserviamo che se gT, hT sono vertici adiacenti in Γ_T allora esiste un solo punto $gx = g \cdot x$ di gT ed un solo $hy = h \cdot y$ in hT (quindi $x, y \in V(T)$) tali che $\{gx, hy\}$ è un arco in Γ; infatti, se cosi non fosse, tenendo conto che gT e hT sono sottoalberi disgiunti di Γ si produrrebbe facilmente un ciclo non banale nell'albero di partenza Γ. A questo punto, presi due elementi distinti g, h in G, e $x \in T$, esiste un unico cammino ridotto da gx a hx in Γ, considerando, di questo cammino, soltanto gli archi che connettono vertici appartenenti a traslati diversi di T, si ottiene un cammino da gT a hT in Γ_T, che, per quanto osservato sopra, risulta il solo cammino ridotto tra tali due vertici del grafo Γ_T. Pertanto, Γ_T è un albero.
Infine, sia $\{gT, hT\}$ un arco dell'albero Γ_T; per quanto osservato prima, esiste un'unico arco $\{gu, hv\} \in E$ con u, v vertici di T . Supponiamo esista $x \in G$ tale che $xgT = x \cdot (gT) = hT$ e $xhT = x \cdot (hT) = gT$; allora $xg = h$, $xh = g$ e $x^2 = 1$; pertanto, $x \cdot \{gu, hv\} = \{xgu, xhv\} = \{hu, gv\} = \{gu, hv\}$, e dunque x inverte l'arco $\{gu, hv\}$ dell'albero Γ. ∎

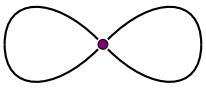
Grafo quoziente. Una costruzione in qualche modo duale a quella della Proposizione 2.6 è il *grafo quoziente* (o grafo delle orbite) Γ/G. Data un'azione senza inversioni del gruppo G sul grafo $\Gamma = (V, E)$ il grafo quoziente è il grafo il cui insieme dei vertici è quello delle orbite di G su V, $\{\mathcal{O}(x) \mid x \in V\}$, e gli archi sono le G-orbite degli archi di Γ. In questo caso non si ottiene generalmente un grafo semplice, dato che ci possono essere archi di Γ non appartenenti alla stessa G-orbita i cui vertici estremi sono invece in orbite uguali; nel grafo quoziente Γ/G ci possono dunque essere archi multipli e cappi (archi i cui estremi sono coincidenti). Non approfondiamo questo punto per ora, limitandoci ad illustrarlo con un esempio[4].

Esempio. Il gruppo $G = \mathbb{Z} \times \mathbb{Z}$ agisce sul grafo Γ descritto nell'esempio 2.3 in modo naturale; per ogni $(a, b) \in G$ ed ogni $(x, y) \in V(\Gamma) = \mathbb{Z}^2$,

$$(a, b) \cdot (x, y) = (x + a, y + b)$$

(si osservi che tale azione è libera e senza inversioni). Ora, G è transitivo sui vertici di Γ ed ha esattamente due orbite sugli archi (archi 'orizzontali' ed archi 'verticali'), per cui il grafo quoziente Γ/G ha il seguente aspetto:

[4]Una nozione più ampia di grafo risulta più funzionale per affrontare questo concetto e le sue importanti derivazioni (che al momento sono al di fuori degli obiettivi di questo corso); per questo, si può consultare il bel libro di Bogopolski [2].



ESERCIZIO 2.16. Sia $\Gamma = (V, E)$; la *suddivisione baricentrica* di Γ è il grafo Γ^o definito mediante $V(\Gamma^o) = V \cup E$ e $E(\Gamma^o) = \{\{x, e\} \in V \times E \mid x \in e\}$. Lo si può raffigurare immaginando di installare un nuovo vertice a mezzo di ogni arco di Γ, e prendere quindi come vertici i vecchi vertici di Γ e questi nuovi aggiunti, e come archi ciascuno dei mezzi archi in cui si ritrova diviso ogni vecchio arco di Γ. Ora, un'azione di un gruppo G su Γ si estende in modo naturale (lo si definisca formalmente) ad un'azione di G su Γ^o; si provi che tale azione è senza inversioni.

ESERCIZIO 2.17. Sia G un gruppo di automorfismi di un albero $T = (V, E)$. Si provi che $Fix_G = \{x \in V \mid g(x) = x \ \forall g \in G\}$ è vuoto oppure il sottografo indotto da Fix_G è un albero.

ESERCIZIO 2.18. Sia G un gruppo di automorfismi dell'albero T. Applicando i due esercizi precedenti, si provi che se esiste un sottogruppo di indice finito H in G che fissa un vertice o un arco di T, allora G fissa un vertice o un arco di T.

ESERCIZIO 2.19. Sia $n \geq 2$ e $V = \{0, 1\}^n$ l'insieme dei vertici dell'ipercubo Q_n (esempio 2.2). Per ogni $1 \leq i \leq n$ sia g_i la permutazione di V che scambia in ogni n-upla, la i-esima componente. Si provi che g_i è un automorfismo del grafo Q_n e che, fissato $1 \leq k \leq n$ il gruppo $\langle g_1 \rangle \times \cdots \times \langle g_k \rangle$ agisce liberamente su Q_n. Si provi che il grafo delle orbite è isomorfo a Q_{n-k}. Si descriva quindi un albero delle orbite T per tale azione e si provi che il grafo $(Q_n)_T$ è isomorfo a Q_k.

ESERCIZIO 2.20. Si consideri l'azione del gruppo $G = \mathbb{Z} \times \mathbb{Z}$ sulla griglia quadrata Γ (esempio 2.3) definita da

$$(a, b) \cdot (x, y) = (x + 2a, y + b),$$

per ogni $(a, b) \in G$ e $(x, y) \in V(\Gamma) = \mathbb{Z}^2$, e si disegni il grafo quoziente Γ/G.

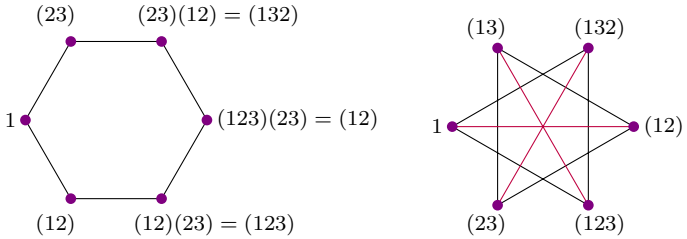
2.4. Grafi di Cayley

Quella dei grafi di Cayley è la maniera più semplice, naturale e fondamentale per legare un oggetto geometrico ad un gruppo.

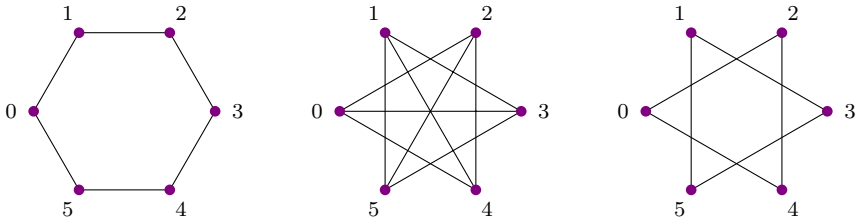
DEFINIZIONE. Sia G un gruppo, e sia S un sottoinsieme di G tale che $1 \notin S$. Il *Grafo di Cayley* $\Gamma[G, S]$ è il grafo il cui insieme dei vertici è G, e gli archi sono tutti i sottoinsiemi $\{g, gs\}$, al variare di $g \in G$ ed $s \in S \cup S^{-1}$ (si osservi che la condizione $1 \notin S$ serve ad assicurare che per ogni $g \in G$ e $s \in S \cup S^{-1}$ l'insieme $\{g, gs\}$ ha effettivamente due elementi)[5].

Si comprende subito che non c'è una stretta corrispondenza tra il gruppo ed un suo grafo di Cayley. Consideriamo, ad esempio, $G = S_3$ il gruppo simmetrico su 3 punti, $S = \{(12), (23)\}$ e $R = \{(12), (123)\}$; allora $S \cup S^{-1} = S$, ed il grafo di Cayley $\Gamma[G, S]$ è un 6-ciclo (a sinistra nella figura), mentre $R \cup R^{-1} = \{(12), (123), (132)\}$ e il grafo $\Gamma[G, R]$ ha l'aspetto (fra i tanti) del grafo a destra in figura (dove sono tracciati in rosso gli archi prodotti dalla moltiplicazione a destra per (12)).

[5]Nel seguito, in molti esempi, sceglieremo normalmente $S = S^{-1}$.

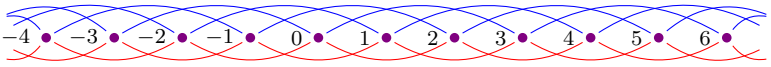


Gli stessi grafi si ottengono come grafi di Cayley del gruppo ciclico di ordine 6; la figura seguente mostra i grafi di Cayley del gruppo additivo (ciclico) $\mathbb{Z}/6\mathbb{Z}$ rispetto al sottoinsiemi: $S = \{1\}$ (il generatore naturale) a sinistra, $S = \{2, 3\}$ al centro, e $S = \{2\}$ a destra (si osservi che nel terzo caso S non è un sistema di generatori del gruppo, e si mostri che anche questo grafo si può ottenere come grafo di Cayley per il gruppo S_3).



Proseguendo su questo esempio, si osserva che, per ogni $n \geq 1$, il $2n$-ciclo si ottiene in maniera ovvia come grafo di Cayley di un gruppo ciclico $\langle g \rangle$ di ordine $2n$ rispetto al sistema di generatori naturale $\{g\}$, ma anche come grafo di Cayley del gruppo diedrale D_{2n}, di ordine $2n$, rispetto ad un sistema di generatori costituito a due involuzioni (esempio 1.5). Questa osservazione arriva fino al gruppo ciclico infinito ed al gruppo diedrale infinito: se $D_\infty = \langle x, y \rangle$, con $|x| = |y| = 2$, allora il grafo $\Gamma[D_\infty, \{x, y\}]$ è il cammino infinito

che è anche il grafo di Cayley $\Gamma[\mathbb{Z}, \{1\}]$. La figura qui sotto mostra invece (una porzione de) il grafo di Cayley $\Gamma[\mathbb{Z}, \{2, 3\}]$.



È certo piuttosto diverso dal cammino infinito di sopra, tuttavia se allontaniamo dall'occhio la pagina i due grafi tendono progressivamente a confondersi in un unica linea. Più avanti, in un luogo piuttosto centrale di queste note, si vedrà come questa immagine, dal gracile valore letterario, abbia un futuro consistentemente matematico.

Sia $\Gamma = \Gamma[G, S]$ un grafo di Cayley nel gruppo G, e supponiamo che S sia finito; risulta allora per costruzione che Γ è un grafo d-regolare, dove $d = |S \cup S^{-1}|$. Un'altra semplice ma importante e proprietà dei grafi di Cayley è descritta nel seguente enunciato.

Lemma 2.7. *Un grafo di Cayley $\Gamma[G, S]$ è connesso se e soltanto se S è un sistema di generatori di G.*

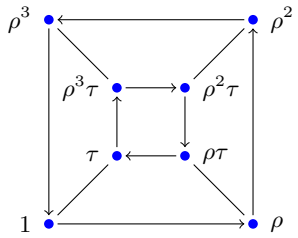
Dimostrazione. Supponiamo che $\Gamma = \Gamma[G;S]$ sia connesso, e sia $y \in G$. Allora esiste un cammino $1 = g_0\ g_1\ g_2 \dots\ g_n = y$ in Γ. Dunque, esistono $s_1, s_2, \dots, s_n \in S \cup S^{-1}$ tali che $g_1 = 1s_1$, $g_2 = g_1 s_2 = 1s_1 s_2$, e così via, sino a $y = g_n = 1s_1 \cdots s_n$. Quindi $y \in \langle S \rangle$. Viceversa, sia $\langle S \rangle = G$, e siano $x, y \in G$ con $x \neq y$. Allora, esistono $s_1, \dots, s_n \in S \cup S^{-1}$ (con $s_{i+1} \neq s_i^{-1}$) tali che $x^{-1}y = s_1 \cdots s_n$. Ponendo $g_0 = x$ e, per ogni $i = 1, \dots, n$, $g_i = x s_1 \cdots s_i$, si descrive un cammino $x = g_0\ g_1\ \dots\ g_n = y$ in Γ. Pertanto, il grafo Γ è connesso. ■

Se S è un sistema di generatori del gruppo G, per ogni $g \in G$ la *lunghezza* di g in S, che denotiamo con $\ell_S(g)$, è il minimo $n \geq 0$ tale che

$$g = x_1 \cdots x_n$$

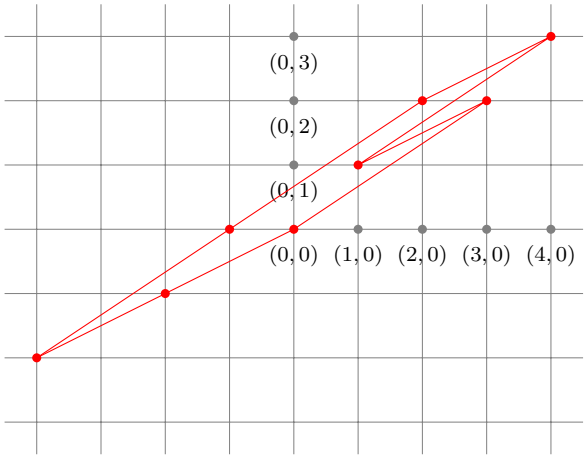
con $x_1, \dots x_n \in S \cup S^{-1}$. Quindi, $\ell_S(g) = 0$ se e solo se $g = 1$ e $\ell_S(g) = 1$ se e solo se $g \in S \cup S^{-1}$. Se $1 \notin S$ e $\Gamma = \Gamma[G,S]$ allora $\ell_S(g)$ coincide con la distanza $d_\Gamma(1,g)$ in Γ; in generale, per ogni $g, h \in G$, si ha $d_\Gamma(g,h) = \ell_S(g^{-1}h)$.

Esempio 2.4. Sia G il gruppo delle simmetrie di un quadrato; allora $|G| = 8$ e $G = \langle \rho, \tau \rangle$, dove ρ è una rotazione di un angolo $\pi/2$ e τ la riflessione con asse una diagonale; si ha $|\rho| = 4$, $|\tau| = 2$ e, come si verifica subito, $\tau\rho\tau = \rho^{-1}$ (di fatto, G è isomorfo al gruppo diedrale di ordine 8). Posto $S = \{\rho, \tau\}$, si trova che il grafo di Cayley $\Gamma[G,S]$ è isomorfo al grafo del cubo



Nel disegno, gli archi orizzontali e verticali corrispondono a moltiplicazione a destra per σ (direzione della freccia) o σ^{-1} (direzione opposta alla freccia), gli archi obliqui a moltiplicazione a destra per $\tau = \tau^{-1}$. Se correttamente disegnato, un grafo di Cayley rappresenta anche relazioni che sussistono nel gruppo: ad esempio $\tau\sigma = \sigma^3\tau = \sigma^2\tau\sigma^{-1}$. □

Esempio 2.5. Nella figura seguente, la griglia quadrata grigia rappresenta la zona intorno a $(0,0)$ del grafo di Cayley $\Gamma[\mathbb{Z} \times \mathbb{Z}, \{(1,0),(0,1)\}]$, mentre in rosso appare un ciclo nel grafo di Cayley $\Gamma[\mathbb{Z} \times \mathbb{Z}, \{(2,1),(3,2)\}]$. □

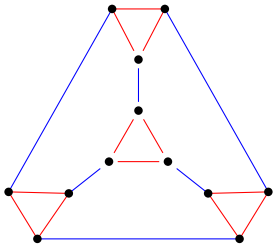


Esempio 2.6. Sia $n \geq 1$ e sia $G = \langle x_1 \rangle \times \ldots \times \langle x_n \rangle$ il prodotto diretto di n gruppi di ordine 2. Posto $S = \{x_1, \ldots, x_n\}$, il grafo di Cayley $\Gamma[G, S]$ è isomorfo al n-ipercubo Q_n (vedi esempio 2.2). □

Esercizio 2.21. Dato un grafo Γ con insieme di vertici $V = V(\Gamma)$, il *grafo complementare* è il grafo $\overline{\Gamma}$ con $V(\overline{\Gamma}) = V$ e insieme di archi il complementare di quello degli archi di Γ, ovvero $E(\overline{\Gamma}) = V^{[2]} \setminus E(\Gamma)$. Si provi che il grafo complementare di un grafo di Cayley è un grafo di Cayley.

Esercizio 2.22. Sia $n \geq 2$, e sia $D_{2n} = \langle y \rangle \rtimes \langle x \rangle$ con $y^n = x^2 = 1$ e $y^x = y^{-1}$, il gruppo diedrale di ordine $2n$. Posto $S = \{y, x\}$, si descriva il grafo di Cayley $\Gamma[D_{2n}, S]$.

Esercizio 2.23. Si provi che il grafo



è il grafo di Cayley $\Gamma[A_4, S]$, dove A_4 è il gruppo alterno su 4 punti e $S = \{(123), (132), (12)(34)\}$.

Esercizio 2.24. Si provi che il grafo di Petersen (esempio 2.1) non è un grafo di Cayley.

2.5. Azione del gruppo sul grafo di Cayley

Siano G un gruppo e $\Gamma = \Gamma[G, S]$ un grafo di Cayley su G. Allora, per ogni $g \in G$, la moltiplicazione a sinistra $\lambda_g : G \to G$, definita da $x \mapsto gx$ (per ogni $x \in G$), è una biezione sull'insieme dei vertici di Γ che conserva la relazione di adiacenza: infatti, per ogni $x \in G$ e ogni $s \in S$, si ha $\lambda_g(\{x, xs\}) = \{gx, (gx)s\})$. Quindi λ_g induce un automorfismo del grafo Γ. Inoltre, la posizione $g \mapsto \lambda_g$ definisce un omomorfismo iniettivo del gruppo G nel gruppo $Aut(\Gamma)$, cioè un azione di G su Γ. Quindi, G è isomorfo ad un sottogruppo del gruppo $Aut(\Gamma)$. Questo può essere visto come una forma evoluta di Teorema di Cayley.
Tale azione è libera (infatti, per cancellazione in G, $gx = x \Rightarrow g = 1$), ed è inoltre transitiva sui vertici di Γ, infatti per ogni coppia (x, y) di vertici di Γ, ponendo $g = yx^{-1}$ si ha $\lambda_g(x) = y$ (in particolare, quindi, i grafi di Cayley sono vertex–transitivi). Queste sono osservazioni fondamentali che fissiamo nella seguente proposizione.

Proposizione 2.8. *Sia $\Gamma = \Gamma[G, S]$ un grafo di Cayley sul gruppo G. Allora, per ogni $g \in G$, la moltiplicazione a sinistra per g induce un automorfismo di Γ. Ne segue che G è isomorfo ad un sottogruppo di $Aut(\Gamma)$ che agisce liberamente ed è transitivo sull'insieme dei vertici di Γ.*

Di fatto, ed è rilevante, sussiste anche una sorta di proprietà inversa.

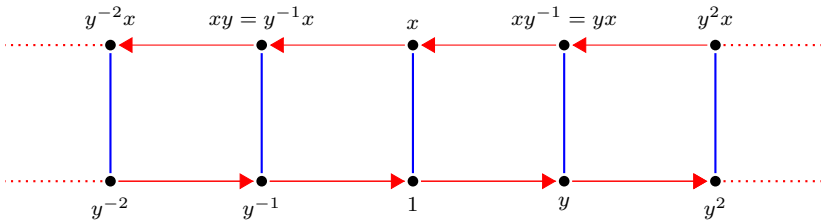
Proposizione 2.9. *Siano $\Gamma = (V, E)$ un grafo e G un gruppo che agisce su Γ. Se l'azione è libera e transitiva su V allora, fissato $x \in V$ e posto*

$$X = \{s \in G \mid \{x, s \cdot x\} \in E\},$$

il grafo di Cayley $\Gamma[G, X]$ è isomorfo a Γ.

Dimostrazione. Siano Γ, G, x e X come nell'enunciato, e poniamo $\Delta = \Gamma[G, X]$. Definiamo l'applicazione $\phi : G \to V$ ponendo, per ogni $g \in G$, $\phi(g) = g \cdot x$. Poichè G agisce transitivamente su V, ϕ è suriettiva; ed è inoltre iniettiva a causa della libertà dell'azione: infatti se per $g, h \in G$ si ha $g \cdot x = h \cdot x$, allora $(h^{-1}g) \cdot x = x$ e dunque $h^{-1}g = 1$, da cui $h = g$. Pertanto ϕ è una biezione da $G = V(\Delta)$ in V. In particolare possiamo identificare $V = \{g \cdot x \mid g \in G\}$ (con g univocamente determinato per ogni distinto vertice in V).
Ora, per l'azione di G su Γ, $\{g \cdot x, h \cdot x\} = \{\phi(g), \phi(h)\} \in E$ (con $g, h \in G$) se e solo se $\{x, (g^{-1}h) \cdot x\} \in E$, se e solo se $g^{-1}h \in X$, ovvero se e solo se $\{g, h\} \in E(\Delta)$. Dunque, ϕ è un isomorfismo da Δ in Γ. ∎

Esempio 2.7. Sia $D = \langle y \rangle \rtimes \langle x \rangle$ con $|y| = \infty, |x| = 2$ e $y^x = y^{-1}$, il gruppo diedrale infinito; allora il grafo di Cayley $\Gamma = \Gamma[D, \{x, y\}]$ ha il seguente aspetto:



dove gli archi in rosso corrispondono al generatore y (con la freccia nel verso $g \mapsto gy$) e in blu gli archi corrispondenti al generatore x. Il gruppo D è identificabile, per moltiplicazione a sinistra, con un sottogruppo di $Aut(\Gamma)$: l'elemento y opera come l'automorfismo che trasla orizzontalmente tutto il diagramma di un passo (verso destra), mentre l'involuzione x opera come una rotazione del diagramma di 180^o intorno al centro dell'arco $\{1, x\}$. Ci sono automorfismi di Γ che non sono indotti da elementi di D, come - ad esempio - la riflessione che scambia i due binari del diagramma (vedi esercizio seguente). □

Esercizio 2.25. Sia Γ il grafo di Cayley sul gruppo D dell'esempio 2.7, e sia $A = Aut(\Gamma)$ (quindi $D \leq A$ mediante la rappresentazione per moltiplicazione a sinistra). Sia v un vertice di Γ e $H = \{\alpha \in A \mid v\alpha = v\}$ lo stabilizzatore in A di v; si provi che $|H| = 2$. Si concluda che $DH = A$, e dunque, in particolare, che $D \trianglelefteq A$.

Nota. Dato un sistema di generatori S del gruppo G e posto $\Gamma = \Gamma[G, S]$, denotiamo con $\widehat{G} \leq Aut(\Gamma)$ l'immagine di G nella sua azione per moltiplicazione a sinistra descritta sopra, e per ogni $g \in G$ indichiamo con $\hat{g}$ la sua immagine in $\widehat{G}$; quindi $\hat{g}(x) = gx$ per ogni $x \in G = V(\Gamma)$. Per quanto visto, $\widehat{G} \simeq G$ e $\widehat{G}$ agisce transitivamente su G.
In generale, come nell'esercizio 2.25, $\widehat{G}$ è un sottogruppo proprio di $Aut(\Gamma)$. Per certi gruppi, si ha $\widehat{G} \neq Aut(\Gamma)$ per ogni grafo di Cayley Γ su G. Ad esempio, se G è un gruppo abeliano e S è un suo sistema di generatori allora l'inversione $x \mapsto x^{-1}$ è un automorfismo del grafo di Cayley $\Gamma = \Gamma[G, S]$, infatti, se $x \in G$ e $s \in S$, allora per commutatività $\{x, xs\}^{-1} = \{x^{-1}, (xs)^{-1}\} = \{x^{-1}, x^{-1}s^{-1}\} \in E(\Gamma)$, Supponiamo esista un elemento $g \in G$ tale che $gx = \hat{g}(x) = x^{-1}$ per ogni $x \in G$; allora necessariamente $g = 1$ e $x^2 = 1$ per ogni $x \in G$; dunque

> *Se G è un gruppo abeliano che non ha esponente 2 (cioè esiste $x \in G$ con $x^2 \neq 1$), allora $\widehat{G} < Aut(\Gamma)$ per ogni grafo di Cayley Γ su G.*

Un grafo di Cayley $\Gamma = \Gamma[G, S]$ tale che $\widehat{G} = Aut(\Gamma)$ si dice una GRR (Graphical Regular Representation) del gruppo G. Per la Proposizione 2.9 determinare i gruppi

che ammettono una GRR equivale a determinare i grafi il cui gruppo degli automorfismi è regolare (cioè transitivo e libero) sull'insieme dei vertici. C'è una letteratura piuttosto ampia su questo, rivolta soprattutto al caso di gruppi (e grafi) finiti; Godsil, completando una ricerca a cui hanno contribuito in diversi ha dimostrato quanto segue.

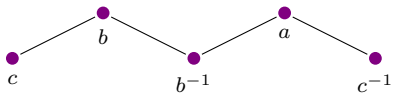
Teorema 2.10. *Un gruppo finito G ammette una GRR se e solo se non è abeliano di esponente diverso da 2, o un gruppo diciclico generalizzato*[6] *o uno di altri 13 casi esplicitamente descritti.*

I prossimi quattro esercizi seguono le prime pagine di [9]. Iniziamo con alcune considerazioni generali (le notazioni sono quelle utilizzate sinora in questa nota).

Esercizio 2.26. Sia S un sistema di generatori per il gruppo G e $\Gamma = \Gamma[G, S]$ il grafo di Cayley corrispondente. Per ogni $x \in G = V(\Gamma)$, sia $A_x = \{\phi \in Aut(\Gamma) \mid \phi(x) = x\}$. Chiaramente, per ogni $x \in G$, A_x è un sottogruppo di $Aut(\Gamma)$; si provi che $A_x = \hat{x} A_1 \hat{x}^{-1}$ e $\widehat{G} A_x = Aut(\Gamma)$. Dedurre che Γ è una GRR per G se e solo se $A_1 = \{1\}$.

Esercizio 2.27. Denotiamo con Γ^* il sottografo di $\Gamma = \Gamma[G, S]$ indotto dai vertici $S \cup S^{-1}$; si osservi che A_1 agisce come un gruppo di automorfismi sul grafo Γ^*. Sia $M \subseteq S \cup S^{-1}$; si provi che se $A_1 = A_u$ per ogni $u \in M$ allora $\phi(g) = g$ per ogni $g \in \langle M \rangle$. In particolare, se M è un sistema di generatori di G con tale proprietà allora $A_1 = \{1\}$ (e quindi Γ è una GRR di G).

Esercizio 2.28. Sia $G = A_5$ (gruppo alterno su $\{1, 2, 3, 4, 5\}$; posto $a = (1\,2)(3\,4)$, $b = (1\,3\,5)$, $c = (1\,2\,3\,4\,5)$, ed $S = \{a, b, c\}$, sia $\Gamma = \Gamma[G, S]$. Il grafo Γ^* è



(la moltiplicazione di permutazioni è a sinistra - come le funzioni di solito). Dedurre, usando gli esercizi precedenti, che A_1 fissa tutti i vertici in Γ^*, e quindi che Γ è una GRR per $G = A_5$.

Esercizio 2.29. Si trovino delle GRR per i gruppi S_5 ed A_6.

Un ultimo esercizio in direzione opposta.

Esercizio 2.30. Fissato $n \geq 3$, sia $G = S_n$ e $S = \{(1\,2), (1\,3), \ldots, (1\,n)\}$, $A_1 \leq Aut(\Gamma)$ come negli esercizi precedenti. È allora definita un'azione naturale di H su S, quindi un'azione di H su $\{2, 3, \ldots, n\}$ (cioè un omomorfismo $H \to S_{n-1}$). Sia $\overline{H} \simeq H$ l'immagine di H in $Sym(\{2, \ldots, n\}$; si provi che $\overline{H} = S_{n-1}$. Si provi poi che $\widehat{G}$ è normalizzato da $\overline{H}$ e quindi che $Aut(\Gamma) \geq \widehat{G} \rtimes \overline{H} \simeq S_n \times S_{n-1}$ (sì, l'ultimo prodotto è diretto).

2.6. "Ends" di un gruppo f.g.

Come abbiamo detto, un grafo di Cayley non individua il gruppo; anzi, sino a qui, a parte la finitezza (ed, in tal caso, il numero di vertici), non abbiamo mostrato nulla che garantisca che grafi (infiniti) possano discriminare tra i gruppi che li ammettano come grafi di Cayley e quelli che non li ammettono. Qui vediamo una prima proprietà del genere, la cui rilevanza (ed anche un poco il significato) sarà ancor più chiara quando vi ritorneremo dopo aver introdotto il concetto di quasi-isometria (Capitolo 4).

Sia $\Gamma = (V, E)$ un grafo connesso, $v \in V$ e $n \in \mathbb{N}$, denotiamo con $\mathcal{B}(v, n)$ la palla di centro v e raggio n secondo la metrica naturale d_Γ, quindi $\mathcal{B}(v, n)$ è l'insieme dei vertici

[6] Un gruppo G è *diciclico generalizzato* se G ha un sottogruppo normale ciclico H di indice 2 ed un elemento x di ordine 4 tale che $x^{-1} h x = h^{-1}$ per ogni $h \in H$.

di Γ che sono connessi a v da un cammino di lunghezza al più n. È evidente che se Γ è localmente finito allora $\mathcal{B}(v,n)$ è finita per ogni $v \in V$ e $n \in \mathbb{N}$.
Se $\Gamma = (V,E)$ un grafo connesso e $X \subseteq V$ denotiamo con $c(X)$ il numero di componenti connesse infinite del sottografo indotto da X. Sia inoltre Γ localmente finito, allora per ogni sottoinsieme finito Y di V, $c(V \setminus Y)$ è finito, e se $Y \subseteq Y'$ con Y' finito, allora $c(V \setminus Y) \leq c(V \setminus Y')$ (esercizio 2.31). In particolare, per ogni $v \in V$ la successione

$$c_n = c(V \setminus \mathcal{B}(v,n)) \tag{2.3}$$

è una successione crescente a valori naturali. Se poi v, w sono due vertici, poiché Γ è connesso esiste un intero $d \geq 1$ tale che $w \in \mathcal{B}(v,d)$ e $v \in \mathcal{B}(w,d)$, e quindi

$$\mathcal{B}(v,n) \subseteq \mathcal{B}(w,n+d) \subseteq \mathcal{B}(v,n+2d)$$

per ogni $n \in \mathbb{N}$; dunque il limite (estremo superiore) della successione in (2.3) non dipende dalla scelta del vertice centrale v. Tale limite

$$e(\Gamma) := \lim_{n\to\infty} c(V \setminus \mathcal{B}(v,n))$$

si dice *numero di ends*[7] di Γ.

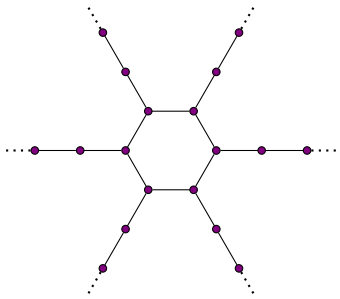
Esempi. • Sia $\Gamma = (V,E)$ un grafo localmente finito e connesso; è chiaro che $e(\Gamma) = 0$ se e solo se Γ è finito.

• Se $\Gamma = P_\infty$ è un cammino semplice infinito, allora il complementare in V di qualsiasi palla è l'unione di due 'semicammini' infiniti non connessi tra loro, quindi $e(P_\infty) = 2$.

• Se Γ è la griglia quadrata su $V = \mathbb{Z}^2$ (vedi esempio 2.3), il complementare di ogni palla (centrata, per dire, in $(0,0)$) è chiaramente connesso, dunque $e(\Gamma) = 1$.

• Se T_d è un albero d-regolare (esempio a pagina 31) con $d \geq 3$, si ha $e(T_d) = \infty$ (vedi anche esercizio 2.32).

• La figura di sotto mostra un'esempio di un grafo Γ con $e(\Gamma) = 6$; questo esempio si può ovviamente adattare a costruire grafi con un numero finito e arbitrario di ends.



Sia ora G un gruppo finitamente generato, siano X, Y due sistemi finiti di generatori di G e Γ_X, Γ_Y i rispettivi grafi di Cayley; si dimostra allora, per ragioni simili, ma un poco meno immediate, a quelle addotte prima per provare l'indipendenza di $e(\Gamma)$ dal vertice iniziale, che $e(\Gamma_X) = e(\Gamma_Y)$ (una dimostrazione è indicata negli esercizi 2.33 e 2.34). Si chiama quindi *numero di ends* del gruppo f.g. G il numero di ends di un suo grafo di Cayley:

$$e(G) = e(\Gamma[G,S])$$

[7] In italiano si potrebbe forse tradurre 'ends' con termini, o terminali, ma ho preferito lasciare il termine inglese, che è quello che si usa ovunque.

con S un sistema finito di generatori di G.

Dagli esempi di prima si ricava quindi $e(G) = 0$ se e solo se G è finito, $e(\mathbb{Z}) = 2$, $e(\mathbb{Z}^2) = 1$. Nel prossimo capitolo incontreremo i gruppi liberi F_n, per $n \geq 1$, il cui naturale grafo di Cayley è un albero $2n$-regolare, dunque $e(F_n) = \infty$ per ogni $n \geq 2$.

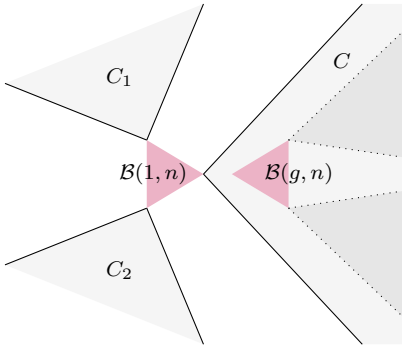
In questi esempi il numero di ends del gruppo f.g. in questione è $0, 1, 2$ oppure ∞; ma questo non è un caso.

Teorema 2.11 (Freudenthal - Hopf)**.** *Sia Γ un grafo connesso localmente finito e vertex-transitivo; allora $e(\Gamma) \in \{0, 1, 2, \infty\}$.*

Dimostrazione. Sia $\Gamma = (V, E)$ un grafo connesso localmente finito, vertex-transitivo, e supponiamo, per assurdo, $3 \leq e(\Gamma) < \infty$. Questo significa che, fissato un vertice $v \in V$, esiste un intero n tale che per ogni $k \geq n$ il numero di componenti connesse infinite del sottografo di Γ indotto da $V \setminus \mathcal{B}_\Gamma(u, k)$ è esattamente $t := e(\Gamma) \geq 3$; in particolare, V è infinito. Sia C (l'insiemi dei vertici di) una componente connessa infinita del grafo indotto da $V \setminus \mathcal{B}(v, n)$; poiché V è infinito (e $\mathcal{B}(u, n)$ finita) esiste $v \in C$ tale che $d_\Gamma(u, v) > 2n$. Per la vertex-transitività esiste $\phi \in Aut(\Gamma)$ tale che $v = \phi(u)$. Questo implica $\phi(\cdot\mathcal{B}(u, n)) = \mathcal{B}(v, n) \subseteq V \setminus \mathcal{B}(u, n)$; quindi $\mathcal{B}(v, n) \subset C$. Ora, $V \setminus C$, che è contenuto in $V \setminus \mathcal{B}(v, n)$, induce un sottografo connesso (dato che contiene $\mathcal{B}(u, n)$), e dunque è contenuto in un'unica componente connessa del grafo indotto da $V \setminus \mathcal{B}(v, n)$. Questo significa che tutte le altre componenti connesse di questo sottografo sono contenute in C. Ma, poiché ϕ è un automorfismo di Γ, il grafo indotto da $V \setminus \mathcal{B}(v, n)$ è isomorfo a quello indotto da $V \setminus \mathcal{B}(u, n)$ e pertanto ha t componenti connesse infinite, $t - 1$ delle quali sono dunque contenute in C.
Consideriamo ora il grafo Δ indotto da $V \setminus \mathcal{B}(u, n + d(u, v))$; poiché

$$\mathcal{B}(u, n) \cup \mathcal{B}(v, n) \subseteq \mathcal{B}(u, n + d(u, v)),$$

ogni componente connessa di Δ è contenuta sia in una componente connessa del grafo indotto da $V \setminus \mathcal{B}(u, n)$ che in una di quello indotto da $V \setminus \mathcal{B}(v, n)$. Da quanto detto prima, segue che Δ ha almeno $2(t - 1)$ componenti connesse infinite e, siccome $t \geq 3$, si trova $2t - 2 > t$, che è assurdo. ∎



Corollario 2.12. *Per ogni gruppo finitamente generato G si ha $e(G) \in \{0, 1, 2, \infty\}$.*

Esercizio 2.31. Sia $\Gamma = (V, E)$ un grafo connesso e localmente finito.

1) Si provi che per ogni sottoinsieme finito Y di V, $c(V \setminus Y)$ è finito, e che se $Y \subseteq Y'$ con Y' finito, allora $c(V \setminus Y) \leq c(V \setminus Y')$.

2) Si provi che $e(\Gamma) = \sup\{c(V \setminus Y) \mid Y \subseteq V,\ Y \text{ finito}\}$.

Esercizio 2.32. Sia T un albero localmente finito privo di vertici di grado 1, e $v \in V(\Gamma)$. Si provi che per ogni $n \in \mathbb{N}$, $c(V \setminus \mathcal{B}(v,n)) = |\mathcal{B}(v,n+1)| - |\mathcal{B}(v,n)|$. Si deduca che un albero infinito localmente finito ha un numero finito di ends se e solo se ha un numero finito di vertici di grado ≥ 3.

Esercizio 2.33. Siano X, Y sistemi finiti di generatori del gruppo G e, per $n \geq 0$, siano $\mathcal{B}_X(n)$ e $\mathcal{B}_Y(n)$, rispettivamente, le palle di centro 1_G e raggio n nei grafi di Cayley $\Gamma[G,X]$ e $\Gamma[G,Y]$. Si provi che esiste una costante $C \geq 1$ tale che, per ogni $g, h \in G$ e ogni $n \geq 0$, se g ed h appartengono ad una stessa componente connessa di $\Gamma[G,X] \setminus \mathcal{B}_X(Cn)$, allora g ed h appartengono ad una stessa componente connessa di $\Gamma[G,X] \setminus \mathcal{B}_Y(n)$.

Esercizio 2.34. Siano X, Y sistemi finiti di generatori del gruppo G; si provi che $e(\Gamma[G,X]) = e(\Gamma[G,Y])$.

Esercizio 2.35. Sia determini $e(D_\infty)$ dove D_∞ è il gruppo diedrale infinito.

Esercizio 2.36.$*$ Sia G un gruppo finitamente generato e sia H un sottogruppo di indice finito di G. Per il Teorema 1.9, H è finitamente generato; si provi che $e(H) = e(G)$.

2.7. Prodotto intrecciato e gruppo del Lampionaio

Il gruppo del Lampionaio è un caso particolare di *prodotto intrecciato*, una delle costruzioni più importanti di nuovi gruppi a partire da due gruppi dati. La versione che introdurremo non è la più generale, ma adatta all'uso che ne faremo, e ad illustrare compiutamente il gruppo del Lampionaio e simili.

Siano A, H gruppi, e sia data un'azione Φ di H su un certo insieme Ω. Per ogni $x \in \Omega$ sia A_x una copia isomorfa del gruppo A, e $B = Dir_{x\in\Omega} A_x$. Adottando il punto di vista della sezione 1.3, possiamo identificare gli elementi di B con le applicazioni $f : \Omega \to A$ tali che $supp(f) = \{x \in \Omega \mid f(x) \neq 1_A\}$ è finito, con l'operazione definita per componenti; per comodità di scrittura scriviamo $f_x = f(x)$ per ogni $f \in B$ ed $x \in \Omega$.
Si definisce quindi un'azione per automorfismi di H su B nel modo seguente

$$(h \cdot f)_x = f_{h\cdot x} \tag{2.4}$$

per ogni $f \in B$, $h \in H$ e $x \in \Omega$.; che in questo modo ad ogni $h \in H$ venga associato un automorfismo di B è immediato; infatti, per ogni $f, g \in B$ e $x \in \Omega$,

$$(h \cdot (fg))_x = (fg)_{h\cdot x} = f_{h\cdot x} g_{h\cdot x} = (h \cdot f)_x (h \cdot g)_x = ((h \cdot f)(h \cdot g))_x$$

e dunque $h \cdot (fg) = (h \cdot f)(h \cdot g)$. Questo definisce un'omomorfismo

$$\phi : H \to Aut(B).$$

Il *prodotto intrecciato*[8] di A per H, associato all'azione Φ, è il prodotto semidiretto definito dall'omomorfismo ϕ,

$$W = B \rtimes_\phi H.$$

[8] Quello che stiamo definendo è in molti testi chamato "prodotto intrecciato *ristretto*", per distinguerlo dal prodotto intrecciato *non-ristretto*, la cui costruzione è simile, con B il prodotto cartesiano (invece di quello diretto) delle copie A_x ($x \in \Omega$) di A.

Denotiamo per ora i suoi elementi come $(f,h) = (f,1)(1,h)$ dove $f \in B$ e $h \in H$ (ricordo che tale scrittura per ogni elemento di W è unica); la regola di moltiplicazione è dunque:

$$(f,h)(f_1,h_1) = (f(h \cdot f_1), hh_1),$$

ed il coniugio,

$$(f,1)^{(1,h)} = (1,h)(f,1)(1,h^{-1}) = (h \cdot f, 1).$$

Con le identificazioni solite, $W = BH$, dove il sottogruppo normale B è detto *base* del prodotto intrecciato e H un complemento. Come detto, B è il prodotto diretto delle copie A_x di A con $x \in \Omega$. Precisamente, per ogni $x \in \Omega$, si ha

$$A_x = \{f \in B \mid f_y = 1 \text{ per ogni } x \neq y \in \Omega\}.$$

Per ogni $h \in H$, l'azione di $h = (1,h)$ per coniugio su B si realizza permutando i sottogruppi A_x allo stesso modo in cui h permuta gli elementi di Ω (più esattamente, si ha $A_x^h = A_{h \cdot x}$ per ogni $x \in \Omega$).

Prodotto intrecciato standard. Con A e H come sopra, il caso in cui $\Omega = H$ e l'azione di H è quella regolare per moltiplicazione a destra, si parla di prodotto intrecciato *standard*. È il caso che utilizzeremo più spesso e denoteremo con

$$A \wr H.$$

La base di questo prodotto intrecciato è quindi il gruppo B, insieme delle applicazioni a supporto finito da H in A; l'azione di H su B è la seguente: per ogni $f \in B$, $h \in H$, $h \cdot f$ è definita da

$$(h \cdot f)(x) = f(xh), \tag{2.5}$$

per ogni $x \in H$. Ciò definisce un omomorfismo iniettivo $\phi : H \to Aut(B)$. Il prodotto intrecciato standard è quindi il prodotto semidiretto

$$A \wr H = B \rtimes_\phi H.$$

Gli elementi di $A \wr H$ si possono perciò scrivere i modo unico nella forma $fx = (f,x)$ con $f \in B$, $x \in H$ (una volta fatte le abituali identificazioni per prodotti semidiretti), e la regola di moltiplicazione è:

$$(fx)(f_1x_1) = ff_1^x xx_1,$$

dove $f_1^x = x \cdot f_1$, quindi $f_1^x(y) = f_1(yx)$ per ogni $y \in H$.

A questo punto, non è difficile stabilire che se A e H sono finitamente generati allora il prodotto intrecciato (ristretto) $A \wr H$ è finitamente generato. Infatti, come nel caso di un prodotto intrecciato generico, la base B è il prodotto diretto dei coniugati tramite gli elementi di H di un unica componente A_x. Nel caso standard, possiamo prendere A_1, che è generalmente identificato con A. Quindi, identificando un elemento $a \in A$ con l'elemento della base B che ha componente uguale ad a in 1 ed ogni altra uguale ad 1, si conclude facilmente che, se U è un sistema di generatori di A e Y un sistema di generatori di H allora

$$\{(a,g) \mid a \in U, g \in Y\}$$

è un sistema di generatori di $A \wr H$.

Esercizio 2.37. Siano A, H gruppi e $G = A \wr H$ il loro prodotto intrecciato standard. Si determini il centro $Z(G)$, mostrando, in particolare, che $Z(G) \simeq Z(A)$ se H è finito, mentre $Z(G) = 1$ se H è infinito.

Esercizio 2.38. Siano A, H gruppi, con A abeliano e sia $G = A \wr H$ il loro prodotto intrecciato standard. Posto B la base di G come insieme delle funzioni $H \to A$ a supporto finito, si provi che

$$N = \{f \in B \mid \prod_{x \in H} f(x) = 1_A\}$$

è un sottogruppo normale di G e che $G/N \simeq A \times H$. Se anche H è abeliano, si provi che N coincide con G', il sottogruppo derivato di G.

Esercizio 2.39. Si provi che $C_2 \wr C_2$ è isomorfo al gruppo diedrale D_8, e che, per ogni $n \geq 3$, $C_3 \wr C_2$ contiene un sottogruppo isomorfo a D_{2n}.

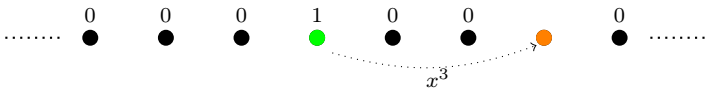
Il gruppo del Lampionaio. È un caso relativamente semplice ma che ha particolare importanza anche nelle applicazioni: il *gruppo del Lampionaio* (*Lamplighter group*), che è definito come il prodotto intrecciato standard

$$L_2 = (\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$$

dove $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ è il gruppo ciclico di ordine 2 e $\mathbb{Z}$ il gruppo additivo degli interi (gruppo ciclico infinito).
Più in generale, per ogni $n \geq 1$ si definisce il gruppo del Lampionaio

$$L_n = (\mathbb{Z}/n\mathbb{Z}) \wr \mathbb{Z}.$$

Gli elementi della base B di tale prodotto intrecciato si possono forse più agevolmente rappresentare come successioni $(a_z)_{z \in \mathbb{Z}}$, in cui ogni componente a_z si può intendere come uno 'stato' a valori in $\{0, 1, \ldots, n-1\}$ e solo un numero finito di componenti sono diverse da 0. L'azione di ogni elemento z del gruppo $\mathbb{Z}$ (che in L_n si traduce nell'azione per coniugio) consiste nel traslare gli stati di un numero di passi uguale a z. Nella figura di sotto, si è preferito usare il generico gruppo ciclico infinito $\langle x \rangle$ (quindi in notazione moltiplicativa) al posto del gruppo additivo $\mathbb{Z}$.



Nel seguito studieremo il gruppo L_2, che chiameremo, senza altre specifiche, gruppo del Lampionaio; le estensioni al caso L_n non sono in genere troppo difficili.

Quindi, $L_2 = B \rtimes \langle x \rangle$ dove B è l'insieme delle funzioni $\mathbb{Z} \to \{0, 1\}$ a supporto finito, ovvero delle successioni $(u_i)_{i \in \mathbb{Z}}$ a valori in $\{0, 1\}$ e quasi ovunque nulle, $\langle x \rangle$ un gruppo ciclico infinito con x che agisce come lo "shift": per ogni $z \in \mathbb{Z}$ e $\mathbf{u} = (u_i)_{i \in \mathbb{Z}} \in B$,

$$(x^z \cdot \mathbf{u})_i = u_{i-z}.$$

Nel prodotto semidiretto l'azione si legge come coniugio: $x^z \cdot \mathbf{u} = \mathbf{u}^{x^z} = x^z \mathbf{u} x^{-z}$. Se $\mathbf{a} = (\delta_{0z})_{z \in \mathbb{Z}}$ (δ_{ij} il delta di Kronecker) allora, per ogni $z \in \mathbb{Z}$, $\mathbf{a}^{\mathbf{u}^m} = (\delta_{mz})_{z \in \mathbb{Z}}$ e, come già osservato, $X = \{\mathbf{a}, x\}$ è un sistema di generatori di L_2. Facciamo ora solo un'osservazione sulla lunghezza degli elementi di B rispetto al sistema X di generatori.

Sia $n \geq 1$ e sia $\mathbf{b} \in B$ tale che il supporto di $\mathbf{b}$ è contenuto in $[-n, n]$; allora esistono interi $-n \leq n_1 < n_2 < \cdots < n_k \leq n$ tali che

$$\mathbf{b} = \mathbf{a}^{x^{n_1}} \mathbf{a}^{x^{n_2}} \cdots \mathbf{a}^{x^{n_k}} = x^{n_1} \mathbf{a} x^{n_2 - n_1} \ldots \mathbf{a} x^{n_k - n_{k-1}} \mathbf{a} x^{-n_k}.$$

Dunque

$$\ell_X(\mathbf{b}) \leq |n_1| + |n_k| + \sum_{j=1}^{k-1} (n_{j+1} - n_j) + k = |n_1| + |n_k| + (n_k - n_1) + k \leq 6n + 1. \quad (2.6)$$

Esercizio 2.40. Siano $L_2 = B \rtimes \langle x \rangle$ e $X = \{\mathbf{a}, x\}$ il sistema di generatori descritto sopra. Sia $\mathbf{b} \in B$ e $n = \ell_X(\mathbf{b})$; si provi che $supp(\mathbf{b}) \subseteq [-s, s]$, dove $s = n - |supp(\mathbf{b})|$.

L'esercizio che segue descrive una realizzazione 'concreta' (e utile) di L_2.

Esercizio 2.41. Sia $A = (\mathbb{Z}/2\mathbb{Z})[x, x^{-1}]$, dove x è un'indeterminata, l'anello dei polinomi di Laurent su $\mathbb{Z}/2\mathbb{Z}$ (quindi, con un numero finito di coefficienti diversi da zero); nel gruppo $GL(2, A)$ si consideri

$$L = \left\{ \begin{pmatrix} x^z & f \\ 0 & 1 \end{pmatrix} \,\middle|\, z \in \mathbb{Z}, f \in A \right\}.$$

(1) Si provi che L è un sottogruppo di G ed è isomorfo al gruppo del Lampionaio.

(2) Si provi che

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

Grafo di Cayley del gruppo del Lampionaio. Vediamo ora come un'interessante grafo si ottenga come grafo di Cayley del gruppo del Lampionaio L_2, anche se non rispetto al sistema di generatori X descritto prima. Cominciamo col definire il tipo di grafo che otterremo.

Grafi di Diestel-Leader. Sia $d \geq 1$ e $D = \{0, \ldots, d-1\} = \mathbb{Z}/d\mathbb{Z}$; per ogni $t \in \mathbb{Z}$ siano $\mathbb{Z}_t = \{z \in \mathbb{Z} \mid z \leq t\}$ e W_t l'insieme delle funzioni da $\mathbb{Z}_t \to D$ a supporto finito (cioè tali che $f(z) \neq 0$ per un numero finito di interi $z \leq t$). Sia $W = \bigcup_{t \in \mathbb{Z}} W_t$ (l'unione è disgiunta!). Ogni elemento f di W proviene quindi da un unico insieme $W_{h(f)}$, e chiamiamo l'intero $h(f)$ il "livello" di f.
Per ogni $t \in \mathbb{Z}$ ed ogni $f \in W_t$ poniamo $\bar{f}$ la restrizione di f a $\mathbb{Z}_{t-1}$, quindi $\bar{f} \in W_{t-1}$; questo definisce una funzione $W \to W$, che chiamiamo 'restrizione'. Osserviamo che tale restrizione è una funzione suriettiva, e che l'immagine reciproca di ogni $f \in W_t$ (per ogni $t \in \mathbb{Z}$) contiene esattamente d funzioni distinte appartenenti a W_{t+1}.

Definiamo il grafo diretto T_d, il cui insieme dei vertici è W e gli archi sono tutte le coppie ordinate $(\bar{f}, f) \in W^2$. Per quanto detto prima, per ogni vertice f di T_d c'è un solo arco che termina in f (che è $(\bar{f}, f)$) e d archi che iniziano in f. Il grafo semplice sotteso T_d^o (ottenuto cioè trascurando la direzione degli archi) è quindi $(d+1)$-regolare; ed è connesso: infatti per ogni $f, g \in W$, poiché sono a supporto finito, esiste un intero s tale che le restrizioni di f e di g a $\mathbb{Z}_s$ coincidono con la funzione nulla, da questa restrizione comune è possibile 'salire' lungo il grafo sino a raggiungere f da una parte e g dall'altra, e quindi f, g sono connesse da un cammino in T_d^o. Inoltre, T_d^o è privo di circuiti non-banali; infatti ogni arco comporta un cambiamento di livello tra gli estremi, in un circuito non-banale ci deve essere un vertice che è estreme di un arco in salita e del successivo in discesa; ma per ogni vertice c'è un solo arco che abbassa il livello, e

quindi i due arche ache arrivane ed escono sono uguali contro il fatto che il circuito sia, per definizione, ridotto. In conclusione, T_d^o *è un albero regolare di grado* $d+1$.

Il *grafo di Diestel-Leader* $DL_2(d)$ è il grafo il cui insieme dei vertici è l'insieme delle coppie

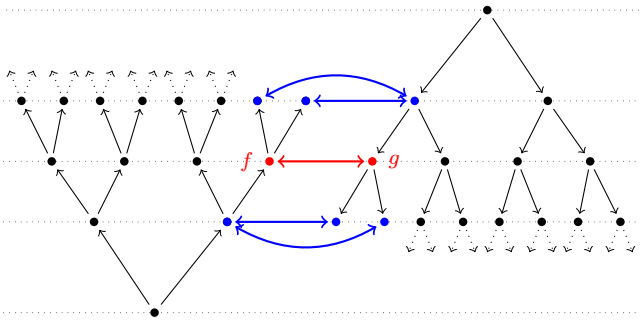
$$V = \{(f,g) \in W \times W \mid h(f) + h(g) = 0\};$$

e gli archi sono costituiti da tutte le coppie $\{(f,g),(f',g')\} \in V^{[2]}$ tali che (f,f') e (g,g') sono archi in T_d (indifferentemente dall'orientazione). Fissato un qualsiasi vertice $(f,g) \in V$, esiste in T_d una sola $f' = \bar{f}$ adiacente a f e tale che $h(\bar{f}) = h(f) - 1$; se $(\bar{f},g')$ è adiacente a (f,g) in $DL_2(d)$ allora

$$h(g') = -h(\bar{f}) = -h(f) + 1 = h(g) + 1$$

e dunque ci sono d scelte per la funzione g'; rovesciando la cosa, esistono d funzioni f' adiacenti a f in T_d e tali che $h(f') = h(f) + 1$, e se (f',g') è adiacente a (f,g) allora $h(g') = -h(f') = -h(f) - 1 = h(g) - 1$, e c'è una sola possiblità $g' = \bar{g}$. In conclusione, abbiamo che il grafo $DL_2(d)$ è regolare di grado $2d$.

Una maniera conveniente per farsi un'idea della cosa, nelle vicinanze di un vertice (f,g), è rappresentare i due alberi T_d 'rovesciati' uno rispetto all'altro, in modo che i livelli (opposti) di f e di g si trovino alla stessa altezza. La figura di sotto è relativa al caso $d = 2$: la freccia rossa rappresenta il vertice (f,g) e le frecce blu i 4 vertici ad essa adiacenti in $DL_2(d)$.



Il grafo $DL_2(d)$ è un grafo di Cayley per il gruppo del lampionaio L_d. Lo proviamo nel caso $d = 2$ (il caso generale non è molto diverso).
Risulta conveniente, in questa circostanza, rappresentare gli elementi di $L_2 = B \rtimes \langle x \rangle$ come coppie (a, x^t), con $a \in B$, l'insieme delle funzioni $\mathbb{Z} \to \{0,1\}$ a supporto finito, e $t \in \mathbb{Z}$ (quindi, su B l'operazione designata è la somma, mentre è la moltiplicazione per il gruppo ciclico infinito $\langle x \rangle$).
Sia V l'insieme dei vertici di $DL_2(2)$; è opportuno denotare gli elementi di V come terne $(f,g;t)$ dove $t = h(f) = -h(g)$ (si osservi che il parametro $t \in \mathbb{Z}$ è già univocamente determinato da f e g, tuttavia è utile evidenziarlo). Per ogni $(f,g;t) \in V$ definiamo $f * g \in B$ ponendo, per ogni $z \in \mathbb{Z}$,

$$(f * g)(z) = \begin{cases} f(z+1) & \text{se } z < t \\ g(-z) & \text{se } z \geq t \end{cases}$$

Questo definisce un'applicazione suriettiva (non iniettiva) $V \to B$, e consente di definire una biezione $\phi : V \to L_2$ ponendo, per ogni $(f,g;t) \in V$,

$$\phi(f,g;t) = (f * g, x^t). \tag{2.7}$$

L'inversa è data da $\phi^{-1}(a, x^t) = (a_t, a_{-t}; t)$ dove $a_t \in W_t$ e $a_{-t} \in W_{-t}$ sono definite da

$$a_t(z) = a(z-1)\ \forall z \leq t, \quad a_{-t}(z) = a(-z)\ \forall z \leq -t. \tag{2.8}$$

Sia ora $a \in B$ definita da $a(z) = \delta_{0z}$ e in L_2 consideriamo $A = \{(0, x), (a, x)\}$; poiché $(a, x)(0, x)^{-1} = (a, 1)$, per quando osservato in precedenza A è un sistema di generatori di L_2; sia Γ il grafo di Cayley $\Gamma[L_2, A]$.
Per ogni $(f, g; t) \in V$,

$$(f * g, x^t)(0, x) = (f * g, x^{t+1}) = (f' * \bar{g}, x^{t+1})$$

dove $f'(z) = f(z)$ se $z \leq t$ e $f'(t+1) = g(-t)$. Ora, $\{(f, g; t), (f', \bar{g}; t+1)\}$ è un arco in $DL_2(2)$, ed abbiamo allora provato che $\{\phi(f, g; t), \phi(f', \bar{g}; t+1)\}$ è un arco in Γ. Similmente,

$$(f * g, x^t)(a, x) = (f * g + a^{x^t}, x^{t+1}) = (f'' * \bar{g}, x^{t+1})$$

dove $f''(z) = f(z)$ se $z \leq t$ e $f'(t+1) = g(-t)+1$, e ancora $\{(f, g; t), (f'', \bar{g}; t+1)\}$ è un arco in $DL_2(2)$ e la sua immagine $\{\phi(f, g; t), \phi(f'', \bar{g}; t+1)\}$ un arco in Γ. In maniera analoga, si prova che esistono $g', g'' \in W_{1-t}$ tali che $\{(f, g), (\bar{f}, g')\}$ e $\{(f, g), (\bar{f}, g'')\}$ sono archi in $DL_2(2)$, e

$$(f * g, x^t)(0, x)^{-1} = (\bar{f} * g', x^{t-1}), \quad (f * g, x^t)(a, x)^{-1} = (\bar{f} * g'', x^{t-1})$$

In conclusione, ϕ è un isomorfismo di grafi $DL_2(2) \to \Gamma$, ed abbiamo provato il seguente rilevante fatto.

Proposizione 2.13. $\Gamma[L_2, A] \simeq DL_2(2)$.

NOTA. É possibile costruire grafi di Diestel-Leader partendo da due alberi regolari di grado rispettivamente d e q con $d \neq q$. In tale caso, i grafi ottenuti sono $(d+q)$-regolari e vertex-transitivi, ma non sono grafi di Cayley di alcun gruppo finitamente generato; anzi, non sono *quasi-isometrici* (la definizione di tale concetto la vedremo nel Capitolo 4) ad alcun grafo di Cayley (questo è il motivo principale per cui Diester e Leader li hanno introdotti in [4]).

ESERCIZIO 2.42. Si completino i dettagli della dimostrazione della Proposizione 2.13.

ESERCIZIO 2.43. Si provi che $e(L_2) = 1$.

ESERCIZIO 2.44. Sia $\langle x \rangle$ un gruppo ciclico di ordine 3 e $G = (\mathbb{Z}/2\mathbb{Z}) \wr \langle x \rangle$. Sia a l'elemento della base di G che assume valore 1 in una sola posizione. Si disegnino i grafi da Cayley $\Gamma[G, \{a, x\}]$ e $\Gamma[G, \{ax, x\}]$ (attenzione all'ordine dell'elemento ax).