Gruppi e Grafi Expander

Carlo Casolo
Dipartimento di Matematica "Ulisse Dini",
Corso di Complementi di Algebra
a.a. 2006/2007

Indice

Capitolo 1

Elementi di Teoria dei Grafi

Sia V un insieme e sia $1 \leq n \in \mathbb{N}$; denotiamo con $V^{[n]}$ l'insieme di tutti i sottoinsiemi di V di cardinalità n (dunque, se V è finito, $|V^{[n]}| = \binom{|V|}{n}$).

Un **grafo** è una tripla $\Gamma = (V, E, \phi)$, dove V ed E sono insiemi, con $V \neq \emptyset$, e ϕ è un'applicazione

$$\phi : E \longrightarrow V^{[2]}.$$

Un grafo $\Gamma = (V, E, \phi)$ si dice **semplice** se l'applicazione ϕ è iniettiva. In tal caso è conveniente identificare E con la sua immagine in $V^{[2]}$ tramite ϕ, e quindi vedere l'insieme degli archi di Γ come un sottoinsieme di $V^{[2]}$. Esplicitamente: un grafo semplice è una coppia (V, E), dove V è un insieme non vuoto ed E è un sottoinsieme (che può anche essere vuoto) dell'insieme dei sottoinsiemi di ordine 2 di V. Chiaramente, la differenza tra grafo e grafo semplice è che, in un grafo semplice, per ogni coppia di vertci c'è al più un arco che ha tali vertici come estremi, mentre in un grafo generico è consentito che ve ne siano più d'uno.
Conviene avvisare che (quasi) tutta la terminologia in teoria dei grafi è soggetta a variazioni da testo a testo. La definizione di grafo che ho scelto non è la più generale, tuttavia in molti testi (soprattutto quelli introduttivi) il termine grafo è riservato a quelli che noi chiamiamo grafi semplici, mentre ciò che abbiamo definito grafo viene dettoto multigrafo. In realtà, in queste note tratteremo a fondo soltanto il caso dei grafi semplici. Tuttavia alcuni risultati possono essere provati senza ulteriore fatica per i grafi in generale, cosa che cercheremo di segnalare.

In generale si è soliti rappresentare uno specifico grafo mediante un diagramma, nel quale i vertici sono punti in un piano, ed ogni lato è rappresentato da una linea (non necessariamente un segmento di retta) che congiunge i due vertici che corrispondono ai suoi estremi.
Ad esempio, sia $X = \{1, 2, 3\}$, e sia Γ il grafo semplice i cui vertici sono i sottoinsiemi di X, e due di essi costituiscono un arco se la loro differenza simmetrica contiene almeno due elementi. Allora, Γ si può rappresentare mediante il diagramma della figura 1.1. La figura 1.2 è invece un esempio di raopresentazione mediante un grafo (in questo caso provvisto di archi multipli) di un entità tratta dal mondo ritenuto reale (la molecola dell'adenina, la cui formula chimice è $H_2C_5N_5$.

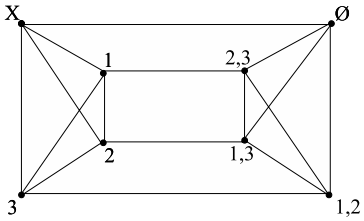


Figura 1.1: un grafo

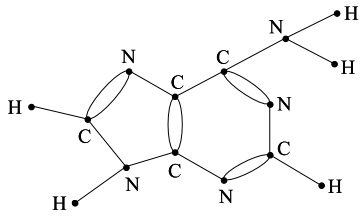


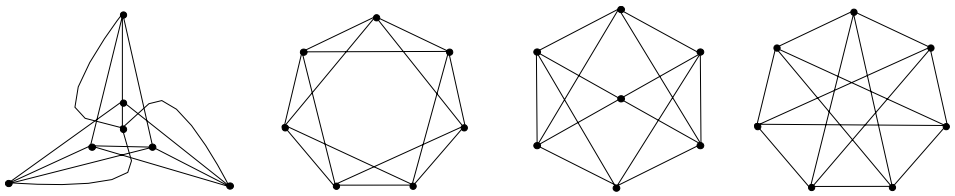
Figura 1.2: la molecola dell'adenina

Due grafi $\Gamma = (V, E, \phi)$ e $\Gamma' = (V', E', \psi)$ si dicono *isomorfi* se esiste una coppia di biezioni, $\alpha : V \to V'$ e $\beta : E \to E'$, tali che, per ogni $e \in E$,

$$\psi(\beta(e)) = \alpha(\phi(e)).$$

Se i due grafi sono semplici, ciò si riduce a richiedere che esista una biezione $\alpha : V \to V'$ tra gli insiemi di vertici tale che, per ogni $x, y \in V$, $\{x, y\} \in E \Leftrightarrow \{\alpha(x), \alpha(y)\} \in E'$.

Esercizio 1.1. Si dica quali tra i seguenti grafi semplici sono tra loro isomorfi:



Un grafo $\Gamma' = (U, F, \phi')$ si dice un *sottografo* del grafo $\Gamma = (V, E, \phi)$ se $\emptyset \neq U \subseteq V$, $F \subseteq E$ e $\phi' = \phi_{|F}$. Un sottografo $\Gamma' = (U, F, \phi')$ di un grafo $\Gamma = (V, E, \phi)$ si dice *sottografo indotto* se, per ogni $\{x, y\} \in U^{[2]}$ si ha $\phi^{-1}(\{x, y\}) \subseteq F$ ovvero se ogni arco di Γ i cui estremi stanno in Γ' è anche un arco di Γ'. Se $\emptyset \neq S \subseteq V$ è un sottoinsieme dell'insieme dei vertici di Γ, il sottografo *indotto* da S è il sottografo indotto di Γ il cui insieme di vertici è S.

Un grafo è *finito* se l'insieme dei suoi vertici e quello dei suoi archi sono finiti (è chiaro che, se richiediamo che il grafo sia semplice allora basta imporre che il numero di vertici sia finito).

A meno che non venga esplicitamente detto il contrario, tutti i grafi che considereremo nel seguito saranno intesi essere finiti.

Un grafo semplice $\Gamma = (V, E)$ si dice *completo* se $E = V^{[2]}$. È chiaro che due grafi completi sono isomorfi se e solo se gli insiemi dei vertici hanno la stessa cardinalità. Se $1 \leq n \in \mathbb{N}$, denotiamo con K_n il grafo completo su n vertici. Ad esempio

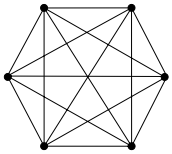


Figura 1.3: il grafo completo K_6

Il grafo semplice in cui i lati sono tutti e soli quelli che costituiscono il perimetro del n-agono, si chiama *ciclo* di lunghezza n (o n-ciclo), e si denota con C_n (ovviamente, in questo caso, il numero di lati è uguale a quello dei vertici).

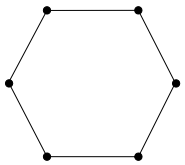


Figura 1.4: il ciclo C_6

Esercizio 1.2. Sia $\Gamma = (V, E)$ un grafo semplice. Il *grafo complementare* $\overline{\Gamma} = (V', E')$ è definito nel modo seguente $V' = V$ e, per ogni $u, v \in V$ con $u \neq v$, $\{u, v\} \in E'$ se e solo se $\{u, v\} \notin E$. Sia Γ un grafo semplice con n vertici e tale che $\overline{\Gamma}$ è isomorfo a Γ. Si dica quanti lati ha Γ (in funzione di n). mostrando che $n \equiv 0, 1 \pmod 4$. Si costruiscano grafi con 4 e con 5 vertici che siano isomorfi al loro grafo complementare.

1.1 Vertici e lati.

Sia $\Gamma = (V, E, \phi)$ un grafo. Se $e \in E$ allora i due vertici appartenenti a $\phi(e)$ si dicono gli *estremi* di e. Un vertice v ed un arco e si dicono *incidenti* se $v \in \phi(e)$ (cioè se v è un estremo di e); due vertici $v, w \in V$ si dicono *adiacenti* se $\{v, w\} \in \phi(E)$ (e quindi, in particolare, $v \neq w$); similmente, diremo che due archi e, $e' \in E$ sono *consecutivi* se hanno un estremo in comune (cioè se $e \neq e'$ ed $\phi(e) \cap \phi(e') \neq \emptyset$). Dato $v \in V$, il **grado** (o *valenza*) di v è il numero di archi incidenti a v (nel caso di grafi semplici coincide con il numero di vertici adiacenti a v), e si denota con $d_\Gamma(v)$. Un vertice che non sia incidente ad alcun arco (cioè tale che $d_\Gamma(v) = 0$) si dice vertice *isolato* di Γ. Il primo risultato generale della teoria dei grafi è una semplice ma fondamentale osservazione:

Teorema 1.1. *Sia $\Gamma = (V, E)$ un grafo. Allora*

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

DIMOSTRAZIONE. Consideriamo l'insiene $S = \{(v, e) \in V \times E \mid v \in \phi(e)\}$. Ora, ogni vertice $v \in V$ è incidente a tanti archi in E quanto è il suo grado; viceversa, ad ogni arco corrispondono esattamente due estremii. Si ha quindi, contando in due modi gli elementi dell'insieme S, facendo cioè separatamente variare in primo luogo la prima componente (i vertici), e quindi la seconda (gli archti):

$$\sum_{v \in V} d_\Gamma(v) = |S| = 2|E|,$$

da cui l'enunciato. ∎

Ovviamente, un vertice di un grafo si dice un vertice (dis)pari se il suo grado è (dis)pari. Poiché una somma di numeri interi è pari se e soltanto se il numero di addendi dispari è pari, dal teorema 1.1 discende subito il seguente

Corollario 1.2. *In un grafo il numero di vertici dispari è pari.*

Esercizio 1.3. Provare che ogni grafo semplice con 2 o più vertici ha almeno due vertici dello stesso grado.

Un grafo si dice **regolare** se tutti i suoi vertici hanno lo stesso grado; se tale grado comune è d, si dice che il grafo è regolare d-valente, o d-regolare. (si osservi che, se Γ è un grafo d-regolare, allora la formula del teorema 1.1 diventa $d|V| = 2|E|$).
Il grafo completo K_n è regolare e $(n-1)$-valente (ed è il solo grafo semplice con tale proprietà su un dato insieme di n vertici); un n-ciclo è un grafo regolare 2-valente; mentre il grafo della Figura 1.1 è regolare 4-valente.

Famosi grafi regolari si ottengono considerando la relazione d'incidenza tra i vertici e gli spigoli dei poliedri regolari (i cosiddetti solidi platonici). La figura 1.5 mostra i grafi del tetraedro, del cubo (esaedro), dell'ottaedro, e del dodecaedro; si disegni per esercizio il grafo dell'icosaedro (20 facce triangolari, 12 vertici e 30 spigoli).

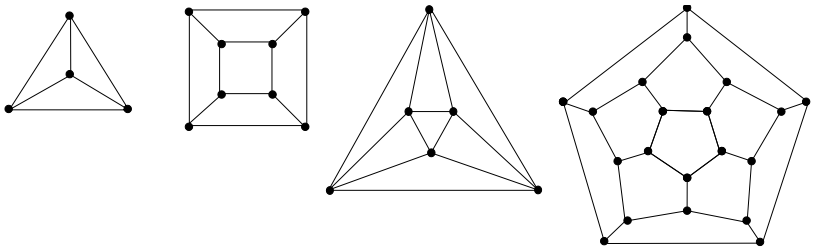


Figura 1.5: i grafi di alcuni solidi regolari

Tra i grafi con un numero ridotto di vertici, uno dei più rinomati è il *grafo di Petersen* della Figura 1.6; si tratta di un grafo regolare 3-valente che gode di molte proprietà interessanti.

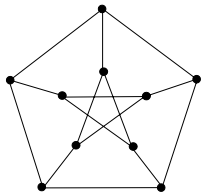
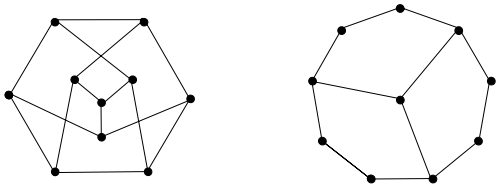


Figura 1.6: il grafo di Petersen

Esercizio 1.4. Sia $\Gamma = (V, E)$ un grafo semplice regolare 3-valente. Si provi che $|V|$ è pari. Si provi che per ogni numero pari n esiste un grafo regolare 3-valente con n vertici. Si provi che, a meno di isomorfismo, esistono 2 grafi semplici 3-regolari con 6 vertici.

Esercizio 1.5. Si provi che il grafo a sinistra nella figura di sotto è isomorfo al grafo di Petersen. Al grafo di destra si aggiungano opportunamente tre lati in modo da ottenere un grafo isomorfo al grafo di Petersen.



1.2 Cammini, circuiti, connessione.

Sia $\Gamma = (V, E, \phi)$ un grafo, e siano $v, w \in V$ due vertici di Γ (non necessariamente distinti). Un **cammino** in Γ da v a w è una sequenza:

$$v = v_0 \ e_1 \ v_1 \ e_2 \ \ldots \ v_{n-2} \ e_{n-1} \ v_{n-1} \ e_n \ v_n = w$$

di vertici $v_0, v_1, \ldots, v_n \in V$ (non necessariamente distinti), ed archi $e_1, e_2, \ldots, e_n \in E$, *tutti distinti* e tali che $\phi(e_i) = \{v_{i-1}, v_i\}$, per ogni $i = 1, 2, \ldots, n$.
L'intero $n \geq 0$ si dice la *lunghezza* del cammino (osserviamo che prendiamo in considerazione anche cammini di lunghezza 0, formati cioè da un solo vertice e nessun arco).
Se $v_0 = v_n$, il cammino è detto **circuito**. Un cammino (circuito) si dice **semplice** se tutti i vertici che lo compongono, tranne eventualmente il primo e l'ultimo, sono diversi; ovvero se, per ogni $1 \leq i, j \leq n$, $i \neq j \Rightarrow v_i \neq v_j$ (il cammino non "ripassa" per uno stesso vertice). Un circuito semplice con almeno tre archi è detto anche **ciclo** (in sostanza, un ciclo di lunghezza n è un sottografo isomorfo al n-ciclo C_n).
Conviene avvisare che, anche in questo contesto, le definizioni non sono universalmente riconosciute. In altri testi viene definito un cammino ciò che noi preferiamo chiamare una *passeggiata*: ovvero una sequenza $v_0 \ e_1 \ v_1 \ e_2 \ \ldots \ v_{n-2} \ e_{n-1} \ v_{n-1} \ e_n \ v_n$ di vertici ed archi consecutivamente incidenti in cui *non* si richiede che gli archi siano tutti distinti.

Un grafo Γ si dice **connesso** se per ogni coppia di suoi vertici v, w, esiste in Γ un cammino tra v e w.

Esercizio 1.6. Siano v, w vertici distinti di un grafo Γ. Si provi che se esiste un cammino in Γ da v a w, allora esiste anche un cammino semplice da v a w.

Esercizio 1.7. Provare che ogni grafo regolare 2-valente connesso e con n vertici è isomorfo al ciclo C_n.

Prima di procedere a provare un'elementare proprietà dei grafi connessi, introduciamo le seguenti e comode notazioni. Sia $\Gamma = (V, E, \phi)$ un grafo; fissato un suo arco $e \in E$, denotiamo con $\Gamma - e$ il grafo ottenuto da Γ togliendo il lato e (ma lasciando tutti i vertici); mentre se $v \in V$ è un vertice di Γ, denotiamo con $\Gamma - v$ il grafo ottenuto da Γ togliendo il vertice v e tutti i lati ad esso adiacenti. Pertanto, se $e \in E$: $\Gamma - e = (V, E \setminus \{e\})$; mentre se $v \in V$, $\Gamma - v$ è il sottografo indotto in Γ dall'insieme di vertici $V \setminus \{v\}$.

Proposizione 1.3. *Sia $\Gamma = (V, E, \phi)$ un grafo finito. Se Γ è connesso allora*

$$|E| \geq |V| - 1.$$

Dimostrazione. Sia $\Gamma = (V, E, \phi)$ un grafo connesso, e procediamo per induzione sul numero n di vertici di Γ (cioè $n = |V|$). Se $n = 1$ o 2 l'asserto è ovvio. Sia $n \geq 3$, ed assumiamo che la proprietà sia soddisfatta da ogni grafo con un numero di vertici strettamente minore di n.
Supponiamo che si abbia $d_\Gamma(v) \geq 2$, per ogni $v \in V$; allora, per il Teorema 1.1,

$$2|E| = \sum_{v \in V} d_\Gamma(v) \geq \sum_{v \in V} 2 = 2|V|$$

e quindi $|E| \geq |V|$. Altrimenti, esiste un vertice v tale che $d_\Gamma(v) = 1$ (essendo connesso con almeno due vertici, Γ non ha vertici isolati). Consideriamo il grafo $\Gamma' = \Gamma - v$. Allora, Γ' è connesso, perché un cammino che in Γ congiunge due vertici diversi da v è tutto contenuto in Γ' (infatti, se passasse per v dovrebbe contenere due volte il solo lato incidente a v). D'altra parte, l'insieme E' dei lati di Γ' è costituito da tutti i lati di Γ con l'esclusione del solo lato incidente a v. Dunque, applicando l'ipotesi induttiva,

$$|E| = |E'| + 1 \geq (|V \setminus \{v\}| - 1) + 1 = |V| - 1$$

come si voleva. ∎

A questo punto è naturale, dato un grafo Γ, introdurre una relazione sull'insieme V dei vertici, dicendo che due vertici sono in relazione se esiste un cammino (eventualmente di lunghezza 0) che li congiunge. È chiaro che tale relazione è un'equivalenza sull'insieme V. Le **componenti connesse** di Γ sono i sottografi indotti dalle singole classi di equivalenza di vertici. Si osserva facilmente che le componenti connesse di un grafo sono i suoi sottografi connessi massimali. È anche immediato provare (lo si faccia per esercizio) che dato un grafo Γ ed un isomorfismo $\phi : \Gamma \to \Gamma'$ di grafi, Γ è connesso se e solo se Γ' è connesso.

Esercizio 1.8. 1) Sia Γ un grafo semplice non connesso. Si provi che il suo grafo complementare (vedi esercizio 1.2) è connesso. Sia $\Gamma = (V, E)$ un grafo semplice con n vertici. Si provi che se $|E| > \binom{n-1}{2}$ allora Γ è connesso. Cosa si può dire se $|E| = \binom{n-1}{2}$?

Esercizio 1.9. Sia Γ un grafo semplice con n vertici e tale che per ogni coppia di vertici v, w non adiacenti si ha $d_\Gamma(v) + d_\Gamma(w) \geq n - 1$. Si provi che Γ è connesso.

Cammini e grafi euleriani. Anche se si tratta di qualcosa che non utilizzeremo mai nel resto dei queste note, è difficile concepire una qualsivoglia introduzione alla teoria dei grafi che eviti di accennare all'atto di nascita riconosciuto della teoria stessa, ovvero dalla memoria di Leonardo Eulero, pubblicata presso gli atti dell'Accademia delle Scienze di Pietroburgo nel 1736. In tale lavoro, Eulero affrontava e risolveva in grande generalità l'allora famoso

Problema dei ponti di Königsberg. La città di Königsberg (oggi Kaliningrad) nella Prussia Orientale (oggi un enclave russa tra la Polonia e la Lituania) sorge alla foce del fiume Pregel, che in quel punto forma due isole. Nel settecento le varie parti della città erano collegate da un sistema di sette ponti:

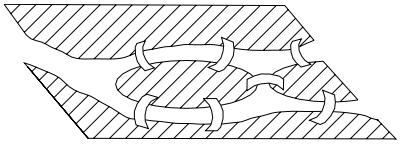


Figura 1.7: i ponti di Königsberg...

ed era costume delle famiglie borghesi del tempo (tra cui immaginiamo la famiglia Kant con il piccolo Immanuel che ancora succhia un lecca-lecca) recarsi a passeggiare, nelle domeniche di bel tempo, lungo le rive del fiume e le sue isole. Assieme ai cittadini, circolava anche il problema seguente: è possibile fare una passeggiata che partendo ed arrivando nello stesso luogo porti ad attraversare una ed una sola volta tutti e sette i ponti di Königsberg?

Sia $\Gamma = (V, E, \phi)$ un grafo. Un cammino $v_0\, e_1\, v_1\, e_2\, v_2 \ldots e_m\, v_m$ in Γ si dice **euleriano** se $\{e_1, \ldots, e_m\} = E$ (ricordiamo che i lati che compongono un cammino sono tutti distinti). Similmente, un circuito si dice euleriano se l'insieme dei lati che lo compongono è tutto E. Un grafo in cui esiste un circuito euleriano si chiama **grafo euleriano**.

Il problema dei ponti di Königsberg è dunque quello dell'esistenza di un circuito euleriano nel grafo di figura 21.8.

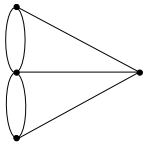


Figura 1.8: ...il loro grafo.

Ecco la risposta di Eulero.

Teorema 1.4. (Eulero). *Un grafo privo di vertici isolati è euleriano se e soltanto se è connesso ed ogni suo vertice ha grado pari.*

DIMOSTRAZIONE. Sia Γ un grafo privo di vertici isolati.
Se Γ è euleriano è ovvio che Γ è connesso. Inoltre, per ciascun vertice v, un fissato circuito euleriano di Γ attraversa una ed una sola volta tutti i lati incidenti a v; poiché ogni volta che il circuito tocca v deve arrivare e uscire per due lati distinti (se v è il vertice iniziale, il circuito inizia e si chiude in v con due lati diversi), si conclude che il grado di v è pari.
Viceversa, supponiamo che Γ sia connesso e che tutti i suoi vertici abbiano grado pari. Proviamo che Γ ha un circuito euleriano per induzione sul numero m di lati di Γ (osserviamo che $m \geq 2$). Se $m = 2$, allora Γ è un multigrafo costituito da due vertici connessi da due lati, e quindi ammette banalmente un cammino euleriano. Sia $m \geq 3$. Allora, poiché ogni vertice di Γ ha grado almeno 2, Γ non è un albero (se Γ fosse un albero, non avrebbe alcun lato multiplo e quindi, per il Lemma 1.15, avrebbe dei vertici di grado 1); quindi Γ ammette dei circuiti. Sia $\mathcal{C}$ un circuito di Γ con il massimo numero possibile di lati e supponiamo, per assurdo, che $\mathcal{C}$ non sia euleriano (cioè che non comprenda tutti i lati di Γ). Allora, il grafo $\Gamma - \mathcal{C}$, ottenuto da Γ togliendo tutti i lati di $\mathcal{C}$, non è formato da soli vertici isolati, e ha pertanto una componente connessa Δ non banale. Ora, poiché nel ricavare $\Gamma - \mathcal{C}$ abbiamo tolto i lati di un circuito, e dunque per ciascun vertice v di Γ, abbiamo tolto un numero pari (eventualmente zero) di lati incidenti a v, ne segue in particolare che in Δ tutti i vertici hanno grado pari e quindi, per ipotesi induttiva, esiste un circuito euleriano $\mathcal{D}$ in Δ. Ora, siccome Γ è connesso, almeno un vertice a del circuito $\mathcal{C}$ appartiene a Δ (e quindi compare in $\mathcal{D}$). Ora, percorrendo il circuito $\mathcal{C}$, a partire da un suo vertice qualsiasi, sino al vertice a, poi percorrendo tutto $\mathcal{D}$ fino a tornare ad a, e quindi riprendendo il tratto non ancora percorso di $\mathcal{C}$, si ottiene un circuito in Γ (dato che i lati di Δ, e quindi quelli che formano $\mathcal{D}$, non compaiono in $\mathcal{C}$) di lunghezza maggiore di $\mathcal{C}$, e questo va contro la scelta di $\mathcal{C}$. Pertanto $\mathcal{C}$ è un circuito euleriano. ∎

Un semplice adattamento della dimostrazione precedente consente di completare il risultato di Eulero al caso dei cammini euleriani.

Teorema 1.5. *Un grafo Γ privo di vertici isolati ha un cammino euleriano non chiuso se e soltanto se è connesso ed ha due vertici dispari. Nel caso Γ abbia due vertici dispari u e v, allora tutti i cammini euleriani di Γ iniziano e terminano in u e v.*

DIMOSTRAZIONE. Esercizio. (suggerimento: se u e v sono i due vertici dispari, aggiungere al grafo un nuovo vertice a e due archi, quindi applicare il Teorema precedente.) ∎

Esercizio 1.10. È possibile tracciare una (e una sola) diagonale su ogni faccia di un cubo in modo che il grafo che si ottiene (i vertici sono quelli del cubo, ed i lati gli spigoli del cubo e le diagonali aggiunte) sia euleriano?

Esercizio 1.11. Sia $n \geq 2$, e siano Γ e Γ' due grafi completi su n vertici. Supponiamo che i due insiemi di vertici siano disgiunti: $V = \{v_1, v_2, \ldots, v_n\}$ l'insieme dei vertici di Γ, e $V' = \{v'_1, v'_2, \ldots, v'_n\}$ quello dei vertici di Γ'. Sia $\Delta_n = (V, E)$ il grafo definito nella maniera seguente: $V = V \cup V'$ ed E è costituito da tutti i lati di Γ e di Γ' con l'aggiunta dei lati del tipo $\{v_i, v'_i\}$, con $i = 1, 2, \ldots, n$. Si dica per quali valori di n il grafo Δ_n è euleriano.

Cicli e grafi hamiltoniani. Sia Γ un grafo. Un cammino $v_0\, e_1\, v_1\, e_2\, v_2 \ldots e_n\, v_n$ in Γ si dice *hamiltoniano* se è semplice e $\{v_0, v_1, \ldots, v_n\} = V$. Un cammino hamiltoniano è quindi un cammino che tocca una ed una sola volta tutti i vertici del grafo. Similmente, un circuito di Γ si dice hamiltoniano se è semplice (cioè è un ciclo) e l'insieme dei vertici che lo compongono è tutto V. Un grafo in cui esiste un ciclo hamiltoniano si chiama *grafo hamiltoniano*. In altre parole, un grafo con n vertici è hamiltoniano se e solo se contiene un sottografo isomorfo al ciclo C_n.

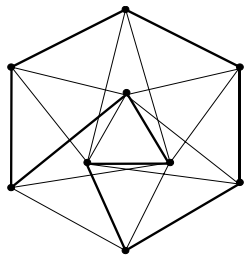


Figura 1.9: un ciclo hamiltoniano.

Mentre è facile implementare un programma efficiente (qualsiasi cosa questo ragionevolmente significhi) che, utilizzando il teorema 1.4, stabilisce se un grafo è euleriano, in generale decidere se un dato grafo ammetta un ciclo (o anche un cammino) hamiltoniano è un problema molto più difficile.

Esercizio 1.12. Si provi che il grafo del dodecaedro è hamiltoniano. Si provi che il grafo di Petersen non è hamiltoniano (si trovi qual'è la lunghezza massima di un ciclo contenuto nel grafo di Petersen.

Di fatto, non si conosce alcuna caratterizzazione dei grafi hamiltoniani analoga ai quella vista per i grafi euleriani, né si sa che non esiste (anche se la cosa è improbabile: per chi ha un poco di dimestichezza con la teoria della complessità, citiamo che è stato dimostrato che il problema di decidere se un grafo è hamiltoniano è NP-completo).
Questa questione ha da sempre attirato l'interesse di diversi studiosi, e sono stati ottenuti vari risultati i quali assicurano che, sotto condizioni di solito abbastanza specifiche, certi grafi sono (o non sono) hamiltoniani. Uno dei più semplici è il seguente, dovuto a O. Ore (1960). Prima di enunciarlo, osserviamo che, banalmente, ogni grafo completo è hamiltoniano.

Teorema 1.6. (Ore). *Sia Γ un grafo con n vertici, tale che per ogni coppia di vertici v, w non adiacenti si ha $d_\Gamma(v) + d_\Gamma(w) \geq n$. Allora Γ è hamiltoniano.*

Dimostrazione. Sia Γ un grafo con n vertici che soddisfa all'ipotesi del Teorema.
Se $n = 1$ non c'è nulla da provare (osserviamo che un grafo con un solo vertice, o più in generale un qualsiasi grafo completo, soddisfa la condizione dell'enunciato, dato che *non ci sono* coppie di vertici non adiacenti). Supponiamo quindi $n \geq 2$, e procediano per induzione sul numero t di coppie (non ordinate) di vertici non adiacenti di Γ. Se $t = 0$ allora Γ è un grafo completo e dunque, per quanto osservato sopra, ammette un cammino hamiltoniano. Sia quindi $t \geq 1$. Allora esistono in Γ due vertici non adiacenti u e w. Consideriamo il grafo

Γ' ottenuto da Γ aggiungendo il lato $e = \{u, w\}$. Chiaramente Γ', che ha lo stesso numero di vertici di Γ e un lato in più, soddisfa le ipotesi del teorema. Ora, Γ' ha una coppia in meno di vertici non adiacenti, e dunque, per ipotesi induttiva, esiste un ciclo hamiltoniano $\mathcal{C}$ di Γ'. Poiché Γ' ha gli stessi vertici di Γ, se $\mathcal{C}$ non contiene il lato aggiunto e, allora è un ciclo hamiltoniano anche di Γ. Supponiamo quindi che il lato $e = e_1$ appartenga al ciclo $\mathcal{C}$. Il resto del ciclo, $w = v_1\ e_2\ v_2\ \ldots\ v_{n-1}\ e_n\ v_n = u$, è un cammino hamiltoniano in Γ. Poniamo

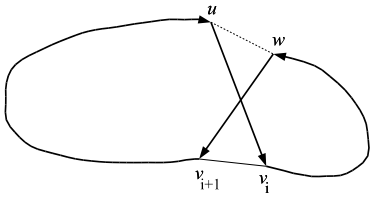
$$A = \{\ v_i \mid 1 \le i \le n,\ u \text{ è adiacente in } \Gamma \text{ a } v_i\ \}$$

$$B = \{\ v_i \mid 1 \le i \le n-1,\ w \text{ è adiacente in } \Gamma \text{ a } v_{i+1}\ \}.$$

Poiché $\{v_1, v_2, \ldots, v_n\}$ è l'insieme di tutti i vertici di Γ, si ha $|A| = d_\Gamma(u)$, $|B| = d_\Gamma(w)$. Quindi, per ipotesi, $|A| + |B| \ge n$. Ora, $u \notin A \cup B$, e dunque

$$|A \cup B| \le n - 1 < |A| + |B|.$$

Da ciò segue $A \cap B \neq \emptyset$. Sia $v_i \in A \cap B$; allora $\{w, v_{i+1}\}$ e $\{u, v_i\}$ sono lati di Γ.

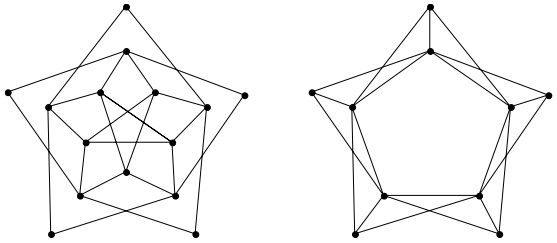


Partendo da w, facendo seguire il lato $\{w, v_{i+1}\}$ (vedi la figura), percorrendo poi il circuito $\mathcal{C}$ da v_{i+1} fino ad u, quindi facendo seguire il lato $\{u, v_i\}$, ed infine percorrendo $\mathcal{C}$ a ritroso da v_i a w (vedi figura) si ottiene un ciclo hamiltoniano di Γ. ∎

Il Teorema di Ore è un raffinamento di un celebre risultato di G. Dirac (1954), che possiamo ricavare come immediato corollario.

Corollario 1.7. *Sia Γ un grafo su n vertici e tale che $d_\Gamma(v) \ge n/2$ per ogni vertice v. Allora Γ è hamiltoniano.*

Esercizio 1.13. Si dica quali tra i seguenti grafi sono hamiltoniani.



Esercizio 1.14. Sia Γ un grafo con n vertici e sia $\kappa = \kappa(\Gamma)$ la lunghezza massima di un cammino semplice di Γ. Si provi che aggiungendo a Γ al più $n - \kappa$ opportuni lati si ottiene un grafo hamiltoniano (si faccia induzione su $n - \kappa$).

1.3 Alberi ed esercizi.

Un **albero** è un grafo semplice connesso privo di circuiti non banali (il che equivale all'essere connesso e privo di cicli). Un grafo privo di cicli (ma non necessariamente connesso) si chiama una **foresta**. È chiaro che un grafo è una foresta se e solo se ogni sua componente connessa è un albero. Gli alberi costituiscono un importante classe di grafi semplici, soprattutto a causa delle loro applicazioni. Gli alberi, infatti, sono spesso un naturale metodo di rappresentare diverse relazioni di dipendenza.

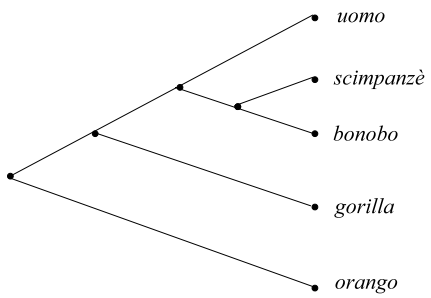


Figura 1.10: l'albero genetico di alcune specie di scimmie

Tuttavia, poiché gli alberi interverranno soltanto in modo occasionale nella specifiche questioni che intendiamo trattare, ho pensato di lasciare come esercizio la studio delle loro proprietà elementari. SI inizi con il dimostrare la seguente osservazione

Esercizio 1.15. Un albero con due o più vertici ha almeno due vertici di grado 1.

Tra i grafi connessi, gli alberi sono caratterizzati da una semplice proprietà numerica.

Esercizio 1.16. Sia $\Gamma = (V, E)$ un grafo semplice connesso. Allora Γ è un albero se soltanto se $|E| = |V| - 1$.

SUGG.: Se Γ non è un albero, allora ammette un cicrcuito non banale. Possiamo quindi togliere un arco di Γ senza perdere la connessione ... Viceversa, se Γ è un albero, si applichi l'esercizio 1.15 e induzione sul numero di archi.

Poiché una foresta Γ è priva di circuiti, ogni sua componente connessa è un albero, e dunque, per l'esercizio 1.16 contribuisce con 1 al valore di $|V| - |E|$. Pertanto

Esercizio 1.17. Sia $\Gamma = (V, E)$ una foresta. Allora, il numero di componenti connesse di Γ è $|V| - |E|$.

Si possono dare altre utili caratterizzazioni degli alberi, che non dovrebbero risultare difficili da provare, che sono suggerite dal seguente fatto.

Esercizio 1.18. Sia Γ un grafo semplice. Le seguenti condizioni sono equivalenti:

(i) Γ è un albero;

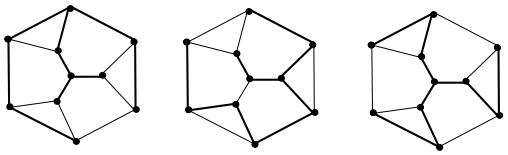
(ii) per ogni coppia di vertici di Γ esiste uno ed un solo cammino che li congiunge;

(iii) Γ è connesso e, per ogni suo lato e, $\Gamma - e$ è non-connesso.

Un concetto importante (soprattutto nelle applicazioni) associato agli alberi è quello di spanning-tree. Sia Γ un grafo: uno *spanning-tree* di Γ è un sottografo che è un albero ed il cui insieme dei vertici coincide con quello di Γ.
Il punto fondamentale è il seguente fatto.

Esercizio 1.19. Si provi che ogni grafo connesso ammette almeno uno spanning-tree.

La figura seguente mostra alcuni spanning-trees di uno stesso grafo. È chiaro che uno spanning-tree non è univocamente individuato, nemmeno a meno di isomorfismo.



Di fatto, si può facilmente osservare che ogni albero con n vertici è isomorfo ad uno spanning-tree del grafo completo K_n.

Esercizio 1.20. Sia Γ un grafo. Si dica quali tra le seguenti affermazioni sono corrette:

1) gli spanning-tree di Γ hanno tutti lo stesso numero di vertici di grado 1;

2) gli spanning-tree di Γ hanno tutti lo stesso numero di lati;

3) gli spanning-tree di Γ hanno tutti lo stesso diametro.

Esercizio 1.21. Siano $1 \leq d_1 \leq d_2 \leq \cdots \leq d_n$ interi positivi tali che $\sum_{i=1}^{n} d_i = 2n - 2$. Si provi che esiste un albero T con n vertici $v_1, v_2, \ldots, v_n$ tale che $d_T(v_i) = d_i$ per ogni $1 \leq i \leq n$.

Esercizio 1.22. Sia Γ un albero, e denotiamo con κ la lunghezza massima di un cammino (semplice) di Γ. Sia quindi

$$v_0\, e_1\, v_1\, e_2\, \ldots\, v_{\kappa-1}\, e_\kappa\, v_\kappa$$

un cammino di lunghezza massima in Γ. Si provi che v_0 e v_κ sono vertici di grado 1. Si supponga quindi che $\kappa = 2t$ sia pari, e sia $v = v_t$ il vertice "centrale" del cammino dato; si provi che ogni altro cammino di lunghezza κ di Γ passa per v. Cosa si può dire se κ è dispari?

1.4 Diametro, calibro e numero cromatico.

In questo paragrafo introduciamo i concetti di diametro, calibro (girth) e numero cromatico, i quali costituiscono tre fra i più importanti parametri numerici associati un grafo (connesso e semplice).

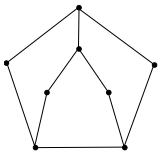
Diametro. Sia Γ un grafo connesso, e siano u, v vertici di Γ; definiamo la *distanza* tra u e v come la lunghezza minima di un cammino tra v e w, e la denotiamno con $d_\Gamma(u, v)$. Il *diametro* di un grafo connesso $\Gamma = (V, E, \phi)$ è la massima distanza che intercorre tra i suoi vertici:

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

Assegnata in questo modo una distanza sul grafo connesso Γ, risulterà utile il concetto di *palla* e di *sfera*. Si tratta di quello familiare: per ogni $v|V$ e $1 \leq k \in \mathbb{N}$ so definisce la palla di centro v e raggio k come l'insieme

$$B_\Gamma(v,k) = \{x \in V \mid d(_\Gamma(v,x) \leq k\}$$

Esercizio 1.23. Si determini il diametro del seguente grafo. Qual è il minimo numero di lati che occorre aggiungere in modo da ottenere un grafo di diametro 2?



Chiaramente, ogni grafo completo K_n ha diametro 1; anzi, un grafo semplice è completo se e soltanto sa ha diametro 1. Quando però si passa a considerare grafi semplici connessi di diametro almeno 2 la faccenda si complica notevolmente: non è possibile dare una classificazione soddisfacente nemmeno per qualli di diamtro 2, anche assumendone la regolarità (vedi parafgrafi 2.1 e 2.4).

Esercizio 1.24. Per ogni $n \geq 2$, sia $I_n = \{1, 2, \ldots, n\}$. Sia quindi $B_n = (V, E)$ il grafo semplice con $V = I_n$, e per $a, b \in V$, $\{a, b\} \in E$ se e solo se $a - b$ è dispari. Si provi che B_n è connesso, che ha diametro 2, e che è regolare se e soltanto se n è pari.

Esercizio 1.25. Sia Γ un grafo semplice connesso e finito, e sia v un vertice fissato di Γ. Si provi che Γ ammette uno spanning–tree A tale che $d_\Gamma(v,x) = d_A(v,x)$ per ogni altro vertice x di Γ.

Esercizio 1.26. Costruire un grafo semplice con sette vertici e diametro quattro, che abbia il massimo numero di archi possibile.

Calibro. Sia Γ un grafo semplice; si chiama **calibro** di Γ (in inglese: *girth*) la lunghezza minima di un ciclo non banale contenuto in Γ; esso è di solito denotato con $g = g(\Gamma)$. Ad esempio, un grafo completo con almeno 3 vertici (o comunque un grafo che contenga un trianglo) ha calibro 3, mentre il grafo dul cubo (figura 1.5) ha calibro 4; il grafo di Petersen ha calibro 5 (lo si verifichi). Per quanto riguarda gli alberi (che non hanno alcun ciclo), si conviene di dire che non hanno calibro, oppure (come preferiamo) che hanno calibro infinito. Il concetto opposto (ma, forse, meno importante) è quello di *circonferenza* di un grafo Γ, che indica la lunghezza massima di un ciclo di Γ.

Esercizio 1.27. Sia Γ un grafo connesso di diametro q e calibro g. Si provi che $g \leq 2q + 1$.

Esercizio 1.28. Costruire un grafo semplice con sette vertici e calibro tre con il massimo numero di lati. Stesso problema per un grafo con sette vertici e calibro quattro.

Esercizio 1.29. Costruire un grafo semplice con 8 lati, calibro 4, ed il minimo numero possibile di vertici (a meno di isomorfismo ci sono due grafi possibili).

Numero cromatico. Una *colorazione* (dei vertici) di un grafo Γ è una assegnazione di un colore a ciascun vertice di Γ in modo che vertici adiacenti non abbiano lo stesso colore (in altri termini: in modo che gli estremi di ogni lato siano colorati con colori diversi). Detto in modo formale, una colorazione di $\Gamma = (V, E, \phi)$ è una applicazione $\gamma : V \to S$, dove S è un insieme non vuoto (i cui elementi sono detti *colori*), tale che per ogni $u, v \in V$, se u e v sono adiacenti allora $\gamma(u) \neq \gamma(v)$.

Sia $1 \leq k \in \mathbb{N}$; un grafo Γ si dice k-colorabile se esiste una colorazione di Γ con k colori. Banalmente, un grafo è 1-colorabile se e solo se non contiene alcun arco. Un grafo è 2–colorabile se l'insieme dei suoi vertici si può decomporre come l'unione di due sottoinsiemi disgiunti tali che nessun arco ha entrambi gli estremi appartenenti allo stesso sottoinsieme (vedi paragrafo seguente). Più in generale, è chiaro che un dire che un grafo è k-scolorabile equivale a dire che ammette una k-partizione dell'insieme dei vertici con tale proprietà.

Un problema di colorazione è quello che forse è il problema più diffusamente nota di teoria dei grafi, ovvero quella della colorazione di una carta geografica politica (che, per brevità, conveniamo di chiamare "mappa"): qual è il minimo numero di colori distinti necessario per colorare una mappa in modo che non vi siano nazioni confinanti dello stesso colore? Per dare un senso a questa affermazione, dobbiamo accennare al concetto di grafo planare. Un grafo $\Gamma = (V, E, \phi)$ è un *grafo piano* se V è un sottoinsieme di punti del piano euclideo $\mathbb{R}^2$ ed E un insieme di archi di curva continua i cui estremi appartengono a V; un grafo si dirà quindi *planare* se è isomorfo ad un grafo piano. Dunque, potremmo dire che un grafo è planare se può essere disegnato su un piano in modo che le linee che rappresentano i suoi lati non si intersecano. Ora, è facile tradurre il problema della mappa in termmini di grafi: ad una data mappa si associa un grafo i cui vertici sono le diverse nazioni e due vertici sono adiacenti se e solo se le corrispondenti nazioni sono confinanti.

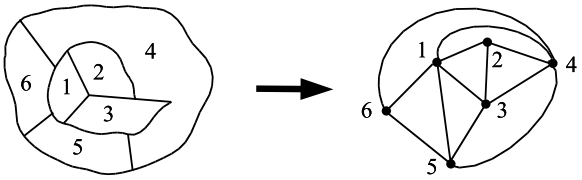


Figura 1.11: una mappa e il suo grafo.

È intuitivo, e non è difficle da provare, che il grafo così ottenuto è un grafo planare (avendo ovviamente definito con precisione cosa si intende con "mappa"). La domanda diventa allora la seguente: qual è il minimo numero di colori con cui è possibile colorare i vertici di un grafo piano? La congettura che siano sempre sufficienti quattro colori ha una storia quasi mitica; comunque, pare (si veda Biggs, Lloyd e Wilson, *Graph Theory 1736–1936*) sia stata esplicitamente formulata per la prima volta da un certo Francis Guthrie, che, tramite il fratello, l'avrebbe comunicata ad Augustus de Morgan, suo professore di matematica al University College di Londra[1]. Mentre dimostrare che cinque colori sono sempre sufficienti (Heawood

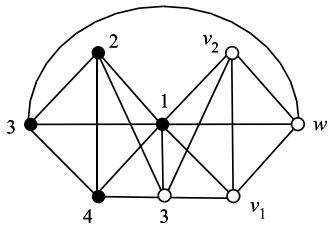
[1]Se poi qualche cinese, o turco, o indiano, per non dire una donna, l'abbia pensata prima e magari l'abbia anche messa per iscritto è una questione che non ha rilevanza per la storiografia occidentale.

1890) è oggi relativamente semplice, la congettura dei quattro colori ha resistito (nonostante numerosi tentativi in entrambi i sensi) sino al 1976 quando è stata provata da Appel e Haken ed è quindi diventata il *Teorema dei quattro colori*[2] (si osservi che la mappa della figura 1.11 richiede effetivamente quattro colori), che può dunque essere formulato nel modo seguente

Teorema 1.8. *Ogni grafo planare è 4-colorabile.*

Dopo questa digrassione, torniamo a considerazioni di carattere generale. È ovvio che ogni grafo finito Γ ammette una colorazione con un numero finito di colori, ed è altresì ovvio che esiste un numero *minimo* di colori mediante i quali è possibile colorare Γ: tale numero è detto **numero cromatico** di Γ e si indica con $\chi(\Gamma)$. Dunque, dato un grafo Γ, $\chi(\Gamma) = k$ se e solo se Γ è k-colorabile e non è $(k-1)$-colorabile.
Ad esempio, è chiaro che $\chi(K_n) = n$ (dove K_n è il grafo completo con n vertici), ed è piutosto facile vedere che, se C_n è il ciclo di lunghezza n, allora $\chi(C_n)$ è uguale a 2 o a 3 a seconda che n sia pari o dispari (lo si dimostri).

Per provare che un grafo Γ ha numero cromatico k, occorre in sostanza provare due cose: che esiste una colorazione di Γ mediante k colori, e che non è possibile colorare Γ con meno di k colori. Consideriamo, ad esempio il seguente grafo



la figura mostra una possibile colorazione con 5 colori (rappresentati da numeri), dove i vertici v_1, v_2, w hanno, ripettivamente, colori 4, 2 e 5. Supponiamo ora di voler colorare il grafo con 4 colori $\{1, 2, 3, 4\}$; allora è chiaro che, essendo a due a due adiacenti, i vertici segnati in nero devono avere colori diversi, che indichiamo con $1, 2, 3, 4$ come nella figura. Il vertice in basso al centro, adiacente ai vertici già colorati con $1, 2, 4$ deve pertanto avere colore 3 (come nella figura). Ora, i vertici v_1 e v_2 non possono essere colorati con 3 e nemmeno con 1, inoltre devono avere colori diversi; quindi i loro colori devono essere 2 e 4, il che forza ad assegnare al vertice w il colore 3, e questo non è consentito dato che w è adiacente al vertice di colore 3 all'estremità sinistra del grafo.

Esercizio 1.30. Si determini il numero cromatico dei grafi dei solidi regolari (figura 1.5).

Chiaramente, il numero cromatico di un grafo è maggiore o uguale a quello di ogni suo sottografo; e, come anche suggerito dall'esempio di sopra, un limite inferiore al numero cromatico di un grafo è certamente dato dall'esistenza di sottografi completi: se infatti Γ contiene un sottografo isomorfo al grafo completo K_n, allora $\chi(\Gamma) \geq \chi(K_n) = n$. D'altra

[2] La dimostrazione ha richiesto un impiego massiccio del calcolatore, e non potrebbe essere verificata da esseri umani (nemmeno se ci si mettesse tutti insieme a lavorare per qualche anno); pertanto è stata ed è oggetto di una certa discussione.

parte, tale limite è in generale lontano dall'effettivo valore di $\chi(\Gamma)$: esistono grafi privi di triangoli il cui numero cromatico è arbitrariamente grande (si veda l'esercizio 1.56 e seguenti). Più in generale, Erdös e Lovász hanno dimostrato, con metodi probabilistici, che per ogni $k, g \geq 4$ esiste un grafo con calibro g e numero cromatico k. Una degli obiettivi di questo corso sarà (se ne avremo il tempo) di fornire una costruzione esplicita di grafi con questa proprietà.

Esercizio 1.31. Si provi che un grafo semplice con dieci vertici e numero cromatico 4 contiene almeno un triangolo.

Esercizio 1.32. Si provi che il grafo di Grötzsch (figura sotto) ha numero cromatico 4.

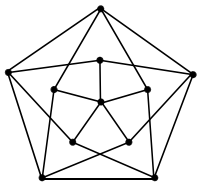


Figura 1.12: il grafo di Grötzsch.

Non è molto complicato descrivere un algoritmo che, dato un grafo Γ ne fornisce una colorazione (pur se in genere non ottimale). Si comincia col fissare un ordinamento qualsiasi $v_1, v_2, v_3, \ldots$ ai vertici di Γ, e si considerano i colori $1, 2, 3, \ldots$. Si assegna colore 1 al vertice v_1, e colore 2 o 1 al vertice v_2 a seconda che sia o no adiacente a v_1; dopo di che si procede scorrendo la lista dei vertici ed assegnando ad ogni nuovo vertice il primo colore dell'elenco che sia ammissibile. In questo modo si ottiene certamente una colorazione di Γ, che tuttavia non è in generale realizzata con il minimo numero possibile di colori; dato che il numero di colori necessario dipende fortemente dalla scelta iniziale dell'ordinamento dei vertici. Ma non è possibile fare molto meglio; ed algoritmi che diano una colorazione ottimale, e quindi forniscano anche il valore esatto del numero cromatico del grafo, non sono noti.
Tuttavia, il semplice algoritmo che abbiamo descritto ci consente di fare un'osservazione non del tutto banale. Per esporla meglio, fissiamo la seguente notazione: se Γ è un grafo, indichiamo con $\Delta(\Gamma)$ il *massimo dei gradi* dei vertici di Γ.
Immaginiamo quindi di operare mediante l'algoritmo di sopra su un grafo Γ, e supponiamo di avere a disposizione un insieme S di colori abbastanza grande. Notiamo allora che ad ogni passo i primi $\Delta(\Gamma) + 1$ colori di S saranno sufficienti a procedere; infatti ad ogni nuovo vertice v è assegnato il primo colore ammissibile, ovvero il primo colore diverso da quelli di ogni vertice già colorato a cui v sia adiacente. Ora, il grado di v è al più $\Delta(\Gamma)$, e quindi ci sono al più $\Delta(\Gamma)$ colori che non possiamo assegnare; dunque almeno un colore tra i primi $\Delta(\Gamma) + 1$ che abbiamo a disposizione è ammissibile, e possiamo procedere. In conclusione, l'algoritmo descritto colora Γ con al più $\Delta(\Gamma) + 1$ colori. In altre parole abbiamo provato

$$\textit{Sia } \Gamma \textit{ un grafo; allora } \chi(\Gamma) \leq \Delta(\Gamma) + 1.$$

I grafi completi K_n ed i cicli di lunghezza dispari C_{2n+1} sono esempi di grafi Γ il cui numero cromatico è uguale a $\Delta(\Gamma) + 1$. Il Teorema seguente (che non dimostriamo) mostra come essi siano essenzialmente i soli grafi con tale proprietà.

Teorema 1.9. (Brooks 1941) *Sia* Γ *un grafo connesso che non sia un ciclo di lunghezza dispari o un grafo completo. Allora* $\chi(\Gamma) \leq \Delta(\Gamma)$.

Esercizio 1.33. Sia $\Gamma = (V, E)$ un grafo semplice e sia $c = \chi(\Gamma)$ il suo numero cromatico. Si provi che $|E| \leq \binom{c}{2}$.

1.5 Grafi bipartiti.

Un grafo il cui numero cromatico è 2, si dice **bipartito**. In altre parole, un grafo è bipartito se esiste un partizione $V = A \cup B$, dell'insieme V dei vertici, in due sottoinsiemi non vuoti (e disgiunti) tale che gli estremi di nessun lato giacciono in uno stesso insieme della partizione (quindi ogni lato congiunge un vertice in A con un vertice in B). Quella dei grafi bipartiti è un'altra importante classe di grafi utile nelle applicazioni: in particolare per i cosiddetti problemi di assegnazione. Non approfondiremo questo aspetto, ma tratteremo brevemente i grafi bipartiti poichè diverse delle famiglie che cotruiremo più avanti saranno costituite da grafi di questo tipo.

Abbiamo già incontrato grafi bipartiti in alcune occasioni; ad esempio sono bipartiti i grafi dell'esercizio 1.24. Negli esercizi 1.54 e 1.55 tratteremo poi i grafi bipartiti completi.
Di fatto, i grafi bipartiti sono più di quelli che a prima vista si direbbe guardando qualche diagramma. Ad esempio il grafo del cubo è bipartito: la figura che segue mostra una possibile partizione dei vertici.

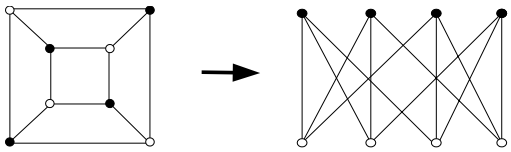
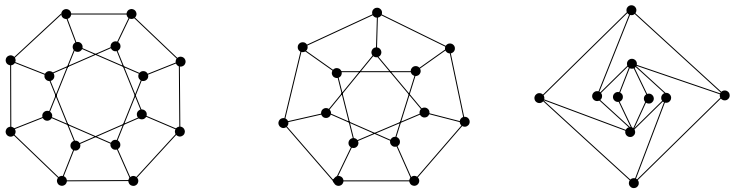


Figura 1.13: bipartizione del cubo.

Esercizio 1.34. Si dica quali tra i seguenti grafi sono bipartiti:



Mentre è chiaro che un grafo che contiene un triangolo o un pentagono (cioè un 5-ciclo) non è bipartito, e dunque gli altri grafi dei solidi platonici non sono bipartiti. Ogni albero è bipartito; questa affermazione è una conseguenza del prossimo Teorema, si cerchi tuttavia di provarla per esercizio facendo induzione sul numero di vertici.

Teorema 1.10. *Un grafo con almeno due vertici è bipartito se e solo se non contiene cicli di lunghezza dispari.*

Alla dimostrazione premettiamo la seguente osservazione (ricordando che una *passeggiata* di lunghezza n in un grafo è una sequenza $v_0\ e_1\ v_1\ e_2\ v_2 \dots v_{n-1}\ e_n\ v_n$, di vertici e lati, sottoposta alla sola condizione che ogni lato e_i congiunge i vertici v_{i-1} e v_i).

Lemma 1.11. *Un grafo in cui è possibile trovare una passeggiata chiusa di lunghezza dispari ha un ciclo di lunghezza dispari.*

Dimostrazione. Sia $\mathcal{P}:\ u = v_0\ e_1\ v_1\ e_2\ v_2 \dots v_{n-1}\ e_n\ v_n = u$ una passeggiata chiusa di lunghezza dispari n in Γ, e procediamo per induzione su n (chiaramente $n \geq 3$). Se $\mathcal{P}$ è un ciclo (cosa che, in particolare, avviene se $n = 3$) non c'è nulla da provare. Supponiamo quindi che $n \geq 5$ e che $\mathcal{P}$ non sia un ciclo. Allora vi sono in essa almeno due vertici ripetuti (di cui almeno uno non agli estremi), diciamo $v_i = v_j$, con $0 \leq i < j \leq n$ (e $(i,j) \neq (0,n)$). Se $j - i$ è pari, allora la passeggiata chiusa

$$u = v_0\ e_1\ v_1\ e_2\ v_2\ \dots\ v_i\ e_{j+1}\ v_{j+1}\ \dots\ v_{n-1}\ e_n\ v_n = u$$

ha una lunghezza dispari strettamente minore di quella di $\mathcal{P}$, e dunque concludiamo per ipotesi induttiva che esiste un ciclo di lunghezza dispari in Γ. Se invece $j - i$ è dispari, allora

$$v_i\ e_{i+1} v_{i+1} \dots\ v_{j-1}\ e_j\ v_j = v_i$$

è una passeggiata chiusa di lunghezza dispari strettamente inferiore ad n, e di nuovo si conclude applicando l'ipotesi induttiva. ∎

Dimostrazione del Teorema 1.10 Possiamo chiaramente assumere che Γ sia connesso.
Se Γ è bipartito sull'insieme $V = A \cup B$ di vertici, allora i vertici di ogni ciclo di Γ, nell'ordine in cui compaiono nel ciclo, appartengono alternativamente ai due insiemi disgiunti A e B. Poiché il ciclo si deve chiudere allo stesso vertice da cui inizia, si conclude che il numero dei suoi lati (cioè di 'salti' tra A e B) deve essere pari.
Viceversa, supponiamo che Γ non contenga cicli di lunghezza dispari. Poiché Γ è connesso, per ogni coppia a e b di vertici è definita la distanza $d_\Gamma(a,b)$. Sull'insieme V dei vertici di Γ definiamo una relazione $\sim$ ponendo $a \sim b$ se $d_\Gamma(a,b)$ è pari. Chiaramente, la relazione $\sim$ è riflessiva e simmetrica. Supponiamo che per $a, b, c \in V$ sia $a \sim b$ e $b \sim c$. Allora esistono due cammini semplici di lunghezza pari, $\mathcal{C}_2$ e $\mathcal{C}_1$, rispettivamente tra a e b, e tra b e c. Supponiamo, per assurdo, che la distanza tra a e c sia dispari; allora esiste un cammino semplice $\mathcal{C}_3$ tra c e a di lunghezza dispari. Percorrendo di seguito i cammini $\mathcal{C}_1$, $\mathcal{C}_2$ e $\mathcal{C}_3$ si ottiene una passeggiata chiusa di lunghezza dispari. Per il Lemma 1.11 esiste allora un ciclo di lunghezza dispari in Γ, e questo contraddice l'ipotesi su Γ. Dunque $\sim$ è una relazione d'equivalenza su V.
Sia ora $e = \{a, b\}$ un lato di Γ (esiste perché Γ ha almeno due vertici ed è connesso), e siano, rispettivamente A e B le classi di equivalenza di a e di b. Poiché $a \not\sim b$, $A \cap B = \emptyset$. Sia $u \in V$, e supponiamo, per assurdo, che u abbia distanza dispari sia da a che da b. Siano $\mathcal{C}_1$ e $\mathcal{C}_2$ cammini di lunghezza minima, rispettivamente tra a e u, e tra u e b. Percorrendo di seguito C_1, C_2 ed il lato e, si ottiene allora una passeggiata chiusa di lunghezza dispari che inizia e termina in a, il che per l'ipotesi su Γ ed il Lemma 1.11, è una contraddizione. Dunque u ha

distanza pari o da a o da b, e dunque $u \in A \cup B$. Pertanto $V = A \cup B$. Chiaramente, infine, nessun lato di Γ congiunge vertici che stanno entrambi in A o in B (perché in tal caso questi avrebbero distanza 1 e non sarebbero quindi in relazione). In conclusione, Γ è bipartito negli insiemi di vertici A e B. ∎

Esercizio 1.35. Sia Γ un grafo connesso e bipartito. Si provi che esiste una sola partizione dell'insieme V dei vertici rispetto alla quale Γ è bipartito.

Esercizio 1.36. Sia $\Gamma = (V_1 \cup V_2, E)$ un grafo bipartito regolare k-valente con almeno 3 vertici. Si provino le seguenti affermazioni:

1) $|V_1| = |V_2|$;

2) Se $k = 2$, allora ogni componente connessa di Γ è un ciclo di lunghezza pari;

3) Se Γ è connesso, allora $\Gamma - e$ è connesso per ogni lato $e \in E$.

1.6 Altri esercizi.

1. Cicli.

Esercizio 1.37. Sia $\Gamma = (V, E)$ un grafo connesso e tale che $\sum_{v \in V} d_\Gamma(v) > 2|V|$. Si provi che Γ ha almeno due cicli distinti (che differiscano, cioè, per almento un vertice).

Esercizio 1.38. Sia Γ un grafo connesso con n vertici, e sia $3 \leq k \leq n$. Assumendo che per ogni coppia di vertici v, w non adiacenti di Γ sia $d_\Gamma(v) + d_\Gamma(w) \geq k$, provare che Γ ha un ciclo di lunghezza almeno $\frac{k+2}{2}$.

Esercizio 1.39. Per $1 \leq n \in \mathbb{N}$, sia

$$h(n) = \frac{n(n-1)}{2} - (n-3) = \frac{n^2 - 3n + 6}{2}.$$

Sia $\Gamma = (V, E)$ un grafo con n vertici; si provi che se $|E| \geq h(n)$ allora Γ è hamiltoniano.

Esercizio 1.40. Sia Γ un grafo connesso e tale che data una qualsiasi terna di vertici di Γ esiste almeno un lato che congiunge due vertici della terna. Si dica se è vero che Γ è hamiltoniano.

Esercizio 1.41. Si dica quali tra i grafi B_n definiti nell'esercizio 1.24 sono euleriani. Provare che B_n è hamiltoniano se e soltanto se n è pari.

2. Line–graph. Dato un grafo semplice $\Gamma = (V, E)$, definiamo il grafo $L(\Gamma) = (V_c, E_c)$ (detto *line graph* associato a Γ) nel modo seguente. I vertici di $L(\Gamma)$ sono i lati di Γ (cioè $V_c = E$), e due elementi $e, e' \in E$ sono congiunti da un lato di $L(\Gamma)$ se e solo se hanno un vertice in comune (cioè se $e \cap e' \neq \emptyset$).

Esercizio 1.42. Si provi che se Γ è privo di punti isolati, allora $L(\Gamma)$ è connesso se e solo se Γ è connesso.

Esercizio 1.43. Dato un grafo Γ, sia $L(\Gamma)$ il grafo descritto nell'esercizio 1.42. Si provi che se Γ è euleriano, allora $L(\Gamma)$ è euleriano.

Esercizio 1.44. Con le notazioni di sopra, si provi che

$$|E_c| = \frac{1}{2}\sum_{v\in V} d_\Gamma(v)(d_\Gamma(v)-1).$$

Si provi quindi che Γ è isomorfo a $L(\Gamma)$ se e soltanto se Γ è un ciclo C_n, dove $n = |V|$.

3. Grafi di Kneser. Siano $1 \leq k < n$, con $n \geq 2k$. Il grafo di *Kneser* $K(n,k)$ è il grafo semplice i cui vertici sono tutti i sottoinsiemi di cardinalità k dell'insieme $\{1,2,3,\ldots,n\}$ (quindi il numero dei vertici è $\binom{n}{k}$), e due vertici sono adiacenti se e solo se la loro intersezione è vuota.

Esercizio 1.45. Si provi che il grafo di Kneser $K(5,2)$ è isomorfo al grafo di Petersen.

Esercizio 1.46. È vero che i grafi di Kneser sono regolari? Dati $2 \leq k$ e $n \geq 3k+1$, si determini il calibro del grafo di Kneser $K(n,k)$. [Si distinguano i tre casi: $n = 2k+1$, $2k+1 < n < 3k$, $n \geq 3k$]

Esercizio 1.47. Siano $k \geq 2$, $n \geq 2k+1$, e $K = K(n,k)$ il grafo di Kneser. Si provi che $\chi(K) \leq n - 2k + 1$. [sugg. interpretando i vertici di K come i sottoinsiemi di cardinalità k dell'insieme $\{1,2,\ldots,n\}$, si assegni un primo colore ai vertici che contengono 1, un secondo colore a quelli che contengono 2 ma non 1 ...]

Esercizio 1.48. Si provi che il grafo di Kneser $K(6,2)$ ha numero cromatico 4.

4. n-Cubi. Dato $n \geq 2$, il grafo Q_n (detto n-cubo) è il grafo i cui vertici sono le n-uple a coefficienti in $\{0,1\}$, ed i cui lati sono tutte e sole le coppie di tali n-uple che differiscono esattamente per una componente.

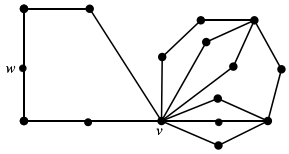
Esercizio 1.49. Per ogni $n \geq 2$ si determini il numero di archi, il diametro e il calibro di Q_n.

Esercizio 1.50. Si provi che, per ogni $n \geq 2$, Q_n è hamiltoniano.

Esercizio 1.51. Si provi che, per ogni $n \geq 2$, il n-cubo Q_n è un grafo bipartito.

5. Grafi casualmente euleriani. Il piano di un museo o di una esposizione può facilmente essere rappresentato mediante un grafo, i cui lati sono le varie gallerie o corridoi del museo, ed i vertici sono le congiunzioni di due o più gallerie. Un visitatore che sia interessato a esaminare l'intera collezione dovrà percorrere almeno una volta tutte le gallerie del museo (archi del grafo), e presumibilmente vorrà percorrerne ciascuna soltanto una volta. In termini del grafo sopra descritto, ciò è possibile se e soltanto se esso ammette un cammino euleriano tra i vertici corrispondenti all'entrata ed all'uscita del museo; nel caso in cui l'entrata e l'uscita coincidano, se e solo se si tratta di un grafo euleriano. In tal caso, la direzione del museo potrebbe fornire una mappa con l'indicazione del circuito euleriano. Ma se tali mappe fossero momentaneamente esaurite, quello che il nostro visitatore auspicherebbe è di

poter comunque effettuare una visita "euleriana" mediante la semplice strategia di scegliere casualemte un nuova galleria (lato del grafo) ad ad ogni congiunzione (vertice) con la sola condizione che questa non sia già stata percorsa in precedenza. Naturalmente, ciò è possibile solo se il grafo del museo gode di proprietà piuttosto forti; ed è quello che viene chiamato un grafo casualmente euleriano (si tratta della solita pessima traduzione dell'inglese *randomly eulerian graph*). Più precisamente, se Γ è un grafo semplice e v un suo vertice, Γ si dice *casualmente euleriano* per v se ogni circuito massimale di Γ che includa il vertice v è un circuito euleriano (ci si convinca che questa definizione, posto v il vertice di entrata–uscita del museo, è equivalente a quella più "operativa" data di sopra). La figura seguente è un esempio di grafo casualmente euleriano per v.



Esercizio 1.52. Sia Γ un grafo e v un suo vertice. Si provi che Γ è casualmente euleriano per v se e solo se Γ è euleriano e ogni ciclo di Γ contiene v.

Esercizio 1.53. Sia Γ_0 una foresta. Si costruisca un grafo Γ aggiungendo un nuovo vertice v a Γ_0, e congiungendo v con tutti e soli i vertici di grado dispari di Γ_0. Si provi che Γ è un grafo casualmente euleriano per v.

6. Grafi bipartiti completi. Siano n, m interi maggiori o uguali ad 1. Il grafo *completo bipartito* $K_{n,m} = (V, E)$ è il grafo semplice definito nel modo seguente: l'insieme dei vertici $V = V_1 \cup V_2$ è unione disgiunta di due sottoinsiemi di ordine ripettivamente n ed m, ed i lati in E sono tutti e soli quelli che congiungono vertici di V_1 con vertici in V_2; ovvero $E = \{\{u, v\} \mid u \in V_1,\, v \in V_2\}$.

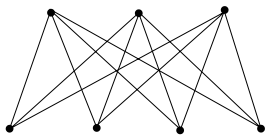


Figura 1.14: $K_{4,3}$

Esercizio 1.54. Dati $1 \leq n, m \in \mathbb{N}$, dire quanti archi ha $K_{n,m}$? Si discuta, al variare di n ed m l'esistenza di un cammino o di un circuito euleriano in $K_{n,m}$.

Esercizio 1.55. Si provi che $K_{n,m}$ è hamiltoniano se e soltanto se $n = m$. Si provi che se $|n - m| = 1$ allora $K_{n,m}$ ha un cammino (ma non un circuito) hamiltoniano.

7. Grafi privi di triangoli e numero cromatico arbitrario. Sia $n \geq 1$ e K_n il grafo completo su un insieme V di n vertici. L'insieme degli archi di K_n è quindi $V^{[2]}$. Sia $1 \leq k \in \mathbb{N}$; con

k-colorazione degli archi di K_n intendiamo una partizione dell'insieme degli archi $V^{[2]}$ in k classi disgiunte (senza nessun altra condizione).
Gli esercizi 1.56 e 1.59 che seguono sono casi particolari dei Teoremi di Ramsey.

Esercizio 1.56. Sia $k \geq 1$. Si provi che esiste un valore $R(k) \in \mathbb{N}$ tale che per ogni $n \geq R(k)$ ed ogni k-colorazione degli archi di K_n esiste in K_n un triangolo monocromatico (cioè un triangolo costituito da archi dello stesso colore). *Suggerimento*: chiaramente $R(1) = 3$; si proceda per induzione su k; sia v un vertice di K_n; se n è sufficientemente grande ci sono $R(k-1)$ archi incidenti a v che hanno il medesimo colore; si consideri il sottografo Γ indotto dai vertici estremi di tali archi e diversi da v; allora $\Gamma \simeq K_{R(k-1)} \dots$

Esercizio 1.57. Dato $n \geq 3$, sia $I_n = \{1, 2, \dots, n\}$. Definiamo un grafo Γ_n il cui insieme dei vertici è l'insieme $I_n^{[2]}$ di tutti i sottoinsiemi di ordine 2 di I_n, e una coppia $\{\{a, b\}, \{c, d\}\}$ di essi è un lato se e solo se $a < b = c < d$. Si provi che Γ_n è privo di triangoli, e che, se $n \geq 5$, $g(\Gamma_n) = 4$.

Esercizio 1.58. Utilizzando il risultato dell'esercizio 1.56 si provi che, per ogni $c \geq 1$, se n è sufficientemente grande allora il numero cromatico $\chi(\Gamma_n)$ del grafo definito nell'esercizio precedente è maggiore di c.

Esercizio 1.59. Si estenda il risultato ottenuto nell'esercizio 1.56. provando che, per ogni $m \geq 3$ ed ogni $k \geq 1$, esiste un intero $R = R(m, k)$ tale che data qualsiasi k–colorazione degli archi di K_R, esiste un sottografo monocromatico isomorfo a K_{n_i}.

Capitolo 2

Teoria Algebrica dei Grafi

2.1 Grafi regolari.

Ricordo che un grafo Γ si dice *regolare* se i suoi vertici hanno tutti lo stesso grado; se tale grado comune è uguale a d si dice che Γ è un grafo d-regolare. Sono, ad esempio, regolari tutti i grafi completi K_n ed i grafi dei poliedri regolari (figura 1.7).

È chiaro che un grafo è 1-regolare se e soltanto se ogni sua componente connessa è composta da due vertici ed un solo lato (un grafo di questo tipo si chiama anche un 1-*fattore*). Anche i grafi 2-regolari si descrivono facilmente: infatti un grafo connesso è 2-regolari se e soltanto se è un ciclo (vedi esercizio 1.7, per dimostrarlo si provi ad esempio a considerare un cammino massimale in un grafo connesso 2-regolare e che cosa se ne può dire). Dunque un grafo è 2-regolare se e soltanto se ogni sua componente connessa è un ciclo.
Quindi, il primo caso significativo è quello dei grafi 3-regolari, che com'è consuetudine chiameremo *grafi cubici*. Di fatto è molto più che un caso "significativo": la complessità della classe dei grafi cubici è notevole, ed è frequente che un problema difficile in teoria dei grafi rimanga difficile anche se ci si limita a considerare i grafi cubici. Esempi di grafi cubici sono i grafi del tetraedro, del cubo, del dodecaedro, e il grafo di Petersen.
Sia $\Gamma = (V, E)$ un grafo cubico semplice; usando la formula del Teorema 1.1 si ottiene $3|V| = 2|E|$; in particolare il numero di vertici di un grafo cubico (o, più in generale, di un grafo regolare di valenza dispari) è pari.

Esercizio 2.1. Per ogni $n \geq 3$ si trovi un grafo cubico semplice e connesso con $2n$ vertici[1].

Sia $v \in V$ un vertice del grafo connesso Γ, e sia $0 \leq q$ un numero intero; la *palla* $B_\Gamma(v, q)$ di raggio q e centro v è l'insieme di tutti i vertici di Γ la cui distanza da v non supera q; ovvero

$$B_\Gamma(v, q) = \{w \in V \mid d_\Gamma(v, w) \leq q \}.$$

[1] Il numero di grafi cubici (a meno di isomorfismo) è stato determinato fino a 40 vertici; ad esempio, il numero di grafi cubici rispettivamente con $10, 12, 14$ e 16 vertici è $21, 94, 540, 4207$; i grafi cubici con 40 vertici sono circa 8×10^{18}. Sono cubici anche i grafi di alcune interessantissime molecole composte da atomi di carbonio, come i fullereni: assomigliano ai vecchi palloni da calcio, e potete vederle, ad esempio, al sito http://www.sussex.ac.uk/Users/kroto/FullereneCentre/main.html

Quindi, $B_\Gamma(v,0) = \{v\}$ e, se d è il grado di v, $B_\Gamma(v,1)$ contiene esattamente $d+1$ elementi.

Lemma 2.1. *Sia $\Gamma = (V,E)$ un grafo semplice connesso k-regolare. Allora, per ogni $v \in V$ ed ogni $q \geq 1$*

$$|B_\Gamma(v,q)| \leq 1 + d \cdot \frac{(k-1)^q - 1}{k-2}.$$

In particolare, se Γ è cubico, $|B_\Gamma(v,q)| \leq 1 + 3(2^q - 1)$.

DIMOSTRAZIONE. Procedendo per induzione su q proviamo che il numero di vertici di Γ la cui distanza da v è esattamente q è al più $k(k-1)^{q-1}$.
Per $q = 1$ la cosa è ovvia, dato che v ha grado $k = k(k-1)^0$.
Sia $q \geq 2$. Osserviamo che ogni vertice la cui distanza da v è uguale a q è adiacente ad un vertice la cui distanza da v è uguale a $q-1$; inoltre ogni vertice w a distanza $q-1$ da v è adiacente ad almeno un vertice di distanza minore, e pertanto, avendo grado d, w può essere adiacente ad al più $(k-1)$ vertici di distanza q da v. Poiché il numero di vertici di siatnza $q-1$ è, per ipotesi induttiva, minore o uguale a $d(d-1)^{q-2}$, si ricava che il numero di vertici a distanza q da v è al più $k(k-1)^{q-2}(k-1) = k(k-1)^{q-1}$, che è quello che si voleva.
A questo punto, siccome la palla $B_\Gamma(v,q)$ è costituita da tutti i vertici la cui distanza da q è compresa tra 0 è q, si ha

$$|B_\Gamma(v,q)| \leq 1 + k + k(k-1) + k(k-1)^2 + \cdots + k(k-1)^{q-1} = 1 + k \cdot \frac{(k-1)^q - 1}{k-2}$$

che è l'enunciato del Lemma. ∎

Un'immediata conseguenza è il seguente risultato. Ricordiamo che il diametro di un grafo è la massima distanza tra due vertici del grafo stesso.

Corollario 2.2. *Sia $\Gamma = (V,E)$ un grafo connesso k-regolare (con $k \geq 3$) di diametro q. Allora,*

$$|V| \leq 1 + k \cdot \frac{(k-1)^q - 1}{k-2}.$$

In particolare, un grafo regolare k-valente di diametro 2 ha al più $k^2 + 1$ vertici; e un grafo cubico di diametro q ha al più $1 + 3(2^q - 1)$ vertici.

Esercizio 2.2. Sia Γ un grafo k-regolare, di diametro q e $1 + k \cdot \frac{(k-1)^q - 1}{k-2}$ vertici. Si provi che per ogni coppia di vertici x, y esiste in Γ uno ed un unico cammino che congiunge x a y la cui lunghezza è minore o uguale a q. Si provi quindi che $g(\Gamma) = 2d + 1$ (grafi di questo tipo sono detti grafi di Moore, e torneremo più diffusamente su di essi nel paragrafo 2.4).

Esercizio 2.3. Avvalendosi di una opportuna variante del Lemma 2.1, si provi che il Corollario 2.2 sussiste sostituendo l'ipotesi che Γ sia regolare con quella che k sia il massimo fra i gradi dei vertici di Γ. Si osservi poi che l'eguaglianza nell'enunciato si può verificare solo nel caso di grafi regolari.

Ricordo che il calibro $g(\Gamma)$ di un grafo Γ è la lunghezza minima di un ciclo contenuto in Γ. Analogamente a quanto provato per il diametro nel Corollario 2.2, anche il valore del calibro di un grafo regolare implica un limite al numero dei vertici (ma in questo caso la limitazione che si ottiene è inferiore).

Proposizione 2.3. *Sia $\Gamma = (V, E)$ un grafo semplice k-regolare con calibro $g \geq 3$, e poniamo $e = [(g-1)/2]$ (la parte intera). Allora*

$$|V| \geq 1 + k \cdot \frac{(k-1)^e - 1}{k-2}.$$

DIMOSTRAZIONE. La dimostrazione sfrutta idee analoghe a quelle utilizzate per quella del Lemma 2.1, e si invita il lettore a cercare di esporla rigorosamente. Fissato un vertice v di Γ, si tratta di provare che due vertici $u_1 \neq u_2$ tali che le loro distanze da v non superano il valore $e-1$ (dove e è quello nell'enunciato)) non possono essere adiacenti ad uno stesso vertice (che non sia eventualmente v), perché in tal caso si troverebbe un ciclo la cui lunghezza viola il limite inferiore imposto dal calibro g. Tenendo conto della regolarità di Γ, con un semplice passo induttivo si prova quindi che, per $1 \leq k \leq e$, il numero di vertici di Γ la cui distanza da v è k è $k(k-1)^{k-1}$. Procedendo poi come nella dimostrazione del Lemma 2.1 si trova che $|B_\Gamma(v, e)| = 1 + k \cdot \frac{(k-1)^e - 1}{k-2}$, valore che ovviamente limita inferiormente il numero di vertici di Γ. ∎

Gabbie. Una classe di grafi cubici che riveste un certo interesse, è quella delle cosiddette gabbie. Un grafo cubico con calibro g è detto una *gabbia cubica* se ha il minimo numero possibile di vertici tra tutti i grafi cubici di calibro g. Si dimostra facilmente che il grafo completo K_4 è la sola gabbia cubica di calibro 3, e non è difficle, ma richiede un po' più di lavoro, provare che il grafo di Petersen è l'unica gabbia cubica di calibro 5. L'unica gabbia cubica di calibro 6 è il grafo di Heawood (1890):

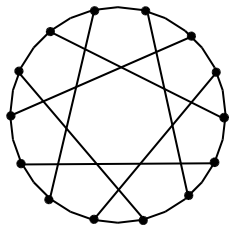


Figura 2.1: Il grafo di Heawood.

La Propisizione 2.3 fornisce un limite inferiore al numero di vertici di una gabbia cubica, che con qualche considerazione aggiuntiva può essere leggermente migliorato, ottenendo:

Il numero di vertici di un grafo cubico di calibro g è almeno

$$n(3, g) = \begin{cases} 1 + 3(2^{(g-1)/2} - 1) & g \text{ dispari} \\ 2(2^{g/2} - 1) & g \text{ pari} \end{cases}$$

Tuttavia, tranne per i casi in cui g è piccola, questa stima inferiore non coincide con il valore minimo esatto del numero di vertici (cioè quello delle corrispondenti gabbie cubiche), che in genere è più grande. La tabella seguente riassume quanto sino ad oggi noto intorno alle gabbie cubiche. La prima colonna g è il valore del calibro, la colonna $|V|$ il numero di vertici

della gabbia (che il lettore può confrontare con il limite inferiore $n(3, g)$), la colonna # indica il numero di gabbie distinte per un certo calibro, e l'ultima colonna fornisce l'indicazione del grafo oppure dei nomi degli scopritori (quando vi siano due date, la prima si riferisce alla costruzione della gabbia, la seconda alla dimostrazione della sua unicità, o alla determinazione del numero esatto di gabbie). Per valori di g maggiori di 12 non si conosce alcuna gabbia, anche se vi sono diverse costruzioni di grafi che forniscono un limite superiore per il numero di vertici di una gabbia.

g	$\|V\|$	#	grafo
3	4	1	K_4
4	6	1	$K_{3,3}$
5	10	1	Petersen
6	14	1	Heawood
7	24	1	McGee
8	30	1	Tutte, Levi
9	58	18	Biggs/Hoare (1980), Brinkmann, McKay, Saager (1995)
10	70	3	O'Keefe, Wong (1980)
11	112	1	Balaban (1973), McKay, Myrvold (2003)
12	126	1	esagono generalizzato

Esercizio 2.4. Si provi che $K_{3,3}$ è l'unica gabbia cubica di calibro 4, e che il grafo di Petersen è l'unica gabbia cubica di calibro 5.

Esercizio 2.5. Costruire un grafo semplice con 8 lati, calibro 4, ed il minimo numero possibile di vertici (a meno di isomorfismo, ci sono due grafi possibili).

2.2 Grafi di Cayley.

Una importante classe di grafi regolari, che svolgerà un ruolo primario nel seguito, è quella dei grafi di Cayley.

Sia G un gruppo, ed S un sottoinsieme di G con le seguenti proprietà

(C1) $1_G \notin S$;

(C2) $S = S^{-1}$;

Il **Grafo di Cayley** $\Gamma[G, S]$ è il grafo semplice il cui insieme dei vertici è G, e gli archi sono tutti i sottoinsiemi $\{g, gs\}$ al variare di $g \in G$ ed $s \in S$.
Si osservi che la condizione (C1) su S serve a far si che $g \neq gs$ per ogni $g \in G$ e $s \in S$, mentre la condizione (C2) serve a rendere simmetrica la relazione di adiacenza, poiché infatti $\{g, gs\} = \{gs, (gs)s^{-1}\}$.

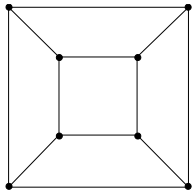
Prima di fare qualche esempio, ricordiamo che se X è un sottoinsieme di un gruppo G, il sottogruppo generato da X, che denotiamo con $\langle X \rangle$, è il minimo sottogruppo di G che contiene X. Si vede facilmente che, se $X \neq \emptyset$, allora $\langle X \rangle$ consiste in tutti e soli i prodotti finiti del tipo $x_1^{\epsilon_1} \cdots x_t^{\epsilon_t}$, con $x_i \in X$ e $\epsilon_i \in \{+1, -1\}$, per $i = 1, \ldots, t$ (con t che varia in $\mathbb{N}$). Nel caso in cui X soddisfi la condizione (C2), allora non è necessario introdurre gli inversi mediante la scelta di $\epsilon_i = -1$, e si ha

$$\langle X \rangle = \{x_1 \cdots x_t \mid t \in \mathbb{N},\ x_1, \ldots, x_t \in X\}.$$

(dove diamo significato anche al prodotto di lunghezza $t = 0$, che è 1_G). In questa situazione è conveniente anche introdurre il concetto di *lunghezza* (o 'peso') $\ell_X(g)$ di un elemento $g \in \langle X \rangle$; essa è il minimo $t \geq 0$ tale che g si scrive come un prodotto di t elementi di X. In particolare $\ell_X(g) = 0 \Leftrightarrow g = 1_G$, e $\ell_X(g) = 1 \Leftrightarrow g \in X$.

Esercizio 2.6. Si provi che il grafo complementare di un grafo di Cayley è un grafo di Cayley.

Vediamo ora qualche esempio di grafo di Cayley. Sia $G = S_3$ il gruppo simmetrico su 3 punti, e sia $S = \{(12), (23)\}$. Allora il grafo di Cayley $\Gamma[G, S]$ è un 6-ciclo. Più in generale, si osserva facilmente che se x, y sono due involuzioni (cioè elementi di ordine 2) di un gruppo finito G, e $G = \langle x, y \rangle$ (in questo caso un semplice argomento mostra che G è un gruppo diedrale), allora $\Gamma[G, \{x, y\}]$ è un ciclo di lunghezza $|G|$.
Si G il gruppo delle simmetrie di un quadrato; allora $|G| = 8$ e $G = \langle \rho, \tau \rangle$ dove ρè una rotazione di un angolo di $\pi/2$ e τ la una riflessione con asse una delle diagonali; 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 $S = \{\rho, \rho^{-1}, \tau\}$, si trova che il grafo di Cayley $\Gamma[G, S]$ è isomorfo al grafo del cubo



Esercizio 2.7. SIa $D_{2n} = \langle x, y \mid y^n = x^2 = 1,\ y^x = y^{-1} \rangle$ il gruppo diedrale di ordine $2n$ e sia $S = \{y, y^{-1}, x\}$; si descriva il grafo $\Gamma[D_{2n}, S]$.

Esercizio 2.8. Si provi che il grafo di Petersen non è un grafo di Cayley. [Si usi il fatto che esistono solo due gruppi di ordine 10: il gruppo ciclico e il gruppo diedrale D_{10}]

Proposizione 2.4. *Sia G un gruppo finito ed S un sottoinsieme di G che soddisfa le condizioni (C1) e (C2); sia $|S| = k$. Allora*

(1) *$\Gamma[G, S]$ è un grafo (semplice) k-regolare;*

(2) *Il numero di componenti connesse di $\Gamma[G, S]$ è uguale all'indice $[G : \langle S \rangle]$; in particolare, $\Gamma[G, S]$ è connesso se e solo se S è un sistema di generatori di G.*

Dimostrazione. Che $\Gamma = \Gamma[G, S]$ sia un grafo semplice risulta dalla costruzione. Inoltre è chiaramente regolare di valenza $k = |S|$, infatti, per ogni vertice $g \in G$, l'insieme dei vertici adiacenti a g è dato dai vertici gs, con $s \in S$ che, al variare di $s \in S$ sono tutti distinti (legge di cancellazione nei gruppi). Questo prova il punto (1).
Per il punto (2), sia $H = \langle S \rangle$. Sia ora $x\, e_1\, g_1\, e_2\, g_2 \ldots e_n\, y \in G$ un cammino in Γ dal vertice x al vertice y. Allora, esistono $s_1, \ldots s_n \in S$ tali che $e_1 = \{x, gs_1\}$, $e_2 = \{xs_1, xs_1s_2\}$ e così via, sino a $e_n = \{xs_1 \cdots s_{n-1}, xs_1 \cdots s_{n-1}s_n = y\}$. Posto $h = s_1 \cdots s_n$, si ha $h \in H$ e $y = xh$, da cui $xH = yH$. Viceversa, siano $x, y \in G$ tali che $xH = yH$. Allora $y \in xH$, e

quindi, per le proprietà di S, esistono $s_1, \dots, s_n \in S$ (con $s_{i+1} \neq s_i^{-1}$) tali che $y = xs_1 \cdots s_n$. Ponendo $e_1 = \{x, xs_1\}$ e, per ogni $i = 2, \dots n$, $e_i = \{xs_1 \cdots s_{i-1}, xs_1 \cdots s_{i-1}s_i\}$, si ricava un cammino $x\, e_1\, xs_1 \cdots e_n\ y$ in Γ. Abbiamo quindi provato che due vertici $x, y \in G$ appartengono alla stessa componente connessa di Γ se e solo se $xH = yH$, il che prova il punto (2). In particolare, l'insieme dei vertici della componente connessa che contiene 1_G è costituito dagli elementi di H, e Γ è connesso se e solo se $H = G$, ovvero S è un sistema di generatori per G. ∎

Osserviamo come dalla dimostrazione del punto (2) segua che se x e y appartengono alla stessa componente connessa di $\Gamma = \Gamma[G, S]$ allora la distanza $d_\Gamma(x, y)$ coincide con la lunghezza minima $\ell_S(h)$ di un elemento $h \in \langle S \rangle$ tale che $y = xh$.

Esercizio 2.9. Sia $n \geq 2$ e sia $G = \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$ il prodotto diretto di n gruppi (ciclici) di ordine 2. Posto $S = \{x_1, \dots, x_n\}$, si provi che il grafo di Cayley $\Gamma[G, S]$ è bipartito. Si calcoli quindi il suo diametro.

Sia Γ un grafo; un isomorfismo $\Gamma \to \Gamma$ si dice un *automorfismo* di Γ. Come in molte altre situazioni, è immediato verificare che l'insieme $Aut(\Gamma)$ degli automorfismi di un grafo Γ è un gruppo rispetto alla composizione. Un grafo semplice $\Gamma = (V, E)$ si dice *vertex–transitivo* se per ogni coppia di vertici distinti $v, w \in V$ esiste un automorfismo α di Γ tale che $\alpha(v) = w$. Chiaramente un grafo vertex–transitivo è regolare.

Esercizio 2.10. Si provi che i grafi di Kneser (esercizio 1.46) sono vertex–transitivi. In particolare, il grafo di Petersen è vertex–transitivo. Quindi si costruisca un grafo cubico che non sia vertex–transitivo, e si cerchi di farlo con il minor numero possibile di vertici.

Sia G un gruppo e $\Gamma = \Gamma[G, S]$ un grafo di Cayley, e sia $g \in G$. Allora la moltiplicazione a sinistra $\lambda_g : G \to G$, definita da $x \mapsto gx$ (per ogni $x \in G$), è una biezione dell'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 (infatti, lo si verifichi per esercizio, la posizione $g \mapsto \lambda_{g^{-1}}$ definisce un omomorfismo iniettivo del gruppo G nel gruppo $Aut(\Gamma)$). Se x, y è una coppia di vertici del grafo di Cayley $\Gamma[G, S]$, ponendo $g = yx^{-1}$, si ha $\lambda_g(x) = y$. Dunque ogni grafo di Cayley e vertex–transitivo. Questa è una importante osservazione che fissiamo nella seguente proposizione.

Proposizione 2.5. *Sia G un gruppo finito ed S un sottoinsieme di G che soddisfa le condizioni (C1) e (C2). Allora, per ogni $g \in G$, la moltiplicazione a sinistra per g induce unn automorfismo di $\Gamma[G, S]$, e G è isomorfo ad un sottogruppo di $Aut(\Gamma)$ che è transitivo sui vertici di Γ. In particolare, $\Gamma[G, S]$ è un grafo vertex–transitivo.*

Questa proprietà dei grafi di Cayley è molto importante. Consente di valutare il comportamento locale del grafo a partire da qualsiasi vertice ci piaccia, in particolare a partire dal vertice 1_G. Così, ad esempio, il diametro di un grafo di Cayley connesso $\Gamma = \Gamma[G, S]$, coincide con $\sup_{g \in G} d_\Gamma(1_G, g)$; per quanto osservato in precedenza possiamo quindi affermare che, se S è un sistema di generatori di G, allora

$$diam(\Gamma[G, S]) = \sup_{g \in G} \ell_\Gamma(g).$$

Analoghe considerazioni valgono per il calibro: il calibro di un grafo di Cayley è la lunghezza minima di un ciclo non banale che inizia nel vertice 1_G, e quindi è il minimo $t \geq 3$ per cui è possibile scrivere $1_G = s_1 s_2 \cdots s_t$, con $s_i \in X$ e $s_{i+1} \neq s_i^{-1}$, per $i = 1, \ldots, t-1$.

2.3 Matrice di adiacenza.

Esistono diverse maniere di associare una matrice ad un grafo (finito). Qui ci limitiamo a descrivere quella che fornirà la base per molta della trattazione algebrica che seguirà.

Sia $\Gamma = (V, E, \phi)$ un grafo finito, e per ogni coppia di vertici u, v denotiamo con A_{uv} il numero di archi i cui estremi sono u e v (quindi $A_{uv} = |\phi^{-1}(\{u, v\})|$). Fissato un ordinamento totale di V, la **matrice di adiacenza** di Γ è la matrice $A(\Gamma)$(che per comodità considereremo come una matrice a coefficienti nel campo complesso $\mathbb{C}$) i cui elementi sono i numeri interi A_{uv}. Indipendentemente dalla scelta dell'ordine su V, se $|V| = n$, $A)\Gamma)$ è una matrice quadrata, simmetrica ed i cui termini diagonali A_{uu} sono tutti nulli. Inoltre, per ogni $u \in V$, si ha $\sum_{v \in V} A_{uv} = d_\Gamma(u)$.
Se il grafo Γ è semplice, $A_{uv} \in \{0, 1\}$, per ogni $u, v \in V$. Se, inoltre, il grafo è k-regolare, allora la somma degli elementi di una riga (o di una colonna) è k.

L'aspetto delle matrici di adiacenza che ci interessa maggiormente è lo studio degli autovalori. Prima di tutto, osserviamo che la matrice di adiacenza A di un grafo con n vertici è simmetrica ed a valori reali (di fatto interi) e quindi, per il Teorema Spettrale, tutti i suoi autovalori sono reali. Li denoteremo, contendone la molteplicità con $\mu_0 \geq m_1 \geq \cdots \geq \mu_{n-1}$ (chiameremo questo lo *spettro* di A).

Per esempio, calcoliamo lo spettro della matrice di adiacenza $A(K_n)$ del grafo completo su n vertici. Si ha, chiaramente, $A(K_n) = J_n - I_n$, dove J_n è la matrice $n \times n$ in cui ogni elemento è 1, e I_n è la matrice identica di ordine n. Ne segue che gli autovalori di $A(K_n)$ sono tutti e soli del tipo $\lambda - 1$, dove λ è autovalore di J_n. Ora, J_n ha rango 1, quindi il suo nucleo ha dimesione $n-1$, e pertanto 0 è autovalore di J_n con molteplicità $n-1$. L'altro autovalore di J_n è n (che, necessariamente, ha molteplicità 1. Pertanto, gli autovalori di $A(K_n)$ sono: $n-1$ con mlteplicità 1, e -1 con molteplicità $n-1$.

Torniamo al caso generale. Per studiare gli autovalori di una matrice quadrata di ordine n è opportuno interpretare questa come la matrice di un endomorfismo di uno spazio n-dimensionale. Sia Γ un grafo, V l'insieme dei suoi vertici, con $|V| = n$, ed A la sua matrice di adiacenza; i cui termini denotiamo con A_{xy} (al variare di x, $y \in V$). Il $\mathbb{C}$-spazio vettoriale che risulta conveniente considerare (essenzialmente dal punto di vista notazionale) è lo spazio $\mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$ di tutte le applicazioni sull'insieme V a valori in $\mathbb{C}$. È uno spazio di dimensione n, una base del quale è costituita dalle applicazioni che assumono valore 1 in uno dei vertici e valore 0 sugli altri. L'azione della matrice A su $\mathcal{C}(\Gamma)$ si descrive facilmente e direttamente: se $f \in \mathcal{C}(\Gamma)$, allora per ogni $x \in V$ si pone

$$(Af)(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{x \sim y} A_{xy} f(y), \tag{2.1}$$

dove $y \sim x$ indica che y varia nell'insieme dei vertici adiacenti ad x (che sono tutti e soli i vertici y per cui $A_{xy} \neq 0$). Se il grafo Γ è semplice, la (2.1) diventa $(Af)(x) = \sum_{x \sim y} f(y)$.

Il caso di cui ci occuperemo principalmente è quello dei grafi regolari. Se Γ è k-regolare (con $k \geq 2$) allora, per ogni vertice v si ha $\sum_{y \in V} A_{xy} = k$. Per la relazione (2.1), ciò significa che la funzione che vale costantemente 1 su V è un autovettore per A relativo all'autovalore k, e quindi che k (il grado di regolarità di Γ) è un autovalore della matrice di adiacenza A. Questa prima osservazione sul legame tra gli autovalori della matrice di adiacenza e le proprietà del grafo è reso più specifico nel primo teorema che vediamo.
In quanto segue, manteniamo la seguente notazione: Γ è un grafo finito con n vertici, $A(\Gamma)$ è la sua matrice di adiacenza, e $\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$ è lo *spettro di* di $A(\Gamma)$ (cioè il multinsieme dei suoi autovalori).

Teorema 2.6. *Sia Γ k-regolare. Allora*

(i) $k = \mu_0$*;*

(ii) $|\mu_i| \leq k$ *per ogni* $i = 1, \ldots, n-1$*;*

(iii) Γ *è connesso se e solo se* $\mu_0 > \mu_1$ *(cioè k è un autovalore di molteplicità* 1*).*

Dimostrazione. Sia Γ un grafo k-regolare, e sia $A = A)\Gamma)$ la sua matrice di adiacenza. Abbiamo già osservato sopra che allora k è un autovalore di A.
Sia μ un autovalore di A e sia $0 \neq f \in \mathcal{C}(\Gamma)$ un autovettore relativo a μ. Scegliamo $x \in V$ tale che $|f(x)|$ è massimo. Osserviamo che, rimpiazzando eventualmente f con $\overline{f(x)}f$, possiamo assumere $\mathbb{R} \ni f(x) > 0$. Allora,

$$|\mu| f(x) = |\mu f(x)| = |Af(x)| = \big|\sum_{y \in V} A_{xy} f(y)\big| \leq \sum_{y \in V} A_{xy} |f(y)| \leq f(x) \sum_{y \in V} A_{xy} = k f(x).$$

Quindi $|\mu| \leq k$, il che prova i punti (i) e (ii) dell'enunciato.

Sia ora $0 \neq f$ un autovettore relativo a k e, come prima, sia $x \in V$ tale che $|f(x)|$ è massimo. Allora

$$k f(x) = Af(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{y \sim x} A_{xy} f(y), \tag{2.2}$$

Dunque $f(x) = \sum_{y \sim x} \frac{A_{xy}}{k} f(y)$. Poiché, per ogni $y \sim x$, $0 < A_{xy}/k \leq 1$ e $\sum_{y \sim y} A_{xy}/k = 1$, l'uguaglianza (2.2) ci dice che il numero complesso $f(x)$ appartiene all'inviluppo convesso dei punti $f(y)$ con $y \sim x$. Poiché ognuno di questi punti $f(y)$ è contenuto nel cerchio di raggio $|f(x)|$, la sola possibilità é che $f(y) = f(x)$ per ogni $y \sim x$. Quindi f è costante sulle componenti connesse di Γ. Pertanto, se Γ è connesso, l'autospazio di A relativo a k consiste in tutte e sole la applicazioni costanti su V, ed ha dunque dimensione 1. Ne segue che la molteplicità di k come autovalore di A è 1, ovvero che $k = \mu_0 > \mu_1$.
Se Γ non è connesso, sia U l'insieme dei vertici di una sua componente connessa e definiamo $f, g \in \mathcal{C}(\Gamma)$ ponendo, per ogni $x \in V$,

$$f(x) = \begin{cases} 1 & \text{se } x \in U \\ 0 & \text{se } x \in V \setminus U \end{cases} \qquad g(x) = \begin{cases} 0 & \text{se } x \in U \\ 1 & \text{se } x \in V \setminus U \end{cases}$$

Allora, f e g sono elementi indipendenti di $\mathcal{C}(\Gamma)$ e, come si verifica facilmente, autovettori di A relativi a k. Quindi, la molteplicità di $\mu_0 = k$ è almeno 2 e pertanto $\mu_0 = \mu_1$. ∎

Esercizio 2.11. Sia Γ un grafo k-regolare. Si provi che la molteplicità di k come autovalore di $A(\Gamma)$ è uguale al numero di componenti connesse di Γ.

Esercizio 2.12. Sia Γ un grafo connesso finito e denotiamo con $\Delta(\Gamma)$ il massimo tra i gradi dei suoi vertici. Sia $A = A(\Gamma)$ la sua matrice di adiacenza. Si provi che per ogni autovalore μ di A si ha $|\mu| \leq \Delta(\Gamma)$. Si provi quindi che $\Delta(\Gamma)$ è un autovalore di A se e solo se Γ è regolare.

Esercizio 2.13. Sia $\Gamma = (V, E)$ un grafo finito semplice, e sia $\alpha : V \to V$ una permutazione dei vertici che induce un isomorfismo di Γ. Per ogni $f \in \mathcal{C}(\Gamma)$ sia $f^\alpha \in \mathcal{C}(\Gamma)$ definita da $f^\alpha(x) = f(\alpha^{-1}(x))$, per ogni $x \in V$. Si provi che se f è un autovettore di $A(\Gamma)$ allora f^α è autovettore relativo allo stesso autovalore.

Esempio. Prima di procedere con i risultati generali, soffermiamoci a calcolare, per esercizio, lo spettro della matrice di adiacenza $A = A(C_n)$ di un n-ciclo. Se $v_0, v_1, \ldots, v_{n-1}$ sono i vertici di C_n elencati in modo che vertici consecutivi siano adiacenti (e V_{n-1} adiacente a v_0), allora

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdot & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} = B + B^T \quad \text{dove} \quad B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdot & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Si osservi che $B^T = B^{-1}$; quindi B e B^T hanno gli stessi autospazi (relativi ad autovalori che sono l'uno l'inverso dell'altro). Ne segue che gli autovalori di A sono del tipo $\lambda + \lambda^{-1}$ dove λ è un autovalore di B. Ora, come si calcola facilmente, il polinomio caratteristico di B è $(-1)^n(x^n - 1)$; quindi gli autovalori di B sono le radice n-esime dell'unità, ovvero $\lambda_t = \cos\frac{2\pi t}{n} + i \sin\frac{2\pi t}{n}$ con $t = 0, 1, \ldots, n-1$. Ne segue che gli autovalori di A sono i numeri reali $\lambda_t + \lambda_t^{-1} = \lambda_t + \overline{\lambda_t} = 2\cos\frac{2\pi t}{n}$, con $t = 0, 1, \ldots, n-1$. Si osservi che $\mu_0 = 2\cos 0 = 2$, che ha molteplicità 1 (come deve essere, dato che C_n è 2-regolare e connesso. Gli altri autovalori hanno molteplicità 2 tranne eventualmente -2, che occorre se e solo se n è pari ed, in tal caso, ha molteplicità 1. Ora, se n è pari, C_n è bipartito. Il prossimo Teorema descrive proprio questa situazione.

Teorema 2.7. *Sia Γ un grafo k-regolare e connesso. Allora sono equivalenti*

(i) *Γ è bipartito;*

(ii) *lo spettro di $A(\Gamma)$ è simmetrico rispetto al 0;*

(iii) *$\mu_{n-1} = -k$.*

Dimostrazione. (i) $\Rightarrow$ (ii). Sia Γ un grafo bipartito, e sia $V = V_1 \cup V_2$ una bipartizione dell'insieme dei vertici di Γ (ciò significa che $V_1 \neq \emptyset \neq V_2$, $V_1 \cap V_2 = \emptyset$ ed ogni arco di Γ ha uno degli estremi in V_1 e l'atro in V_2). Sia μ un autovalore di $A = A(\Gamma)$ e sia $0 \neq f \in \mathcal{C}(\Gamma)$ un autovettore relativo a μ; quindi $Af = \mu f$. Definiamo $g \in \mathcal{C}(\Gamma)$ ponendo, per ogni $x \in V$,

$$g(x) = \begin{cases} f(x) & \text{se } x \in V_1 \\ -f(x) & \text{se } x \in V_2 \end{cases}$$

Allora, $g \neq 0$. Se $x \in V_1$ allora $y \sim x \Rightarrow\ y \in V_2$, e si ha

$$Ag(x) = \sum_{y \sim x} A_{xy} g(y) = \sum_{y \sim x} A_{xy}(-f(y)) = -Af(x) = -\mu f(x) = -\mu g(x).$$

Analogamente si vede che se $x \in V_2$ allora $Ag(x) = Af(x) = \mu f(x) = -\mu g(x)$. Pertanto, $Ag = -\mu g$, il che prova che $-\mu$ è un autovalore di A, e dunque che (ii) è soddisfatta.

(ii) $\Rightarrow$ (iii). Poiché dal Teorema 2.6 segue che $k = \mu_0$ è autovalore di A con il massimo modulo, da (ii) segue che $-k$ è un autovalore di A, e quindi che $\mu_{n-1} = -k$.

(iii) $\Rightarrow$ (i). Assumiamo che $-k$ sia un autovalore di A; sia $0 \neq f$ uan autovettore relaivo a $-k$ e sia $x \in V$ tale che $|f(x)|$ è massimo. Come nella dimostrazione del punto (i) del Teorema 2.6 possiamo assumere che $\mathbb{R} \ni f(x) > 0$. Poniamo $V_1 = \{y \in V \mid f(y) = f(x)\}$, $V_2 = \{y \in V \mid f(y) = -f(x)\}$ e proviamo che $V_1 \cup V_2$ è una bipartizione di V. Chiaramente $V_1 \cap V_2 = \emptyset$. Poiché Γ è connesso, per ogni $y \in V$ è definita la distanza $d_\Gamma(x, y) = d_y$. Procedendo per induzione su d_y proviamo che $y \in V_1$ se d_y è pari, mentre $y \in V_2$ se d_y è dispari. Ora,

$$|f(x)| = f(x) = -\frac{1}{k} Af(x) = -\frac{1}{k} \sum_{y \sim x} A_{xy} f(y) = \sum_{y \sim x} \frac{A_{xy}}{k}(-f(y)),$$

e quindi, come nella dimostrazione del punto (ii) di 2.6, $f(y) = -f(x) < 0$ per ogni $V \ni y \sim x$. Pertanto $\{y \in V \mid d_y = 1\} \subseteq V_2$. Questo stesso argomento fornisce il metodo per provare il passo induttivo, e quindi la correttezza dell'affermazione fatta sopra. Ne segue che $V_1 \cup V_2 = V$ è una bipartizione di V. ∎

Esercizio 2.14. Si determini lo spettro della matrice di adiacenza del grafo del cubo.

Esercizio 2.15. Dato $n \geq 2$, si determini lo spettro della matrice di adiacenza del grafo completo bipartito $K_{n,n}$ (vedi esercizio 1.54).

Esercizio 2.16. Sia $\Gamma = (V, E)$ un grafo semplice con $|V| = n$, e sia $\mu_0 \geq \cdots \geq \mu_{n-1}$ lo spettro della matrice di adiacenza $A(\Gamma)$. Si provi che $\sum_{i=0}^{n-1} \mu_i = 0$, e che $\sum_{i=0}^{n-1} \mu_i^2 = 2|E|$.

Orientazione. I grafi possono essere visti come spazi topologici 1-dimensionali. La nozione di orientazione è, nel caso dei grafi, particolarmente semplice. Sia Γ in grafo; un'*orientazione* di Γ è un ordinamento totale sull'insieme dei suoi vertici. Questo fornisce ad ogni archo di Γ un verso, nel senso che possiamo descrivere ogni arco $e \in E$ come una coppia ordinata di vertici: $e = (e_-, e_+)$, dove $e_- < e_+$ sono gli estremi di e.

L'operatore di Laplace. Sia $\Gamma = (V, E)$ un grafo con n vertici. Il $\mathbb{C}$-spazio vettoriale n-dimensionale $\mathcal{C}(\Gamma)$ è naturalmente dotato del prodotto scalare hermitiano standard $<,>$, definito da, per ogni $g, h \in \mathcal{C}(\Gamma)$,

$$< f, g >= \sum_{x \in V} f(x)\overline{g(x)}.$$

Sia A la matrice di adiacenza di Γ. Poiché A è reale e simmetrica, l'operatore lineare su $\mathcal{C}(\Gamma)$ ad essa associato è hermitiano, ovvero $< Af, g >=< f, Ag >$ per ogni $f, g \in \mathcal{C}(\Gamma)$. Ciò

implica, in particolare, che esiste una base ortonormale di $\mathcal{C}(\Gamma)$ composta da autovettori di A, e da questo discende che per ogni $f \neq \in \mathcal{C}(\Gamma)$,

$$Q_A(f) = \frac{<Af, f>}{<f, f>} \in [\mu_{n-1}, \mu_0] \tag{2.3}$$

dove, secondo la notazione già fissata, μ_0 e μ_{n-1} sono, rispettivamente, il massimo ed il minimo autovettore di A.

Esercizio 2.17. Si dimostri la correttezza di (2.3).

Assumiamo ora che Γ sia semplice, e fissiamo una sua orientazione.
La *matrice d'incidenza* B è la matrice indicizzata su $V \times E$ (quindi, se $|E| = m$, è una matrice $n \times m$) dove, per ogni $x \in V$ e ogni $e \in E$,

$$B_{xe} = \begin{cases} 1 & \text{se } x = e_+ \\ -1 & \text{se } x = e_- \\ 0 & \text{se } x \notin e \end{cases} \tag{2.4}$$

Analogamente per quanto fatto con i vertici, sia $\mathcal{E}(\Gamma)$ il $\mathbb{C}$-spazio vettoriale (m–dimensionale) di tutte le applicazioni $u : E \to \mathbb{C}$. Allora B è la matrice dell'applicazione lineare

$$\delta : \mathcal{E}(\Gamma) \to \mathcal{C}(\Gamma),$$

dove, per ogni $u \in \mathcal{E}(\Gamma)$, ed ogni $x \in V$, $\delta u(x) = \sum_{e \in E} B_{xe} u(e)$.
L'operatore trasposto $\delta^* : \mathcal{C}(\Gamma) \to \mathcal{E}(\Gamma)$ è associato dalla matrice trasposta B^t, ed è dato da, per ogni $f \in (\Gamma)$, ed $e \in E$,

$$\delta^* f(e) = \sum_{x \in V} B_{xe} f(x) = f(e_+) - f(e_-). \tag{2.5}$$

E sia ha, per ogni $f \in \mathcal{C}(\Gamma)$ ed ogni $u \in \mathcal{E}(\Gamma)$, $< f, \delta u > = < \delta^* f, u >$ (dove, ovviamente, il termine a destra è l'ovvio prodotto hermitiano definito su $\mathcal{E}(\Gamma)$).

Definiamo a questo punto la matrice $D = D(\Gamma)$ come la matrice diagonale $n \times n$, i cui elementi (indicizzati sulle coppie di vertici di Γ) sono

$$D_{xy} = \begin{cases} d_\Gamma(x) & \text{se } \ x = y \\ 0 & \text{se } \ x \neq y \end{cases}$$

Lascio per esercizio la semplice dimostrazione del seguente fatto.

Lemma 2.8. *Sia $\Gamma = (V, E)$ un grafo semplice orientato, B la matrice d'incidenza, e A la matrice di adiacenza. Allora*

$$BB^t = D - A.$$

L'*operatore di Laplace* di Γ è l'operatore sullo spazio $\mathcal{C}(\Gamma)$ la cui matrice è $L(\Gamma) = D - A$. Per il Lemma 2.8 tale operatore coincide con $\delta\delta^*$; è un operatore reale, simmetrico, quindi hermitiano, e per esso valgono le considerazioni fatte in precedenza per A.

Quando Γ sia k-regolare, la cosa assume un aspetto ancor più accattivante, dato che, in tal caso, si ha $D = kI_n$ e quindi, dal Lemma 2.8, $L = kI_n - A$. Ne segue che gli autovalori di L sono (dal più piccolo al più grande),

$$0 \leq k - \mu_1 \leq \cdots \leq k - \mu_{n-1}. \tag{2.6}$$

Se, inoltre, Γ è connesso, allora l'autovalore 0 di L ha molteplicità 1 e l'autospazio corrispondente coincide con l'autospazio di A relativo all'autovalore k, che, come abbiamo visto è lo spazio $\mathcal{Z}$ delle funzioni costanti $V \to \mathbb{C}$. Abbiamo cioè il seguente fatto

Lemma 2.9. *Sia $k \geq 2$ e sia $\Gamma = (V, E)$ un grafo semplice connesso k regolare. Allora il nucleo dell'operatore di Laplace di Γ è costituito dall funzioni costanti in $\mathcal{C}(\Gamma)$.*

Poiché L è hermitiano, gli auovettori relativi agli altri autovalori di L appartengono (sempre nel caso in cui Γ sia regolare e connesso) allo spazio ortogonale $\mathcal{Z}^\perp$ di $\mathcal{Z}$ che, come si verifica immediatamente, è $\mathcal{Z}^\perp = \{f \in \mathcal{C}(\Gamma) \mid \sum_{x \in V} f(x) = 0\}$. Applicando all'operatore L ed agli elementi $f \in \mathcal{Z}^\perp$ l'osservazione (2.3) si conclude con la seguente proposizione.

Proposizione 2.10. *Sia $k \geq 2$ e sia $\Gamma = (V, E)$ un grafo semplice connesso e k regolare. Sia L l'operatore di Laplace di Γ. Allora per ogni $f \in \mathcal{C}(\Gamma)$ tale che $\sum_{x \in V} f(x) = 0$, si ha*

$$Q_L(f) = \frac{< Lf, f >}{< f, f >} \geq k - \mu_1.$$

Si osservi che in generale, se Γ è come nella Proposizione precedente, per ogni $f \in \mathcal{C}(\Gamma)$ si ha

$$Q_L(f) \in [0, k - \mu_+ n - 1].$$

Esercizio 2.18. Si dimostri il Lemma 2.8.

Esercizio 2.19. Si dia una dimostrazione diretta del Lemma 2.9.

Esercizio 2.20. Sia $\Gamma = (V, E)$ un grafo semplice regolare su n vertici, e sia $\mu_0, \ldots, \mu_{n-1}$ lo spettro della sua matrice di adiacenza. Si descriva (in funzione di quello di Γ) lo spettro della matrcie di adiacenza del grafo complementare $\overline{\Gamma}$ (esercizio 1.2).

2.4 Grafi di Moore.

La matrice di adiacenza, e in particolare il suo spettro, forniscono metodi di approccio ai grafi che risultano particolarmente utili quando i grafi in questione hanno un elevato livello di simmetria. Noi li utilizzeremo in seguito per trattare particolari grafi di Cayley (che sono vertex-transitivi). In questo paragrafo vediamo invece una classica applicazione dello studio dello spettro della matrice di adiacenza: ovvero lo studio dei grafi di Moore.

Un grafo semplice, connesso, k-regolare di diametro d, si dice *grafo di Moore* (di diametro d) se $g(\Gamma) = 2d + 1$ (ovvero, Γ ha il massimo calibro possibile per un grafo di diametro d). Per $k = 2$ i grafi di Moore sono i cicli C_{2d+1}.

Esercizio 2.21. Sia Γ un grafo semplice connesso, con diametro d e tale che $g(\Gamma) = 2d + 1$. Si provi che Γ è regolare.

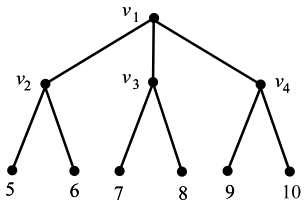
Se $k \geq 3$, dal Corollario 2.2 e la proposizione 2.3 segue che il numero di vertici di un grafo di Moore di valenza k e diametro d è

$$n = 1 + k \cdot \frac{(k-1)^d - 1}{k-2}$$

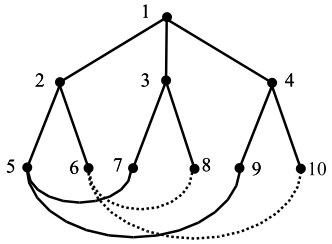
Damerell, Bannai e Ito hanno provato che, per diametro $d \geq 3$, il solo grafo di Moore di diametro d è il ciclo C_{2d+1}. Noi considereremo solo il caso (che è fondamentale) dei grafi di Moore di diametro 2; in tal caso, se il grafo è k-regolare il numero dei vertici è $n = 1 + k^2$. Chiaramente, il ciclo C_5 è l'unico grafo di Moore con grado 2 e diamtero 2. Il caso $k = 3$ è meno banale, ma anch'esso non richiede strumenti particolarmente raffinati.

Proposizione 2.11. *Il grafo di Petersen è l'unico grafo di Moore cubico di diametro* 2.

DIMOSTRAZIONE. Si verifica direttamente che il grafo di Petersen è un grafo cubico di diametro 2 e calibro 5; quindi è un grafo di Moore. Viceversa, sia Γ un grafo di Moore cubico di diametro 2; allora Γ ha 10 vertici, che denotiamo con $v_1, v_2, \ldots, v_{10}$, e ponendo che i vertici adiacenti al vertice v_1 siano quelli denotati con v_2, v_3, v_4. Siccome Γ ha diametro 2, considerando anche tutti i vertici adiacenti a qualcuno dei vertici v_2, v_3, v_4, otteniamo tutti i vertici di Γ. Poiché ogni vertice v_2, v_3, v_4 ha esattamente 2 vertici adiacenti diversi dal vertice v_1, e Γ ha 10 vertici si deduce che ogni vertice diverso da v_1, v_2, v_3, v_4 è adiacente ad uno e uno solo dei vertici v_2, v_3, v_4. Abbiamo cioè la situazione illustrata dalla seguente figura.



Poiché il vertice v_5 ha distanza 2 sia da v_3 che da v_4, si avrà che v_5 è adiacente ad uno tra i vertici v_7, v_8, e ad uno tra v_9, v_{10}; eventualmente cambiando gli indici, possiamo supporre che v_5 sia adiacente a v_7 e a v_9. Questo forza il vertice v_6 ad essere adiacente a v_9 e a v_{10}.



Ora, v_7 deve essere adiacente a v_9 oppure a v_{10}; siccome v_7 deve avere distanza 2 da v_6, l'unica possibilità è che v_7 sia adiacente a v_{10}; conseguentemente, v_8 è adiacente a v_9, e non vi siano altri lati in Γ. A questo punto si verifica facilmente che Γ è isomorfo al grafo di Petersen. ■

Il risultato principale di questo paragrafo è il seguente.

Teorema 2.12. *Se Γ è un grafo di Moore k-regolare di diametro 2, allora $k = 2, 3, 7, 57$.*

DIMOSTRAZIONE. Il ciclo C_5 è l'unico grafo di Moore 2-regolare con diametro 2. Sia quindi $k \geq 3$, e sia $\Gamma = (V, E)$ un grafo di Moore k-regolare di diametro 2; allora Γ ha $n = 1 + k^2$ vertici. Sia A la sua matrice di adiacenza, e poniamo $B = A^2$. Allora, per ogni $x, y \in V$, B_{xy} è il numero di percorsi tra x e y di lunghezza 2. Poiché $diam(\Gamma) = 2$ e Γ non ha cicli di lunghezza ≤ 4, si ha,

$$B_{xy} = \begin{cases} k & \text{se } x = y \\ 0 & \text{se } x \sim y \\ 1 & \text{se } d(x, y) = 2 \end{cases}$$

Pertanto si ha $J_n = B - (k-1)I_n + A$, dove J_n è la matrice in cui ogni elemento è 1. Ovvero

$$A^2 + A - (k-1)I = J \tag{2.7}$$

Poiché gli autovalori di J (che abbiamo già trovato in precedenza) sono 0 (con mlteplicità $n - 1 = k^2$) e n (con molteplicipt̀à 1, da (2.7) segue che ogni autovalore λ di A soddisfa

$$\lambda^2 + \lambda - (k-1) \in \{0, n\}. \tag{2.8}$$

Ora, il valore $n = 1 + k^2$ in (2.8) si ottiene per $\lambda = k$ (che ci deve essere perché Γ è k–regolare, ed ha molteplicità 1). Gli altri autovalori di A sono le due radici λ_1 e λ_2 del polinomio $\lambda^2 + \lambda - (k-1) = 0$ (che sono reali). Fissiamo gli indici in modo che $\lambda_1 \geq \lambda_2$, e denotiamo con m_1 e m_2 le loro rispettive molteplicità (potrebbe darsi che una sola radice sia autovalore per A, in tal caso assegneremo all'altra molteplicità 0) . Allora, tenendo presente che la somma degli autovalori di A (con molteplicità) è uguale alla traccia di A, che è 0, si ha

$$\begin{cases} m_1 + m_2 = n - 1 = k^2 \\ m_1\lambda_1 + m_2\lambda_2 = -k \end{cases} \tag{2.9}$$

Sia $\Delta = 1 + 4(k-1)$. Allora da (2.9) e dal fatto che $\lambda_1 + \lambda_2 = -1$, segue

$$\sqrt{\Delta}m_2 = (\lambda_1 - \lambda_2)m_2 = \lambda_1 k^2 + k = \frac{-1 + \sqrt{\Delta}}{2}k^2 + k, \tag{2.10}$$

da cui si ricava $\sqrt{\Delta}(k^2 - 2m_2) = k^2 - 2k$.
Se $k^2 - 2k = 0$, allora $k = 2$, e $n = 5$.
Altrimenti, $\sqrt{\Delta} \in \mathbb{Q}$, e quindi λ_1 e λ_2 sono razionali. Poiché sono radici di un polinomio intero monico, si ha che λ_1, λ_2 sono interi. Posto $\lambda_1 = z$, si ha $\sqrt{\Delta} = 2z + 1$, e da (2.4) segue

$$\frac{k(kz+1)}{2z+1} = m_2 \in \mathbb{Z}. \tag{2.11}$$

Ora, tenendo conto che $k = z^2 + z + 1$, vediamo che

$$(kz + 1, 2z + 1) = (2z + 1, k - 2) = (2z + 1, z^2 + z - 1)|5$$

$$(k, 2z + 1) = (z^2 + z + 1, 2z + 1)|3.$$

Quindi, da (2.11) segue che $2z+1 \in \{3,5,15\}$, e conseguentemente $z \in \{1,2,7\}$. Pertanto $k = z^2+z+1 \in \{3,7,57\}$. La dimostrazione è completa. ∎

Come per $k = 2, 3$, si può provare che esiste un unico grafo di Moore, detto grafo di Hoffman–Singleton (dai nomi dei suoi scopritori), con valenza $k = 7$ e diametro 2 (vedi esercizi 2.37 – 2.40); mentre non è tuttora noto se esistano grafi di Moore di valenza $k = 57$ e diametro 2 (un tale grafo, se esiste, ha 3250 vertici).

Esercizio 2.22. Usando la tecnica della dimostrazione del Teorema 2.12 si determini lo spettro della matrice di adiacenza del grafo di Petersen.

Esercizio 2.23. Sia Γ un grafo semplice. Una *passeggiata* in Γ di lunghezza $t \geq 0$, è una successione $x_0, x_1, \ldots, x_t$ di vertici consecutivamente adiacenti. Sia $A = A(\Gamma)$ la matrice di adiacenza di un grafo semplice finito. Si provi che, per ogni $t \geq 0$ e ogni coppia x, y di vertici $(A^r)_{xy}$ è uguale al numero di passeggiate di lunghezza t il cui primo e ultimo vertice sono, rispettivamente, x e y.

2.5 Costante isoperimetrica ed expanders.

Sia $\Gamma = (V, E)$ un grafo semplice connesso. Per ogni sottoinsieme di vertici, $\emptyset \neq F \subseteq V$, la *frontiera* di F, che denotiamo con ∂F, è l'insieme di tutti gli archi di Γ che hanno un estremo in F e l'altro in $V \setminus F$.
La **costante isoperimetrica** (o costante di Cheeger) del grafo Γ è definita da

$$h(\Gamma) = \inf \left\{ \frac{|\partial F|}{\min\{|F|, |V \setminus F|\}} \;\middle|\; F \subseteq V,\ 0 < |F| < \infty \right\}. \tag{2.12}$$

Se V è finito (come sarà sempre nei casi che studieremo), si ha chiaramente

$$h(\Gamma) = \min \left\{ \frac{|\partial F|}{|F|} \;\middle|\; F \subseteq V,\ 0 < |F| \leq |V|/2 \right\}. \tag{2.13}$$

Consideriamo, ad esempio, il grafo completo K_n (con $n \geq 3$). Se $F \neq \emptyset$ è un sottoinsieme di m vertici di K_n (quindi $1 \leq m \leq n$, allora $|\partial F| = m(n-m)$ e quindi $|\partial F|/|F| = n - m$. da ciò segue che

$$h(K_n) = n - \left[\frac{n}{2}\right] = \begin{cases} n/2 & \text{se } n \text{ è pari} \\ (n+1)/2 & \text{se } n \text{ è dispari} \end{cases} \tag{2.14}$$

Vediamo ora il caso del ciclo C_n ($n \geq 3$). Se $F \neq \emptyset$ è un suo sottoinsieme di vertici con $|F| \leq n/2$, allora $2 \leq |\partial F| \leq 2|F|$, e il valore minimo di $|\partial F|/|F|$ si ottiene prendendo come F un insieme di $[n/2]$ vertici consecutivi. Si ha dunque

$$h(C_n) = \frac{2}{[n/2]} = \begin{cases} n4/n & \text{se } n \text{ è pari} \\ 4/(n-1) & \text{se } n \text{ è dispari} \end{cases} \tag{2.15}$$

Esercizio 2.24. Per ogni $n \geq 2$ si determini la costante isoperimetrica del grafo bipartito completo $K_{n,n}$ (vedi esercizio 1.54). [Si distiguano i casi n pari e n dispari]

Esercizio 2.25. Sia Γ un grafo connesso 3-regolare. Si provi che $h(\Gamma) \leq 1$.

Teorema 2.13. *Sia Γ un grafo finito semplice, connesso e k-regolare, e $\mu_0 \geq \cdots \geq \mu_{n-1}$ lo spettrro della matrice di adiacenza di Γ. Allora*

$$h(\Gamma) \geq \frac{\mu_0 - \mu_1}{2} = \frac{k - \mu_1}{2}.$$

DIMOSTRAZIONE. Sia $\Gamma = (V, E)$ come nelle ipotesi, e sia F un sottoinsieme non-vuoto di V. Definiamo $f \in \mathcal{C}(\Gamma)$ ponendo, per ogni $x \in V$,

$$f(x) = \begin{cases} |V| - |F| & \text{se } x \in F \\ -|F| & \text{se } x \in V \setminus F \end{cases}$$

Si ha quindi

$$\sum_{x \in V} f(x) = |F|(|V| - |F|) - |V \setminus F||F| = 0$$

e dunque (con le notazioni della sezione 2.3), $f \in \mathcal{Z}^{\perp}$. Inoltre

$$< f, f >= \sum_{x \in V} f(x)^2 = (|V| - |F|)^2|F| + |F|^2(|V| - |F|) = |V||F|(|V| - |F|). \tag{2.16}$$

Fissato un orientamento di Γ, sia $\delta^* : \mathcal{C}(\Gamma) \to \mathcal{E}(\Gamma)$ l'applicazione lineare definita in (2.5). Allora, per ogni $e \in E$,

$$\delta^* f(e) = f(e_+) - f(e_-) = \begin{cases} \pm|V| & \text{se } e \in \partial F \\ 0 & \text{se } e \notin \partial F \end{cases} \tag{2.17}$$

Sia $L = \delta\delta^*$ l'operatore di Laplace di Γ. Allora, tenendo conto di (2.17)

$$< Lf, f >=< \delta^* f, \delta^* f >= \sum_{e \in E} (\delta^* f(e))^2 = |V|^2 |\partial F|.$$

Applicando ora la Proposizione 2.10, si ricava

$$k - \mu_1 \leq \frac{< Lf, f >}{< f, f >} = \frac{|V|^2|\partial F|}{|V||F|(|V| - |F|)} = \frac{|V||\partial F|}{F|(|V| - |F|)}. \tag{2.18}$$

Prendendo F tale che $|F| \leq |V|/2$, dalla (2.18) segue

$$\frac{|\partial F|}{|F|} \geq \frac{k - \mu_1}{2}$$

da cui l'asserto. ∎

Esercizio 2.26. Sia P il grafo di Petersen; si provi che $h(P) = (k - \mu_1)/2$. Si verifichi che lo stesso vale per il grafo bipartito completo $K_{n,n}$ con n pari.

Se Γ è un grafo connesso (e finito), il numero reale $k-\mu_1$ (o, più in generale, senza assunzione di regolarità, $\mu_0-\mu_1$) è un parametro estremamente importante, e viene chiamato *intervallo spettrale principale* del grafo Γ. L'intervallo spettrale principale determina anche un limite superiore alla costante isoperimetrica di un grafo regolare. Si ha infatti il seguente risultato

Teorema 2.14. *Sia Γ un grafo finito semplice, connesso e k-regolare. Allora*

$$h(\Gamma) \leq \sqrt{2k(k-\mu_1)}.$$

DIMOSTRAZIONE. Sia $\Gamma = (V, E)$ un grafo finito semplice, connesso e k-regolare con n vertici. Sia $f \in \mathcal{C}(\Gamma)$; diciamo che f è non-negativa se $0 \leq f(x) \in \mathbb{R}$ per ogni $x \in V$. La prima parte della dimostrazione consiste nel provare alcuni fatti relativi alle funzioni $f \in \mathcal{C}(\Gamma)$ non-negative.
Fissiamo quindi $f \in \mathcal{C}(\Gamma)$, f non-negativa. Siano $b_0 < b_1 < \cdots < b_r$ i valori distinti assunti da f su V, ordinati secondo l'ordine naturale. Scegliamo un'orientazione di Γ (cioè un ordinamento totale di V) in modo che per ogni $x, y \in V$ si abbia: $f(x) > f(y) \Rightarrow x \geq y$ (questo è certamente possibile farlo). Poniamo

$$R_f = \sum_{e \in E} \left[f(e_+)^2 - f(e_-)^2 \right].$$

Per ogni $i = 0, \ldots, r$ sia $F_i = \{x \in V \mid f(x) \geq b_i\}$, Il primo passo è il seguente.

$$R_f = \sum_{i=1}^{r} |\partial F_i| (b_i^2 - b_{i-1}^2) \tag{2.19}$$

(e $B_f = 0$ se f è una costante). Poniamo E_f l'insieme degli archi che danno un effettivo contributo nella somma R_f, cioè (per come è stata scelta l'orientazione)

$$E_f = \{e \in E \mid f(e_+) > f(e_-)\}.$$

Quindi, per ogni $i = 0, \ldots, r-1$, si ha

$$\partial F_i \setminus \partial F_{i+1} = \{e \in E_f \mid f(e_+) = b_i\} \qquad \text{e} \qquad \partial F_{i+1} \setminus \partial F_i = \{e \in E_f \mid f(e_-) = b_i\}.$$

Dunque

$$|\partial F_i| - |\partial F_{i+1}| = |\{e \in E_f \mid f(e_+) = b_i\}| - |\{e \in E_f \mid f(e_-) = b_i\}|.$$

Inoltre $\partial F_1 = \{e \in E_f \mid f(e_-) = b_0\}$ e $\partial F_r = \{e \in E_f \mid f(e_+) = b_r\}$. Si ha pertanto

$$\begin{aligned} R_f &= \sum_{e \in E_f} (f(e_+)^2 - f(e_-)^2) = \sum_{e \in E_f} f(e_+)^2 - \sum_{e \in E_f} f(e_-)^2 = \\ &= |\partial F_r| b_r^2 - |\partial F_1| b_0^2 + \sum_{i=1}^{r-1} (|\partial F_i| - |\partial F_{i+1}|) b_i^2 = \sum_{i=1}^{r} |\partial F_i| b_i^2 - \sum_{i=0}^{r-1} |\partial F_{i+1}| b_i^2 = \\ &= \sum_{i=1}^{r} |\partial F_i| b_i^2 - \sum_{i=1}^{r} |\partial F_i| b_{i-1}^2 = \sum_{i=1}^{r} |\partial F_i| (b_i^2 - b_{i-1}^2) \end{aligned}$$

e l'uguaglianza (2.19) è provata.

Il secondo passo consiste nel provare (sempre assumendo f non-negativa) che

$$R_f^2 \leq 2k < Lf, f >< f, f > \tag{2.20}$$

Dove $L = kI_n - A(\Gamma)$ è l'operatore di Laplace di Γ. Infatti, applicando la formula di Cauchy-Schwartz e il fatto che per ogni $a, b \in R$ si ha $2(a^2 + b^2) \geq (a + b)^2$, si ha

$$\begin{aligned} R_f^2 &= \Big[\sum_{e\in E}(f(e_+) - f(e_-))(f(e_+) + f(e_-))\Big]^2 \\ &\leq \sum_{e\in E}(f(e_+) - f(e_-))^2 \sum_{e\in E}(f(e_+) + f(e_-))^2 \\ &\leq 2 < \delta^* f, \delta^* f > \sum_{e\in E}\big(f(e_+)^2 + f(e_-)^2\big) \\ &= 2 < Lf, f > \cdot k \sum_{x\in V} f(x)^2 = 2k < Lf, f >< f, f > \end{aligned}$$

e anche (2.20) è provata.

Sia $supp(f) = \{x \in V \mid f(x) \neq 0$. Nel terzo passo proviamo che (se f è non negativa)

$$|supp(f)| \leq |V|/2 \quad \Rightarrow \quad R_f \geq h(\Gamma) < f, f > . \tag{2.21}$$

Se f è non-negativa e $|supp(f)| \leq |V|/2$ allora, con le notazioni usate in precedenza, $b_0 = 0$, e per ogni $i = 1, \ldots, r$, $|F_i| \leq |V|/2$. Quindi, per $i = 1, \ldots, r$, $|\partial F_i| \geq h(\Gamma)|L_i|$. Dunque, applicando (2.19)

$$\begin{aligned} R_f \geq h(\Gamma)\sum_{i=1}^{r}|F_i|(b_i^2 - b_{i-1}^2) &= h(\Gamma)\Big\{|F_r|b_r^2 + \sum_{i=1}^{r-1}|F_i \setminus F_{i+1}|b_i^2 - |F_1|b_0\Big\} \\ &= h(\Gamma)\sum_{x\in V} f(x)^2 = h(\Gamma) < f, f > . \end{aligned}$$

Conclusione. Sia $0 \neq g \in \mathcal{C}(\Gamma)$ una autovettore per L relativo all'autovalore $k - \mu_1$. Poiché L e $k - \mu_1$ sono reali, possiamo assumere che g sia a valori reali. Sia $U = \{x \in V \mid g(x) > 0\}$; rimpiazzando eventualmente g con $-g$, possiamo supporre $|U| \leq |V|/2$ (osserviamo che $U \neq \emptyset$ perchè - vedi il commento che segue il Lemma 2.9 - $\sum_{x\in V} g(x) = 0$).

Definiamo una funzione non-negativa $f \in \mathcal{C}(\Gamma)$ ponendo, per ogni $x \in V$, $f(x) = \max\{g(x), 0\}$. Poiché g è negativa in $V \setminus U$, per ogni $x \in U$ si ha

$$\begin{aligned} Lf(x) &= kf(x) - \sum_{x\sim y\in U} f(y) = kg(x) - \sum_{x\sim y\in U} g(y) \leq \\ &\leq kg(x) - \sum_{y\in V} g(y) = (kI_n - A)g(x) = Lg(x) = (k - \mu_1)g(x) \end{aligned}$$

Quindi

$$\begin{aligned} < Lf, f > &= \sum_{x\in U} Lf(x)f(x) = \sum_{x\in U} Lf(x)g(x) \leq \\ &\leq (k - \mu_1)\sum_{x\in U} g(x)^2 = (k - \mu_1)\sum_{x\in U} f(x)^2 = (k - \mu_1) < f, f >, \end{aligned}$$

e pertanto $< Lf, f > \leq (k - \mu_1) < f, f >$. Applicando (2.21) e (2.20) si ricava finalmente

$$h(\Gamma) < f, f > \leq R_f \leq \sqrt{2k < Lf, f >< f, f >} \leq \sqrt{2k(k - \mu_1)} < f, f >$$

da cui (poiché $< f, f > \neq 0$) deriva l'asserto del Teorema. ∎

Expanders. Sia $k \geq 3$; una famiglia infinita di grafi semplici finiti $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, si dice una *famiglia di k-expanders* se

- Γ_n è k-regolare per ogni $n \geq 1$;
- $\lim_{n\to\infty} |V_n| = \infty$;
- esiste $\epsilon > 0$ tale che $h(\Gamma_n) \geq \epsilon$ per ogni $n \geq 1$.

Dai Teoremi 2.13 e 2.14 segue immediatamente il seguente importante fatto. Dato un grafo connesso k-regolare Γ denotiamo con $\mu_1(\Gamma)$ il massimo autovalore di $A(\Gamma)$ diverso da k.

Corollario 2.15. *Una famiglia infinita di grafi semplici connessi k-regolari* $(\Gamma_n)_{n\geq 1}$*, con* $\lim_{n\to\infty} |V_n| = \infty$*, è una famiglia di k-expanders se e solo se esiste un numero reale* $\epsilon > 0$ *tale che* $k - \mu_1(\Gamma_n) \geq \epsilon$ *per ogni* $n \geq 1$*.*

L'obiettivo primario di questo corso è la costruzione (per certi valori di k) di famiglie di k-expanders. Per fare ciò seguiremo da vicino la trattazione data in: G. Davidoff, P. Sarnak, A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, London Mathematical Society Student Texts **55**, 2003.

Si capisce che una famiglia $(\Gamma_n)_{n\geq 1}$ di k-expanders sarà tanto più pregiata quanto maggiore è il limite inferiore ϵ delle costanti $h(\Gamma_n)$. Si può provare che questo, asintoticamente, non può essere molto grande. Sussiste infatti il seguente risultato (che non dimostriamo).

Teorema 2.16. *Sia* $k \geq 2$*, e sia* $\Gamma_n = (V_n, E_n)$*,* $1 \leq n \in \mathbb{N}$*, una famiglia di grafi seplici connessi e k-regolari, tale che* $|V_n| \to \infty$ *quando* $n \to \infty$*. Allora*

$$\liminf_{n\to\infty} \mu_1(\Gamma_n) \geq 2\sqrt{k-1}.$$

Sia $k \geq 3$. Un grafo semplice finito connesso e k-regolare Γ si dice un *grafo di Ramanujan* se ogni autovalore $\mu \neq \pm k$ della sua matrice di adiacenza soddisfa $\mu \leq 2\sqrt{k-1}$.
Il Teorema 2.16 ci dice che le famiglie di k-expanders teoricamente più efficienti sono quelle (se esistono) costituite da grafi di Ramanujan. Nel seguito vedremo la costruzione di famiglie infinite di grafi k-regolari di Ramanujan per $k = p + 1$, dove p è un primo dispari. Gli altri valori di k per i quali è stata provata l'esistenza di famiglie infinite di grafi k-regolari di Ramanujan sono $k = 3$ e $k = q + 1$, dove q è una potenza di un numero primo. La costruzione esplicita di famiglie infinite di grafi di Ramanujan per un $k \geq 3$ arbitrario è ancora una questione aperta. Recentemente, è stato provato da Friedman che, per ogni $k \geq 3$ ed $\epsilon > 0$, la probabilità che per un grafo connesso k-regolare Γ, $\mu_1(\Gamma) \leq 2\sqrt{k-1} + \epsilon$ sia di Ramanujan tende ad 1 al quando il numero di vertici di Γ tende ad infinito. Sempre di recente, Kassabov, Lubotzky e Nikolov hanno dimostrato che esistono $k \geq 3$ ed $\epsilon > 0$ con la proprietà che per quasi tutti i gruppi semplici finiti è possibile determinare un sistema di k generatori tale che per il grafo di Cayley corrispondente si ha $k - \mu_1 \geq \epsilon$.

2.6 Altri esercizi.

1. Grafi fortemente regolari. Siano k, a, b numeri interi con $k \geq 2$, $a \geq 0$ e $b \geq 1$. Un grafo finito semplice connesso Γ si dice un grafo *fortemente regolare* con parametri (k, a, b) se: Γ è k-regolare e non completo, e per ogni coppia x, y di vertici distinti di Γ il numero di vertici adiacenti sia ad x che a y è a se $x \sim y$, mentre è b se $x \not\sim y$.

Esercizio 2.27. Si provi che il grafo di Petersen è fortemente regolare e che in generale, i grafi di Kneser $K(n, 2)$ (esercizio 1.46) sono fortemente regolari.

Esercizio 2.28. Sia Γ un grafo fortemente regolare su n vertici con parametri (k, a, b), e sia A la sua matrice di adiacenza. Si provi che $A^2 = (a - b)A + bJ_n + (k - b)I_n$.

Esercizio 2.29. Si usi l'esercizio precedente per dimostrare il seguente risultato: un grafo semplice regolare connesso e non completo Γ è fortemente regolare se e solo $A(\Gamma)$ ha esattamente tre autovalori distinti.

2. n-Cubi. Ricordo la definizione (vedi esercizi 1.49 e seguenti). Sia $n \geq 2$: il grafo Q_n, detto n-cubo, è il grafo i cui vertici sono le n-uple a coefficienti in $\{0, 1\}$, ed i cui lati sono tutte e sole le coppie di tali n-uple che differiscono esattamente per una componente.

Esercizio 2.30. Si provi che, per ogni $n \geq 2$, il grafo Q_n è un grafo di Cayley. [si rifletta sull'esercizio 2.9]

Esercizio 2.31. Per $n \geq 2$, sia $A_n = A(Q_n)$ la matrice di adiacenza di Q_n. Si provi che, per ogno $n \geq 2$ e considerato un opportuno ordinamento dei vertici di Q_{n+1}, si ha

$$A_{n+1} = \begin{pmatrix} A_n & I_n \\ I_n & A_n \end{pmatrix}.$$

Esercizio 2.32. Procedendo per induzione su $n \geq 2$, si provi che gli autovalori di $A(Q_n)$ sono $n - 2t$, con $t \in \mathbb{N}$, $0 \leq t \leq n$; e che la molteplicità dell'autovalore $n - 2t$ è $\binom{n}{t}$. [Si osservi che se A, M, P sono matrici quadrate con P invertibile, M diagonale e $PA = MP$, allora

$$\begin{pmatrix} P & P \\ P & -P \end{pmatrix} \begin{pmatrix} A & I \\ I & A \end{pmatrix} = \begin{pmatrix} M + I & 0 \\ I_0 & M - I \end{pmatrix} \begin{pmatrix} P & P \\ P & -P \end{pmatrix}$$

(dove I è la matrice identica), e si applichi l'esercizio precednte]

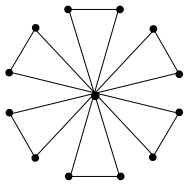
Esercizio 2.33. Si provi che, per ogni $n \geq 2$, $h(Q_n) = 1$.

3. Mulini. In inglese lo chiamano "friendship theorem": in una società con un numero finito $n \geq 4$ di persone ed in cui ogni coppia di membri ha un unico amico in comune esiste uno ed un solo membro che è amico di tutti. Ne vediamo una dimostrazione che utilizza i grafi.

Esercizio 2.34. Sia Γ un grafo finito semplice con n vertici in cui per ogni coppia di vertici distinti x, y esiste un unico vertice che è adiacente sia ad x che a y. Si osservi che Γ non ha quadrati; si provi quindi che se x e y sono vertici non adiacenti allora $d_\Gamma(x) = d_\Gamma(y)$. Si provi poi che se non esiste alcun vertice di grado $n - 1$ allora per ogni coppia di vertici esiste almeno un vertice che non è adiacente ad entrambi. Si concluda che Γ è regolare oppure ammette un vertice di grado $n - 1$.

Esercizio 2.35. Nelle stesse ipotesi su Γ, provare, usando il metodo degli autovalori, che se Γ è regolare allora Γ è un triangolo. [studiare il quadrato della matrice di adiacenza...]

Esercizio 2.36. Nelle stesse ipotesi su Γ delle esercizio 2.34, si provi che se Γ ammette un elemento di grado $n-1$, allora Γ è un grafo del tipo "mulino a vento":



4. Il grafo di Hoffman–Singleton. A meno di isomorfismi, esiste un unico grafo di Moore di valenza 7 e diametro 2, detto grafo di Hoffman–Singleton; tale grafo ha 50 vertici e 175 archi. Ne esistono diverse costruzioni in letteratura; nei prossimi esercizi ne vediamo una classica.

Esercizio 2.37. Sia T l'insieme delle terne (sottoinsiemi di ordine 3) di $\{1, 2, \cdots, 7\}$; quindi $|T| = 35$. Si provi che se $S \subseteq T$ è tale che $|a \cap b| = 1$ per ogni $a, b \in S$, allora $|S| \leq 7$. Un sottoinsieme di ordine 7 di T con tale proprietà si chiama *settetto*; ad esempio

$$123 \quad 145 \quad 167 \quad 246 \quad 257 \quad 347 \quad 356.$$

Una *triade* in T è un insieme di tre elementi a, b, c di T tali che $a \cap b = a \cap c = b \cap c$ ha ordine 1; ad esempio è una triade: 123, 145, 167. Si provi che il numero di triadi di T è 105; si provi quindi che ogni triade è contenuta in esattamente 2 settetti. Dedurre che il numero di settetti distinti di T è 30. L'azione su $\{1, 2, \ldots, 7\}$ del gruppo S_7 si estende in modo naturale ad una azione di S_7 su T, e di conseguenza sull'insieme dei settetti; si provi che tale ultima azione è transitiva.

Esercizio 2.38. Usiamo le notazioni dell'esercizio precedente. Si considera un'orbita del gruppo alterno A_7 sull'insieme dei settetti di T. Tale orbita, che denotiamo con U contiene 15 settetti. Ad esempio, fissiamo l'orbita:

123	123	123	124	127	125	125	124	124	125	127	127	126	126	126
145	157	147	135	136	136	134	137	136	137	135	134	137	135	134
167	146	156	167	145	147	167	156	157	146	146	156	145	147	157
247	245	246	236	246	234	246	235	237	236	234	236	234	237	235
256	267	257	257	235	267	237	267	256	247	256	245	257	245	247
357	356	345	347	347	357	356	346	345	345	367	357	356	346	367
346	347	367	456	567	456	457	457	467	567	457	467	467	567	456

Definiamo quindi il grafo Γ il cui insieme dei vertici è $T \cup U$, e gli archi sono descritti dalle seguenti regole:

se $a, b \in T$, $a \sim b \Leftrightarrow a \cap b = \emptyset$;
se $a \in T$ e $\sigma \in U$, $a \sim \sigma \Leftrightarrow a \in \sigma$;
non ci sono archi tra gli elementi di U.

(si osservi quindi, che il sottografo di Γ indotto da T è il grafo di Kneser $K(7, 3)$). Si dimostri che il grafo Γ così definito è un grafo di Moore di diametro 2 e valenza 7.

Esercizio 2.39. Si provi che il grafo di Kneser $K(7,3)$ ha numero cromatico 3. Si deduca che il grafo di Hoffman–Singleton ha numero cromatico 4.

Esercizio 2.40. (Un'altra costruzione, dovuta a Hafner a partire da una di Robertson) In questa contruzione, l'insieme dei vertici è l'insieme delle terne: $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. La relazione di adiacenza $\sim$ è definita nel modo seguente:

$$\begin{array}{lllll} 1) & (0,x,y) \sim (0,x',y') & \text{se e solo se} & x = x' \ \text{ e } \ y - y' = \pm 1 \\ 2) & (1,m,c) \sim (1,m',c') & \text{se e solo se} & m = m' \ \text{ e } \ c - c' = \pm 2 \\ 3) & (0,x,y) \sim (1,m,c) & \text{se e solo se} & y = mx + c \end{array}$$

dove i calcoli si intendono modulo 5. Si provi che il grafo così definito è 7-regolare, ha diametro 2, e che quindi è un grafo di Moore (per l'unicità è il grafo di Hoffman–Singleton).

5. Indice di stabilità. Un sottoinsieme S dell'insieme dei vertici di un grafo Γ si dice *stabile* (o *indipendente*) se nessuna coppia di elementi di S è adiacente in Γ. L'*indice di stabilità* di un grafo Γ è la massima cardinalità di un suo sottoinsieme stabile di vertici; lo denoteremo con $\alpha(\Gamma)$

Esercizio 2.41. Si determini l'indice di stabilità dei grafi di Kneser (esercizio 1.46 e seguenti), e quello del n-cubo Q_n.

Esercizio 2.42. Sia Γ un grafo con n vertici ed m lati. Si provi che $\alpha(\Gamma)^2 \leq n^2 - 2m$.

Esercizio 2.43. Sia Γ un grafo semplice con n vertici. Si provi che $\alpha(\Gamma)\chi(\Gamma) \geq n$.

Esercizio 2.44. Sia $k \geq 2$, e sia $\Gamma = (V,E)$ un grafo k-regolare con n vertici. Sia μ_{n-1} l'autovalore minimo della matrice di adiacenza di Γ. Scegliendo un sottoinsieme stabile di ordine massimo di V, ed utilizzando le tecniche della dimostrazione del Teorema 2.13, si provi che $\alpha(\Gamma)(k - \mu_{n-1}) \leq -\mu_{n-1}n$. Si concluda che $\chi(\Gamma) \geq 1 - k/\mu_{n-1}$.

Capitolo 3

SL(2,K).

Le famiglie di grafi expanders che descriveremo sono costituite da grafi di Cayley in gruppi di matrici 2×2 invertibili a coefficienti in un campo di ordine primo. Sia per la loro definizione che per dimostrare che tali grafi soddisfano le proprietà che ci interessano, avremo bisogno di diverse informazioni intorno ai gruppi di questo tipo. Questo capitolo serve quindi come introduzione ai gruppi speciali lineari, e comprende qualcosa di più di quanto sarà strettamente necessario per la successiva costruzione dei grafi.

3.1 Definizioni e prime proprietà.

Siano K un campo, $n \geq 1$ un intero positivo., e sia $M_n(K)$ l'anello delle matrici quadrate di ordine n a coefficienti in K. Il gruppo degli elementi invertibili di $M_n(K)$ si denota con $GL(n, K)$ e si chiama il gruppo *Generale Lineare* di ordine n su K. È un fatto ben noto che

$$GL(n, K) = \{A \in M_n(K) \mid \det A \neq 0\},$$

Il determinante definisce un omomorfismo suriettivo

$$\det : \ GL(n, K) \to K^*$$

dove K^* è il gruppo moltiplicativo del campo K. Il nucleo di questo omomorfismo

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

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

$$GL(n, K)/SL(n, K) \simeq K^*. \tag{3.1}$$

Noi saremo interessati prevalentemente al caso in cui K è un campo finito di ordine q. In tal caso, poiché un campo finito è determinato a meno di isomorfismi dal suo ordine[1], si scrive $GL(n, q)$ e $SL(n, q)$ invece di $GL(n, K)$ e $SL(n, K)$.

[1] Ricordiamo che ogni campo finito ha ordine p^m dove p è un numero primo, e che per ogni primo p ed ogni $m \geq 1$ esiste (a meno di isomorfismo) uno ed un solo campo di ordine $q = p^m$, che denoteremo con $\mathbb{F}_q$. In particolare, se p è primo, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Non è difficile determinare gli ordini di questi gruppi. Il numero di vettori (colonna) di dimensione n su un campo con q elementi è q^n. Gli elementi di $GL(n,q)$ sono tutte e sole le matrici di ordine n i cui vettori colonna formano un sistema di vettori linearmente indipendenti: abbiamo quindi $q^n - 1$ scelte per la prima colonna; e in generale il numero di possibilità per la i-esima colonna ($2 \leq i \leq n$), è dato dal numero di vettori colonna che possono essere scelti al di fuori del sottospazio genarato dalle precedenti $i-1$ colonne, tale sottospazio (avendo dimensione $i-1$) contiene q^{i-1} vettori; quindi il numero di scelte per la i-esima colonna è $q^n - q^{i-1} = q^{i-1}(q^{n-i+1} - 1)$. In totale si ottiene

$$|GL(n,q)| = \prod_{i=1}^{n} q^{i-1}(q^{n-i+1} - 1) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1).$$

Poichè, per (3.1), $|GL(n,q)/SL(n,q)| = q - 1$, ricaviamo

$$|SL(n,q)| = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n}(q^i - 1). \tag{3.2}$$

In particolare, per $n = 2$,

$$|SL(2,q)| = q(q^2 - 1) = q(q-1)(q+1). \tag{3.3}$$

Torniamo al caso di un campo qualsiasi K. Se $1 \leq i, j \leq n$, denotiamo con e_{ij} la matrice $n \times n$ i cui coefficienti sono tutti 0 tranne quello di posto (i,j) che è $1 = 1_K$. Per ogni $b \in K$ ed indici i, j come sopra, poniamo $t_{ij}(b) = 1 + be_{ij}$; (dove per comodità scriviamo $1 = I_n$ 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 $t_{ij}(b) \in SL(n,K)$.
Il prodotto di matrici del tipo e_{ij} è facilmenmte descritto; si ha

$$e_{ij} \cdot e_{kt} = \begin{cases} e_{it} & \text{se} \quad j = k \\ 0 & \text{se} \quad j \neq k \end{cases} \tag{3.4}$$

da cui, per distributività, scende facilmente la regola per moltiplicare matrici del tipo $t_{ij}(b)$. In particolare si vede che, per ogni $i \neq j$ e $b \in K$, $t_{ij}(b)^{-1} = t_{ij}(-b)$. È conveniente anche osservare le seguenti formule per commutatori: (1) se i, j, k sono tutti distinti

$$[t_{ik}(b), t_{kj}(c)] = t_{ik}(-b)t_{kj}(-c)t_{ik}(b)t_{kj}(c) = t_{ij}(bc) \tag{3.5}$$

Lemma 3.1. *Per $n \geq 2$ ed ogni campo K, il gruppo $SL(n,K)$ è generato dall'insieme $T = \{t_{ij}(b) \mid i \neq j,\ b \in K\}$.*

Tralasciamo i dettagli della dimostrazione di questo Lemma. Si tratta essenzialmente della riduzione in forma diagonale di una matrice quadrata mediante le cosiddette trasformazioni elementari. Non è difficile vedere che ogni trasformazione elementare può essere interpretata come il risultato di moltiplicare (a destra o a sinistra) per opportune matrici del tipo $t_{ij}(b)$. Ad esempio: sommare, nella matrice A, alla j-esima riga la i-esima moltiplicata per b significa moltiplicare A a destra per $t_{ij}(b)$, e così via. Dunque se A è una matrice di ordine n su K

esistono P, Q matrici appartenenti al sottogruppo di $GL(n,K)$ generato dalle $t_{ij}(b)$ tali che $D = PAQ$ è diagonale, e quindi $A = P^{-1}DQ^{-1}$; se $\det A = 1$ allora (poiché $\det P = 1$ e $\det Q = 1$, si ha che anche il determinante di D è 1. Rimane quind da provare che se D è una matrice diagonale e $\det D = 1$, allora D è un prodotto di matrici del tipo $t_{ij}(b)$. Per $n = 2$, basta osservare che, se $0 \neq d \in K$,

$$\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} = t_{21}(-1)t_{12}(1)t_{21}(-1)t_{12}(-d)t_{21}(d^{-1})t_{12}(-d). \tag{3.6}$$

Per il caso generale sia $n \geq 3$, e, con l'ovvio significato, $D = diag(d_1, d_1, \ldots, d_n)$ con $d_1 d_2 \cdots d_n = 1$. Procediamo per induzione sul numero di $d_i \neq 1$. Non è difficile vedere che possiamo supporre $d_1 \neq 1 \neq d_2$. Calcolando come in (3.6) si ha che $D_1 = disg(d_1^{-1}, d_1, 1, \ldots, 1)$ è un prodotto di matrici del tipo $t_{ij}(b)$; e poiché anche $D_1 D$ lo è per ipotesi induttiva, si conclude che D è un prodotto di matrici $t_{ij}(b)$.

Esercizio 3.1. Svolgere nei dettagli la dimostrazione del Lemma 3.1 abbozzata sopra.

Il Lemma 3.1 ci sarà molto utile più avanti. Per il momento osserviamo che da esso segue che (per $n \geq 2$) $g \in GL(n,K)$ commuta con ogni elemento di $SL(n,K)$ se e soltanto se commuta con ogni matrice del tipo $t_{ij}(b)$, eventualità che a sua volta si verifica se e solo se g commuta con ogni matrice e_{ij} con $i \neq j$. Ovvero, con le usuali notazioni di teoria dei gruupi, posto $G = GL(n,K)$ e $S = SL(n,K)$, $C_G(S) = \bigcap_{i \neq j} C_G(e_{ij})$. Ora, si vede facilmente in modo diretto che una matrice g commuta con ogni e_{ij} se e solo se g è una matrice scalare $g = aI_n$, per qualche $a \in K$, e di conseguenmza g commuta con ogni matrice. Se poi, come nel nostro caso, vogliamo che g sia invertibile, si ha $g = aI_n$ con $a \in K^*$. Denotiamo con K^*I_n l'insieme di tutte le matrici di questo tipo; posto $G = GL(n,K)$, abbiamo quindi[2]

$$C_G(SL(n,K)) = K^*I_n = Z(G).$$

Si ha perciò,

$$Z(SL(n,K)) = K^*I_n \cap SL(n,K) = \{aI_n \mid a \in K^*,\ a^n = 1\}. \tag{3.7}$$

I gruppi quoziente di $GL(n,K)$ e di $SL(n,K)$ modulo i propri centri, si chiamano, rispettivamente, il gruppo *Proiettivo Generale Lineare* ed il gruppo *Proiettivo Speciale Lineare* di ordine n su K, e si denotano con

$$PGL(n,K) \qquad \text{e} \qquad \mathrm{PSL(n,K)}.$$

È chiaro che la assegnazione $a \mapsto aI_n$ definisce un isomorfismo tra il gruppo moltpilicativo K^* e K^*I_n. Se K e finito di ordine q, K^* è un gruppo ciclico di ordine $q-1$, e segue dalla teoria elementare dei gruppi ciclici che l'insieme $\{a \in K^* \mid a^n = 1\}$ è un sottogruppo di K^* il cui ordine coincide con il massimo comun divisore $(n, q-1)$. Quindi, dalla formula (3.2) si ottiene

$$|PSL(n,q)| = \frac{q^{\frac{n(n-1)}{2}}(q^2-1)\cdots(q^n-1)}{(n,q-1)}. \tag{3.8}$$

[2]Ricordo che se G è un gruppo, $Z(G)$ denota il *centro* di G, ovvero l'insieme di tutti gli elementi $x \in G$ tali che $gx = xg$ per ogni $g \in G$. È immediato verificare che il centro è un sottogruppo normale (e abeliano) di G.

In particolare, per $n = 2$ e q non è una potenza di 2,

$$|PSL(n,q)| = \frac{q(q-1)(q+1)}{2} \tag{3.9}$$

(in questo caso $1 \neq -1$ e $Z(SL(2,q)) = \{I_n, -I_n\}$). Mentre nel caso $q = 2^m$ si ha $PSL(2,2^m) = SL(2,2^m)$ per ogni $m \geq 1$.

Esercizio 3.2. Si provi che se $\mathrm{char}(K) \neq 2$ allora $SL(2,K)$ contiene un unico elemento di ordine 2 (cioè $g \neq 1$ con $g^2 = 1$) che è $-I_2$.

Sottogruppi notevoli. Ricordiamo che se s^m è la massima potenza di un primo s che divide l'ordine di un certo gruppo finito G, allora G ammette sottogruppi di ordine s^m (detti s-sottogruppi di Sylow); se S_1 e S_2 sono due distinti s-sottogruppi di Sylow di G allora S_1 e S_2 sono *coniugati*, ovvero esiste $g \in G$ tale che $S_2^g = S_1$.

Sia $q = p^m$, con p un numero primo e $m \geq 1$. Allora, le formule (3.1), 3.2) e (3.8), assicurano che i p-sottogruppi di Sylow di $SL(n,q)$ coincidono con quelli di $GL(n,q)$ ed hanno ordine $q^{\frac{n(n-1)}{2}}$. Iinoltre, i p-sottogruppi di Sylow del quoziente $PSL(n,q)$ sono tutti e soli quelli del tipo $\bar{U} = UZ/Z$ con U un p-sottogruppo di Sylow di $SL(n,q)$ (e $Z = Z(SL(n,q))$.
È facile trovare un p-sottogruppo di Sylow di $SL(n,q)$: si considera l'insieme $U = UT(n,q)$ di tutte le matrici unitriangolari superiori di ordine n (gli elementi di U sono tutte e sole le matrici (a_{ij}) su $\mathbb{F}_q$ ccn $a_{ij} = 0$ se $i > j$ e $a_{ii} = 1$). U è un sottogruppo di $SL(n,q)$, ed il suo ordine è quello giusto: infatti gli elementi di U si ottengono scegliendo in tutti i modi possibili i coefficient a_{ij} con $i < j$; poiché il numero di tali coefficienti è $n(n-1)/2$ e per ognuno di essi ci sono q scelte, si ricava

$$|U| = q^{\frac{n(n-1)}{2}}$$

e dunque U è un p-sottogruppo di Sylow di $SL(n,q)$. Gli altri sono, per il Teorema di Sylow ricordato prima, tutti e soli i coniugati di U.

Esercizio 3.3. Con le notazioni di sopra, si provi che $U = \langle t_{ij}(b) \mid 1 \leq i < j \leq n,\ b \in \mathbb{F}_q \rangle$.

Consideriamo l'azione naturale di $G = SL(n,K)$ sullo spazio vettoriale $V = K^n$. Sia H un sottogruppo di G, W un sottospazio H-invariante di V, e $g \in N_G(H)$; allora è immediato vedere che anche $g(W)$ è un sottospazio H-invariante.
Sia B l'insieme delle matrici triangolari superiori in $G = SL(n,K)$, quindi

$$B = \{(a_{ij}) \in SL(n,K) \mid a_{ij} = 0 \text{ se } i > j\}$$

(B è detto un *sottogruppo di Borel* di $SL(n,K)$). Sia $e_1, e_2, \ldots, e_n$ la base canonica di K^n. Allora i sottospazi di V che sono U-invarianti sono tutti e soli quelli che costituiscono la catena

$$\{0\} < \langle e_1 \rangle < \langle e_1, e_2 \rangle < \cdots < \langle e_1, e_2, \ldots, e_{n-1} \rangle < V.$$

Poiché dunque sottospazi U-invarianti distinti hanno dimensioni diverse, segue da quanto ossrvato sopra che $N_G(U)$ lascia invarianti tutti i sottospazi della catena di sopra, quindi

gli elementi di $N_G(U)$ sono matrici triangolari superiori, cioè $N_G(U) \leq B$. Poiché è facile verificare anche l'inclusione inversa si ricava

$$N_{SL(n,K)}(U) = B. \tag{3.10}$$

Sia H il gruppo delle matrIci diagonali in $SL(n, K)$

$$H = \left\{ \left(\begin{array}{cccc} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \cdot & \cdot & \cdots & \\ 0 & 0 & \cdots & a_n \end{array} \right) \middle| \, a_i \in K^*, \ a_1 a_2 \cdots a_n = 1 \right\}.$$

Allora $B = UH$ e $U \cap H = 1$. Inoltre $|H| = (q-1)^{n-1}$, e $|B| = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}$ (da cui posso ricavare il numero di p-sottogruppi di Sylow di $SL(n, K)$, che è $|SL(n, K)|/|B|$).

Esercizio 3.4. Sia V spazio vettoriale sul campo K, di dimensione $n \geq 1$. Siano date due catene di sottospazi, $\{0\} = U_0 < U_1 < \cdots < U_n$ e $\{0\} = W_0 < W_1 < \cdots < W_n$, tali che $\dim(U_i) = i = \dim(W_i)$ per ogni $0 \leq i \leq n$. Si provi che esiste $g \in SL(n, K)$ tale che $U_i^g = W_i$ per ogni $i = 0, 1, \ldots, n$.

3.2 Permutazioni.

Una breve digressione per ricordare alcuni aspetti di base riguardanti le azioni di gruppi come gruppi di permutazioni. Questo ci servirà per dimostrare la semplicità (in quasi tutti i casi) di $PSL(n, q)$.

Sia G un gruppo che opera (come permutazioni) sull'insieme non vuoto Ω: utilizzeremo la notazione a destra per le permutazioni e se $g \in G$ denoteremo con la stessa lettera g la permutazione indotta da g su Ω. Per ogni $x \in \Omega$ indichiamo con G_x lo *stabilizzatore* di x in G, ovvero

$$G_x = \{g \in G \mid x^g = x\}.$$

È ben noto che G_x è un sottogruppo di G e che l'insieme delle classi laterali destre di G modulo G_x è naturalmente in corrispondenza biunivoca con l'orbita di x tramite G, $\{x^g \mid g \in G\}$. Ancora, $\bigcap_{x \in \Omega} G_x$ è il *nucleo* dell'azione; l'azione si dice *fedele* se il nucleo è $\{1_G\}$.

Un"azione di G su Ω si dice *transitiva* se per ogni $x, y \in \Omega$ esiste un $g \in G$ tale che $x^g = y$. Se $k \geq 1$, l'azione si dice *k-transitiva* se per ogni due k-uple ordinate di elementi distinti di Ω, $(x_1, \ldots, x_k)$ e $(y_1, \ldots, y_k)$, esiste $g \in G$ tale che $x_i^g = y_i$ per ogni $i = 1, \ldots, k$.
Un altro concetto che ci serve richiamare è quello di azione primitiva. Una partizione $\mathcal{F}$ di Ω si dice G-invariante se $X^g \in \mathcal{F}$ per ogni $X \in \mathcal{F}$ ed ogni $g \in G$ (dove ovviamente $X^g = \{x^g \mid x \in X\}$). Se $|\Omega| > 1$ ci sono in ogni caso almeno due partizioni G-invarianti di Ω: quella i cui elementi (detti *blocchi*) sono i singoletti $\{x\}$ $(x \in \Omega)$, e quella costituita da un unico blocco che è Ω stesso. Queste due partizioni sono chiamate le partizioni banali, ed un'azione del gruppo G su Ω si dirà *primitiva* se quelle banali sono le sole partizioni G-invarianti di Ω.
Sia data un'azione di un gruppo G su un insieme Ω; per ogni $g \in G$ denotiamo con Ω^g l'insieme dei *puinti fissi* di g, ovvero $\Omega^g = \{x \in \Omega \mid x^g = x\}$.

Lemma 3.2. *Se il gruppo fiinito G opera transitivamente sull'insieme finito Ω, allora*

$$\sum_{g\in G} |\Omega^g| = |G|.$$

DIMOSTRAZIONE. Calcolando la cardinalità dell'insieme $S = \{(x, g) \in \Omega \times G \mid x^g = x\}$ in due modi, si trova

$$\sum_{g\in G} |\Omega^g| = |S| = \sum_{x\in\Omega} |G_x|.$$

Poiché l'azione è transitiva, per ogni $x \in \Omega$, si ha $|\Omega| = |G : G_x] = |G|/|G_x|$. Quindi

$$\sum_{g\in G} |\Omega^g| = \sum_{x\in\Omega} \frac{|G|}{|\Omega|} = |\Omega|\frac{|G|}{|\Omega|} = |G|$$

come si voleva dimostrare. ∎

Esercizio 3.5. Si generalizzi il Lemma precedente, provando che data un'azione del gruppo finito G sull'insieme finito Ω, se t è il numero di orbite, allora $\sum_{g\in G} |\Omega^g| = t|G|$.

Esercizio 3.6. Sia data un'azione transitiva del gruppo finito G sull'insieme Ω. Sia $x \in \Omega$, e sia r il numero di orbite che lo stabilizzatore G_x ha su Ω. Si provi che

$$r|G| = \sum_{g\in G} |\Omega^g|^2.$$

Esercizio 3.7. Sia data una azione del gruppo G sull'insieme non vuoto Ω.

(i) Si provi che se l'azione è primitiva allora è transitiva.

(ii) Si provi che l'azione è primitiva se e solo se per ogni $x \in \Omega$, lo stabilizzatore G_x è un sottogruppo massimale di G.

Proposizione 3.3. *Sia G un gruppo che opera sull'insieme Ω Se l'azione è 2-transitiva allora è primitiva.*

DIMOSTRAZIONE. Sia il gruppo G 2-transitivo su Ω e sia $\mathcal{F}$ una partizione G-invariante di Ω. Supponiamo, per assurdo che $\mathcal{F}$ non sia una delle due partizioni banali; allora esiste $X \in \mathcal{F}$, tale che $1 < |X|$ e $X \neq \Omega$. Siano dunque x_1, x_2 elementi distinti di X e $y \in \Omega \setminus X$. Per la 2-transitività di G su Ω esiste allora un $g \in G$ tale che

$$\begin{cases} x_1^g = x_1 \\ x_2^g = y \end{cases}$$

da cui $x_1 \in X \cap X^g$ e $y \in X^g \setminus X$, in contraddizione con l'assunzione che $\mathcal{F}$ fosse una partizione G-invariante. Dunque le sole partizioni G-invarianti di Ω sono quelle banali e pertanto G è primitivo per definizione. ∎

Esercizio 3.8. Per $n \geq 4$ sia D_n il gruppo dei movimenti rigidi di un n-agono regolare Ω_n, e si consideri l'azione di D_n sull'insieme dei vertici di Ω_n. Si provi che tale azione è transitiva ma non 2-transitiva, e che è primitiva se e soltanto se n è un numero primo.

Lemma 3.4. *Sia G un gruppo che opera sull'insieme Ω, ed N il nucleo dell'azione.*

(1) Sia G primitivo; se $H \trianglelefteq G$ è tale $H \not\leq N$ allora H è transitivo su Ω.

(2) Se $H \leq G$ è transitivo su Ω allora $G = G_x H$ per ogni $x \in \Omega$.

DIMOSTRAZIONE. (1) Sia G primitivo ed H un suo sottogruppo normale non contenuto nel nucleo N dell'azione. Poiché $H \neq N$, esiste $x \in \Omega$ che non è fissato da tutti gli elementi di H. Denotiamo con $X = x^H$ l'orbita di x rispetto all'azione di H. Allora $\mathcal{F} = \{X^g \mid g \in G\}$ è una partizione G-invariante di Ω (lo si dimostri). Siccome $|X| > 1$ e G è primitivo su Ω, si conclude che $|\mathcal{F}| = 1$, cioè che $X = \Omega$, provando che H è transitivo.

(2) Sia H un sottogruppo di G che è transitivo su Ω, e sia $x \in \Omega$ fissato. Preso $g \in G$, esiste per ipotesi un $h \in H$ tale $x^g = x^h$. Dunque $x^{gh^{-1}} = x$, ovvero $gh^{-1} \in G_x$. Quindi $g = (gh^{-1})h \in G_x H$. Pertanto $G = G_x H$. ∎

Torniamo ora ai gruppi di matrici. Il gruppo $G = GL(n, K)$ è il gruppo delle trasformazioni lineari invertibili dello spazio vettoriale $V = K^{(n)}$. Tale azione determina una azione di G sullo spazio proiettivo $(n-1)$-dimesionale su K, il cui nucleo è il centro $Z(G)$ (quindi il gruppo proiettivo $PGL(n, K)$ ha una azione fedele sullo spazio proiettivo $(n-1)$-dimensionale). A noi interessa semplicemente l'azione di G come gruppo di permutazioni sull'insieme $P(n-1, K)$ dei punti di tale spazio proiettivo. Tale insieme è l'insieme dei sottospazi 1-dimensionali di V, quindi

$$P(n-1, K) = \{vK \mid 0 \neq v \in V\},$$

e l'azione di G è data de $(vK)^g = g^{-1}(v)K$ per ogni $g \in G$ e $vK \in P(n-1, K)$.

Proposizione 3.5. *Sia K un campo e $n \geq 2$. L'azione del gruppo $SL(n, K)$ su $P(n-1, K)$ è 2-transitiva.*

DIMOSTRAZIONE. Siano v_1K, v_2K, y_1K, y_2K elementi di $P(n-1, K)$ con $v_1K \neq v_2K$ e $y_1K \neq y_2K$. Allora (v_1, v_2) e (y_1, y_2) sono due coppie di vettori indipendenti di $V = K^{(n)}$. Possiamo quindi completare v_1, v_2 ad una base ordinata $v_1, v_2, \ldots, v_n$ di V, e lo stesso facciamo con y_1, y_2 ottenendo la base $y_1, y_2, \ldots, y_n$. È un fatto ben noto che esiste allora una trasformazione lineare invertibile di V (cioè un elemento g di $GL(n, K)$) tale che $g(y_i) = v_i$ per $i = 1, 2, \ldots, n$. Quindi, in particolare, $(v_1K)^g = y_1K$ e $(v_2K)^g = y_2K$. Per provare che un tale elemento g può essere preso in $SL(n, K)$ (completando quindi la dimostrazione che $SL(n, K)$ opera 2-transitivamente su $P(n-1, K)$) si osservi che se $0 \neq \delta \in K$ allora $vK = (\delta v)K$ (si prosegua per esercizio). ∎

Facciamo anche un'altra osservazione, che ci sarà utile più avanti, quando studieremo in dettaglio il caso bidimensionale.

Lemma 3.6. *Se $g \in SL(2, K)$ fissa tre punti distinti di $P(1, K)$ allora g fissa tutti i punti di $P(1, K)$ (quindi $g \in Z(SL(2, K))$).*

DIMOSTRAZIONE. Si osservi, in generale, che se $vK \in P(n-1, K)$ è un punto fisso per $g \in GL(n, K)$ allora v è un autovettore di g. Nel caso $n = 2$ l'enunciato segue facilmente dalla teoria elementare degli autovettori ed autovalori di una matrice.
Volendo vedre la cosa in modo diretto, siano uK, vK, wK tre punti distinti di $P(1, K)$ che sono fissati da g. Allora esistono degli scalari $\alpha, \beta, \gamma \in K \setminus \{0\}$ tali che $g(u) = \alpha u$, $g(v) = \beta v$ e

$g(w) = \gamma(w)$. Ma, poichè $uK \neq vK$, u e v sono vettori indipendenti e pertanto costituiscono una base di $V = K^{(2)}$; w è quindi una combinazione lineare di essi: $w = \lambda u + \eta v$ (e siccome wK è diverso sia da uK che da vK, λ e η sono entrambi diversi da zero). Pertanto $\gamma w = g(w) = \lambda g(u) + \eta g(v) = \lambda\alpha u + \eta\beta v$. Dunque, $\gamma\lambda = \lambda\alpha$ e $\gamma\eta = \eta\beta$, e poiché $\lambda \neq 0 \neq \eta$ si ricava $\alpha = \gamma = \beta$. Dunque g è una matrice scalare $g = \alpha I_2$, come si voleva dimostrare. ∎

Spesso può essere conveniente descrivere l'azione di $G = GL(2, K)$ sulla retta proiettiva $P(1, K)$ mediante le trasformazioni di Möbius. Secondo tale punto di vista la retta proiettiva è vista come l'insieme $P = K \cup \{\infty\}$, con le usuali regole di calcolo riguardo al punto ∞; e l'azione di G su P è quella che a ciascuna matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ di G associa la trasformazione di P data da, per ogni $z \in P$,

$$z \mapsto \frac{az + b}{cz + d}.$$

Esercizio 3.9. Si adotti questo punto di vista per dare un'altra dimostrazione del Lemma 3.6. Usando sempre le trasformazioni di Möbius, si determini lo stabilizzatore in $G = GL(2, K)$ di un punto di $P = P(1, K)$, e quello di due punti (per la 2-transitività é sufficiente scegliere in modo opportuno, prima un punto di P, e poi una coppia di punti).

3.3 Semplicità.

Ricordiamo che se G è un gruppo, il *sottogruppo derivato* G' è il minimo sottogruppo normale di G tale che il quoziente $G/.G'$ è abeliano. È un fatto del tutto elementare che G' è il saottogruppo generato dall'insieme di tutti i *commutatori* $[x, y]$, dove, per ogni $x, y \in G$, $[x, y] = x^{-1}y^{-1}xy$. Un gruppo si dice *perfetto* se coincide con il proprioo derivato.

Dimostreremo che, se $n \geq 3$ oppure K è un campo con almeno 4 elementi, allora $PSL(n, K)$ è un gruppo semplice. Cominciamo col provare che, tranne pochi casi, $SL(n, K)$ è perfetto.

Lemma 3.7. *Sia $n \geq 2$. Tranne i casi $(n, q) = (2, 2), (2, 3)$, $SL(n, K) = SL(n, K)'$.*

Dimostrazione. Sia $K = \mathbb{F}_q$. Per il Lemma (3.1) è sufficiente dimostrare che ogni matrice $t_{ij}(b)$, con $i \neq j$ e $b \in K$, appartiene al sottogruppo derivato $SL(n, q)'$, cioè è un prodotto di commutatori di elementi di $SL(n, q)$.
Se $n \geq 3$, esiste un indice $1 \leq k \leq n$, con $i \neq k \neq j$, ed applicando la formula (3.5) si ottiene $[t_{ik}(1), t_{kj}(b)] = t_{ij}(b)$.
Sia quindi $n = 2$ ed assumiamo che il campo K contenga almeno 4 elementi. Esiste quindi un elemento $d \in K$ con $d \neq 0$ e $d^2 - 1 \neq 0$. Scelto un tale d abbiamo

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \in SL(2, K).$$

Per $b \in K$, sia $c = b(d^2 - 1)^{-1}$; allora

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c(d^2 - 1) \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$$

cioè

$$t_{12}(b) = \left[\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right] \in SL(2,K)'.$$

Similmente si dimostra che, per ogni $b \in K$, $t_{21}(b) \in SL(2,K)$, concludendo dunque che $SL(2,K) = SL(2,K)'$. ∎

Per provare la semplicità di $PSL(n,K)$ utilizzeremo l'azione di esso sullo spazio proiettivo $P(n-1,K)$, che abbiamo già visto essere 2-transitiva.

Proposizione 3.8. *Sia G un gruppo che opera sull'insdieme Ω, e sia N il nucleo dell'azione. Supponiamo che*

(i) G è primitivo su Ω;

(ii) $G = G'$;

(iii) esiste $x \in \Omega$ ed esiste un sottogruppo abeliano A di G tali che $A \trianglelefteq G_x$ e $G = \langle A^g \mid g \in G \rangle$.

Allora G/N è un gruppo semplice.

Dimostrazione. Siano G, $x \in \Omega$ ed A come nelle ipotesi. Sia H/N un sottogruppo normale di G/N con $H/N \neq 1$. Allora $H \trianglelefteq G$ e $H \not\leq N$. Per il punto (2) della Proposizione 3.3, H è transitivo su Ω, e per il punto (3) della stessa Proposizione, $G = G_x H$ per ogni $x \in \Omega$. Siano $x \in \Omega$ e $A \trianglelefteq G_x$ come nell'ipotesi (iii) (si osservi che la transitività comporta che la scelta di x è irrilevante). Allora (poiché $H \trianglelefteq G$) $AH \trianglelefteq G_x H = G$. Quindi, per ogni $g \in G$, $AH = (AH)^g \geq A^g$ e dunque, per (iii), $AH = G$. Ora, per il 2^o teorema di omomorfismo, $G/H = AH/H \simeq A/A \cap H$, e dunque G/H è abeliano. Quindi $H \geq G'$ e pertanto, per l'ipotesi (ii), $H = G$. Dunque $H/N = G/N$, provando che G/N è semplice. ∎

Questo fatto è quello che ci serve per dimostrare la semplicità (in quasi tutti i casi) dei gruppi $PSL(n,K)$.

Teorema 3.9. *Sia K un campo e $n \geq 2$. Sia inoltre $|K| > 3$ se $n = 2$. Allora il gruppo $PSL(n,K)$ è semplice (non abeliano).*

Dimostrazione. Applicheremo la Proposizione 3.8 al gruppo $G = SL(n,K)$, nella sua azione sulla retta proiettiva $P(1,K)$.
Tale azione è 2-transitiva per la Proposizione 3.5, ed è quindi primitiva per la Proposizione 3.3; inoltre, nelle ipotesi dell'enunciato, $G = G'$ per il Lemma 3.7. Quindi le condizioni (i) e (ii) della Proposizione 3.8 sono soddisfatte. Rimane da verificare che anche (iii) è soddisfatta. Consideriamo $SL(n,K)$ nella sua rappresentazione naturale come gruppo di automorfismi dello spazio vettoriale K^n rispetto alla base canonica $e_1, \ldots, e_n$, e fissiamo il punto $x = e_1 K$ dello spazio proiettivo $P(n-1,K)$. Lo stabilizzatore in G di x è quindi l'insieme degli automorfismi ϕ di V che ammettono e_1 come autovettore, ovvero tali che $\phi(e_1 K) = e_1 K$. Come matrici, sono tutte e sole quelle del tipo

$$\left(\begin{array}{c|c} a_{11} & a_{12}\, a_{13} \cdots\ a_{1n} \\ \hline 0 & \mathrm{B} \\ \vdots & \end{array} \right)$$

con $a_{11} \det B = 1$. Consideriamo il sottoinsieme A di G_x costituito da tutte e sole le matrici del tipo

$$\left(\begin{array}{c|c} 1 & a_{12}\, a_{13} \cdots\ a_{1n} \\ \hline 0 & \\ & I_{n-1} \\ & \end{array}\right)$$

In termini di operatori lineari, A può essere descritto nel modo seguente

$$A = \{\phi \in SL(n,K) \mid \phi(v) - v \in e_1 K \ \forall v \in V\}. \tag{3.11}$$

Si verifica facilmente che A è un sottogruppo abeliano di G_x (ed è isomorfo al prodotto diretto di $n-1$ copie del gruppo additivo $(K,+)$). Proviamo che A è normale in G_x. Siano dunque $\phi \in A$ e $\eta \in G_x$. Allora, $\eta(e_1K) = e_1K$ e, per ogni $v \in V$, $\phi(\eta(v)) - \eta(v) \in e_1K$. Quindi, per ogni $v \in V$,

$$\phi^\eta(v) - v = \eta^{-1}\phi(\eta(v)) - \eta^{-1}(\eta(v)) = \eta^{-1}(\phi(\eta(v)) - \eta(v)) \in \eta^{-1}(e_1K) = e_1K,$$

e dunque $\phi^\eta \in A$ per (3.11). Ciò prova $A \trianglelefteq G_x$.
Dobbiamo ora dimostrare che $A^G = G$, dove $A^G = \langle A^g \mid g \in G\rangle$. Per fare questo cominciamo con l'osservare che A^G è normale in G e che

$$A = \langle t_{1j}(b) \mid 1 < j \leq n,\ b \in K\rangle. \tag{3.12}$$

Applicando la formula (3.5) si ottiene che, per $2 \leq i,k \leq n$ con $j \neq k$,

$$A^G \ni [t_{j1}(b), t_{1k}(1)] = t_{jk}(b) \tag{3.13}$$

per ogni $b \in K$. Sia $2 \leq j \leq n$; se $n \geq 3$ esiste un indice k con $1 \neq k \neq j$, e tenuto conto che $t_{jk}(b) \in A^G$ per (3.13), applicando ancora la (3.5) si ha

$$A^G \ni [t_{jk}(1), t_{k1}(b)] = t_{j1}(b).$$

Se invece $n = 2$, ponendo $h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, si ha $h \in G$ e, per qualsiasi $b \in K$,

$$A^G \ni h^{-1} t_{12}(-b) h = t_{21}(b).$$

In ogni caso, quindi otteniamo che A^G contiene $t_{ij}(b)$ per ogni coppia di indici $i \neq j$ ed ogni $b \in K$. Per il Lemma 3.1 si conclude che $A^G = G$.
Dunque tutte le ipotesi dell'enunciato della Proposizione 3.8 sono soddisfatte da G e pertanto (poichè $Z = Z(G)$ è il nucleo dell'azione di G su $P(1,K)$) si ha che $PSL(n,K) = G/Z$ è semplice. ∎

Esercizio 3.10. Si provi che $SL(2,2) = GL(2,2) \simeq S_3$, e che $PGL(2,3) \simeq S_4$.

Esercizio 3.11. Si provi che $SL(2,4) \simeq A_5 \simeq PSL(2,5)$ (dove, per $n \geq 2$, con A_n denotiamo il sottogruppo alterno di S_n).

3.4 Sottogruppi di PSL(2,q).

Da qui in avanti ci occuperemo del caso 2-dimensionale, proponendoci di descriverne i sottogruppi. Di fatto, sarebbe possibile descrivere con precisione tutti i sottogruppi di $PSL(2,q)$ per q una potenza di un primo (un risultato dovuto essenzialmente a E. Dickson nei primi anni del $'900$; si veda e.g. B. Huppert, *Endlichen Gruppen, I*). Per semplicità ci limitiamo a trattare in modo più approfondito il caso in cui q è un primo dispari, che è poi quello che ci serve per le applicazioni.

Manteniamo alcune delle notazioni introdotte nella sezione 3.1. Fissato un primo dispari q, poniamo $G = SL(2,q)$. Indichiamo quindi con U il gruppo delle matrici unitriangolari

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \Big| b \in \mathbb{F}_q \right\}$$

con B il suo normalizzante, ovvero il sottogruppo di Borel

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \Big| a, b \in \mathbb{F}_q,\ a \neq 0 \right\}$$

quindi $|B| = q(q-1)$, e $B = N_G(U) = UH$, con $U \cap H = \{1\}$, dove

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \Big| 0 \neq a \in \mathbb{F}_q \right\}.$$

(Chi preferisce la descrizione di $PSL(2,q)$ mediante le trasformazioni di Möbius, vedrà che U è il sottogruppo costituito dalle traslazioni $z \mapsto z + b$ (con $b \in \mathbb{F}_q$), e H quello costituito dalle omotetie $z \mapsto a^2 z$ (per $0 \neq a \in \mathbb{F}_q$)).
Abbiamo già osservato che U è un q-sottogruppo di Sylow di G, e quindi ogni elemento di ordine q è contenuto in qualche coniugato di U. Inoltre, poiché U ha ordine primo, deduciamo che, per ogni $g \in G$,

$$g \notin B \ \Rightarrow\ U \cap U^g = \{1\}. \tag{3.14}$$

Scriviamo $\mathbb{F} = \mathbb{F}_q$, e consideriamo l'azione naturale di G sullo spazio vettoriale $V = \mathbb{F}^2$, che vediamo dotato della base canonica $e_1 = (1,0)$ e $e_2 = (0,1)$, e quindi l'azione di G sulla retta proiettiva

$$P(1,q) = \{v\mathbb{F} \mid 0 \neq v \in V\}.$$

Vediamo allora che B è lo stabilizzatore del punto $e_1\mathbb{F}$, ovvero $B = G_{e_1\mathbb{F}}$. Poiché l'azione è transitiva si ha (confermando quello che si vede usando semplicemente il teorema di Lagrange),

$$[G : B] = |P(1,q)| = q + 1. \tag{3.15}$$

(ricordo che, poiché $B = N_G(U)$, questo è il numero di coniugati distinti di U in G).
Vediamo poi che H è lo stabilizzatore della coppia ordinata $(e_1\mathbb{F}, e_2\mathbb{F})$; siccome G è 2-transitivo su $P(1,q)$, ne segue che se $g \in G$ fissa due punti distinti di $P(1,q)$ (e quindi la loro coppia ordinata) allora g appartiene a qualche coniugato di H. Inoltre, poiché per il

Lemma 3.6 solo gli elementi nel nucleo dell'azione (ovvero quelli del centro $Z(G) = \{aI_n \mid a \in K, a^n = 1\}$ fissano tre punti distinti, anche per H si ha qualcosa di analogo alla (3.14),

$$g \in B \setminus N_G(H) \;\Rightarrow\; H \cap H^g = Z(G). \tag{3.16}$$

Non è difficile capire chi è $N_G(H)$. Sia $\rho = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Nell'azione su $P(1,q)$, ρ scambia $e_1\mathbb{F}$ e $e_2\mathbb{F}$. Facendo i calcoli, oppure ragionando che $N_G(H)$ è lo stabilizzatore di $\{e_1\mathbb{F}, e_2\mathbb{F}\}$ (come sottoinsieme) si trova che $N_G(H) = H\langle\rho\rangle$. In particolare $|N_G(H)| = 2|H| = 2(q-1)$ e, di conseguenza, il numero di coniugati distinti di H in G è

$$[G : N_G(H)] = |G|/|N_G(H)| = q(q+1)/2. \tag{3.17}$$

Osserviamo anche che, siccome $H \simeq F_q^*$ è un gruppo ciclico di ordine $q-1$, $N_G(H)$ è un gruppo diedrale di ordine $2(q-1)$.

Esercizio 3.12. Si dimostri nei dettagli l'ultima affermazione intorno a $N_G(H)$.

Esercizio 3.13. Si provi che l'implicazione (3.14) sussiste anche nel caso in cui q non sia un numero primo (q è comunque una potenza di un numero primo).

Ricapitolando, relativamente all'azione di $g \in G$ su $P(1,q)$, abbiamo sinora mostrato che

1) g ha esattamente un punto fisso se e solo se $1 \neq g$ appartiene ad un coniugato di U.

2) g ha esattamente due punti fissi se e solo se g appartiene ad un coniugato di H e $g \notin Z$.

3) (Lemma 3.6) g ha 3 o più punti fisso se e solo se $g \in Z$ (cioè g è nel nucleo dell'azione).

Esercizio 3.14. Si verifichi direttamente, a partire da quanto osservato e da (3.16) e (3.17), che per l'azione di G su P sussiste l'uguaglianza del Lemma 3.2.

Restano da individuare gli elementi di G che agiscono senza punti fissi su $P(1,q)$. Ciò è un poco meno immediato. Per farlo, osserviamo innanzi tutto che, poiché $\mathbb{F}_q$ è un sottocampo di $\mathbb{F}_{q^2}$, G è in modo naturale un sottogruppo del gruppo $SL(2,q^2)$ ed eredita quindi da quest'ultimo una azione sulla retta proiettiva $P(1,q^2)$.
Sia α un generatore del gruppo moltiplicativo di $\mathbb{F}_{q^2}$, e $\gamma = \alpha^{q-1}$; poiché $|\alpha| = q^2 - 1$, si ha $|\gamma| = q+1$. Poniamo $\beta = \gamma + \gamma^{-1}$; allora,

$$\beta^q = (\gamma + \gamma^{-1})^q = \gamma^q + \gamma^{-q} = \gamma^{-1} + \gamma = \beta$$

e quindi $\beta \in \mathbb{F}_q$. Ne segue che le matrici

$$a = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix} \in SL(2,q^2) \qquad b = \begin{pmatrix} \beta & -1 \\ 1 & 0 \end{pmatrix} \in G$$

hanno lo stesso polinomio caratteristico e dunque sono coniugate in $GL(2,q^2)$. In paricolare $|b| = |a| = q+1$. Quindi G contiene sottogruppi ciclici di ordine $q+1$. Il generatore b di uno di questi non ha punti fissi sulla retta proiettiva $P(1,q)$, poiché la radici α ed α^{-1} del suo polinomio caratteristico non appartengono a $\mathbb{F}_q$ (mentre ha due punti fissi su $P(1,q^2)$); quindi b è uno degli elementi che stiamo cercando. Sia $C = \langle b\rangle$. Ora, $b^{\frac{q+1}{2}} = -I$; siccome l'ordine

degli elementi di G che fissano un punto su $P(1,q)$ divide $q(q-1)$, e $(q+1, q(q-1)) = 2$, ne segue che $C \geq Z$ e che tutti gli elementi di $C \setminus Z$ non hanno punti fissi su $P(1,q)$. Inoltre, il centralizzante in $SL(2,q^2)$ di a è il gruppo delle matrici diagonali, che è ciclico di ordine q^2-1; ne segue che $C_G(b)$ è anch'esso ciclico, e si verifica quindi facilmente che $C_G(b) = C$. Ancora, il normalizzante di $\langle a \rangle$ in $SL(2,q^2)$ (analogamente al caso di $SL(2,q)$) è diedrale e $\langle a \rangle$ interseca nel centro i suoi coniugati distinti; da ciò segue che $N_G(C)$ è diedrale di ordine $2|C| = 2(q+1)$ e quindi che C ha $|G|/2(q+1) = \frac{q(q-1)}{2}$ coniugati distinti in G; inoltre per ogni $g \in G \setminus N_G(C)$, $C \cap C^g = Z$. Guardando le cose nel gruppo proiettivo $\overline{G} = PSL(2,q) = G/Z$, si ha

$$|\overline{C}| = \frac{q+1}{2}; \qquad [\overline{G} : N_{\overline{G}}(\overline{C})] = \frac{q(q-1)}{2} \tag{3.18}$$

e, per ogni $g \in \overline{G} \setminus N_{\overline{G}}(\overline{C})$,

$$\overline{C} \cap \overline{C}^g = 1 \tag{3.19}$$

Esercizio 3.15. Si dimostrino nei dettagli le ultime affermazioni.

Tiriamo le somme, riferendoci al caso $\overline{G} = PSL(2,q)$. Se avete svolto l'esercizio 3.14, avrete trovato che il numero di elementi di $\overline{G}$ che, rispettivamente, hanno esattamente uno, due o tre punti fissi su $P = P(1,q)$ è

$$f_1 = (q-1)(q+1), \qquad f_2 = \frac{(q-3)q(q+1)}{4}, \qquad f_3 = 1.$$

Ora, da (3.18) e (3.19) segue che il numero di elementi non banali appartenenti a coniugati di $\overline{C}$ (che quindi agiscono senza punti fissi su P), è

$$f_0 = \frac{(q-1)^2 q}{4}.$$

Poiché $f_0 + f_1 + f_2 + f_3 = \frac{q(q-1)(q+1)}{2} = |\overline{G}|$, concludiamo che *gli elementi di $PSL(2,q)$ che agiscono senza punti fissi su $P(1,q)$ sono tutti e soli quelli contenuti nei coniugati di $\overline{C}$ e diversi da I*. Similmente per $SL(2,q)$, per cui possiamo enunciare la seguente

Proposizione 3.10. *Sia q un primo, $q \geq 5$, e sia $g \in SL(2,q) \setminus \{\pm I_2\}$. Allora g appartiene ad uno ed un solo tra i coniugati di P, H e C.*

Descritti gli elementi (e quindi i sottogruppi ciclici) di $SL(2,q)$, possiamo ora iniziare la descrizione dei sottogruppi in generale. Iniziamo con una semplice osservazione (il cui caso particolare $K = 1$ è rilevante).

Lemma 3.11. *Sia G un gruppo, $K \trianglelefteq G$, e sia $S \leq G$ tale che, per ogni $g \in G \setminus N_G(S)$, $S \cap S^g = K$. Allora, per ogni $x \in S \setminus K$, $N_G(\langle x \rangle) \leq N_G(S)$.*

Dimostrazione. Siano S, K come nelle ipotesi; sia $x \in S \setminus K$ e sia $g \in N_G(\langle x \rangle)$. Allora g normalizza $K\langle x \rangle \leq S$, e quindi $K\langle x \rangle \leq S \cap S^g$. Poiché $x \notin K$ (e quindi $K\langle x \rangle > K$), le ipotesi forzano $g \in N_G(S)$. ∎

Lemma 3.12. *Sia $q \geq 3$ un numero primo, $G = SL(2,q)$, e sia $1 \neq g \in G$ con $q \neq |g|$. Allora $g \in Z(G)$, oppure $N_G(\langle g \rangle)$ è ciclico o diedrale. Quindi, se $S \leq G$ è tale che q non divide $|S|$, e M è un sottogruppo ciclico massimale di S, allora $|N_S(M) : M| = 1, 2$.*

DIMOSTRAZIONE. Sia $1 \neq g \in SL(2,q) = G$. Supponiamo che g non appartenga al centro Z; allora, per la Proposizione 3.10, g appartiene ad uno ed un solo tra i coniugati di P, H o C, che chiamiamo X. Per il Lemma 3.12, $N_G(\langle g \rangle) \leq N_G(X)$. Ora, siccome $|g| \neq q$, X è un coniugato di H o di C, e dunque, per quanto visto in precedenza, $N_G(X)$ è diedrale. Ne segue che $N_G(\langle g \rangle)$ è ciclico o diedrale. L'ultima affermazione dell'enunciato si dimostra ora facilmente. ∎

Lemma 3.13. *Sia $S \leq SL(2,q)$ con q un numero primo. Se S contiene due coniugati distinti di U, allora $S = SL(2,q)$.*

DIMOSTRAZIONE. Sia $G = SL(2,q)$. Per provare il Lemma è chiaramente sufficiente provare che se $g \in G \setminus N_G(U)$, allora $\langle U, U^g \rangle = G$. Poiché l'azione di $SL(2,q)$ su $P(1,q)$ è 2-transitiva, possiamo assumere che U^g stabilizzi il punto $e_2\mathbb{F}$, e quindi che

$$U^g = V := \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \middle| b \in \mathbb{F}_q \right\}$$

Proviamo quindi che $H := \langle U, V \rangle = G$. Siano $a, d, c \in \mathbb{F}_q$ con $c \neq 0$; allora

$$H \ni \begin{pmatrix} 1 & c^{-1}(a-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & c^{-1}(d-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & c^{-1}(ad-1) \\ c & d \end{pmatrix}$$

Quindi H contiene tutte le matrici $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ con $c \neq 0$. Sia quindi $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$; allora $a \neq 0$ e $d = a^{-1}$, pertanto, per quanto visto sopra,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix} \in H,$$

e dunque

$$g = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix} \in H,$$

completando così la dimostrazione ∎

Possiamo ora dimostrare il risultato principale di questa sezione.

Teorema 3.14. *Sia q un primo, $q \geq 5$, e sia S un sottogruppo proprio di $PSL(2,q)$.*

(i) Se q divide $|S|$, allora S è contenuto in un coniugato del sottogruppo di Borel $\overline{B}$. In particolare S è metaciclico e $|S|$ divide $\frac{1}{2}q(q-1)$.

(ii) Se q non divide $|S|$, S è ciclico, diedrale o isomorfo a A_4, S_4 o A_5.

DIMOSTRAZIONE. Sia $G = PSL(2,q)$ con q primo, e sia S un sottogruppo proprio di G.

(i) Supponiamo che q divide $|S|$. Poiché S è un sottogruppo proprio di G, il teorema di Sylow ed il Lemma 3.13, implicano che S contiene uno ed un solo coniugato di U. Quindi, a meno di coniugare per un elemento di g, possiamo assumere che $U \leq S$; ma allora per ogni $x \in S$, $U^x \leq S$ e dunque $U^x = U$. Dunque $S \leq N_G(U) = B$, che, a meno di coniugio, è quello che si voleva dimostrare.

(ii) Supponiamo ora che q non divida $|S|$.
Sia $K_1, K_2, \dots K_t$ un insieme di rappresentanti delle classi di coniugio di sottogruppi ciclici massimali di S. Per quanto osservato sinora, i sottogruppi $K_1, \dots, K_t$ ed i loro coniugati hanno a due a due intersezione identica; la loro unione è peraltro tutto S. Quindi

$$|S| - 1 = \sum_{i=1}^{t} [S : N_S(K_i)](|K_i| - 1). \tag{3.20}$$

Per ogni $1 \leq i \leq t$ poniamo $z_i = |K_i|$. Dal Lemma 3.12 segue che $|N_S(K_i)| = \varepsilon_i z_i$, dove $\varepsilon_i \in \{1, 2\}$. Sia $0 \leq s \leq t$, tale che $\varepsilon_i = 1$ per $i \leq s$ e $\varepsilon_i = 2$ per $s + 1 \leq i \leq t$. Allora la (3.20) diventa

$$|S| = 1 + \sum_{i=1}^{s} \frac{|S|}{z_i}(z_i - 1) + \sum_{i=s+1}^{t} \frac{|S|}{2z_i}(z_i - 1) = 1 + s|S| - |S| \sum_{i=1}^{s} \frac{1}{z_i} + (t - s)\frac{|S|}{2} - |S| \sum_{i=s+1}^{t} \frac{1}{2z_i}$$

da cui

$$1 = \frac{1}{|S|} + s - \sum_{i=1}^{s} \frac{1}{z_i} + (t - s)\frac{1}{2} - \sum_{i=s+1}^{t} \frac{1}{2z_i} > s - \frac{s}{2} + \frac{t - s}{2} - \frac{t - s}{4}$$

e quindi

$$4 > s + t.$$

Dunque

$$(s, t) \in \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2)\}. \tag{3.21}$$

1) Se $t = 1$ allora S è ciclico. (e il suo ordine divide $\frac{q \pm 1}{2}$).

2) Sia $(s, t) = (1, 2)$. In tal caso S ha due classi di coniugio di sottogruppi ciclici massimali K_1, K_2, e la (3.20) si scrive

$$|S| = 1 + |S|\frac{z_1 - 1}{z_1} + |S|\frac{z_2 - 1}{2z_2}$$

da cui

$$1 > \frac{z_1 - 1}{z_1} + \frac{z_2 - 1}{2z_2}. \tag{3.22}$$

con $z_1, z_2 \geq 1$. Se $z_1 = 2$, allora $|S| = 2z_2$; quindi $S = N_S(K_2)$ è un gruppo diedrale. Se $z_1 > 2$, allora da (3.22) segue

$$\frac{z_2 - 1}{2z_2} < \frac{1}{3}$$

e quindi $z_2 = 2$. Da ciò segue a sua volta $z_1 = 3$ e $|S| = 12$; si dimostra allora (vedi esercizio 3.25) che $S \simeq A_4$.

3) Sia $(s,t) = (0,2)$. In questo caso si avrebbe

$$|S| = 1 + |S|\frac{z_1 - 1}{2z_1} + |S|\frac{z_2 - 1}{2z_2}$$

da cui

$$|S| = \frac{2z_1 z_2}{z_1 + z_2};$$

e poiché $2z_1$ divide $|S|$, si ricava l'assurdo $\frac{z_2}{z_1+z_2} \in \mathbb{N}$.

4) Sia $(s,t) = (0,3)$. In questo caso l'equazione 3.20 ci dà:

$$\frac{1}{2}\Big(\frac{z_1 - 1}{z_1} + \frac{z_2 - 1}{z_2} + \frac{z_3 - 1}{z_3}\Big) < 1. \tag{3.23}$$

Possiamo porre $z_1 \geq z_2 \geq z_3$; allora da (3.23) segue $(z_3 - 1)/z_3 < 2/3$, e pertanto $z_3 = 2$. Ancora da (3.23) si ricava quindi

$$\frac{z_1 - 1}{z_1} + \frac{z_2 - 1}{z_2} < 2 - \frac{1}{2} = \frac{3}{2},$$

e dunque $z_2 = 2, 3$.
Sia $z_2 = 2 = z_3$. Allora l'equazione (3.20) diventa

$$|S| - 1 = 1 + \frac{z_1 - 1}{z_1}|S|$$

da cui segue $|S| = 2z_1$, e dunque $S = N_S(K_1)$ è un gruppo diedrale.
Sia $z_2 = 3$, $z_3 = 2$. Allora da (3.23) segue $z_1 \in \{3, 4, 5\}$.

Se $z_1 = 3$, $|S| = 12$ e ciò non è possibile (perché un tale S avrebbe due classi di coniugio di 3-sottogruppi di Sylow).

Se $z_1 = 4$, allora $|S| = 24$ e si può provare (esercizio 3.26) che $S \simeq S_4$.

Se $z_1 = 5$, allora $|S| = 60$ e si può provare (esercizio 3.27) che $S \simeq A_5$.

La dimostrazione è completa. ∎

Si dice che un gruppo G è *metaciclico* se G ammette un sottogruppo normale N tale che sia N che G/N sono ciclici. Un gruppo diedrale è chiaramente metaciclico.

Corollario 3.15. *Sia q un numero primo e S un sottogruppo proprio del gruppo $PSL(2,q)$ con $|S| > 60$. Allora S è metaciclico.*

Esercizio 3.16. Sia q^m una potenza di un primo dispari q. Si provi che il gruppo $SL(2,q^m)$ contiene sottogruppi ciclici di ordine $q^m - 1$ e $q^m + 1$.

3.5 Rappresentazioni di $SL(2,q)$.

Sia G un gruppo, e sia K un campo. Una *K-rappresentazione* (lineare) di G è un omomorfismo di gruppi

$$\Phi : G \longrightarrow GL_K(V)$$

dove V è un K-spazio vettoriale di dimensione finita. La dimensione di V è detta il *grado* della rappresentazione. La rappresentazione Φ è *fedele* se $\ker \Phi = \{1\}$ (cioè se Φ è iniettiva), mentre è detta *banale* se $\ker \Phi = G$.

Il primo, ovvio, ma importante, esempio di rappresentazione di un gruppo G è la cosiddetta *rappresentazione banale*: essa è definita, per ogni campo K ed ogni K-spazio di dimensione finita V, come l'omomorfismo che ad ogni elemento di G associa l'applicazione identica su V. Osserviamo che se $\pi : G \to H$ è un omomorfismo di gruppi e $\Phi : H \to GL_K(V)$ una rappresentazione di H, allora $\Phi \circ f$ è una rappresentazione di G sul medesimo spazio V. In particolare, se $N \trianglelefteq G$ allora ogni rappresentazione di G/N può essere "sollevata" ad una rappresentazione di G.

Data una rappresentazione $\Phi : G \to GL_K(V)$, un sottospazio $U \leq V$ si dice G-invariante se $u^{\Phi(g)} \in U$ per ogni $u \in U$. La rappresentazione è detta *irriducibile* (o *semplice*) se $V \neq \{0\}$ e $\{0\}$ e V sono i soli sottospazi G-invarianti di V, ed è detta *semisemplice* se V è la somma diretta di sottospazi G-invarianti irriducibili (cioè se esistono sottospazi G-invarianti $V_1, \ldots, V_r$ tali che ogni V_i è irriducibile per l'azione di G indotta da quella su V, e $V = V_1 \oplus \cdots \oplus V_r$.

Osservazione. Sia $\Phi : G \longrightarrow GL_K(V)$ una rappresentazione del gruppo G sul K-spazio V e supponiamo $V \neq \{0\}$. Allora, poiché V ha dimensione finita, l'insieme dei sottospazi non nulli e G-invarianti di V ha elementi minimali. La restrizione della rappresentazione a tali sottospazi dà chiaramente luogo a rappresentazioni semplici di G.

Esercizio 3.17. Siano U e T sottospazi G-invarianti in una rappresentazione di G sullo spazio V. Si provi che $T + U$ e $T \cap U$ sono sottospazi G-invarianti.

Lemma 3.16. *Sia G un gruppo, K un campo, e sia data una K-rappresentazione di G sullo spazio V. Allora sono equivalenti.*

(i) Per ogni sottospazio G-invariante U di V esiste un sottospazio G-invariante W tale che $V = U \oplus W$.

(ii) La rappresentazione di G su V è semisemplice.

Dimostrazione. (i) $\Rightarrow$ (ii). Supponiamo che la rappresentazione Φ di G su V soddisfi (i). Poiché V ha dimensione finita, esiste un sottospazio G-invariante U massimale tale che la restrizione di Φ ad U (ovvero l'omomorfismo da G in $GL_K(U)$ che ad ogni $g \in G$ associa la restrizione di $\Phi(g)$ ad U) è semisemplice. Se $U = V$ siamo a posto. Altrimenti, per la proprietà (i) esiste un sottospazio G-invarinate W di V tale che $V = U \oplus W$; poiché $U \neq V$, W è non nullo, e quindi, per l'osservazione che precede il Lemma, W contiene un sottospazio G-invariante semplice e non nullo U_1. Ma allora $U + U_1 = U \oplus U_1$ è un sottospazio G-invariante semisemplice, il che contraddice la scelta di U.

(ii) $\Rightarrow$ (i). Esercizio. ∎

Teorema 3.17. *Sia G un gruppo finito, e K un campo di caratteristica 0. Allora, ogni K-rappresentazione di G è semisemplice.*

DIMOSTRAZIONE. Sia data una K-rappresentazione $\Phi : G \to GL_K(V)$, e per comodità usiamo lo stesso simbolo g per indicare l'elemento $g \in G$ e l'automorfismo $\Phi(g)$ di V associato a g. Per il punto (i) del Lemma 3.16 è sufficiente provare che se U è un sottospazio G-invariante di V, allora esiste un complemento di U in V anch'esso G-invariante.
Sia dunqu $U \leq V$ un sottospazio G-invariante. Se $U = V$ non c'è quasi nulla da provare (il suo solo complemento è lo spazio nullo che è chiaramente G-invariante). Sia dunque $U \neq V$, e sia W un suo sottospazio complementare; ovvero

$$V = U \oplus W \tag{3.24}$$

(che esiste per ragioni elementari di algebra lineare). Sia $\eta : V \to U$ la proiezione di V su U rispetto alla decomposizione (3.24). Allora $\eta \in End(V)$; d'altra parte anche $g = \Phi(g)$ è un endomorfismo di V per ogni $g \in G$. Dunque anche

$$\sigma = \sum_{x \in G} x \circ \eta \circ x^{-1}$$

è un endomorfismo di V. Notiiamo in primo luogo che (nell'anello degli endomorfismi di V),

$$\forall g \in G \ : \ g\sigma = \sigma g. \tag{3.25}$$

Sia infatti $g \in G$, allora

$$g\sigma = \sum_{x \in G} gx\eta x^{-1} = \sum_{x \in G} gx\eta x^{-1}g^{-1}g = \Big(\sum_{x \in G} gx\eta x^{-1}g^{-1}\Big)g = \Big(\sum_{x \in G} gx\eta (gx)^{-1}\Big)g = \sigma g.$$

Osserviamo quindi che, $Im\,\sigma \leq U$; infatti per ogni $v \in V$ ed ogni $x \in G$, $v^{x\eta} = (v^x)^\eta \in U$, quindi $v^{x\eta x^{-1}} \in U$ e pertanto $v^\sigma \in U$. Inoltre,

$$\forall u \in U \ : \ u^\sigma = |G|u. \tag{3.26}$$

Sia infatti $u \in U$; allora $\eta(u) = u$ e, poiché U è G-invariante, $u^g \in U$ per ogni $g \in G$, e dunque $u^{g\eta} = u^g$; quindi

$$u^\sigma = \sum_{x \in G} u^{x\eta x^{-1}} = \sum_{x \in G} u^{xx^{-1}} = \sum_{x \in G} u^1 = |G|u.$$

Sia ora $T = \ker \sigma$. Poiché il campo K su cui V è definito ha caratteristica 0, la (3.26) (assieme con quanto osservato prima) implica $U = Im\,\sigma$ e $T \cap U = \{0\}$. Ora, per un fatto ben noto di algebra lineare, $\dim V = \dim T + \dim U$. Pertanto T è un complemento di U, ovvero

$$V = U \oplus T.$$

La dimostrazione si completa provando che T è G-invariante. Ciò segue immediatamente da (3.25). Infatti, per ogni $w \in T = \ker \sigma$ ed ogni $g \in G$ si ha

$$(w^g)^\sigma = w^{g\sigma} = w^{\sigma g} = (w^\sigma)^g = 0^g = 0,$$

dunque $w^g \in \ker \sigma = T$, il che prova che T è G-invariante. ∎

Esercizio 3.18. Si completi la dimostrazione del Lemma 3.16.

Esercizio 3.19. Sia K un campo, $V = K \times K$ e sia

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \Big| \, a \in K \right\}.$$

Si provi che la rappresentazione naturale di G su V non è semisemplice.

Esercizio 3.20. Sia data una rappresentazione del gruppo G sullo spazio vettoriale V, e sia $N \trianglelefteq G$. Si provi che G agisce come un gruppo di permutazioni sull'insieme dei sottospazi N-invarianti e semplici (per l'azione di N).

Proposizione 3.18. *Sia $G = \langle g \rangle$ un gruppo ciclico finito di ordine $n \geq 2$, e sia data una rappresentazione irriducibile di G sul $\mathbb{C}$-spazio vettoriale V. Allora* $\dim V = 1$ *e g opera su V come la moltiplicazione per una radice n-esima dell'unità.*

Dimostrazione. Siano $G = \langle g \rangle$ e V come nelle ipotesi. Poiché $g^n = 1_G$, ciò vale anche per l'automorfismo A di V associato a g. Quindi, in $End_{\mathbb{C}}(V)$, $A^n = 1$. Ne segue che gli autovalori di A sono radici n-esime dell'unità. Sia ζ uno di questi; poiché $\zeta \in \mathbb{C}$, V contine in autovalore $v \neq 0$ relativo a ζ (quindi $v^g = Av = \zeta v$. Sia W il sottospazio $v\mathbb{C}$ generato da v, chiaramente $\{0\} \neq W$ è un sottospazio G-invariante di V, Per l'irriducibilità dell'azione si ha allora $W = V$, che è quello che si voleva. ∎

La teoria delle rappresentazioni dei gruppi lineari (per la quale rimandiamo ad altri testi) ha una lunga e gloriosa storia. Utilitaristicamente, ci limiteremo a dimostrare solo quello che ci serve, ovvero il seguente risultato (che risale a Frobenius, 1896).

Teorema 3.19. *Sia q un numero primo, $q \geq 5$. Allora ogni $\mathbb{C}$-rappresentazione non banale di $PSL(2,q)$ (e di $SL(2,q)$) ha grado almeno $(q-1)/2$.*

Dimostrazione. Poiché $PSL(2,q)$ è un quoziente di $SL(2,q)$, per quanto già osservato, ogni rappresentazione di $PSL(2,q)$ si solleva ad una di $SL(2,q)$ sullo stesso spazio (e dunque con lo stesso grado). Pertanto è sufficiente dimostrare l'asserto del Teorema per il gruppo $G = SL(2,q)$.
Sia quindi V un $\mathbb{C}$-spazio vettoriale, con $\dim V = n \geq 1$, e sia data una rappresentazione non banale di G su V. Essendo la rappresentazione non banale, il suo nucleo K è un sottogruppo proprio e normale di G; poiché $q \geq 5$, per il Teorema 3.9, $PSL(2,q) = G/Z(G)$ è semplice, i soli sottogruppi normali propri di G sono contenuti in $Z(G)$, che ha ordine 2: dunque i soli sottogruppi normali propri di G sono $Z(G)$ e $\{1\}$. In particolare, una rappresentazione non banale di G è fedele o ha nucleo $Z(G)$ (ed ogni rappresentazione non banale di $PSL(2,q)$ (con $q \geq 5$) è fedele).
Utilizzando le notazioni introdotto nella sezione precedente, sia

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \Big| \, b \in \mathbb{F}_q \right\} \qquad \text{e} \qquad \mathrm{H} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \Big| \, 0 \neq \mathrm{a} \in \mathbb{F}_{\mathrm{q}} \right\} ..$$

Allora, $|U| = q$, $U = \langle g \rangle$, con $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$; H è ciclico di ordine $q-1$, e $N_G(U) = UH$.

Per il Teorema 3.17 e la Proposizione 3.18, abbiamo

$$V = V_1 \oplus \cdots \oplus V_t \tag{3.27}$$

dove $V_1, \ldots, V_t$ sono gli autospazi distinti di g. Mostriamo che gli elementi di H (o meglio, volendo essere pignoli, le trasformazioni lineari di V associate agli elementi di H) permutano gli autospazi V_i. Infatti, sia W_λ l'autospazio di g relativo all'autovalore λ (dunque, W_λ è uno dei V_i), e sia $x \in H$; allora $xgx^{-1} = g^m$ per qualche $1 \leq m \leq q-1$, e quindi, se $0 \neq v \in W_\lambda$,

$$(v^x)^g = v^{xg} = v^{xgx^{-1}x} = (v^{g^m})^x = (\zeta^m v)^x = \zeta^m v^x$$

e dunque v^x è autovalore per g relativo all'autovalore λ^m. Ciò significa che $W_\lambda^x \leq W_{\lambda^m}$. Provare che, viceversa, $W_{\lambda^m} \leq W_\lambda^x$ è facile, e dunque $W_\lambda^x = W_{\lambda^m}$. Ciò dimostra che H permuta l'insieme $\{V_1, \ldots, V_t\}$ degli autospazi di g.
Osserviamo che poiché g non è contenuto nel nucleo della rappresentazione, possiamo assumere che V_1 sia un autospazio di g relativo ad un autovalore $\zeta \neq 1$. ζ è quindi una radice primitiva q-esima dell'unità. Supponiamo ora che x sia un elemento dello stabilizzatore in H di V_1, ovvero che $V_1^x = V_1$. Allora, per quanto osservato sopra, $\zeta^m = \zeta$, e quindi (poiché $1 \leq m \leq q-1$ e ζ è una radice primitiva q-esima) $m = 1$, ovvero $x \in C_H(g) = C_H(U) = Z$. Dunque, $Z = \{\pm I\}$ è lo stabilizzatore di V_1 in H. Ne segue che l'orbita di V_1 tramite H ha cardinalità $|H/Z| = \frac{q-1}{2}$. Quindi, $t \geq \frac{q-1}{2}$. Siccome, chiaramente $t \leq n = \dim V$, ciò completa la dimostrazione. ∎

3.6 Esercizi.

1. Rango di un gruppo di permutazioni. Sia G un gruppo di permutazioni (che scegliamo subito transitivo) su Ω Allora G opera su $\Omega \times \Omega$ nel modo naturale: per ogni $(x, y) \in \Omega \times \Omega$ e $g \in G$: $(x, y)^g = (x^g, y^g)$. Le orbite di G su $\Omega \times \Omega$ sono dette *orbitali* di G, e il numero di orbitali è detto *rango* di G (come gruppo di permutazioni su Ω). Osserviamo che l'insieme diagonale $D = \{(x, x) | x \in \Omega\}$ è un orbitale (poiché G è transitivo), detto orbitale banale, e quindi che G è 2-transitivo su Ω se e solo se D e $\Omega \times \Omega \setminus D$ sono gli orbitali di G, ovvero se e solo se G ha rango 2. Sia $x, \in \Omega$ con $x \neq y$ e supponiamo che esista $g \in G$ tale che $x^g = y$ e $y^g = x$; allora (y, x) appartiene all'orbitale $\mathcal{O}$ di (x, y) (in tal caso l'orbitale $\mathcal{O}$ si dice 'reciproco'). Questo consente di associare all'orbitale $\mathcal{O}$ un grafo, il cui insieme di vertici è Omega e gli archi sono le coppie $\{a, b\}$ con $(a, b) \in \mathcal{O}$. Un grafo costruito in tal modo si dice grafo orbitale (per l'azione di G su Ω).

Esercizio 3.21. Sia $G = S_4$ il gruppo simmetrico su $I = \{1, 2, 3, 4\}$ e si consideri l'azione naturale di G su $\Omega = T^{[2]} = \{\{a, b\} \mid a, b \in I,\ a \neq b\}$. Si descrivano gli orbitali di tale azione e, quando, possibile i relativi grafi.

Esercizio 3.22. Sia G un gruppo di permutazioni su Ω di rango 3, e siano O_1 e O_2 gli orbitali non banali. Si assuma che G contenga una involuzione (cioè un elemento di ordine 2). Si provi che i due orbitali $\mathcal{O}_1$, $\mathcal{O}_2$ sono reciproci, e che i grafi ad essi associati sono complementari.

Esercizio 3.23. Nelle stesse ipotesi dell'esercizio precedente, si provi che i grafi orbitali indotti da $\mathcal{O}_1$ e da $\mathcal{O}_2$ sono grafi fortemente regolari (vedi esercizio 2.28). I grafi costruiti in questo modo si chiamano grafi di rango 3.

Esercizio 3.24. Sia $I = \{1, 2, 3, 4, 5\}$ e si consideri il gruppo alterno A_5 nella sua azione naturale su $\Omega = I^{[2]}$. Si provi che tale azione è transitiva e che, se $a \in \Omega$, allora $G_a \simeq S_3$. Si provi che G (su Ω) ha rango 3. Si provi che il grafo associato all'orbitale di $(\{1, 2\}, \{3, 4\})$ è isomorfo al grafo di Petersen. È sempre possibile rappresentare un grafo di Kneser (esercizio 1.46) come un grafo orbitale (non necessariamente di rango 3) ?

2. Piccoli gruppi.

Esercizio 3.25. Sia S un gruppo finito in cui ogni elemento non banale ha ordine 2 o 3. Si provi che se S ha un'unica classe di coniugio di sottogruppi di ordine 2, un'unica classe di coniugio di sottogruppi di ordine 3, e se $C = N_S(C)$ per ogni sottogruppo ciclico C di ordine 3, allora $G \simeq A_4$. [Si imposti l'equazione delle classi (3.20), deducendo che $|S| = 12$; si consideri poi l'azione di S sull'insieme dei coniugati di un sottogruppo di ordine 3 . . .]

Esercizio 3.26. Sia S un gruppo finito idi ordine 24 e C un sottogruppo (ciclico) di ordine 3. Si provi che $C \trianglelefteq S$, oppure esiste un omomorfismo $S \to S_4$; infine, si provi che se $C = C_S(C)$, allora $S \simeq S_4$.

Esercizio 3.27. Sia S un gruppo finito di ordine 60 in cui ogni elemento ha ordine $1, 2, 3$ o 5. Si provi che $S \simeq A_5$. [Si osservi che un 2-sottogruppo di Sylow Q di S ha ordine 4, e che per ogni $1 \neq x \in Q$, $C_S(x) = Q$; concludere che $|N_S(Q)| = 12$, e considerare l'azione di S sull'insieme dei coniugati di S]

3. Rappresentazioni e permutazioni. In questi esercizi, sia G un gruppo finito e sia data un'azione di G sull'insieme finito Ω (e denotiamo con la stessa lettera sia l'elemento $g \in G$ che la permutazione di Ω ad esso associata.
Sia V il $\mathbb{C}$-spazio delle funzioni da Ω in $\mathbb{C}$: $V = \{f \mid f : X \to \mathbb{C}\}$. Per ogni $g \in G$ si definisce $\phi_g : V \to V$, ponendo, per ogni $f \in V$

$$\phi_g(f)(x) = f(x^{g^{-1}}).$$

Esercizio 3.28. Si provi che per ogni $g \in G$, ϕ_g è una trasformazione lineare invertibile di V, e che l'applicazione $\Phi : G \to GL(V)$ data da $\Phi(g) = \phi_g$ (per ogni $g \in G$) è una rappresentazione lineare di G.

Esercizio 3.29. Siano $I = \{f \in V \mid \sum_{x \in \Omega} f(x) = 0\}$ e $M = \{f \in V \mid f \text{ costante }\}$. Si provi che I ed M sono sottospazi G-invarianti di V, e che $V = I \oplus M$.

Esercizio 3.30. Sia q un numero privo. Si provi che il gruppo $SL(2, q)$ ammette una $\mathbb{C}$-rappresentazione fedele di grado q (*un punto più difficile* è dimostrare che tale rappresentazione è semplice).

Esercizio 3.31. Questo tipo di rappresentazioni (ottenute a partire da un'azione come gruppo di permutazioni su Ω) si può fare prendendo i coefficienti in qualsiasi campo fissato K; basta considerare V l'insieme delle funzioni da Ω a K. Si faccia quindi un esempio di come, scegliendo opportunamente il gruppo G ed il campo K, l'ultima affermazione dell'esercizio 3.29 non vale.

Capitolo 4

Teoria dei Numeri

4.1 Somme di quadrati.

Dato un numero intero $n \geq 1$, consideriamo l'equazione diofantea:

$$y_0^2 + y_1^2 = n. \tag{4.1}$$

Non per ogni n l'equazione (4.1) ammette soluzioni intere; a tal proposito sussiste un famoso risultato di Eulero (per la dimostrazione, si vedano gli esercizi 4.14 – 4.17). .

Teorema 4.1. *Sia $1 \leq n \in \mathbb{N}$. Allora l'equazione (4.1) è risolubile in $\mathbb{Z}$ se e solo se ogni primo $p \equiv 3\,(mod\,4)$ compare con esponente pari nella fattorizzazione in potenze di primi distinti di n.*

Per campi finiti le cose vanno diversamente; infatti vale la seguente osservazione.

Proposizione 4.2. *Sia K un campo finito. Allora ogni elemento di K è una somma di 2 quadrati.*

Dimostrazione. Sia F un campo finito. Allora $|F| = q$ dove q è la potenza di un primo p. Se $p = 2$, allora l'applicazione $x \mapsto x^2$ da F in sé è iniettiva, dunque è suriettiva ed ogni elemento di F è un quadrato.
Sia p dispari, allora, per ogni $0 \neq x \in F$, $x \neq -x$ e $x^2 = (-x)^2$; quindi, denotato con $\mathcal{Q}$ l'insieme dei quadrati di F, si ha

$$|\mathcal{Q}| = 1 + \frac{p-1}{2} = \frac{p+1}{2}.$$

Sia $a \in F$, e sia $a - \mathcal{Q} = \{a - y \mid y \in \mathcal{Q}\}$. Allora $|\mathcal{Q}| + |a - \mathcal{Q}| = \frac{p+1}{2} + \frac{p+1}{2} = p + 1 > |F|$. Quindi $\mathcal{Q} \cap (a - \mathcal{Q}) \neq \emptyset$. Pertanto, esistono $x, y \in F$ tali che $x^2 = a - y^2$. Quindi $a = x^2 + y^2$ che è ciò che si voleva. ∎

Nel 1770 Lagrange dimostrò, confermando una congettura di Fermat, che ogni intero positivo è la somma di 4 quadrati interi, ovvero che per ogni $n \in \mathbb{N}$, esistono $y_1, y_2, y_3, y_4 \in \mathbb{Z}$ tali che

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = n. \tag{4.2}$$

Teorema 4.3. (Lagrange). *Ogni numero naturale è somma di* 4 *quadrati.*

DIMOSTRAZIONE. (all'incirca la stessa di Lagrange) Useremo la seguente identità (dovuta ad Eulero)

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{4.3}$$

dove

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \ . \end{aligned}$$

Il risultato è banalmente vero per $n = 0, 1, 2$; l'identità 4.3 assicura quindi che è sufficiente dimostrarlo per un primo $p \geq 3$. Sia dunque p un primo dispari.
Sappiamo dalla proposizione 4.2 che ogni intero è congruo modulo p ad una somma di due quadrati. Dunque, esistono x_0, y_0 tali che $x^2 + y^2 \equiv -1\,(mod\,p)$. Tali interi x, y possono essere presi in modo che $0 \leq x, y \leq \frac{p-1}{2}$. Dunque sistono interi positivi x, y ed m tali che

$$1 + x^2 + y^2 = mp \tag{4.4}$$

ed inoltre $0 < 1 + x^2 + y^2 < 1 + 2(\frac{p}{2})^2 < p^2$; e quindi

$$0 < m < p \ .$$

Sia ora m_0 il più piccolo intero positivo tale che m_0p è somma di quattro quadrati. Vogliamo provare che $m_0 = 1$. Per la (4), si ha $0 < m_0 < p$.
Siano x_1, x_2, x_3, x_4 interi tale che

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0p \ . \tag{4.5}$$

Supponiamo per assurdo, $m_0 \geq 2$, ed analizziamo separatamente i due casi: I) m_0 è pari; II) m_0 è dispari.

I) Se m_0 è pari, allora $x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0p$ è pari; quindi $x_1 + x_2 + x_3 + x_4$ è pari. Dunque si verifica una delle seguenti posssibilità:
i) x_1, x_2, x_3, x_4 sono tutti pari;
ii) x_1, x_2, x_3, x_4 sono tutti dispari;
iii) x_1, x_2, x_3, x_4 sono due pari e due dispari; in questo caso possiamo assumere che x_1, x_2 siano pari, e x_3, x_4 siano dispari.
In tutti e tre i casi si ha che

$$x_1 + x_2,\ x_1 - x_2,\ x_3 + x_4,\ x_3 - x_4$$

sono interi pari. Ma allora

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

il che, poichè $\frac{m_0}{2}$ è un intero, contraddice la scelta di m_0.

II) Sia m_0 dispari; e quindi $m_0 \geq 3$. Allora, dividendo gli x_i per m_0; è possibile trovare interi b_i e y_i, per $i = 1, 2, 3, 4$, tali che

$$y_i = x_i - b_i m_0 \qquad \text{con} \quad |y_i| < \frac{m_0}{2} \ .$$

Osserviamo che, poichè m_0 non divide p, almeno uno degli x_i non è divisibile per m_0, e quindi che almeno uno degli y_i è diverso da 0. Dunque

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 = 4\left(\frac{m_0}{2}\right)^2 = m_0^2$$

ed inoltre

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \, (mod\, m_0)$$

ovvero, mettendo insieme queste due proprietà,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0 \tag{4.6}$$

per qualche $0 < m_1 < m_0$. Moltiplicando membro a membro l'uguaglianza (5) e la (6), otteniamo

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p$$

dove gli z_i sono dati dall'identità di Eulero (3). Ora, si osserva che

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i(x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \, (mod\, m_0) \ .$$

Analogamente si prova che, per $i = 1, 2, 3, 4$, si ha $z_i \equiv 0 \, (mod\, m_0)$. Esistono quindi interi positivi t_1, t_2, t_3, t_4 tali che

$$z_i = m_0 t_i \qquad \text{per} \quad i = 1, 2, 3, 4 \ .$$

ma allora

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p$$

che, ancora una volta, è in contraddizione con la scelta di m_0.
Pertanto, deve essere $m_0 = 1$, e dunque p è somma di quattro quadrati, completando così la dimostrazione del Teorema. ∎

Sia $n \geq 1$; si denota con $\sigma(n)$ la somma dei divisori interi (positivi) di n, ovvero

$$\sigma(n) = \sum_{d|n} d.$$

Dati $0 < k, n \in \mathbb{N}$, si denota con $r_k(n)$ il numero di k-uple distinte $(y_1, \ldots, y_k) \in \mathbb{Z}^k$ tali che$n = y_1^2 + \cdots + y_k^2$; così, in particolare, $r_4(n)$ è il numero di 4-uple distinte $(y_1, y_2, y_3, y_4) \in \mathbb{Z}^4$ che soddisfano l'uguaglianza (4.2).

Teorema 4.4. (Jacobi) *Sia $n \geq 1$ un numero intero dispari. Allora*

$$r_4(n) = 8\sigma(n).$$

Per il momento, omettiamo la dimostrazione di questo importante risultato.

Esercizio 4.1. Sia p un numero primo e sia $m \geq 1$. Si provi che

$$\sigma(p^m) = \frac{p^{n+1} - 1}{p - 1}.$$

Non tutti i numeri naturali sono somme di tre quadrati interi. A tal proposito sussiste il seguente risultato di K. F. Gauss

Teorema 4.5. *Un numero naturale n si esprime come la somma di tre quadrati interi se e solo se n non è della forma*

$$n = 4^s(8t + 7),$$

con $s, t \in \mathbb{N}$.

Quindi $r_3(n) = 0$ se e solo se $n = 4^s(8t + 7)$ (con $s, t \in \mathbb{N}$). Alla fine di queste note ci servirà la seguente informazione sul comportamento asintotico di $r_3(n)$, che non dimostriamo.

Proposizione 4.6. *Sia $0 < \epsilon \in \mathbb{R}$. Allora*

$$r_3(n) = O(n^{1/2+\epsilon}).$$

4.2 Algebre dei quaternioni.

Sia R un anello commutativo con identità. L'**algebra dei quternioni** $\mathbb{H}(R)$ su R è l'anello i cui elementi sono tutti quelli del tipo:

$$a_0 1 + a_1 i + a_2 j + a_3 k \tag{4.7}$$

con $a_0, a_1, a_2, a_3 \in R$. L'addizione e la moltiplicazione per un elemento di R sono definite nel modo ovvio (formalmente: $\mathbb{H}(R)$ è il R-modulo libero (sinistro) generato da $1, i, j, k$):

$$(a_0 1 + a_1 i + a_2 j + a_3 k) + (b_0 1 + b_1 i + b_2 j + b_3 k) = (a_0 + b_0)1 + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$$

$$\text{per a} \in \text{R} \ : \ \text{a}(\text{a}_0 1 + \text{a}_1 \text{i} + \text{a}_2 \text{j} + \text{a}_3 \text{k}) = \text{aa}_0 1 + \text{aa}_1 \text{i} + \text{aa}_2 \text{j} + \text{aa}_3 \text{k}.$$

La moltiplicazione in $\mathbb{H}(R)$ è definita dalle relazioni:

(H1) $1x = x1 = x \quad \forall x \in \mathbb{H}(R)$

(H2) $i^2 = j^2 = k^2 = -1$

(H3) $ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$

e dalla proprietà distributiva. Si verifica che, con tali operazioni, $\mathbb{H}(R)$ è un anello (o meglio, una R-algebra). Naturalmente, d'ora in avanti ometteremo quasi sempre di scrivere il simbolo 1 nella scrittura (4.7).

Sia $\mathbb{H}(R)$ un'algebra dei quaternioni. Il *coniugio* è l'applicazione $\overline{\cdot} : \mathbb{H}(R) \to \mathbb{H}(R)$ definita da, per ogni $u = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(R)$,

$$\overline{u} = a_0 - a_1 i - a_2 j - a_3 k.$$

La *norma* su $\mathbb{H}(R)$ è l'applicazione $N : \mathbb{H}(R) \to R$ definita da, per ogni $u = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(R)$,

$$N(u) = u\overline{u} = a_0^2 + a_1^2 + a_2^2 + a_3^2. \tag{4.8}$$

Si verifica facilmente che la norma è moltiplicativa; ovvero

$$N(uv) = N(u)N(v) \qquad \forall\ u, v \in \mathbb{H}(R).$$

Un' altro fatto importante e di facile verifica è che ogni omomorfismo di anelli commutativi $\phi : R \to S$ si estende in modo canonico (ed ovvio) ad un omomorfismo (di anelli)

$$\overline{\phi} : \mathbb{H}(R) \to \mathbb{H}(S).$$

Ad esempio, se p è un numero primo, la *riduzione modulo p* è un omomorfismo suriettivo da $\mathbb{H}(\mathbb{Z})$ in $\mathbb{H}(\mathbb{F}_p)$.

Esercizio 4.2. Si provi che il coniugio è un *antiautomorfismo* moltiplicativo; ovvero che, per ogni $a, b \in \mathbb{H}(R)$, si ha $\overline{ab} = \overline{b}\overline{a}$.

Esercizio 4.3. Si provi che in $\mathbb{H}(\mathbb{Z})$ vale la legge di cancellazione; ovvero, per ogni $a, b, c \in \mathbb{H}(\mathbb{Z})$ con $c \neq 0$, $ac = bc \ \Rightarrow\ a = c$ (e lo stesso a sinistra). Si provi che se F è un campo finito, allora la legge di cancellazione non vale in $\mathbb{H}(F)$.

Proposizione 4.7. *Sia K un campo di caratteristica $\neq 2$, e tale che esistono $x, y \in K$ con $x^2 + y^2 + 1 = 0$. Allora l'algebra dei quaternioni $\mathbb{H}(K)$ è isomorfa all'algebra delle matrici quadrate di ordine due, $M_2(K)$. In particolare, $\mathbb{H}(F) \simeq M_2(F)$ per ogni campo finito F di caratteristica $\neq 2$.*

Dimostrazione. Sia K come nell'ipotesi e siano $x, y \in K$ tali che $x^2 + y^2 = -1$. Definiamo $\psi : \mathbb{H}(K) \to M_2(K)$ ponendo, per ogni $a_0.a_1, a_2, a_3 \in K$,

$$\psi(a_0 + a_1 i + a_2 j + a_3 k) = \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}.$$

Si verifica direttamente (facendo i conti) che ψ è un omomorfismo di K-algebre. Inoltre,

$$\det \begin{pmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & -x & 0 & -y \end{pmatrix} = -4(x^2 + y^2) = 4 \neq 0.$$

Le colonne della matrice di sinistra sono le componenti, rispettivamente, di $\psi(1), \psi(i), \psi(j)$ e $\psi(k)$ rispetto alla base $E_{11}.E_{12}, E_{21}, E_{22}$ di $M_2(K)$.
L'ultima affermazione dell'enunciato discende ora dalla Proposizione 4.2. ∎

Osservazione. A proposito della dimostrazione precedente, osserviamo che, facendo i calcoli, si trova che, per ogni $a \in \mathbb{H}(K)$, $\det \psi(a) = N(a)$.

Esercizio 4.4. Sia ψ l'applicazione definita nella dimostrazione della Proposizione 4.7. Si verifichi che, per ogni $a \in \mathbb{H}(K)$, $\mathrm{Tr}(\psi(a)) = a + \overline{a}$, e che se $a = \overline{a}$ allora $\psi(a)$ è una matrice scalare.

4.3 Quaternioni interi.

Ci occupiamo ora più specificatamente dell'algebra dei quaternioni interi $\mathbb{H}(\mathbb{Z})$.

Lemma 4.8. *Sia $u \in \mathbb{H}(\mathbb{Z})$. Le seguenti proprietà sono equivalenti:*

(i) *u è invertibile;*

(ii) *$N(u) = 1$;*

(ii) *$u \in \{\pm 1, \pm i, \pm j, \pm k\}$.*

L'insieme degli elementi invertibili di $\mathbb{H}(\mathbb{Z})$ forma un gruppo moltiplicativo di ordine 8, detto *gruppo dei quaternioni* Q_8.

Esercizio 4.5. Si dimostri il Lemma 4.8.

Esercizio 4.6. Sia q un numero primo con $q \equiv 3, 5$ (*mod* 8). Si provi che un 2-sottogruppo di Sylow di $SL(2, q)$ è isomorfo a Q_8.

Siano $a, b \in \mathbb{H}(\mathbb{Z})$; b si dice *associato destro* di a se esiste un elemento invertibile u di $\mathbb{H}(\mathbb{Z})$ tale che $ub = a$. Questo definisce una relazione d'equivalenza su $\mathbb{H}(\mathbb{Z})$ (lo si dimostri); inoltre, dall'esercizio 4.3 segue che ogni classe di associati destri, diversa da quella contenente solo lo zero, contiene esattamente 8 elementi.

Un elemento $0 \neq a \in \mathbb{H}(\mathbb{Z})$ si dice *irriducibile* se

- a non è invertibile (cioè $N(a) > 1$);
- se $a = bc$ (con $b, c \in \mathbb{H}(\mathbb{Z})$) allora o b o c è invertibile.

Dal Lemma 4.8 e dalla moltiplicatività della norma segue subito

Lemma 4.9. *Sia $a \in \mathbb{H}(\mathbb{Z})$. Se $N(a) = p$ è un numero primo, allora a è irriducibile.*

Quello che vogliamo provare è che tale implicazione si inverte, ovvero che ogni elemento di $\mathbb{H}(\mathbb{Z})$ la cui norma è un numero primo è irriducibile.

Siano $a, d \in \mathbb{H}(\mathbb{Z})$ con $d \neq 0$. Si dice che d è un *divisore destro* di a se esiste $c \in \mathbb{H}(\mathbb{Z})$ tale che $a = cd$; in tal caso scriveremo $d|_r a$. Similmente si definiscono divisori sinistri.

Lemma 4.10. *Siano $a, b \in \mathbb{H}(\mathbb{Z})$ con $N(b)$ dispari. Allora esistono $c, d \in \mathbb{H}(\mathbb{Z})$ tali che $a = cb + d$ e $N(d) < N(b)$.*

Dimostrazione. Siano a, b come nell'ipotesi. Allora $b \neq 0$. Poniamo $m = N(b)$, e consideriamo $s = a\bar{b} = s_0 + s_1 i + s_2 j + s_3 k$. Poiché $m \neq 0$ è dispari, per ogni $\nu = 0.1, 2, 3$ esiste $r_\nu \in \mathbb{Z}$ tale che

$$|s_\nu - m r_\nu| < m/2.$$

Sia $c = r_0 + r_1 i + r_2 j + r_3 k$, e $d = a - cb$. Allora $a = cb + d$,

$$N(d) = N(a\bar{b} - cb\bar{b})N(b)^{-1} = N(s - cm)m^{-1} = m^{-1}\sum_{\nu=0}^{3}(s_\nu - m r_\nu)^2 < m^{-1} 4 (m/2)^2 = m.$$

Il Lemma è quindi dimostrato. ∎

Esercizio 4.7. Si provi che l'enunciato del Lemma 4.10 non è più valido se si toglie l'ipotesi che $N(b)$ sia dispari.

Lemma 4.11. *Sia $0 \neq a \in \mathbb{H}(\mathbb{Z})$ tale che $N(a)$ è pari. Allora almeno uno tra $1+i, 1+j, 1+k$ è un divisore destro di a, ed almeno uno è un divisore sinistro di a.*

DIMOSTRAZIONE. Sia $a = a_0 + a_1 i + a_2 j + a_3 k$. Poiché $N(a) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ è pari, esiate $s \in \{1, 2, 3\}$ tale che $a_0 \equiv a_s \pmod 2$. Supponiamo $s = 1$ (gli altri due casi si trattano analogamente); allora anche $a_2 \equiv a_3 \pmod 2$. Siano

$$b_0 = \frac{a_0 + a_1}{2},\ b_1 = \frac{a_1 - a_0}{2},\ b_2 = \frac{a_2 - a_3}{2},\ b_3 = \frac{a_2 + a_3}{2}.$$

Allora $b = b_0 + b_1 i + b_2 j + b_3 k \in \mathbb{H}(\mathbb{Z})$, e facendo il conto si verifica che $a = b(1 + i)$.
La procedura per trovare un divisore sinistro è simile e lasciata per esercizio. ∎

Esercizio 4.8. Sia $0 \neq a \in \mathbb{H})\mathbb{Z})$. Si provi che a ammette un'unica fattorizzazione del tipo $a = 2^k \pi a_0$, dove $k \geq 0$, $N(a_0)$ è dispari e $\pi \in \{1, 1_i, 1 + j, 1 + k, (1 + i)(1 + j), (1 + i)(1 - k)\}$.

Lemma 4.12. *Sia $0 \neq a \in \mathbb{H}(\mathbb{Z})$, e sia $p \in \mathbb{N}$ un primo dispari tale che $p|N(a)$. Allora esiste $d \in \mathbb{H}(\mathbb{Z})$ con $d|_r a$ e $N(d) = p$.*

DIMOSTRAZIONE. Procediamo per induzione su $N(a)$. Se $N(a) = p$ allora $d = a$.
Sia quindi $N(a) > p$. Per il Lemma 4.11 possiamo assumere che $N(a)$ sia dispari.

(1) Sia $p < N(a) < p^2$, ovvero $N(a) = pm$ con $3 \leq m \leq p - 2$ (quindi $p \geq 5$).
Per il Lemma 4.10 esistono $b, c \in \mathbb{H}(\mathbb{Z})$ con $N(c) < N(a)$ e $p = ba + c$ (qui, ovviamente, $p = p1 \in \mathbb{H}(\mathbb{Z})$). Allora

$$N(b)N(a) = N(p - c) = (p - c)(p - \overline{c}) = p^2 - (c + \overline{c})p + N(c) \tag{4.9}$$

e quindi p divide $N(c)$ (in $\mathbb{Z}$). Se $c = 0$ allora da (4.9) segue $N(a) = p^2$ che non è il nostro caso. Dunque $c \neq 0$, e allora, per ipotesi induttiva, esistono $u, d \in \mathbb{H}(\mathbb{Z})$ con $c = ud$ e $N(d) = p$. Dividiamo a per d (Lemma 4.10): $a = qd + d_1$ con $N(d_1) < N(d)$. Se $d_1 = 0$ abbiamo finito. Sia quindi $d_1 \neq 0$; allora

$$\overline{d}d = N(d) = p = ba + c = b(qd + d_1) + ud$$

da cui segue $bd_1 = (\overline{d} - u - bq)d$. Quindi $p = N(d)$ divide $N(b)N(d_1)$ e pertanto $p|N(b)$. Osserviamo ora che (4.9) implica $p^2 - (c + \overline{c})p + N(c) > 0$ e dunque $(c + \overline{c})^2 - 4N(c) < 0$, da cui (poiché $N(c) \geq 5$)

$$|c + \overline{c}| \leq 2\sqrt{N(c)} < N(c) \leq N(a) - p \tag{4.10}$$

che sostituita a sua volta in (4.9) dà

$$N(a)N(b) < p^2 + (N(a) - p)p + N(a).$$

Conseguentemente, $N(a)N(b) < N(a)(p+1)$ e dunque $N(b) < p+1$. Poiché $p|N(b)$ otteniamo $N(b) = p$. Sostituendo ancora in (4.9),

$$N(a) = p - (c + \overline{c}) + \frac{N(c)}{p}$$

e dunque, tenendo conto che $p \geq 5$ e $N(c) < p^2$,

$$N(a) \leq p + 2\sqrt{N(c)} + \frac{N(c)}{p} < 4p.$$

Dunque $N(a) = 3p$, e $N(c) = \epsilon p$ con $\epsilon \in \{1, 2\}$. Ancora da (4.9) si ricava

$$3p^2 = p^2 - (c + \overline{c})p + \epsilon p$$

quindi $2p = \epsilon - (c + \overline{c})$ da cui la contraddizione $-(c + \overline{c}) > p$.

(2) Supponiamo ora $N(a) \geq p^2$. Dividendo a per p, esistono $b, c \in \mathbb{H}(\mathbb{Z})$ tali che $a = bp + c$ e $N(c) < N(p) = p^2$.
Sia $c = 0$. Per il teorema di Lagrange esiste $d \in \mathbb{H}(\mathbb{Z})$ tale che $p = \overline{d}d$; quindi $a = (b\overline{d})d$ e siamo a posto.
Sia $c \neq 0$, allora $0 < N(c) < N(p) = p^2$. Inoltre,

$$N(c) = N(a - bp) = (a - bp)(\overline{a} - \overline{b}p) = a\overline{a} - (a\overline{b} + b\overline{a})p + b\overline{b}p^2 = N(a) - (a\overline{b} + \overline{a\overline{b}})p + N(b)p^2$$

e quindi $p|N(c)$.
Per il punto precedente, esistono allora $u, d \in \mathbb{H}(\mathbb{Z})$ con $c = ud$ e $N(d) = \overline{d}d = p$. Dunque

$$a = bp + c = (b\overline{d})d + ud = (b\overline{d} + u)d$$

e la dimostrazione è ccmpleta. ∎

Proposizione 4.13. *Sia $a \in \mathbb{H}(\mathbb{Z})$; a è irriducibile se e solo se $N(a)$ è un numero primo.*

Dimostrazione. In un verso, l'affermazione è il Lemma 4.9. Sia, viceversa, $a \in \mathbb{H}(\mathbb{Z})$ un elemento irriducibile. Poicjé a non è invertibile, $N(a) > 1$, e dunque esiste un numero primo p che divide $N(a)$. Ma allora i Lemmi 4.11 e 4.12 (rispettivamente per $p = 2$ e $p \geq 3$) assicurano che in $\mathbb{H}(\mathbb{Z})$ esiste un divisore destro d di a con $N(d) = p$. L'irriducibilità di a comporta allora $N(a) = p$. ∎

Corollario 4.14. *Ogni $0 \neq a \in \mathbb{H}(\mathbb{Z})$ che non sia invertibile si puø' scrivere come il prodotto di elementi irriducibili.*

Ovviamente, in tali fattorizzazioni in irriducibili di $\mathbb{H}(\mathbb{Z})$ non c'è in genere alcun forma di unicità. Ci restringiamo al caso in cui $N(a)$ sia una potenza di un dato primo (dispari) p.

Sia quindi $p \geq 3$ un primo dispari fissato. Per il Teorema di Jacobi (4.4) il numero di quaternioni $a \in \mathbb{H}(\mathbb{Z})$ tali che $N(a) = p$ è uguale a $8\sigma(p) = 8(p + 1)$.
Osserviamo che. se $N(a) = p$, allora $N(ua) = p$ per ogni invertibile u di $\mathbb{H}(\mathbb{Z})$, Dunque l'insieme degli elementi di norma p è unione di classi di associati destri, ognuna delle quali contiene esattamente 8 elementi (e quindi il numero di classi è $p+1$). Il primo passo consiste nel selezionare un rappresentante per ciascuna classe.
Sia $a = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z})$ tale che

$$N(a) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = p.$$

Allora, poiché p è dispari, possiamo affermare che

- se $p \equiv 1 \pmod 4$ allora uno ed un solo a_i è dispari;
- se $p \equiv 3 \pmod 4$ allora uno ed un solo a_i è pari;

in ogni caso c'è una ed una sola coordinata la cui parità è diversa da quella delle altre tre; se tale coordinata distinta è diversa da 0, allora esiste uno ed un solo associato destro a' di a la cui prima coordinata a'_0 è il valore assoluto della coordinata distinta di a, ed in questo caso scegliamo a' come rappresentante; se invece la coordinata distinta è zero, allora le altre sono interi dispari (quindi questo caso si può verificare solo per $p \equiv 3 \pmod 4$) ed esistono due associati la cui prima coordinata è 0, in tal caso ne scegliamo uno dei due come rappresentante. Osserviamo che, se α è un rappresentate del primo tipo (ovvero tale che $\alpha_0 > 0$), allora anche il suo coniugato $\overline{\alpha}$ è un rappresentante (ed è diverso da α); se invece β è un rappresentante del secondo tipo (quindi $\beta_0 = 0$), allora $\overline{\beta} = -\beta$ appartiene alla stessa classe di β e quindi non è uno dei rappresentanti scelti; osserviamo che, nel primo caso $\alpha\overline{\alpha} = p$ e, mentre, nel secondo caso, $\beta^2 = -\beta\overline{\beta} = -p$.

Denotiamo con S_p l'insieme dei rappresentanti così scelti. Come già ricordato, $|S_p| = p = 1$; e possiamo scrivere

$$S_p = \{\alpha_1, \overline{\alpha}_1, \alpha_2, \overline{\alpha}_2, \ldots, \alpha_s, \overline{\alpha}_s, \beta_1, \ldots, \beta_t\},$$

dove gli α_i sono i rappresentanti la cui prima coordinata è > 0, i β_j quelli la cui prima coordinata è nulla, e $2s + t = p + 1$ (e $t = 0$ se $p \equiv 1 \pmod 4$).
Una *parola ridotta* in S_p è un prodotto di elementi di S_p in cui non compaiono sottosequenze del tipo $\alpha_i\overline{\alpha}_i$, $\overline{\alpha}_i\alpha_i$, $\beta_j\beta_j$, con $1 \le i \le s$ e $0 \le j \le t$; naturalmente, è compresa la parola nulla, che è 1.

Teorema 4.15. *Sia p un intero primo dispari e sia $a \in \mathbb{H}(\mathbb{Z})$ tale che $N(a) = p^k$, con $k \ge 1$. Allora a ammette una ed una sola fattorizzazione del tipo*

$$a = up^r w_m \tag{4.11}$$

dove u è un invertibile di $\mathbb{H}(\mathbb{Z})$, $r \ge 0$, e w_m è una parola ridotta in S_p, di lunghezza $m = k - 2r$.

Dimostrazione. *Esistenza.* Sia $N(a) = p^k$ con $k \ge 1$, e sia p^r la massima potenza di p che divide tutti i coefficienti di a. Allora $a = p^r a'$, dove $N(a') = p^{k-2r}$ e p non divide almeno uno dei coefficienti di a'. Per il Corollario 4.14, a' si fattorizza nel prodotto di irriducibili, ciascuno dei quali, per la proposizione 4.13, ha norma p; pertanto $a' = d_1 \ldots d_m$, con $N(d_i) = p$ per $i = 1, \ldots, m = k - 2r$. Dunque, per ogni $i = 1, \ldots, m$ esistono un invertibile u_i di $\mathbb{H}(\mathbb{Z})$ ed un (unico) elemento $s_i \in S_p$ tali che $d_i = u_i s_i$. Quindi

$$a' = u_1 s_1 \cdots u_k s_k. \tag{4.12}$$

Osserviamo però che se u è un invertibile e $s \in S_p$, allora $N(su) = p$, e dunque esistono $s' \in S_p$ e un invertibile u' tali che $su = u's'$; questo consente di riscrivere la (4.12) nella forma

$$a = p^r a' = p^r u s'_1 s'_2 \cdots s'_m = up^r s'_1 s'_2 \cdots s'_m. \tag{4.13}$$

con u invertibile e $s'_1, \ldots, s'_m \in S_p$. Osserviamo poi che $s'_1 s'_2 \cdots s'_m$ è una parola ridotta in S_p; se infatti in essa vi fossero termini consecutivi, s'_i ed s'_{i+1}, coniugati oppure uguali e del tipo

β (con $\beta = -\overline{\beta}$), allora $s'_i s'_{i+1} = \pm p$, e quindi potremmo raccogliere un altro fattore uguale a p, il che contraddice il fatto che p non divide almeno uno dei coefficienti di a' (e quindi non divide almeno uno di coefficienti di $s'_1 \cdots s'_m$).

Unicità. L'unicità delle fattorizzazioni cercate è stabilita se proviamo che il numero (che denotiamo con ℓ) di espressioni del tipo $up^r w_m$ con u invertibile, $k = 2r + m$ e w_m una parola ridotta in S_p, coincide con il numero di elementi di $\mathbb{H}(\mathbb{Z})$ la cui norma è p^k. Per il Teorema di Jacobi 4.4, quest'ultimo è uguale a (vedi anche l'esercizio 4.1)

$$8\sigma(p^k) = 8(1 + p + \cdots + p^k) = 8\,\frac{p^{k+1} - 1}{p - 1}. \tag{4.14}$$

Ora il numero di parole ridotte di lunghezza 0 è ovviamente 1 (la parola nulla), mentre se $m \geq 1$, l il numero di parole ridotte di lunghezza m in S_p è

$$(p + 1) \cdot p \cdot \cdots \cdot p = (p + 1)p^{m-1} \tag{4.15}$$

(infatti, vi sono $p + 1 = |S_p|$ scelte per la prima lettera, ed ogni lettera seguente può essere scelta in p modi). Poiché il numero di elementi invertibile è 8, possiamo affermare che

- se k è pari

$$\ell = 8\Big(\sum_{r=o}^{k/2-1} (p + 1)p^{k-2r-1} + 1\Big) = 8\big[(p + 1)(p + p^3 + \cdots + p^{k-1}) + 1\big] = 8\,\frac{p^{k+1} - 1}{p - 1};$$

- se k è dispari

$$\ell = 8\sum_{r=o}^{(k-1)/2} (p + 1)p^{k-2r-1} = 8(p + 1)(1 + p^2 + \cdots + p^{k-1}) = 8\,\frac{p^{k+1} - 1}{p - 1};$$

Il Teorema è quindi provato. ∎

4.4 Esercizi.

1. Funzioni moltiplicative. Scriviamo $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Sia A un dominio d'integrità (che in generale, ma non sempre, è l'anello $\mathbb{C}$ dei numeri complessi). Una funzione $f : \mathbb{N}^* \to A$ si dice *moltiplicativa* se, per ogni $n, m \in \mathbb{N}^*$

$$(n, m) = 1 \quad \Rightarrow \quad f(nm) = f(n)f(m)\ .$$

(Se f è una funzione moltiplicativa, $f(1) = 1_A$. Infatti, $f(1) = f(1)f(1)$ e ciò implica (poichè A è un dominio d'integrità) $f(1) = 1_A$).

Esercizio 4.9. Sia $f : \mathbb{N}^* \to A$ una funzione moltiplicativa, e sia $F : \mathbb{N}^* \to A$, definita ponendo, per ogni $n \in \mathbb{N}^*$

$$F(n) = \sum_{d|n} f(d)\ .$$

Si provi che F è moltiplicativa. Si deduca che sono moltiplicative le funzioni τ e σ dove, per ogni $n \in \mathbb{N}^*$, $\tau(n)$ è il numero di divisori interi (positivi) di n, mentre $\sigma(n)$ ne è la somma.

Esercizio 4.10. Sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la fattorizzazione in primi di $n \in \mathbb{N}^*$; si provi che

$$\tau(n) = \prod_{i=1}^{k} (1 + \alpha_i) \quad \text{e} \quad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \ .$$

Esercizio 4.11. Siano f e g funzioni moltiplicative (a valori in $\mathbb{C}$). Si provi che la funzione $f * h$ definita da

$$(f * h)(n) = \sum_{d|n} f(d) g(n/d)$$

è moltiplicativa. Si dimostri poi che l'operazione $*$ (detta prodotto di convoluzione) è un'operazione associativa e commutativa nell'insieme delle funzioni moltiplicative a valori in $\mathbb{C}$.

Esercizio 4.12. Si provi che per ogni $n \geq 1$

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

Esercizio 4.13. (Olimpiadi Matem. 1998) Sia $k \in \mathbb{N}^*$. Si provi che esiste $n \in \mathbb{N}$ tale che

$$\frac{\tau(n^2)}{\tau(n)} = k$$

se e solo se k è dispari.

2. Somme di due quadrati. Ricordiamo ora la definizione dell'anello degli interi di Gauss, $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. L'usuale norma su $\mathbb{C}$ induce una norma su $\mathbb{Z}[i]$, per ogni $z = a + ib \in \mathbb{Z}[i]$, $N(z) = (a + ib)(a - ib) = a^2 + b^2$. Ricordiamo che $N(uv) = N(u)N(v)$, per ogni $u, v \in \mathbb{C}$ e $N(u) = 0$ se e solo se $u = 0$. Ricordiamo anche che, rispetto alla norma, $\mathbb{Z}[i]$ è un dominio Euclideo (e quindi un un dominio a fattorizzazione unica). Gli elementi irriducibili di $\mathbb{Z}[i]$ sono chiamati *primi di Gauss* (mentre, in questi esercizi, chiameremo primi razionali i primi di $\mathbb{Z}$).

Esercizio 4.14. Si provi che gli elementi invertibili di $\mathbb{Z}[i]$ sono $1, -1, i, -i$.

Esercizio 4.15. Sia π un primo di Gauss; si provi che $N(\pi) = p, p^2$ per qualche primo razionale p.

Esercizio 4.16. Sia p un numero primo razionale. Si provi che sono equivalenti:

(1) $p = N(\pi)$ per qualche primo di Gauss π;

(2)] $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$;

(3) $p \equiv 1 \, (mod\, 4)$ oppure $p = 2$.

Esercizio 4.17. Usando l'esercizio precedente e l'identità (per numeri complessi)

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2.$$

si dimostri il teorema 4.1.

3. Divisione nei quaternioni. Sia $\mathbb{Z}_2 = \mathbb{Z}\left[\frac{1}{2}\right] = \{2^z m \mid m, z \in \mathbb{Z}\}$; si verifichi che $\mathbb{Z}_2$ è un anello con unità (questo è facile) e si trovino i suoi elementi invertibili.

Esercizio 4.18. Sia $a \in \mathbb{H}(\mathbb{Z}_2)$; utilizzando eventualmente il Lemma 4.11 (o l'esercizio 4.8) si provi che a è invertibile se e solo se $N(a) = 2^z$ per qualche $z \in \mathbb{Z}$. Si deduca che ogni elemento non nullo $a \in \mathbb{H}(\mathbb{Z}_2)$ è un prodotto $a = ua_1$, dove u è un invertibile di $\mathbb{H}(\mathbb{Z}_2)$ e $a_1 \in \mathbb{H}(\mathbb{Z})$ con $N(a_1)$ dispari.

Esercizio 4.19. Per ogni $a \in \mathbb{H}(\mathbb{Z})$ si ha $N(a) = 2^n N(a)_0$ con n e $N(a)_0$ intero positivo dispari. Si usi l'esercizio precedente ed il Lemma 4.10 per provare il seguiente fatto. Siano $a, b \in \mathbb{H}(\mathbb{Z}_2)$, $b \neq 0$; allora esistono $c, d \in \mathbb{H}(\mathbb{Z}_2)$ tali che $a = cb + d$ e $N(d)_0 < N(b)_0$.

Esercizio 4.20. Siano $a, b \in \mathbb{H}(\mathbb{Z})$ due quaternioni interi non nulli. un $d \in \mathbb{H}(\mathbb{Z})$ è detto un MCD destro di a e b (denotato con $(a, b)_r$) se

- d è un divisore destro di a e di b;
- Se d_1 è un divisore destro di a e di b, allora d_1 è un divisore destro di d.

Si provi che un MCD destro, se esiste, è definito a meno di associati destri. Quindi, applicando l'esercizio precedente, e mediante un algoritmo di tipo euclideo, si provi che per ogni $a, b \in \mathbb{H}(\mathbb{Z})$ con $N(b)$ dispari esiste una MCD destro $(a, b)_r$. SI provi infine che, dati a, b come prima, vale una relazione alla Bezout: esistono $\alpha, \beta \in \mathbb{H}(\mathbb{Z}_2)$ tali che $(a, b)_r = \alpha a + \beta b$.

Esercizio 4.21. Siano $a \in \mathbb{H}(\mathbb{Z})$ e $n \in \mathbb{Z}$, n dispari. Si provi che $(a, n)_r = 1$ se e solo se $(n, N(a)) = 1$.

Capitolo 5

Expanders

Finalmente siamo in grado di illustrare la costruzione, per ogni primo dispari p, di famiglie di grafi $(p+1)$-expanders (e, di fatto, grafi di Ramanujan). Ci sarà utile costruirli in due modi diversi, ciascuno dei quali risulta più conveniente per provare le proprietà che ci interessano.

5.1 I grafi $Y_{p,q}$ e $X_{p,q}$

Riprendiamo le notazioni della fine del capitolo precedente; in particolare, fissato un primo dispari p, S_p è il sistema di rappresentanti di classi associate destre dell'insieme degli elementi $a \in \mathbb{H}(\mathbb{Z})$ tali che $N(a) = p$, descritto nella sezione 4.3 (in particolare $|S_p| = p+1$). Sia ora

$$\Lambda' = \{a \in \mathbb{H}(\mathbb{Z}) \mid a = \pm p^r w,\ r \geq 0 \text{ e } w \text{ una parola in } S_p\}$$

Quindi, $S_p \subseteq \Lambda'$, $1 \in \Lambda'$ e $N(a)$ è una potenza di p, per ogni $a \in \Lambda'$; inoltre Λ' è moltiplicativamente chiuso. Su Λ' si definisce la relazione d'equivalenza $\sim$,

$$a \sim b \quad \Leftrightarrow \quad a = \pm p^s b \ \text{ oppure } \ b = \pm p^s a \ \text{ per qualche } s \geq 0.$$

Sia $\Lambda = \Lambda'/\sim$ l'insieme quoziente, e $\pi : \Lambda' \to \Lambda$ la proiezione canonica. Denotiamo con $[a] = \pi(a)$ la classe d'equivalenza di $a \in \Lambda'$
La relazione $\sim$ è una congruenza per la moltiplicazione: ovvero, per $a, b, a', b' \in \Lambda$,

$$\begin{cases} a \sim a' \\ b \sim b' \end{cases} \quad \Rightarrow \quad ab \sim a'b'.$$

Dunque Λ è un monoide moltiplicativo. Di più, Λ *è un gruppo.* Infatti, sia $a \in \Lambda'$, allora $a = \pm p^s w$ con $r \geq 0$ e w una parola in S_p. Se $w = 1$, allora $[a] = [\pm p^r] = [1]$; se $w = s_1 \cdots s_m$ (con $s_i \in S_p$), allora $\overline{w} = \overline{s_m} \ldots \overline{s_1}$ è a meno del segno una parola in S_p; quindi $\overline{a} \in \Lambda'$, e si ha, in Λ,

$$[a][\overline{a}] = [p^r w][p^r \overline{w}] = [p^{2r+m}] = [1]$$

Dunque, Λ è un gruppo rispetto alla moltiplicazione indotta da $\mathbb{H}(\mathbb{Z})$. Osserviamo che, in tale gruppo, il sottoinsieme $\pi(S_p)$ soddisfa alle condizioni per poter generare un grafo di Cayley; denotiamo con Y^p il grafo di Cayley $\Gamma(\Lambda, \pi(S_p))$.

Proposizione 5.1. *Il grafo Y^p è un albero regolare di grado $p+1$.*

DIMOSTRAZIONE. Osserviamo che per $a, b \in S_p$, $a \neq b \Rightarrow [a] \neq [b]$. Quindi $|\pi(S_p)| = |S_p| = p+1$. Inoltre, per ogni $u = \pm p^r w \in \Lambda'$, $[u] = [p^r][w] = [1][w] = [w]$, e dunque $\pi(S_p)$ è un sistema di generatori di Λ. Pertanto, il grafo di Cayley Y^p è connesso e $(p+1)$-regolare. La Proposizione è dimostrata se proviamo che Y^p è privo di circuiti. Procediamo per assurdo e supponiamo quindi che $[a_0], [a_1], \ldots, [a_n] = [a_0]$ (con $n \geq 3$)sia la successione dei vertici in un ciclo non banale di Y^p. Allora, per definizione di grafo di Cayley, esistono $s_1, \ldots, s_n \in S_p$ tali che

$$[a_0] = [a_n] = [a_0][s_1][s_2] \ldots [s_n];$$

e, moltipliocando a sinistra per $[\overline{a}_0] = [a_0]^{-1}$, $[1] = [s_1 s_2 \ldots s_n]$. Ciò significa che

$$s_1 s_2 \ldots s_n = \pm p^r, \tag{5.1}$$

per qualche $r \geq 0$. Ma, poiché gli s_i sono associati agli archi consecutivi di un ciclo, si ha che, per ogni $1 \leq i \leq n-1$, $[[s_{i+1}] \neq [s_i]^{-1}$; quindi, a seconda che la prima coordinata di s_i sia $\neq 0$ oppure $= 0$, si ha che s_{i+1} è diverso da $\overline{s_i}$ o da s_i. Quindi $s_1 s_2 \ldots s_n$ è una parola ridotta in S_p, e questo è in contraddizione con (5.1). ∎

Fissato un altro numero primo $q \neq p$, vogliamo ora "ridurre" il grafo Y^p modulo q.
Sia $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ il campo con q elementi e sia

$$\tau : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q) \tag{5.2}$$

la riduzione modulo q. Denotiamo con $\mathbb{H}(\mathbb{F}_q)^*$ l'insieme degli elementi invertibili di $\mathbb{H}(\mathbb{F}_q)$. Sia $a \in \Lambda'$, allora $a\overline{a} = N(a) = p^k$ con $k \geq 0$; poiché p è invertibile in $\mathbb{F}_q$, abbiamo $\tau(a) \cdot (p^{-k}\tau(\overline{a})) = p^{-k}\tau(a\overline{a}) = 1$. Quindi

$$\tau(\Lambda') \subseteq \mathbb{H}(\mathbb{F}_q)^*.$$

Sia $Z_q = \{u \in \mathbb{H}(\mathbb{F}_q)^* \mid a = \overline{a}\}$. Allora, chiaramente, $Z_q \simeq \mathbb{F}_q^*$ (come gruppi moltiplicativi); inoltre Z_q è contenuto nel centro di $\mathbb{H}(\mathbb{F}_q)$, in particolare Z_q è un sottogruppo normale di $\mathbb{H}(\mathbb{F}_q)^*$. Ora, per ogni $a, b \in \Lambda'$,

$$a \sim b \quad \Rightarrow \quad \tau(a)^{-1}\tau(b) \in Z_q \quad \Leftrightarrow \quad \tau(a)Z_q = \tau(b)Z_q.$$

Quindi la restrizione di τ all'omomorfismo moltiplicativo $\Lambda' \to \mathbb{H}(\mathbb{F}_q)^*$, induce a sua volta un omomorfismo di gruppi

$$\Pi_q : \Lambda \longrightarrow \mathbb{H}(\mathbb{F}_q)^*/Z_q. \tag{5.3}$$

Scriviamo $\Lambda(q) = \ker(\Pi_q)$, e, a norma del teorema di omomorfismo per gruppi, identifichiamo $Im(\Pi_q)$ con $\Lambda/\Lambda(q)$. Poniamo infiine $T_{p,q} = (\Pi_q \circ \pi)(S_p)$ (quindi gli elementi di $T_{p,q}$ sono le classi $\tau(s)Z_q$ con $s \in S_p$).

Lemma 5.2. *Con le notazioni di sopra, si ha:*

$$\Lambda(q) = \{[a] \in \Lambda \mid a = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda',\ q | a_1, a_2, a_3\}.$$

DIMOSTRAZIONE. Questo è chiaro dalla definizione di Π_q. ∎

Definiamo ora il grafo $Y_{p,q}$; si tratta del grafo di Cayley

$$Y_{p,q} = \Gamma(\Lambda/\Lambda(q), T_{p,q}). \tag{5.4}$$

Lemma 5.3. *Se $q > 2\sqrt{p}$ allora $|T_{p,q}| = p + 1$.*

DIMOSTRAZIONE. Basta provare che se $a = a_0 + a_1 i + a_2 j + a_3 k$ e $b = b_0 + b_1 i + b_2 j + b_3 k$ sono elementi distinti di S_p, allora $\tau(a)Z_q \neq \tau(b)Z_q$.
Poiché $N(a) = p = N(b)$, tutti i coefficienti a_i e b_i appartengono all'intervallo $(-\sqrt{p}, \sqrt{p})$. Quindi, se $q > 2\sqrt{p}$, $\tau(a) = \tau(b) \Leftrightarrow a = b$.
Sia $q > 2\sqrt{p}$, e supponiamo per assurdo che $\tau(a)Z_q = \tau(b)Z_q$. Dalla definizione di Z_q segue che esiste $\lambda \in \mathbb{F}_q^*$ tale che $\tau(b) = \lambda\tau(a)$. Allora

$$\tau(p) = \tau(b\bar{b}) = \tau(\lambda a)\tau(\lambda\bar{a}) = \lambda^2\tau(a\bar{a}) = \lambda^2\tau(p),$$

e siccome, in $\mathbb{F}_q$, $\tau(p) \neq 0$, si ha $\lambda^2 = 1$, cioè $\lambda = \pm 1$. Per quanto osservato sopra, rimane da discutere il caso $\tau(b) = -\tau(a)$. Ma per la scelta degli elementi di S_p, abbiamo $a_0, b_0 \geq 0$; e dunque il solo caso rimasto è quando $a_0 = b_0$. In tal caso $\tau(b) = -\tau(a)$ comporta $b = \bar{a}$, che per la scelta degli elementi in S_p, implica $a_0 > 0$, una contraddizione.. ∎

Da questo Lemma e dal fatto, ovvio, che $\Lambda/\Lambda(q)$ è generato da $T_{p,q}$ (dato che Λ è generato da $\pi(S_p)$), e dai risultati della sezione 2.2, segue il seguente fatto.

Proposizione 5.4. *Sia $q > 2\sqrt{p}$. Allora $Y_{p,q}$ è un grafo $(p+1)$-regolare e connesso.*

Ci occorre ora una stima sul calibro (da cui seguirà una sul numero di vertici) di $Y_{p,q}$.

Proposizione 5.5. $g(Y_{p,q}) \geq 2\log_p q$.

DIMOSTRAZIONE. Sia $g = g(Y_{p,q})$, e siano $x_0, x_1, \ldots, x_{g-1}, x_g = x_0$ (elementi di $\Lambda/\Lambda(q)$) i vertici di un cilco di lunghezza g in $Y_{p,q}$. Per la vertex–transitività dei grafi di Cayley, possiamo assumere $x_0 = x_g = 1$. Esistono quindi $t_1, \ldots t_g \in T_{p,q}$ (univocamente determinati) tali che $x_i = t_1 \ldots t_i$ per ogni $1 \leq i \leq g$, e per ogni t_i sia $\gamma_i \in S_p$, tale che $x_i = \Pi_q([\gamma_1])$. Infine, siano $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ tali che

$$a_0 + a_1 i + a_2 j + a_3 k = a = \gamma_1 \ldots \gamma_g$$

ed osserviamo che $a \in \Lambda'$, e che a è ridotta. Ora, in Λ, $[a] = [\gamma_1] \cdots [\gamma_g] \neq [1]$, quindi $a \not\sim 1$, e pertanto

$$\text{almeno uno tra } a_1,\ a_2,\ a_3 \text{ è diverso da 0.} \tag{5.5}$$

D'altra parte, $\Pi_q([a]) = t_1 \ldots t_g = x_g = 1$, e quindi $[a] \in \Lambda(q)$, che, per 5.2, implica

$$q \text{ divide } a_1,\ a_2,\ a_3. \tag{5.6}$$

Da ciò e (5.5) segue che almeno uno tra a_1, a_2 e a_3 è in modulo maggiore o uguale a q; quindi

$$p^g = N(a) \geq q^2$$

da cui segue $g \geq 2\log_p q$. ∎

Corollario 5.6. $|\Lambda/\Lambda(q)| \geq q/p$.

DIMOSTRAZIONE. $n = \Lambda(/\Lambda(q)$ è il numero di vertici del grafo $Y_{p,q}$. Per la proposizione precedente e la 2.3 si ha quindi

$$n \geq 1 + (p+1)\frac{p^{\log_p q - 1} - 1}{p-1} = 1 + (p+1)\frac{qp^{-1} - 1}{p-1} > \frac{q}{p},$$

come si voleva. ■

* * *

Siano p, q come nella parte precedente. Per la Proposizione 4.7, esiste un isomorfismo (di $\mathbb{F}_q$-algebre):

$$\psi : \mathbb{H}(\mathbb{F}_q) \longrightarrow M_2(\mathbb{F}_q), \tag{5.7}$$

e, per ogni $a \in \mathbb{H}(\mathbb{F}_q)$ valgono (si vedano l'osservazione e l'esercizio che seguono la dimostrazione della Proposizione 4.7) le seguenti condizioni:

- $\det \psi(a) = N(a)$.
- $\mathrm{Tr}(\psi(a)) = a + \overline{a}$, e se $a = \overline{a}$ allora $\psi(a)$ è una matrice scalare.

La composizione della proiezione τ in (5.2) con ψ dà luogo ad un omomorfismo suriettivo (di anelli)

$$\psi \circ \tau : \mathbb{H}(\mathbb{Z}) \longrightarrow M_2(\mathbb{F}_q). \tag{5.8}$$

Sia $s \in S_p$; poiché $q \neq p$, $N(s) = p \neq 0$ in $\mathbb{F}_q$, e quindi, per quanto osservato sopra,

$$\det(\psi\tau(s)) \neq 0.$$

Dunque $\psi\tau(s)$ è un elemento invertibile di $M_2(\mathbb{F}_q)$. Pertanto

$$\psi\tau(S_p) \subseteq GL(2, q). \tag{5.9}$$

Sia $Z = \{kI_n \mid 0 \neq k \in \mathbb{F}_q\}$ il centro di $GL(2, q)$, e sia ϕ la proiezione sul quoziente $GL(2, q)/Z = PGL(2, q)$. Poniamo infine

$$S_{p,q} = \phi\psi\tau(S_p).$$

Adotteremo ora una restrizione sui primi q, che non è strettamente necessaria, ma che semplifica le cose, ed in particolare ci consente di lavorare nel gruppo speciale $PSL(2, q)$. Per descrivere questa condizione conviene ricordare un concetto fondamentale nelle teoria elementare dei numeri, e precisamente quello di residuo quadratico.
Sia p un numero primo dispari, e $a \in \mathbb{Z}$. Si dice che a è un *residuo qadratico* modulo p, se la classe di congruenza $a + p\mathbb{Z}$ è un quadrato in $\mathbb{Z}/p\mathbb{Z}$, ovvero se la congruenza $x^2 \equiv a \pmod{p}$ ammette soluzioni intere. Il *simbolo di Legendre* è poi definito nel modo seguente:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{se } p|a; \\ 1 & \textit{se } (p, a) = 1 \textit{ ed } a \textit{ è un residuo quadr. modulo } p; \\ -1 & \textit{se } a \textit{ non è un residuo quadr. modulo } p. \end{cases}$$

Supponiamo quindi che per i primi p e q valga $\left(\frac{p}{q}\right) = 1$, e sia $a \in \mathbb{F}_q$ tale che $a^2 = p$. Allora, se $s \in S_p$, abbiamo $\det(\psi\tau(s) = p = a^2$ in $\mathbb{F}_q$; poniamo $z = a^{-1}I_2 \in Z$, che è un elemento del centro di $GL(2,q)$. Quindi $\det(z \cdot \psi\tau(s) = 1$ e pertanto $z \cdot \psi\tau(s) \in SL(2,q)$. Di conseguenza

$$\phi\psi\tau(s) = \phi(z \cdot \psi\tau(s)) \in PSL(2,q).$$

In conclusione, abbiamo provato che

$$\text{se } \left(\frac{\mathrm{p}}{\mathrm{q}}\right) = 1 \text{ allora } \mathrm{S_{p,q}} \subseteq \mathrm{PSL(2,q)}.$$

D'ora in avanti, per semplificare le cose, assumeremo quasi sempre che $\left(\frac{p}{q}\right)$ (condizioone che, fissato il primo p, si può dimostrare essere comunque soddisfatta da infiniti primi q).

Definiamo il grafo $X_{p,q}$ come il grafo di Cayley

$$X_{p,q} = \Gamma(PSL(2,q), S_{p,q}) \tag{5.10}$$

se $\left(\frac{p}{q}\right) = 1$; mentre $X_{p,q} = \Gamma(PGL(2,q), S_{p,q})$ se $\left(\frac{p}{q}\right) = -1$.

Sia $Z_q = \{a \in \mathbb{H}(F_q)^* \mid a = \overline{a}\}$. Allora Z_q è un sottogruppo del gruppo moltiplicativo $\mathbb{H}(F_q)^*$, ed è infatti il centro di tale gruppo. Per le osservazioni che seguono la definizione dell'applicazione $\psi : \mathbb{H}(\mathbb{F}_q) \to M_2(\mathbb{F}_q)$, si ha che $\psi(a)$ è una matrice scalare per ogni $a \in Z_q$, e dunque $\psi(Z_q) \leq Z$. Ciò significa che porre, per ogni $u \in \mathbb{H}(F_q)^*$, $\beta(uZ_q) = \phi(\psi(u))$ definisce un isomorfismo

$$\beta : \mathbb{H}(F_q)^*/Z_q \longrightarrow PGL(2,q). \tag{5.11}$$

Osserviamo anche che, per definizione, $\phi\psi = \beta\pi$, se π è la proiezione $\mathbb{H}(F_q)^* \to \mathbb{H}(F_q)^*/Z_q$, e quindi che $S_{p,q} = \beta(T_{p,q})$.

Teorema 5.7. *Sia $p \geq 5$, e $q > p^8$. Allora $X_{p,q}$ è connesso e isomorfo a $Y_{p,q}$.*

Dimostrazione. Ricordiamo che $Y_{p,q}$ è il grafo di Cayley $\Gamma(\Lambda/\Lambda(q), T_{p,q})$, e che, mediante l'omomorfismo Π_q di (5.3) ed il teorema di omomorfismo, $\Lambda/\Lambda(q)$ è identificato con $Im(\Pi_q) \leq \mathbb{H}(F_q)^*/Z_q$, e che infine $T_{p,q} = \Pi_q(S_p\Lambda)$. Ora, $\Lambda/\Lambda(q)$ è generato da $T_{p.q}$, e quindi $Y_{p,q}$ è connesso. Ma $\Lambda/\Lambda(q)$ è un sottogruppo di $\mathbb{H}(F_q)^*/Z_q$. Quindi, $Y_{p,q}$ è una componente connessa del grafo di Cayley $\Gamma(\mathbb{H}(F_q)^*/Z_q, T_{p,q})$. Ora, applicando la funzione β definita in 5.11, otteniamo un isomorfismo $\overline{\beta}$ da tale grafo nel grafo di Cayley $\Gamma(PGL(2,q), S_{p,q})$, che a sua volta contiene il grafo $X_{p.q}$ come unione di componenti connesse. Poiché $\beta(T_{p,q}) = S_{p,q}$, in tale isomorfismo l'immagine di $Y_{p,q}$ è contenuta (come sottografo indotto) in $X_{p,q}$; per le proprietà dei grafi di Cayley, si ha pertanto che $\overline{\beta}(Y_{p,q})$ è una componente connessa di $X_{p,q}$. Dunque, dimostrare che $Y_{p,q}$ e $X_{p,q}$ sono isomorfi si riduce a provare che $X_{P,q}$ è connesso.

Per semplicità, dimostreremo questo fatto solo nel caso in cui $\left(\frac{p}{q}\right) = 1$ (il caso generale funziona con lo stesso tipo di argomenti, ma è un poco più lungo). Alloar, per definizione, $X_{p,q} = \Gamma(PSL(2,q), S_{p,q})$. Sia H il sottogruppo generato in $PSL(2,q)$ da $S_{p,q}$. Per quanto abbiamo visto sui grafi di Cayley, $X_{p,q}$ è connesso se e solo se $H = PSL(2,q)$.

Ora, per quello che abbiamo osservato sopra, H è isomorfo a $\beta(\Lambda/\Lambda(q))$. Poiché $q > p^8$, per il Corollario 5.6 abbiamo

$$|H| = |\Lambda/\Lambda(q)| \geq p^7 > 60.$$

Mettiamo ora a frutto quanto dimostrato nel capitolo 3. Per il Corollario 3.15, se H fosse un sottogruppo proprio di $PSL(2,q)$, allora sarebbe metaciclico. Quindi $H = PSL(2,q)$ (e il nostro Teorema è dimostrato) se H non è metaciclico. Per provare quest'ultima affermazione è sufficiente provare che H non è metabeliano; cioè che il derivato H' non è un gruppo abeliano. Basterà dunque trovare elementi $g_1, g_2, g_3, g_4 \in H$ tali che

$$[[g_1, g_2], [g_3, g_4]] \neq 1. \tag{5.12}$$

Prendiamo x_1 un qualsiasi elemento di $T_{p,q}$; poiché $p > 5$, possiamo trovare altri elementi x_2, x_3 di $T_{p,q}$ tali che

$$x_2 \neq x_1^{\pm 1} \quad e \quad x_3 \notin \{x_1^{\pm 1}, x_2^{\pm 1}\}.$$

Consideriamo quindi gli elementi di H, $g_1 = \beta(x_1)$, $g_2 = g_4 = \beta(x_2)$ e $g_3 = \beta(x_3)$. Ricordando che il commutatore in un gruppo è definito da $[a,b] = a^{-1}b^{-1}ab$, sviluppando il doppio commutatore in (5.12) si ricava una parola di lunghezza 16 in g_1, g_2, g_3. Questa, a sua volta è l'immagine, tramite β, di un prodotto (parola) di lunghezza 16 in x_1, x_2, x_3, e quindi di un percorso (che parte da 1) nel grafo $Y_{p,q}$. Per la scelta di x_1, x_2, x_3 in $T_{p,q}$, si tratta di un percorso senza iversioni. Se fosse $[[g_1, g_2], [g_3, g_4]] = 1$, allora tale percorso ritornerebbe al vertice iniziale 1, e quindi dovrebbe includere un ciclo non banale di $Y_{p,q}$. Ma dalla Proposizione 5.5, e la scelta di q, ricaviamo

$$g(Y_{p,q}) \geq 2\log_p q > 2 \cdot 8 = 16.$$

Dunque, qualsiasi ciclo non banale in $Y_{p,q}$ è espresso da un aprola di lunghezza almeno 17 nei generatori $T_{p,q}$. Dunque la (5.12) è soddisfatta, e pertanto H non è metabeliano. Quindi $H = PSL(2,q)$, $X_{p,q}$ è connesso e, di conseguenza, $X_{p,q} \simeq Y_{p,q}$. ∎

Esempio. Vediamo, come esempio, il caso non contemplato dal Teorema 5.7 di $p = 3$. La sola maniera per scrivere 3 come somma di al più quattro quadrati è: $1+1+1$. Consideriamo i seguenti elementi di $\mathbb{H}(\mathbb{Z})$:

$$\begin{aligned} a &= i + j + k \\ b &= i - j + k \\ c &= i + j - k \\ d &= i - j - k. \end{aligned}$$

Per come abbiamo definito l'insieme S_3, possiamo porre $S_3 = \{a, b, c, d\}$.
Sia q un altro primo, con 3 un quadrato modulo q (utilizzando il classico teorema di reciprocità quadratica di Gauss, si può provare che ciò equivale $q \equiv \pm 1 \pmod{12}$). Per definire l'applicazione ψ in (5.7) occorre, per la Proposizione 4.7, fissare due elementi $x, y \in \mathbb{F}_q$ tali che $x^2 + y^2 + 1 = 0$. Per semplificare le cose, scegliamo q in modo che -1 sia un quadrato in $\mathbb{F}_q$; ciò si verifica se e solo se $q \equiv 1 \pmod 4$ (quindi, assieme alla condizione precedente scegliamo $q \equiv 1 \pmod{12}$[1]). Allora, basta prendere un elemento $x \in \mathbb{F}_q$ tale che $x^2 = -1$, e

[1] Per un teorema di Dirichlet, esistono infiniti primi q con questa proprietà.

l'applicazione ψ è data da

$$a_0 + a_1 i + a_2 j + a_3 k \ \mapsto \begin{pmatrix} a_0 + a_1 x & a_2 + a_3 x \\ -a_2 + a_3 x & a_0 - a_1 x \end{pmatrix}$$

In particolare, posto $S = S_{3,q} = \psi()$, sia ha

$$S = \left\{ \begin{pmatrix} x & x+1 \\ x-1 & -x \end{pmatrix}, \begin{pmatrix} x & x-1 \\ x+1 & -x \end{pmatrix}, \begin{pmatrix} x & -x+1 \\ -x-1 & -x \end{pmatrix}, \begin{pmatrix} x & -x-1 \\ -x+1 & -x \end{pmatrix} \right\}.$$

Mettiamoci ora nel caso specifico $q = 13$. Allora $x = 5$ o 8. Scegliamo $x = 5$; quindi, gli elementi di $S_{3,13}$ sono

$$A = \begin{pmatrix} 5 & 6 \\ 4 & -5 \end{pmatrix} \qquad B = \begin{pmatrix} 5 & 4 \\ 6 & -5 \end{pmatrix} \qquad C = \begin{pmatrix} 5 & -4 \\ -6 & -5 \end{pmatrix} \qquad D = \begin{pmatrix} 5 & -6 \\ -4 & -5 \end{pmatrix}.$$

Si osserverà che questi elementi hanno determinante 3, che è un quadrato modulo 13 – infatti $3 \equiv 4^2 \pmod{13}$ – dunque ciascuno di essi si scrive come il prodotto di una matrice scalare per una di $SL(2, 13)$, ad esemipo

$$A = \begin{pmatrix} 9 & 0 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 2 & 5 \\ -1 & -2 \end{pmatrix};$$

e quindi appartengono a $PSL(2, 13)$. Inoltre si noti gli elementi di $S_{3,13}$ hanno ordine 2 (in $PSL(2, 13)$); infatti, provengono da quaternioni interi la cui prima componente è 0.
Ora, $X_{3,13}$ è il grafo di Cayley $\Gamma(G, S_{3,13})$, dove $G = PSL(2, 13)$.
Per esercizio si cerchi ora di dimostrare che G è generato da $S_{3,13}$. Per la prima parte della dimostrazione di 5.7, ne segue che $X_{3,13}$ è connesso e isomorfo s $Y_{3,13}$. $X_{3,13}$ è un grafo 4-regolare (vertex-tranxitivo) su $|G| = 1092$ vertici.

5.2 Formule per gli autovalori

Per poter dedurre che i grafi $X_{p,q}$ definiti nella sezione precedente costituiscono (fissato il primo p) una famiglia di $(p+1)$-expanders, abbiamo bisogno di tornare per un momento alla teoria generale dei grafi.

Sia $\Gamma = (V, E)$ un grafo semplice con n vertici; siano $x, y \in V$, ed $r \geq 0$. Un *percorso senza inversioni* (S.I.) di lunghezza r da x a y è una successione

$$x = x_0, \ x_1, \ \ldots, \ x_r = y$$

di vertici di Γ, tale che $\{x_i, x_{i+1}\} \in E$ per ogni $i = 0, \ldots, r-1$, e $x_{i-1} \neq x_{i+1}$, per ogni $i = 1, \ldots, r-1$.
Denotiamo con $(A_r)_{xy}$ il numero di percorsi S.I. di lunghezza r da x a y, e con A_r la matrice $n \times n$ i cui coefficienti sono gli interi $(A_r)_{xy}$ (al variare di $x, y \in V$). È evidente quindi che, per ogni $r \geq 0$, A_r è una matrice simmetrica, che $A_0 = I_n$, e che $A_1 = A(\Gamma)$ è la matrice di adiacenza di Γ. Se Γ è regolare possiamo dire di più:

Proposizione 5.8. *Sia $k \geq 2$. Sia Γ un grafo semplice k-regolare ed $A = A(\Gamma)$ la sua matrice di adiacenza. Allora*

(1) $A^2 = A_2 + kI$;

(2) per $r \geq 2$: $AA_r = A_r A = A_{r+1} + (k-1)A_{r-1}$.

DIMOSTRAZIONE. Il punto (1) è immediato dalle definizioni. ∎

Polinomi di Čebishev. Per ogni $m \geq 0$ il m-esimo polinomio di Čebishev $U_m(x)$ è il polinomio definito da

$$U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}$$

per ogni $\theta \in \mathbb{R}$. Che queste relazioni definiscano dei polinomi (a coefficienti interi) si verifica abbastanza facilmente. Infatti $U_0 = 1$. Quindi, da

$$\frac{\sin 2\theta}{\sin\theta} = \frac{2\sin\theta\cos\theta}{\sin\theta} = 2\cos\theta$$

si ricava

$$U_1(x) = 2x.$$

Similmente, sviluppando $\sin 3\theta / \sin\theta$, si trova

$$U_2(x) = 4x^2 - 2,$$

ed, in generale, che vale la seguente formula ricorsiva:

$$U_{m+1}(x) = 2xU_m(x) - U_{m-1}(x). \tag{5.13}$$

Torniamo ora ad un grafo semplice $\Gamma + (V, E)$, ed alle matrici $A = A_1 = A(\Gamma)$ e A_r definite sopra. Per ogni $m \geq 0$, poniamo

$$T_m = \sum_{r=0}^{[m/2]} A_{m-2r}. \tag{5.14}$$

Proposizione 5.9. *Sia Γ un grafo k-regolare, ed A la sua matrice di adiacenza. Allora per ogni $m \geq 0$ si ha:*

$$T_m = (k-1)^{m/2} U_m\left(\frac{A}{2\sqrt{k-1}}\right).$$

DIMOSTRAZIONE. Chiaramente, $T_0 = I = A_0$, e l'affermazione è vera perché U_0 è la costante 1. Sia $m = 1$, allora $U_1(x) = 2x$, e

$$T_1 = A_1 = A = \sqrt{k-1}\,U_1\Big(\frac{A}{2\sqrt{k-1}}\Big)$$

come si vuole. Procediamo quindi per induzione su m, e sia $m \geq 1$. Allora

$$(k-1)^{\frac{m+1}{2}} U_{m+1}\Big(\frac{A}{2\sqrt{k-1}}\Big) = (k-1)^{\frac{m+1}{2}}\Big[\frac{A}{\sqrt{k-1}}\Big(\frac{A}{2\sqrt{k-1}}\Big) - U_m\Big(\frac{A}{2\sqrt{k-1}}\Big)\Big] =$$
$$= (k-1)^{\frac{m}{2}} A \cdot U_m\Big(\frac{A}{2\sqrt{k-1}}\Big) - (k-1)(k-1)^{\frac{m-1}{2}} U_{m-1}\Big(\frac{A}{2\sqrt{k-1}}\Big) =$$
$$= AT_m - (k-1)T_{m-1}.$$

Applicando l'ipotesi induttiva e la Proposizione 5.8 si ricava

$$(k-1)^{\frac{m+1}{2}} U_{m+1}\Big(\frac{A}{2\sqrt{k-1}}\Big) = \sum_{r=0}^{m/2} A \cdot A_{m-2r} - (k-1) \sum_{r=0}^{(m-1)/2} A_{m-1-2r} =$$
$$= \sum_{r=0}^{m/2} \big[A \cdot A_{(m+1)-2r} + (k-1)A_{(m-1)-2r}\big] - (k-1) \sum_{r=0}^{(m-1)/2} A_{m-1-2r} =$$
$$= \sum_{r=0}^{[m/2]} A_{(m+1)-2r} = T_{m+1}.$$

che è quanto si voleva ottenere. ∎

Denotiamo ora, come di consueto con

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$$

lo *spettro* di $A = A(\Gamma)$, ovvero l'insieme degli autovalori con molteplicità di A ordinato nel verso decrescente. Ricordo che se Γ è k-regolare, allora $\mu_0 = k$ e $|\mu_i| \leq k$ per ogni $i = 0, n-1$. Per ogni vertice $x \in V$ del grafo k-regolare $\Gamma = (V, E)$,ed ogni $t \geq 0$, denotiamo con $f_{t,x}$ il numero di percorsi S.I. di lunghezza t che iniziano e terminano in x. In altre parole, $f_{t,x} = (A_t)_{xx}$ è il termine diagonale di posto x della matrice A_t.

Teorema 5.10. *Sia $m \geq 0$, e Γ k-regolare su n vertici; allora*

$$\sum_{x \in V} \sum_{r=0}^{m/2} f_{m-2r,x} = (k-1)^{m/2} \sum_{j=0}^{n-1} U_m\Big(\frac{\mu_j}{2\sqrt{k-1}}\Big).$$

Dimostrazione. Sia $m \geq 0$. Dalla Proposizione 5.9 si ha

$$Tr(T_m) = (k-1)^{m/2} \sum_{j=0}^{n-1} U_M\Big(\frac{\mu_j}{2\sqrt{k-1}}\Big).$$

D'altra parte, dalla definizione (5.14) segue

$$Tr(T_m) = \sum_{x \in V} \sum_{r=0}^{m/2} (A_{m-2r})_{x,x} = \sum_{x \in V} \sum_{r=0}^{m/2} f_{m-2r,x}$$

da cui il risultato. ∎

Se inoltre il grafo Γ è *vertex–transitivo* (come sappiamo essere tutti i grafi di Cayley), allora è chiaro che, per ogni $t \geq 0$, il valore $f_{t,x}$ è lo stesso per tutti i vertici x di Γ, ovvero dipende solo da t; possiamo quindi denotarlo senz'altro con f_t, e ricavare pertanto dal teorema 5.10 il seguente e importante corollario.

Corollario 5.11. *Sia Γ un grafo k-regolare vertex–transitivo su n vertici. Allora per ogni $m \geq 0$,*

$$n \cdot \sum_{r=0}^{m/2} f_{m-2r} = (k-1)^{m/2} \sum_{j=0}^{n-1} U_m\Big(\frac{\mu_j}{2\sqrt{k-1}}\Big).$$

Nel caso particolare di $\Gamma = X_{p,q}$ (con $q \geq p^8$) tale formula divents:

$$\sum_{r=0}^{m/2} f_{m-2r} = \frac{p^{m/2}}{n} \sum_{j=0}^{n-1} U_m\Big(\frac{\mu_j}{2\sqrt{p}}\Big). \tag{5.15}$$

5.3 Verifica che gli $X_{p,q}$ sono una famiglia di expanders

In questa sezione, supponiamo di avere fissato un primo $p \geq 5$, e di utilizzare primi q che soddisfano alle ipotesi del Teorema 5.7 (cioè $q > p^8$) e per i quali vale $\left(\frac{p}{q}\right) = 1$. Quindi $X_{p,q}$ è il grafo $\Gamma(PSL(2,q), S_{p,q})$.

Sia $n = |PSL(2,q)|$ il numero di vertici di $X_{p,q}$ e sia

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$$

lo spettro degli autovalori di $X_{p,q}$ (cioè, della sua matrice di adiacenza). Poiché $X_{p,q}$ è $(p+1)$-regolare e connesso, sappiamo che $p+1 = \mu_0 > \mu_1$, e che $|\mu_i| \leq p+1$ per ogni $i = 1, \ldots, n-1$.

Lemma 5.12. *Sia μ un autovalore non banale di $X_{p,q}$, e sia $M(\mu)$ la sua molteplicità. Allora*

$$M(\mu) \geq \frac{q-1}{2}.$$

(Ricordo che se Γ è un grafo k-regolare, un autovalore μ di Γ si dice *non banale* se $|\mu| \neq k$.)

Dimostrazione. Come introdotto nel capitolo 2, consideriamo la matrice di adiacenza $A = A(X_{p,q})$ come quella di un operatore lineare sullo spazio $\mathcal{C}(\Gamma)$, e denotiamo con U l'autospazio relativo all'autovalore μ; quindi $Af = \mu f$ per ogni $f \in U$. Ora, il gruppo $G = PSL(2,q)$ opera in modo naturale su $\mathcal{C}(\Gamma)$, mediante

$$f^g(x) = f(xg^{-1})$$

per ogni $g \in G$, $f \in \mathcal{C}(\Gamma)$ e, ancora, $x \in G$ (questa volta G è l'insieme dei vertici di $X_{p,q}$). Questo in effetti è valido in generale per i grafi di Cayley (si veda, ad esempio, l'esercizio

2.13). Ora, tale azione di G è lineare e lascia gli autospazi invarianti. Infatti, sia $f \in U$ e $g \in G$; allora, per ogni $x \in G$:

$$Af^g(x) = Af(xg^{-1}) = \mu f(xg^{-1}) = \mu f^g(x)$$

e quindi $Af^g = \mu f^g$, ovvero $f^g \in U$.
Pertanto, restringendo l'azione ad U, abbiamo una rappresentazione lineare di $G = PSL(2,q)$ sul $\mathbb{C}$–spazio U. Se tale rappresentazione è banale, allora $f^g = f$ per ogni $f \in U$ e $g \in G$, il che comporta che, per ogni $x \in G$

$$f(x^{-1}) = f(1 \cdot x^{-1}) = f^x(1) = f(1)$$

dunque f è costante, ed allora $\mu = \mu_0 = p+1$ è l'autovalore banale. Quindi se, come nelle ipotesi, μ non è un autovalore banale, la rappresentazione di G sul suo autospazio è non banale. Dunque per il teorema 3.19

$$M(\mu) = \dim U \geq \frac{q-1}{2}$$

che è ciò che volevamo. ∎

Per ogni $m \geq 1$, indichiamo con $s(q,p^m)$ il numero di quadruple $\mathbf{x} = (x_1,x_2,x_3,x_4) \in \mathbb{Z}^4$ tali che

$$\begin{cases} x_0^2 + q^2(x_1^2+x_2^2+x_3^2) = p^m \\ x_0 \text{ ha parità diversa da quella di } x_1,x_2,x_3. \end{cases} \tag{5.16}$$

Ad ogni tale quadrupla $\mathbf{x}$ associamo il quaternione $\underline{\mathbf{x}} = x_0 + (qx_1)i + (qx_2)j + (qx_3)k$. Allora si ha $N(\underline{\mathbf{x}}) = p^m$, e la condizione sulla diversa parità dei coefficienti in (5.16) comporta che $\underline{\mathbf{x}} \in \Lambda'$. Otteniamo quindi un'applicazione iniettiva $\mathbf{x} \mapsto \underline{\mathbf{x}} \in \Lambda'$. Per il Lemma 5.2 l'immagineè di tale applicazione è costituita dagli elementi di Λ' che modulo la relazione definita nella prima parte del capitolo, appartengono al nucleo $\Lambda(q)$ di Π_q; detto per bene

$$s(q,p^m) = \big|\{a \in \Lambda' \mid N(a) = p^m \text{ e } [a] \in \Lambda(q)\}\big| \tag{5.17}$$

Lemma 5.13. *Per ogni $m \geq 1$,*

$$s(q,p^m) = \frac{2}{n} p^{m/2} \sum_{j=0}^{n-1} U_m\Big(\frac{\mu_j}{2\sqrt{p}}\Big).$$

Dimostrazione. Utilizzeremo il fatto che, nelle nostre ipotesi generali, $X_{p,q} \simeq Y_{p,q}$. Sia $\ell \geq 0$, e sia

$$1 = x_0, x_1, \ldots, x_{\ell-1}, x_\ell = 1 \tag{5.18}$$

un percosrso senza inversioni in $Y_{p,q}$ con vertice iniziale e finale 1. Allora, per definizione di grafo di Cayley, per ogni $1 \leq i \leq \ell$, esiste un unico $t_i \in T_{p,q}$ tale che

$$x_i = t_1 t_2 \cdots t_i \tag{5.19}$$

per ogni $1 \leq i \leq \ell$. Ora, per ogni tale indice i, esiste $a_i \in S_p$ per cui $t_i = \Pi_q([a_i])$, e conseguentemente

$$\Pi_q([a_1][a_2]\cdots[a_\ell]) = \Pi_q([a_1])\Pi_q([a_2])\cdots\Pi_q([a_\ell]) = t_1t_2\cdots t_\ell = x_\ell = 1$$

Quindi

$$[a_1][a_2]\cdots[a_\ell] \in \Lambda(q). \tag{5.20}$$

Ora, poiché il percorso (5.18) è senza inversioni, il prodotto $[a_1][a_2]\cdots[a_\ell]$ è ridotto in $\pi(S_p)$. Abbiamo quindi provato che, per ogni $\ell \geq 0$,

$$f_\ell = \text{numero di parole ridotte di lunghezza } \ell \text{ in } \Lambda(q). \tag{5.21}$$

dove f_ℓ è la quantità definita a pag. 92 per il grafo $Y_{p,q} = X_{p,q}$.
Ora sia $a = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda'$ con $[a] \in \Lambda(q)$ (quindi $a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod q$). Se $N(a) = p^m$, allora $a = \pm p^t w_{m-2t}$ dove w_{m-2t} è una parola ridotta in S_p, e quindi $[a] \in \Lambda(q)$ è un prodotto ridotto di lunghezza $m - 2t$. Viceversa, ogni parola ridotta w di lunghezza $m - 2t$ in S_p, produce 2 distinti elementi $a = \pm p^t w$ di λ', tali che $N(a) = p^m$ e $[a] \in \Lambda(q)$. Quindi, fissato $m \geq 1$, per la (5.21) e la (5.17) abbiamo

$$2\sum_{t=0}^{m/2} f_{m-2t} = \big|\{a \in \Lambda' \mid N(a) = p^m \text{ e } [a] \in \Lambda(q)\}\big| = s(q, p^m).$$

Applicando infine la (5.15) si ricava l'identità nell'enunciato del Lemma. ∎

Possiamo ora dimostrare che, fissato $p \geq 5$, al crescere di q la famiglia di grafi $X_{p,q}$ è una famiglia di $(p+1)$-expanders. Ricordando quanto provato al termine del capitolo 2 (Corollario 2.15), è sufficiente provare che esiste un numero reale $\epsilon > 0$ tale che $(p+1) - \mu_1(X_{p,q}) \geq \epsilon$ per ogni q sufficientemente grande.
Questo fatto è una immediata comnseguenza del seguente Teorema, che è quindi il nostro ultimo risultato.

Teorema 5.14. *Sia $p \geq 5$ un numero primo e sia $0 < \epsilon < 1/6$. Allora, per q un numero primo sufficientemente grande, e μ è un autovalore non banale di $X_{p,q}$,*

$$|\mu| \leq p^{\frac{5}{6}+\epsilon} + p^{\frac{1}{6}-\epsilon}.$$

DIMOSTRAZIONE. Fissiamo un primo $p \geq 5$. Come già ricordato, un Teorema di Dirichlet assicura che esistono infiniti (e quindi, arbitrariamente grandi) primi q tali che $q \geq p^8$ e $\left(\frac{p}{q}\right) = 1$. Possiamo quindi assumere di lavorare sempre in questa situazione. Quindi $G = PSL(2,q)$, e $X_{p,q}$ è il grafo di Cayley $\Gamma(G, S_{p,q})$. Sia

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$$

lo spettro degli autovalori di $X_{p,q}$ (dove $n = |G|$). Poiché $X_{p,q}$ è $(p+1)$-regolare e connesso, $p + 1 = \mu_0 > \mu_1$; inoltre, gli autovalori sono tutti reali e

$$|\mu_i| \leq p + 1 \tag{5.22}$$

per ogni $i = 1, \ldots, n-1$. Consideriamo il seguente sottoinsieme di $\mathbb{C}$:

$$\Delta = [i \log \sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + i \log \sqrt{p}]$$

dove $[0, \pi]$ è l'intervallo reale, $[i \log \sqrt{p}, 0] = \{iy \mid 0 \leq y \leq log\sqrt{p}\}$ e, in maniera analoga, $[\pi, \pi + i \log \sqrt{p}] = \{\pi + iy \mid 0 \leq y \leq log\sqrt{p}\}$.
Ricordiamo le definizioni di seno e coseno di numeri complessi:

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}$$

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}$$

Si verifica ora facilmente che la assegnazione

$$\theta \mapsto 2\sqrt{p} \cos \theta \tag{5.23}$$

realizza una biezione (anzi, un omeomorfismo) tra Δ è l'intervallo reale $[-(p+1), p = 1]$. Per la (5.22) esiste quindi, per ogni $0 \leq i \leq n-1$ un $\theta_i \in \Delta$ tale che $\mu_i = 2\sqrt{p} \cos \theta_i$. Ora, in tale biezione, il pezzo reale $[0, \pi]$ di Δ corrisponde (invertendo l'ordinamento) all'intervallo $[-2\sqrt{p}, 2\sqrt{p}]$. Per ogni $0 \leq i \leq n-1$ tale che $\mu_i \notin [-2\sqrt{p}, 2\sqrt{p}]$ definiamo quindi ψ_i nel modo seguente:

$$\begin{cases} \theta_i = i\psi_i & \text{se} \quad 2\sqrt{p} < \mu_i \leq p+1 \\ \theta_i = \pi + i\psi_i & \text{se} \quad -(p+1) \leq \mu_i < -2\sqrt{p} \end{cases} \tag{5.24}$$

Quindi, in ogni caso $0 < \psi_i \leq \log \sqrt{p}$.
Ricordiamo oar le definizioni di seno iperbolico e coseno iperbolico di numeri complessi:

$$\cosh z = \cos(-iz) = \frac{e^z + e^{-z}}{2}$$

$$\sinh z = i \sin(-iz) = \frac{e^z - e^{-z}}{2}.$$

A questo punto, se $m \in \mathbb{N}$ è un numero *pari*, e $\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$, si ha

$$\frac{\sin(m+1)\theta_j}{\sin \theta_j} = \frac{\sin(i(m+1)\psi_j)}{\sin(i\psi_j)} = \frac{\sinh(m+1)\psi_j}{\sinh \psi_j} \geq 0. \tag{5.25}$$

Fissiamo ora un autovalore non-banale μ_k con $\mu_k \notin [-2\sqrt{p}, 2\sqrt{p}]$. Sia $m \in \mathbb{N}$ pari, e sia $s(q, p^m)$ come definito in (5.17). Per il Lemma 5.13 e la definizione dei polinomi di Čebichev abbiamo

$$s(q, p^m) = \frac{2}{n} p^{m/2} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_k}{\sin \theta_k}; \tag{5.26}$$

per cui, denotanto con $M(\mu_k)$ la molteplicità di μ_k,

$$s(q, p^m) = \frac{2}{n} p^{m/2} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} + \frac{2}{n} p^{m/2} \sum_{j \,:\, \mu_j \neq \mu_k} \frac{\sin(m+1)\theta_j}{\sin \theta_j}; \tag{5.27}$$

quindi, applicando l'osservazione (5.25),

$$s(q,p^m) \geq \frac{2}{n}p^{m/2}M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} + \frac{2}{n}p^{m/2}\sum_{j\,:\,|\mu_j|\leq 2\sqrt{p}}\frac{\sin(m+1)\theta_j}{\sin\theta_j}. \tag{5.28}$$

Ora, se $|\mu_j| \leq 2\sqrt{p}$ (cioè $\mu_j \in [-2\sqrt{p}, 2\sqrt{p}]$), θ_j è un numero reale, e, poiché m è pari

$$\left|\frac{\sin(m+1)\theta_j}{\sin\theta_j}\right| \leq m+1.$$

Possiamo quindi riproporre la (5.28) nella forma

$$s(q,p^m) \geq \frac{2}{n}p^{m/2}M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} - 2p^{m/2}(m+1). \tag{5.29}$$

Diamo ora una maggiorazione per $s(q,p^m)$. Si osserva che, siccome m è pari, dalla definizione (5.16) segue che $s(q,p^m)$ è il numero di soluzioni intere di

$$p^m = y_0^2 + 4q^2(y_1^2+y_2^2+y_3^2). \tag{5.30}$$

Diamo una stima di questo numero. Si ha $y_0^2 \equiv p^m \pmod{q^2}$, per cui $y_0 \equiv \pm p^{m/2} \pmod{q^2}$, ed essendo y_0 e q dispari, $y_0 \equiv \pm p^{m/2} \pmod{2q^2}$; siccome poi $|y_0| \leq p^{m/2}$, si conclude che il numero di scelte per y_0 è limitato da

$$1 + \frac{p^{m/2}}{q^2}. \tag{5.31}$$

Per ogni scelta di y_0 in (5.30), il numero di possibilità per la rimanente terna (y_1,y_2,y_3) è ovviamente il numero di soluzioni di $y_1^2+y_2^2+y_3^2 = \frac{p^m-y_0^2}{4q^2}$, ovvero (vedi sezione 4.1) $r_3\left(\frac{p^m-y_0^2}{4q^2}\right)$. Ora, per il Lemma 4.6, fissato $\epsilon > 0$, esiste una costante $C = C(\epsilon)$ tale che

$$r_3\left(\frac{p^m-y_0^2}{4q^2}\right) \leq C\cdot\left(\frac{p^m}{q^2}\right)^{\frac{1}{2}+\epsilon}. \tag{5.32}$$

Combinando questa limitazione con (5.31) si ricava che, per m sufficientemente grande

$$s(q,p^m) \leq C\cdot\frac{p^{m/2+\epsilon m}}{q^{1+2\epsilon}}\left(1+\frac{p^{m/2}}{q^2}\right) \leq C\cdot\left[\frac{p^{m(1+\epsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\epsilon)}}{q}\right]. \tag{5.33}$$

Confrontando con la (5.29) si ottiene

$$\frac{2}{n}p^{m/2}M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} - 2p^{m/2}(m+1) \leq C\cdot\left[\frac{p^{m(1+\epsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\epsilon)}}{q}\right], \tag{5.34}$$

quindi

$$\frac{M(\mu_k)}{n}\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} \leq \frac{C}{2}\left[\frac{p^{m(\frac{1}{2}+\epsilon)}}{q^3} + \frac{p^{m\epsilon}}{q}\right] + (m+1). \tag{5.35}$$

Ora, osservando che $n < q^3$ (si ricordi che $n = |PSL(2,q)|$), si trova (con una costante C_1):

$$M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} \leq C_1 \cdot [q^{3+6\epsilon} + q^{2+6\epsilon}] + q^3(6\log_p q + 1). \tag{5.36}$$

Poiché $\sinh\psi_k \leq sinh(\log\sqrt{p})$, si conclude che

$$M(\mu_k)\sinh(m+1)\psi_k = O\big(q^{3+6\epsilon}\big). \tag{5.37}$$

Scegliendo quindi m il più grande intero pari tale che $p^{m/2} \leq q^3$ (cioè, $m = 2[3\log_p q]$), per q abbastanza grande (e tenendo conto che $\psi_k \leq \log\sqrt{p}$), si ha

$$\sinh(m+1)\psi_k \geq \frac{e^{(m+1)\psi_k}}{3} \geq \frac{e^{(-1+6\log_p q)\psi_k}}{3} \geq \frac{\sqrt{p}}{3}e^{6\psi_k\log_p q},$$

che assieme alla (5.36), dà

$$M(\mu_k) = O\Big(q^{3+6\epsilon-\frac{6\psi_k}{\log p}}\Big). \tag{5.38}$$

Ora, per il Lemma 5.12,

$$M(\mu_k) \geq \frac{q-1}{2}.$$

Da (5.38) si deduce quindi che, per q sufficientemente grande

$$3 + 6\epsilon - \frac{6\psi_k}{\log p} \geq 1,$$

e conseguentemente,

$$\psi_k \leq \Big(\frac{1}{3} + \epsilon\Big)\log p. \tag{5.39}$$

Ricordando che $\mu_k \notin [-2\sqrt{p}, 2\sqrt{p}]$, e quindi che, per (5.24), $\mu_k = 2\sqrt{p}\cos\theta_k$, con $\theta_k = i\psi_k$ oppure $\theta_k = \pi + i\psi_k$, applicando (5.39) otteniamo

$$|\mu_k| = 2\sqrt{p}|\cos\theta_k| = 2\sqrt{p}|\cosh\psi_k| \leq p^{5/6+\epsilon} + p^{1/6-\epsilon}$$

che è quello che volevamo dimostrare (infatti, tale relazione è banalmente soddisfatta per quegli autovalori μ che appartengono all'intervallo $[-2\sqrt{p}, 2\sqrt{p}]$). ∎