UNIVERSITÀ DEGLI STUDI DI PADOVA
Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea Magistrale in Matematica

Sistemi di transitività nei gruppi finiti

Relatore:
Prof. Andrea Lucchini

Candidato:
Veronica Papo
Numero di matricola:
1207415

17 luglio 2020 - Anno Accademico 2019/2020

Introduzione

Dati un gruppo G finitamente generato e un intero $n \geq d(G)$, dove $d(G)$ indica il minimo numero di generatori di G, il gruppo G è immagine epimorfa del gruppo libero F_n di rango n con generatori $x_1, \ldots, x_n$ e di conseguenza l'insieme $\Sigma(G, n)$ dei G-defining subgroup, cioè dei sottogruppi normali N di F_n tali che $F_n/N \simeq G$, è non vuoto.

É possibile definire un'azione del gruppo $Aut(F_n)$ degli automorfismi di F_n sull'insieme $\Sigma(G, n)$ ponendo $N \cdot \sigma = N\sigma$ per ogni $N \in \Sigma(G, n)$, $\sigma \in Aut(F_n)$. Le orbite di questa azione sono i sistemi di transitività, detti anche T_n-system o T-system, di G. Il numero di sistemi di transitività di un gruppo indica quindi in quanti modi il gruppo può essere descritto come quoziente di un gruppo libero, in quanto corrisponde al numero di G-defining subgroup che non possono essere trasformati l'uno nell'altro con un automorfismo di $Aut(F_n)$.

I T_n-system di un gruppo G n-generato possono essere descritti anche in termini di vettori generatori di lunghezza n, cioè di n-uple di elementi di G che generano il gruppo. Sull'insieme di tutti i vettori generatori $V(G, n)$ si può infatti definire un'azione del gruppo $Aut(G)$ degli automorfismi di G, ponendo $(g_1, \ldots, g_n) \cdot \alpha = (g_1\alpha, \ldots, g_n\alpha)$ per ogni $\alpha \in Aut(G)$, $(g_1, \ldots, g_n) \in V(G, n)$. Risulta allora esserci una biezione tra l'insieme $\hat{V}(G, n)$ delle $Aut(G)$-orbite su $V(G, n)$ e l'insieme $\Sigma(G, n)$.

Analogamente, si ottiene un'azione del gruppo $Aut(F_n)$ su $V(G, n)$ ponendo $(g_1, \ldots, g_n) \cdot \sigma = (w_1(g_1, \ldots, g_n), \ldots, w_n(g_1, \ldots, g_n))$, dove per ogni $i = 1, \ldots, n$, $w_i(x_1, \ldots, x_n)$ è una parola del gruppo libero F_n tale che $x_i\sigma^{-1} = w_i(x_1, \ldots, x_n)$. Inoltre, il gruppo $Aut(F_n)$ è generato dai morfismi elementari $P(i, k), \sigma(i), R(i, k), L(i, k)$ che, rispettivamente, hanno l'effetto di scambiare tra loro i generatori x_i, x_k, mandare x_i nel suo inverso ${x_i}^{-1}$, moltiplicare a destra x_i per x_k, moltiplicare a sinistra x_i per x_k. L'azione di ogni automorfismo di F_n su un vettore generatore $g = (g_1, \ldots, g_n)$ sarà allora composizione di un numero finito delle seguenti mosse, dette trasformazioni di Nielsen: scambio di due entrate di g, inversione di un'entrata di g, sostituzione di un'entrata con il suo prodotto a destra o a sinistra con un'altra entrata.

L'azione di $Aut(F_n)$ che viene indotta sull'insieme $\hat{V}(G, n)$ delle $Aut(G)$-orbite è allora equivalente all'azione di $Aut(F_n)$ su $\Sigma(G, n)$ e due vettori

generatori g, h corrispondono a elementi di $\Sigma(G, n)$ appartenenti allo stesso sistema di transitività se e solo se g, h possono essere ottenuti l'uno dall'altro applicando una sequenza finita di automorfismi di G e/o trasformazioni di Nielsen.

Introdotti negli anni '50 dai coniugi Bernhard H. e Hanna Neumann durante i loro studi sulle presentazioni di gruppi, ultimamente i T-system hanno ripreso importanza, anche se in un differente contesto: in questi ultimi anni l'interesse per i sistemi di transitività si è infatti riacceso grazie al loro legame con un algoritmo per la generazione di elementi casuali di un gruppo, l'algoritmo PRA (Product Replacement Algorithm).

L'algoritmo prevede, dato un vettore generatore $g = (g_1, \ldots, g_n)$, di scegliere a caso una coppia (i, j) di entrate distinte, di eseguire con uguale probabilità una delle seguenti *mosse*

$$R^{\pm 1}(i,j) : (g_1, \ldots, g_i, \ldots, g_n) \longrightarrow (g_1, \ldots, g_i g_j^{\pm 1}, \ldots, g_n)$$
$$L^{\pm 1}(i,j) : (g_1, \ldots, g_i, \ldots, g_n) \longrightarrow (g_1, \ldots, g_j^{\pm 1} g_i, \ldots, g_n)$$

e di ripetere questi passaggi un certo numero di volte, applicando questo stesso procedimento al vettore generatore ottenuto nell'iterazione precedente. Scegliendo infine un elemento a caso del vettore generatore ottenuto nell'ultima iterazione si ha un elemento casuale del gruppo. L'algoritmo PRA corrisponde quindi a una passeggiata aleatoria nel grafo $\Gamma_n(G)$ avente come insieme di vertici l'insieme dei vettori generatori e lati corrispondenti alle mosse consentite $R^{\pm 1}(i, j), L^{\pm 1}(i, j)$.

Consideriamo ora il grafo avente come vertici i vettori generatori di G e lati corrispondenti alle trasformazioni di Nielsen e agli automorfismi di G. Il numero $t_n(G)$ di componenti connesse di quest'ultimo grafo coincide allora con il numero di T_n-system di G e può essere usato per stimare il numero $\chi_n(G)$ di componenti connesse del grafo $\Gamma_n(G)$. Si ha infatti $t_n(G) \leq \chi_n(G)$.

In questo lavoro vogliamo raccogliere alcuni dei principali risultati ottenuti sui sistemi di transitività dei gruppi finiti.

Dopo aver introdotto nel capitolo 1, la definizione di sistema di transitività e la caratterizzazione con i vettori generatori, passeremo ad analizzare nel capitolo 2 i sistemi di transitività di alcune classi di gruppi finiti. In particolare vedremo che i gruppi abeliani hanno un unico T_n-system per ogni valore di n ammissibile, mentre al contrario per un gruppo nilpotente il numero di sistemi di transitività può essere arbitrariamente grande, così come per i gruppi semplici non ciclici, il cui numero di T_2-system tende a infinito se l'ordine del gruppo tende a infinito.

Nel terzo capitolo, ci sposteremo invece nel caso dei gruppi profiniti e mostreremo che per questi gruppi esiste un unico sistema di transitività per ogni valore di n.

I risultati qui raccolti sono soltanto una parte di ciò che ad oggi è noto sui sistemi di transitività. Tuttavia la conoscenza sui T-system è ancora

frammentaria e limitata e numerosi sono i problemi aperti e le congetture non ancora risolte.

Indice

Definizioni preliminari: gruppi liberi, generatori,azioni

In questo capitolo richiamiamo le principali definizioni e proposizioni riguardanti gruppi liberi, generatori di gruppi e azioni.

0.1 Generatori e gruppi liberi

Definizione 0.1. Sia G un gruppo, X un sottoinsieme di G. Il *sottogruppo generato da* X, denotato da $\langle X \rangle$ è l'intersezione di tutti i sottogruppi di G che contengono X e corrisponde quindi al più piccolo sottogruppo di G che contiene X. Si può verificare che

$$\langle X \rangle = \{\prod_{i=1}^{n} {g_i}^{m_i} | n \in \mathbb{N}, g_i \in X, m_i \in \mathbb{Z}\}.$$

Un insieme $X \subseteq G$ tale che $\langle X \rangle = G$ è detto un *insieme di generatori* per G. Un gruppo G si dice*finitamente generato* se ammette un insieme finito di generatori.

Un sottoinsieme X di G è quindi un insieme di generatori se e solo se ogni elemento di G può essere scritto come il prodotto di un numero finito di elementi di X. Ogni gruppo G ammette un insieme di generatori, infatti l'insieme costituito da tutti gli elementi di G genera il gruppo. Inoltre in generale, possono esistere più insiemi di generatori. Se G è finitamente generato indicheremo con $d(G)$ la minima cardinalità di un insieme di generatori per G.

In generale, dato un insieme di generatori X, la scrittura degli elementi del gruppo come prodotto di elementi di X non è unica.

Definizione 0.2. Sia G un gruppo. Un insieme $X \subseteq G$ è un *insieme libero di generatori* se è un insieme di generatori e se $\forall n \in \mathbb{N}, m_1, \ldots, m_n \in \mathbb{Z} \setminus 0, x_i \in X$ tali che $x_i \neq x_{i+1}$ si ha che $\prod_{i=1}^{n} {x_i}^{m_i} \neq 1$.

Un *gruppo libero* è un gruppo che ammette un insieme libero di generatori X. La cardinalità di X è detta il *rango* del gruppo.

Si può vedere che X è un insieme libero di generatori di un gruppo se e solo se ogni elemento del gruppo si scrive in maniera unica come prodotto di un numero finito di elementi di X.

Osservazione 0.1. Dato un insieme $X \neq \emptyset$ è possibile costruire un gruppo libero con insieme libero di generatori X. Denoteremo tale gruppo $F^{(X)}$.

Infatti, dato X consideriamo un insieme X^* tale che $|X| = |X^*|$ e una biezione $f : X \longrightarrow X^*$. Per ogni x in X, denotiamo con x^* la sua immagine tramite f. Una parola nell'alfabeto $X \cup X^*$ di lunghezza n è una n-upla $x_1x_2 \dots x_n$ dove gli x_i sono elementi di $X \cup X^*$. L'unica parola di lunghezza zero è la parola vuota. Denotiamo con W_n l'insieme delle parole di lunghezza n. L'insieme $W = \bigcup_{n\geq 0, n\in\mathbb{N}} W_n$ è un monoide, con identità la parola vuota, rispetto all'operazione $\star$ di giustapposizione definita da $(x_1 \dots x_m) \star (y_1 \dots y_n) = x_1 \dots x_m y_1 \dots y_n$.
Consideriamo la congruenza $\sim$ sul monoide W generata dalle relazioni $xx^* \sim 1, x^*x \sim 1$ per ogni $x \in X$. L'insieme $G = W/\sim$ è un gruppo libero generato da X.

In particolare quindi esiste un gruppo libero di rango n per ogni numero naturale $n \geq 1$.

Proposizione 0.1 (Proprietà universale dei gruppi liberi)**.** *Sia F un gruppo libero, sia X un suo insieme libero di generatori e sia $\varepsilon : X \hookrightarrow F$ la mappa di inclusione. Allora per ogni gruppo G e per ogni mappa $f : X \longrightarrow G$ esiste un unico morfismo di gruppi $\tilde{f} : F \longrightarrow G$ che estende f , cioè tale che $xf = x\varepsilon\tilde{f}$ $\forall x \in X$.*

Proposizione 0.2. *Siano F, G due gruppi liberi con insieme di generatori liberi X e Y rispettivamente. Se $|X| = |Y|$ allora $F \simeq G$.*

Proposizione 0.3. *Ogni gruppo è immagine epimorfa di un gruppo libero. Ogni gruppo finitamente generato è immagine epimorfa di un gruppo libero finitamente generato.*

Dimostrazione. Sia G un gruppo e sia X un insieme di generatori. Consideriamo il gruppo libero $F^{(X)}$ generato da X e consideriamo la mappa $f : X \longrightarrow G$ definita da $xf = x$. Allora per la proprietà universale dei gruppi liberi, esiste un unico morfismo $\tilde{f} : F^{(X)} \longrightarrow G$ che estende f. Tale morfismo è suriettivo perché la sua immagine contiene il sottogruppo di G generato da X ed è quindi tutto G.

Se G è finitamente generato è sufficiente prendere come insieme X un insieme finito di generatori. In questo modo il gruppo $F^{(X)}$ è anch'esso finitamente generato. □

0.2 Azioni

Definizione 0.3. Siano G un gruppo e Ω un insieme. Un'*azione* di G su Ω è una mappa

$$\begin{aligned} \Omega \times G &\longrightarrow \Omega \\ (\omega, g) &\longrightarrow \omega \cdot g \end{aligned}$$

tale che :

(i) $\omega \cdot 1 = \omega \ \forall \omega \in \Omega$

(ii) $\omega \cdot (gh) = (\omega \cdot g) \cdot h \ \forall g, h \in G, \omega \in \Omega$.

Per ogni elemento $\omega \in \Omega$ l'*orbita* di ω è l'insieme $O_G(\omega) = \{\omega \cdot g | g \in G\}$.

Se G è un gruppo che agisce su due insiemi T e S e $\varphi : T \longrightarrow S$ è una biezione, diremo che l'azione di G su T è equivalente all'azione di G su S se

$$(t \cdot g)\varphi = (t\varphi) \cdot g \qquad \forall t \in T, g \in G.$$

Capitolo 1

T-system e vettori generatori

In questo capitolo introduciamo i sistemi di transitività (detti brevemente T-system o T_n-system se è specificato il valore di n) di un gruppo, dandone la definizione e una caratterizzazione con i vettori generatori [3].

1.1 Definizione di T-system

I $T_n - system$ di un gruppo n-generato sono definiti come orbite di una particolare azione del gruppo degli automorfismi di un gruppo libero di rango n su un insieme di suoi sottogruppi. Per poter definire i $T_n - system$ dobbiamo prima introdurre il concetto di *G-defining subgroup*.

Nel seguito G denoterà un gruppo, F_n un gruppo libero di rango n.

Definizione 1.1. Un *G-defining subgroup* è un sottogruppo normale N di F_n tale che $G \simeq F_n/N$. Indichiamo con $\Sigma(G, n)$ l'insieme di tutti i *G-defining subgroup* di F_n.

Osservazione 1.1. L'insieme $\Sigma(G, n)$ è non vuoto se e solo se G può essere generato da n elementi.
Infatti, sia $\Sigma(G, n) \neq \emptyset$ e sia $N \trianglelefteq F_n$ tale che $G \simeq F_n/N$. Se $x_1, \ldots, x_n$ sono i generatori di F_n, allora F_n/N è generato dagli elementi $x_1N, \ldots, x_nN$. Quindi anche G è n-generato, in quanto isomorfo a un gruppo n-generato.
Viceversa, ogni gruppo n-generato è immagine epimorfa di un gruppo libero di rango n, quindi $\Sigma(G, n) \neq \emptyset$.

E' possibile definire un'azione del gruppo degli automorfismi $Aut(F_n)$ su $\Sigma(G, n)$ ponendo:

$$\begin{aligned} \Sigma(G,n) \times Aut(F_n) &\longrightarrow \Sigma(G,n) \\ (N, \sigma) &\longrightarrow N\sigma. \end{aligned} \tag{1.1}$$

L'azione è ben definita perché:

- se $N \in \Sigma(G,n)$ e $\sigma \in Aut(F_n)$ si ha che $N\sigma \in \Sigma(G,n)$.
  Infatti $F_n/N\sigma \simeq F_n/N$ tramite l'isomorfismo

$$\begin{aligned} \theta : F_n/N &\longrightarrow F_n/N\sigma \\ xN &\longrightarrow (x\sigma)N\sigma \end{aligned} \tag{1.2}$$

- $N \cdot id = N \ \forall N \in \Sigma(G,n)$
- $(N\sigma)\cdot\rho = N\cdot(\sigma\rho) \ \forall N \in \Sigma(G,n) \ \forall \sigma,\rho \in Aut(F_n)$.

Possiamo ora dare la definizione di sistema di transitività.

Definizione 1.2. I *sistemi di transitività*, detti anche T_n*-system* o T*-system*, di G sono le orbite dell'azione di $Aut(F_n)$ su $\Sigma(G,n)$ definita da

$$\begin{aligned} \Sigma(G,n) \times Aut(F_n) &\longrightarrow \Sigma(G,n) \\ (N,\sigma) &\longrightarrow N\sigma. \end{aligned}$$

Per quanto visto nell'osservazione 1.1 i T_n-system di un gruppo G sono non vuoti per $n \geq d(G)$.

1.2 Un'azione equivalente

L'azione di $Aut(F_n)$ su $\Sigma(G,n)$ risulta poco pratica da utilizzare per studiare i T_n*-system* di uno specifico gruppo. In questo paragrafo introdurremo un'azione, definita da B.H. Neumann e H. Neumann, che è equivalente a quella data nella definizione di sistema di transitività ma più maneggevole, in quanto lavora, anziché sull'insieme $\Sigma(G,n)$, sull'insieme dei vettori generatori.

Definizione 1.3. Sia G un gruppo. Un *vettore generatore di* G di lunghezza n è una n-upla ordinata $(g_1,\dots,g_n)$ tale che $\langle g_1,\dots,g_n\rangle = G$. L'insieme di tutti i vettori generatori di G di lunghezza n viene indicato con $V(G,n)$.

Fissiamo un insieme libero di generatori $x_1,\dots,x_n$ di F_n e sia $E = \{f : F_n \to G |$ f epimorfismo$\}$ l'insieme degli epimorfismi da F_n a G. Possiamo definire un'azione di $Aut(F_n)\times Aut(G)$ su E ponendo

$$\begin{aligned} E \times (Aut(F_n)\times Aut(G)) &\longrightarrow E \\ (\rho,(\sigma,\alpha)) &\longrightarrow \sigma^{-1}\rho\alpha. \end{aligned} \tag{1.3}$$

Identifichiamo $Aut(F_n)$ e $Aut(G)$ con le loro copie in $Aut(F_n)\times Aut(G)$. Vale il seguente:

Lemma 1.1. *Siano* $\rho_1,\rho_2 \in E$. *Allora* ρ_1,ρ_2 *appartengono alla stessa* $Aut(G)$ *orbita, i.e.* $\exists\alpha \in Aut(G)$ *tale che* $\rho_1 = \rho_2\alpha$, *se e solo se* $ker(\rho_1) = ker(\rho_2)$.

Dimostrazione. "⇒" Siano $\rho_1, \rho_2 \in E$ tali che $\rho_1 = \rho_2\alpha$ per qualche $\alpha \in Aut(G)$. Allora

$$ker(\rho_1) = ker(\rho_2\alpha) = \{x \in F_n | x\rho_2 \in \ker(\alpha)\} = \{x \in F_n | x\rho_2 = 1\} = ker(\rho_2).$$

"⇐" Siano $\rho_1, \rho_2 \in E$ tali che $ker(\rho_1) = ker(\rho_2)$. Poniamo $\forall g \in G\ g\alpha = x_g\rho_1$ dove x_g è un elemento dell'antimmagine tramite ρ_2 di g, cioè $x_g \in F_n$ tale che $x_g\rho_2 = g$.
Allora α è un automorfismo di G e $\rho_1 = \rho_2\alpha$. Infatti,

- α ben definito: siano $x, x' \in F_n$ tali che $x\rho_2 = x'\rho_2 = g$. Allora $x^{-1}x' \in ker(\rho_2) = ker(\rho_1)$, quindi da $(x^{-1}x')\rho_1 = 1$ segue $x'\rho_1 = x\rho_1 = g\alpha$.
- α morfismo: siano $g, h \in G$ proviamo che $(gh)\alpha$=$(g\alpha)(h\alpha)$, cioè che $x_{gh}\rho_1 = (x_g\rho_1)(x_h\rho_1)$.

  Si ha che $x_{gh}\rho_2 = gh$ e $(x_gx_h\rho_2) = (x_g\rho_2)(x_h\rho_2) = gh$, quindi x_{gh} e x_gx_h sono due elementi dell'antimmagine di gh tramite ρ_2 che possono essere utilizzati per determinare l'immagine di gh tramite α. Dato che α è ben definito vale $(gh)\alpha = x_{gh}\rho_1 = (x_gx_h)\rho_1 = (x_g\rho_1)(x_h\rho_1) = (g\alpha)(h\alpha)$.
- α iniettivo: sia $g \in ker(\alpha)$. Da $1 = g\alpha = x_g\rho_1$ si ha $x_g \in ker(\rho_1) = ker(\rho_2)$, quindi $g = x_g\rho_2 = 1$.
- α suriettiva: sia $g \in G$ allora per la suriettività di ρ_1 $\exists x \in F_n$ tale che $x\rho_1 = g$. Poniamo $h = x\rho_2$ allora si ha che $h\alpha = x\rho_1 = g$.
- infine dalla definizione di α segue immediatamente che $\rho_1 = \rho_2\alpha$.

□

Grazie a questo lemma, è possibile stabilire una corrispondenza biunivoca tra l'insieme $\hat{E}$ delle $Aut(G)$ orbite di E e $\Sigma(G, n)$.

Lemma 1.2. *La mappa $\Lambda : \hat{E} \longrightarrow \Sigma(G, n)$ definita da $\hat{\rho}\Lambda = ker(\rho)$ dove $\hat{\rho}$ indica l'orbita in $\hat{E}$ contenente ρ, è una biezione.*

Dimostrazione. La mappa Λ è ben definita, perché per il lemma 1.1 si ha che se due epimorfismi ρ, ρ' appartengono alla stessa $Aut(G)$ orbita allora hanno lo stesso nucleo quindi l'immagine di $\hat{\rho}$ non dipende dal rappresentante di $\hat{\rho}$ scelto. Inoltre per i teoremi di omomorfismo $F_n/ker(\rho) \simeq G$ quindi $ker(\rho) \in \Sigma(G, n)$.
L'iniettività di Λ segue sempre dal lemma 1.1, mentre la suriettività è garantita dalla definizione di G-defining subgroup. Infatti se $N \in \Sigma(G, n)$ allora esiste un isomorfismo $\bar{\rho} : F_n/N \longrightarrow G$. Definiamo per ogni $x \in F_n$ $x\rho = (xN)\bar{\rho}$. In questo modo otteniamo un epimorfismo $\rho : F_n \longrightarrow G$ tale che $\ker(\rho) = N$. Infatti ρ è un morfismo perché per ogni $x, x' \in F_n$ si ha

che $(xx')\rho = (xx'N)\bar{\rho} = (xN\bar{\rho})(x'N\bar{\rho}) = (x\rho)(x'\rho)$ ed è suriettivo perché per ogni $g \in G$ per la suriettività di $\bar{\rho}$ esiste un elemento $x \in F_n$ tale che $g = (xN)\bar{\rho} = x\rho$. Infine $ker(\rho) = \{\, x \in F_n \mid (xN)\bar{\rho} = 1 \,\} = N$. □

Osservazione 1.2. L'azione di $Aut(F_n)$ su E induce un'azione di $Aut(F_n)$ su $\hat{E}$ definita da $\hat{\rho} \cdot \sigma = \widehat{\sigma^{-1}\rho}$.

Infatti l'azione è ben definita perché se $\rho, \rho' \in \hat{\rho}$ allora $\exists \alpha \in Aut(G)$ tale che $\rho' = \rho\alpha$. Perciò se $\sigma \in Aut(F_n)$ si ha $\rho' \cdot \sigma = \sigma^{-1}\rho' = \sigma^{-1}(\rho\alpha) = (\sigma^{-1}\rho)\alpha = (\rho \cdot \sigma)\alpha$ e quindi $\rho' \cdot \sigma$ e $\rho \cdot \sigma$ appartengono alla stessa $Aut(G)$ orbita.

Proposizione 1.1. *L'azione di $Aut(F_n)$ su $\hat{E}$ è equivalente all'azione di $Aut(F_n)$ su $\Sigma(G, n)$.*

Dimostrazione. Sia Λ la biezione del lemma 1.2, $\sigma \in Aut(F_n), \hat{\rho} \in \hat{E}$. Dobbiamo verificare che $(\hat{\rho} \cdot \sigma)\Lambda = (\hat{\rho}\Lambda) \cdot \sigma$.

Se $ker(\rho) = N$ si ha $(\hat{\rho} \cdot \sigma)\Lambda = ker(\sigma^{-1}\rho) = \{x \in F_n | x\sigma^{-1} \in N\} = N\sigma = (\hat{\rho}\Lambda) \cdot \sigma$. □

Abbiamo così definito un'azione di $Aut(F_n)$ su $\hat{E}$ equivalente a quella della definizione 1.2. Il prossimo passo sarà costruire una biezione tra gli insiemi E e $V(G, n)$ che ci permetta di trasferire l'azione di $Aut(F_n) \times Aut(G)$ su E a un'azione su $V(G, n)$, da cui poi ricaveremo un'azione di $Aut(F_n)$ su $V(G, n)$ equivalente all'azione (1.1).

Lemma 1.3. *La mappa $\pi : E \longrightarrow V(G, n)$ data da $\rho\pi = (x_1\rho, \ldots, x_n\rho)$ è una biezione. Inoltre π ci permette di trasferire l'azione di $Aut(F_n) \times Aut(G)$ su E a un'azione su $V(G, n)$ data da*

$$\begin{aligned} V(G, n) \times (Aut(F_n) \times Aut(G)) &\longrightarrow V(G, n) \\ (\rho\pi, (\sigma, \alpha)) &\longrightarrow \sigma^{-1}\rho\alpha\pi. \end{aligned} \tag{1.4}$$

Dimostrazione. La mappa π è ben definita perché se $\rho \in E$ si ha che $\langle x_1\rho, \ldots, x_n\rho \rangle = Im(\rho) = G$. Inoltre la mappa è iniettiva e suriettiva perché per la proprietà universale dei gruppi liberi per ogni vettore generatore $g = (g_1, \ldots, g_n)$ esiste un unico morfismo di gruppi $\rho : F_n \longrightarrow G$ tale che $x_i\rho = g_i \ \forall i = 1, \ldots, n$ e tale morfismo è suriettivo perché la sua immagine contiene i generatori g_i. Il fatto che (1.4) sia un'azione segue immediatamente dalla corrispondente azione di $Aut(F_n) \times Aut(G)$ su E. □

L'azione (1.4) di $Aut(F_n) \times Aut(G)$ su $V(G, n)$ è equivalente all'azione di $Aut(F_n) \times Aut(G)$ su E per come è definita. Inoltre l'azione di $Aut(F_n)$ sulle $Aut(G)$ orbite di $V(G, n)$ è equivalente alla sua azione sulle $Aut(G)$ orbite di E. Infine, considerando la proposizione 1.1 si ottiene

Proposizione 1.2. *L'azione di $Aut(F_n)$ su $\Sigma(G, n)$ è equivalente all'azione di $Aut(F_n)$ sull'insieme $\hat{V}(G, n)$ delle $Aut(G)$ orbite di $V(G, n)$.*

Dimostrazione. La mappa $\eta = \Lambda^{-1}\pi$, dove Λ è la biezione della proposizione 1.2 e π è la biezione tra gli insiemi $\hat{E}$ e $\hat{V}(G,n)$ indotta dalla mappa del lemma 1.3, è una biezione tra $\Sigma(G,n)$ e $\hat{V}(G,n)$. Dobbiamo verificare che per ogni $N \in \Sigma(G,n)$, $\sigma \in Aut(F_n)$ si ha $(N \cdot \sigma)\eta = (N\eta) \cdot \sigma$.

Si ha che $(N \cdot \sigma)\eta = (N \cdot \sigma)(\Lambda^{-1}\pi) = ((N \cdot \sigma)\Lambda^{-1})\pi$. Per la proposizione 1.1 si ha che l'azione di $Aut(F_n)$ su $\Sigma(G,n)$ è equivalente all'azione di $Aut(F_n)$ su E, quindi vale $((N\cdot\sigma)\Lambda^{-1})\pi = ((N\Lambda^{-1})\cdot\sigma)\pi = (\sigma^{-1}(N\Lambda^{-1}))\pi = (N\Lambda^{-1}\pi)\cdot\sigma = (N\eta)\cdot\sigma$. □

Consideriamo ora le azioni di$Aut(G)$ e $Aut(F_n)$ su $V(G,n)$ indotte dall'azione (1.4). Anche in questo caso identifichiamo $Aut(F_n)$ e $Aut(G)$ con le loro copie in $Aut(F_n) \times Aut(G)$.
Sia $g = (g_1, \ldots, g_n) \in V(G,n)$. Per il lemma 1.3 $\exists \rho \in E$ tale che $g = \rho\pi = (x_1\rho, \ldots, x_n\rho)$.

Azione di $Aut(G)$ su $V(G,n)$

Usando la formula (1.4) possiamo determinare esplicitamente l'azione di α $\forall \alpha \in Aut(G)$:

$$g\alpha = \rho\pi(id, \alpha) = \rho\alpha\pi = (x_1\rho\alpha, \ldots, x_n\rho\alpha) = (g_1\alpha, \ldots, g_n\alpha). \tag{1.5}$$

Possiamo quindi concludere:

Proposizione 1.3. *L'azione di $Aut(G)$ su $V(G,n)$ è data da*

$$(g_1, \ldots, g_n)\alpha = (g_1\alpha, \ldots, g_n\alpha) \tag{1.6}$$

$\forall (g_1, \ldots, g_n) \in V(G,n), \alpha \in Aut(G)$.

Azione di $Aut(F_n)$ su $V(G,n)$

Sia $\sigma \in Aut(F_n)$. Dalla formula (1.4) si ha :

$$g\sigma = \rho\pi(\sigma, id) = \sigma^{-1}\rho\pi = (x_1\sigma^{-1}\rho, \ldots, x_n\sigma^{-1}\rho). \tag{1.7}$$

Supponiamo che

$$\begin{aligned} x_1\sigma^{-1} &= w_1(x_1, \ldots, x_n) \\ &\vdots \\ x_n\sigma^{-1} &= w_n(x_1, \ldots, x_n). \end{aligned} \tag{1.8}$$

Allora sostituendo questi valori in (1.7), otteniamo:

$$(x_1\sigma^{-1}\rho, \ldots, x_n\sigma^{-1}\rho) = (w_1\rho, \ldots, w_n\rho) = (w_1(g_1, \ldots, g_n), \ldots, w_n(g_1, \ldots, g_n)).$$

Perciò vale:

Proposizione 1.4. *L'azione di $Aut(F_n)$ su $V(G,n)$ è data da*

$$(g_1,\dots,g_n)\sigma = (w_1(g_1,\dots,g_n),\dots,w_n(g_1,\dots,g_n)) \tag{1.9}$$

dove $(g_1,\dots,g_n) \in V(G,n), \sigma \in Aut(F_n)$ e $x_i\sigma^{-1} = w_i(x_1,\dots,x_n)$ per ogni $i = 1,\dots,n$

Possiamo descrivere in maniera ancora più esplicita l'azione di $Aut(F_n)$ su $V(G,n)$ considerando i generatori di $Aut(F_n)$.

Definizione 1.4. Sia $n \geq 2, n \in \mathbb{N}$. I *morfismi elementari* di $Aut(F_n)$ sono gli automorfismi

$$\begin{aligned} P(i,k) &: x_i \longrightarrow x_k, x_k \longrightarrow x_i \\ \sigma(i) &: x_i \longrightarrow x_i^{-1} \\ R(i,k) &: x_i \longrightarrow x_i x_k \\ L(i,k) &: x_i \longrightarrow x_k x_i \end{aligned}$$

dove $1 \leq i,k \leq n$, $i \neq k$ e i generatori non menzionati sono fissati dall'automorfismo.

Proposizione 1.5. *Per $n \geq 2$ $Aut(F_n)$ è generato dai suoi automorfismi elementari.*

I quattro morfismi elementari di $Aut(F_n)$ (con $n \geq 2$) danno vita ad altrettante operazioni elementari sui vettori generatori, dette *trasformazioni di Nielsen.*

Definizione 1.5. Le *trasformazioni di Nielsen* sono le quattro trasformazioni di $V(G,n)$ con $n \geq 2$ definite da:

(i) scambio di due entrate:
$(g_1,\dots,g_i,\dots,g_k,\dots,g_n) \longrightarrow (g_1,\dots,g_i,\dots,g_k,\dots,g_n)$

(ii) inversione di un'entrata:
$(g_1,\dots,g_i,\dots,g_n) \longrightarrow (g_1,\dots,g_i^{-1},\dots,g_n)$

(iii) moltiplicazione a destra di un'entrata per un'altra:
$(g_1,\dots,g_i,\dots,g_k,\dots,g_n) \longrightarrow (g_1,\dots,g_ig_k,\dots,g_k,\dots,g_n)$

(iv) moltiplicazione a sinistra di un'entrata per un'altra:
$(g_1,\dots,g_i,\dots,g_k,\dots,g_n) \longrightarrow (g_1,\dots,g_kg_i,\dots,g_k,\dots,g_n)$.

Ognuna delle quattro trasformazioni di Nielsen corrisponde all'azione su $V(G,n)$ di uno dei quattro automorfismi elementari, per questo talvolta useremo le notazioni $P(i,k), \sigma(i), L(i,k), R(i,k)$ anche per indicare le trasformazioni di Nielsen.

Proposizione 1.6. *Sia $n \geq 2$. Due elementi di $V(G,n)$ appartengono alla stessa $Aut(F_n)$ orbita se e solo se possono essere trasformati l'uno nell'altro applicando una sequenza finita di trasformazioni di Nielsen.*

Dimostrazione. Due vettori generatori g, g' appartengono alla stessa $Aut(F_n)$ orbita se e solo se esiste un automorfismo $\omega \in Aut(F_n)$ tale che $g' = g \cdot \omega$. Ogni automorfismo di F_n è composizione di un numero finito di automorfismi elementari , quindi $\omega = \omega_1\omega_2 \dots \omega_k$ con ω_i morfismo elementare $\forall i = 1, \dots, k$, $k \in \mathbb{N}$.

Perciò $g' = g \cdot \omega = g \cdot (\omega_1\omega_2 \dots \omega_k) = (g \cdot \omega_1) \cdot (\omega_2 \dots \omega_k)$ che corrisponde ad applicare un numero finito di trasformazioni di Nielsen. □

Abbiamo visto finora che esiste una corrispondenza biettiva tra l'insieme $\Sigma(G,n)$ e l'insieme $\hat{V}(G,n)$ delle $Aut(G)$ orbite di $V(G,n)$ e inoltre l'azione di $Aut(F_n)$ su questi due insiemi è equivalente. Nello studio dei T_n-*system* con $n \geq 2$ di un gruppo G possiamo quindi considerare le azioni di $Aut(G)$ e $Aut(F_n)$ su $V(G,n)$ definite nelle proposizioni 1.3 e 1.4.

Due vettori generatori g, g'

- corrispondono allo stesso elemento di $\Sigma(G,n)$ se e solo possono essere ottenuti l'uno dall'altro applicando l'azione di un automorfismo di G
- corrispondono a elementi di $\Sigma(G,n)$ appartenenti allo stesso T_n-*system* se e solo se g e g' possono essere ottenuti l'uno dall'altro applicando un numero finito di trasformazioni di Nielsen e/o l'azione di un numero finito di automorfismi di G.

  In tal caso diremo che g e g' sono equivalenti e scriveremo $g \sim g'$.

Nel caso invece $n = 1$, cioè nel caso in cui G è un gruppo ciclico, proveremo nel prossimo capitolo che G ha un unico T-system.

Capitolo 2

T-system di alcune classi di gruppi finiti

2.1 T-system di gruppi abeliani finiti

In questa sezione dimostreremo che ogni gruppo abeliano finito G ha un unico $T_n - system$ per ogni $n \geq d(G), n \in \mathbb{N}$.

Inizieremo presentando alcuni lemmi che saranno poi usati per dimostrare il teorema principale.

Remark 2.1. Nella definizione 1.5 abbiamo definito le trasformazioni di Nielsen come funzioni che agiscono sull'insieme dei vettori generatori. Più in generale, dato $n \in \mathbb{N}$ le trasformazioni di Nielsen possono essere applicate a una qualunque n-upla di elementi di G, diventando in questo modo funzioni da G^n in G^n.

Se G è un gruppo abeliano additivo la trasformazione $\sigma(i)$ sostituisce l'entrata i-esima g_i di una n-upla di elementi di G con $-g_i$, le trasformazioni $R(i,k)$ e $L(i,k)$ hanno invece lo stesso effetto di sostituire l'entrata i-esima con la sua somma con l'entrata k-esima.

Remark 2.2. Dati $a, b \in \mathbb{Z}$ con $a \neq 0$ possiamo determinare il loro m.c.d in un numero finito di passi con l'algoritmo di Euclide:
poniamo $a = r_0, b = r_{-1}$ ed eseguiamo partendo da $i = 0$ le divisioni intere $r_{i-1} \div r_i$, ottenendo la successione $r_{i-1} = q_{i+1}r_i + r_{i+1}$. La successione termina quando otteniamo resto nullo.

Se la successione termina al passo n (quindi $r_{n+1} = 0$), l'ultimo resto non nullo r_n è il m.c.d. tra a e b.

Il massimo comun divisore di due numeri entrambi nulli è invece 0.

Consideriamo ora il gruppo abeliano additivo $(\mathbb{Z}, +)$.

Lemma 2.1. *Siano $a, b \in \mathbb{Z}$ e sia $d = m.c.d(a,b)$. Allora esiste una sequenza finita di trasformazioni di Nielsen che trasforma (a,b) in $(d,0)$.*

Dimostrazione. Sia $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. Se $a = 0$ allora $m.c.d(a,b) = b$. Scambiando tra loro le due entrate si ottiene $(b,0) = (d,0)$ e la tesi è verificata.

Supponiamo allora $a \neq 0$. Possiamo determinare d usando l'algoritmo di Euclide. Poniamo $a = r_0, b = r_{-1}$ e sia n tale che $r_{n+1} = 0$ e $r_n = d$.

Riscriviamo (a,b) come $(r_0, q_1 r_0 + r_1)$ e applichiamo questa sequenza di trasformazioni di Nielsen: sostituiamo la prima entrata con il suo inverso, sommiamo per q_1 volte la prima entrata alla seconda, sostituiamo la prima entrata con il suo inverso:

$$\begin{aligned}(r_0, q_1 r_0 + r_1) &\xrightarrow{\sigma(1)} (-r_0, q_1 r_0 + r_1) \xrightarrow{L(2,1)^{q_1}} (-r_0, -q_1 r_0 + q_1 r_0 + r_1) \\ &= (-r_0, r_1) \xrightarrow{\sigma(1)} (r_0, r_1).\end{aligned}$$

Abbiamo così trasformato (a,b) in (r_0, r_1) attraverso la sequenza finita di trasformazioni di Nielsen $\theta_1 = \sigma(1)L(2,1)^{q_1}\sigma(1)$.

Se $n = 1$ allora $(r_0, r_1) = (d, 0)$ e la tesi è verificata.

Altrimenti, per ogni $i = 2, \ldots, n$ applichiamo al vettore (r_{i-2}, r_{i-1}) ottenuto al passo precedente, la sequenza θ_i di trasformazioni di Nielsen data da $P(1,2)\sigma(1)L(2,1)^{q_i}\sigma(1)$.
In questo modo, otteniamo:

$$\begin{aligned}(r_{i-2}, r_{i-1}) &\xrightarrow{P(1,2)} (r_{i-1}, r_{i-2}) \xrightarrow{\sigma(1)} (-r_{i-1}, r_{i-2}) = \\ (-r_{i-1}, q_i r_{i-1} + r_i) &\xrightarrow{L(2,1)^{q_i}} (-r_{i-1}, -q_i r_{i-1} + q_i r_{i-1} + r_i) = \\ &= (-r_{i-1}, r_i) \xrightarrow{\sigma(-1)} (r_{i-1}, r_i).\end{aligned}$$

Al passo n si otterrà $(r_{n-1}, r_n) = (d, 0)$ e dunque la sequenza $\theta_1 \ldots \theta_n$ trasforma il vettore (a,b) in $(d,0)$. □

Lemma 2.2. *Siano $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e sia $d = m.c.d.(a_1, \ldots, a_n)$. Allora esiste una sequenza finita di trasformazioni di Nielsen che trasforma $(a_1, \ldots, a_n)$ in $(d, 0, \ldots, 0)$.*

Dimostrazione. Sia $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Consideriamo le ultime due entrate a_{n-1}, a_n e poniamo $d_{n-1} = m.c.d(a_{n-1}, a_n)$. Per il lemma 2.1 possiamo trasformare (a_{n-1}, a_n) in $(d_n, 0)$ con una sequenza finita di trasformazioni di Nielsen, quindi esiste una sequenza finita θ_1 di trasformazioni di Nielsen che agisce solamente sulle ultime due entrate tale che

$$(a_1, \ldots, a_{n-1}, a_n) \xrightarrow{\theta_1} (a_1, \ldots, a_{n-2}, d_{n-1}, 0).$$

Per ogni $i = 2, \ldots, n-1$ definiamo $d_{n-i} = m.c.d(a_{n-i}, d_{n-i+1})$ e applichiamo il precedente ragionamento al vettore ottenuto nell'ultima iterazione: al passo i trasformiamo la coppia (a_{n-i}, d_{n-i+1}) di entrate di posto i e $i+1$ rispettivamente, nella coppia $(d_{n-i}, 0)$.

In questo modo all'iterazione i si avrà

$$(a_1, \ldots, a_{n-i-1}, a_{n-i}, d_{n-i+1}, 0, \ldots, 0) \xrightarrow{\theta_i} (a_1, \ldots, a_{n-i-1}, d_{n-i}, 0, \ldots, 0).$$

Dato che $d_1 = m.c.d.(a_1, d_2) = m.c.d.(a_1, \ldots, a_n) = d$, al passo $n-1$ avremo trasformato con una sequenza finita di trasformazioni di Nielsen il vettore $(a_1, \ldots, a_n)$ in $(d, 0, \ldots, 0)$. □

Lemma 2.3. *Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n. Ogni sequenza di generatori $(g^{\omega_1}, \ldots, g^{\omega_m})$ è equivalente al vettore generatore di lunghezza m $(g, 1, \ldots, 1)$.*

Dimostrazione. Sia $(g^{\omega_1}, \ldots, g^{\omega_m})$ un vettore generatore. Per il lemma 2.2 la m-upla degli esponenti $(\omega_1, \ldots, \omega_m) \in \mathbb{Z}^m$ può essere trasformata in $(d, 0, \ldots, 0)$ con una sequenza finita λ di trasformazioni di Nielsen di $(\mathbb{Z}, +)$, dove $d = m.c.d.(\omega_1, \ldots, \omega_m)$.

Osserviamo che sommare gli esponenti ω_i e ω_k corrisponde a moltiplicare g^{ω_i} e g^{ω_k}, sostituire l'esponente ω_i con il suo opposto corrisponde a sostituire g^{ω_i} con il suo inverso.

Applicando quindi al vettore $(g^{\omega_1}, \ldots, g^{\omega_m})$ la sequenza λ vista come sequenza di trasformazioni di Nielsen di $(G, \cdot)$ si ottiene il vettore generatore $(g^d, 1, \ldots, 1)$. Infine essendo g^d un generatore di G, esiste un automorfismo $\beta : g^d \longrightarrow g$ e quindi $(g^d, 1, \ldots, 1)\beta = (g, 1, \ldots, 1)$. □

Ricordiamo che per i gruppi abeliani finiti vale il seguente teorema di struttura:

Teorema 2.1. *Sia G un gruppo abeliano finito, $d = d(G)$.*

Allora $G = C_1 \times C_2 \times \cdots \times C_d$ dove i C_i sono gruppi ciclici di ordine n_i tali che $n_{i+1} \mid n_i$ per ogni $i \in \{1, \ldots, d-1\}$. Inoltre tale decomposizione è unica.

Possiamo finalmente dimostrare il seguente:

Teorema 2.2. *Sia G un gruppo abeliano finito. Allora G ha un unico $T_n - system$ per ogni $n \geq d(G)$.*

Dimostrazione. Sia G un gruppo abeliano finito. Per il teorema 2.1 possiamo decomporre G come $G = \langle g_1 \rangle \times \cdots \times \langle g_d \rangle$ con $|g_i| = n_i$ e $n_{i+1} \mid n_i$ per ogni $i \in \{1, \ldots, d-1\}, d = d(G)$.

Per provare che esiste un unico $T_n - system$ è sufficiente verificare che tutti i vettori generatori siano equivalenti a uno stesso vettore.

Sia $(h_1, \ldots, h_n) \in V(G, n)$ con $n \geq d(G)$. Vogliamo provare che

$$(h_1, \ldots, h_n) \sim (g_1, \ldots, g_d, 1, \ldots, 1).$$

Procediamo per induzione su d.

Se $d = 1$ allora G è un gruppo ciclico e quindi la tesi vale grazie al lemma 2.3.
Se $d \geq 1$, poniamo $R = \langle g_1 \rangle \times \cdots \times \langle g_{d-1} \rangle$ e $M = \langle g_d \rangle$.

In questo modo $G = R \times M$ e quindi per ogni $i = 1, \ldots, n$ si ha che $h_i = r_i m_i$ per qualche $r_i \in R, m_i \in M$.

Inoltre gli elementi $r_1, \ldots, r_n$ generano R, perché per ogni $j = 1, \ldots, d-1$ vale

$$g_j = \prod_{i=1}^{n} h_i^{\alpha_{i,j}} = \prod_{i=1}^{n} (r_i m_i)^{\alpha_{i,j}} = \prod_{i=1}^{n} r_i^{\alpha_{i,j}} \prod_{i=1}^{n} m_i^{\alpha_{i,j}}$$

con $\alpha_{i,j} \in \mathbb{Z}$, quindi identificando R e M con le loro copie in G

$$g_j \prod_{i=1}^{n} r_i^{-\alpha_{i,j}} = \prod_{i=1}^{n} m_i^{\alpha_{i,j}} \in R \cap M = 1$$

da cui si ottiene

$$g_j = \prod_{i=1}^{n} r_i^{\alpha_{i,j}}.$$

Essendo $d(R) = d - 1 < d$ e R abeliano, per ipotesi induttiva esiste una sequenza finita λ di trasformazioni di Nielsen e automorfismi di R tale che

$$(r_1, \ldots, r_n) \xrightarrow{\lambda} (g_1, \ldots, g_{d-1}, 1, \ldots, 1).$$

Ogni automorfismo di R può essere esteso a un automorfismo di G che fissa g_d, perciò, sostituendo nella sequenza λ gli automorfismi di R con la loro estensione ad automorfismi di G, si ottiene una sequenza finita λ' di trasformazioni di Nielsen e automorfismi di G tale che

$$(h_1, \ldots, h_n) = (r_1 m_1, \ldots, r_n m_n) \xrightarrow{\lambda'} (g_1 v_1, \ldots, g_{d-1} v_{d-1}, v_d, \ldots, v_n)$$

dove $v_1, \ldots, v_n$ sono opportuni elementi di M.

Osserviamo ora che ponendo

$$g_i \beta = g_i v_i \quad \forall i = 1, \ldots, d-1, \qquad g_d \beta = g_d$$

si ottiene un automorfismo β di G. Infatti,

- β è ben definito perché per ogni $i = 1, \ldots, d-1$ si ha

$$g_i^{n_i} = 1 \quad \text{e} \quad g_i^{n_i} \beta = (g_i v_i)^{n_i} = g_i^{n_i} v_i^{n_i} = 1 = 1\beta$$

dato che $n_i = |g_i|$ e $v_i \in M = \langle g_d \rangle$ e $n_d | n_i$. Inoltre

$$g_d{}^{n_d} = 1 \quad \text{e} \quad g_d{}^{n_d} \beta = g_d{}^{n_d} = 1 = 1\beta.$$

- β é iniettivo perché se $g = {g_1}^{\alpha_1} \dots {g_d}^{\alpha_d} \in ker(\beta)$ allora

$$\begin{aligned} 1 = g\beta = ({g_1}^{\alpha_1} \dots {g_d}^{\alpha_d})\beta &= {g_1}^{\alpha_1} \dots {g_d}^{\alpha_d} {v_1}^{\alpha_1} \dots {v_{d-1}}^{\alpha_{d-1}} \\ &= g{v_1}^{\alpha_1} \dots {v_{d-1}}^{\alpha_{d-1}}. \end{aligned}$$

  Allora $g = {v_1}^{-\alpha_1} \dots {v_{d-1}}^{-\alpha_{d-1}}$ implica che $g \in M \cap ker(\beta)$ perciò g è fissato da β e quindi $1 = g\beta = g$ e β è iniettivo.

Infine, dato che G è un gruppo finito β è anche suriettivo ed è quindi un automorfismo.

Definiamo $\gamma = \beta^{-1}$. Si ha

$$(g_1 v_1, \dots, g_{d-1} v_{d-1}, v_d, \dots, v_n) \xrightarrow{\gamma} (g_1, \dots, g_{d-1}, v_d, \dots, v_n).$$

Dato che $\langle g_1, \dots, g_{d-1}, v_d, \dots, v_n \rangle = G$ si deve avere $\langle v_d, \dots, v_n \rangle = M$.

Infine, essendo M un gruppo ciclico, per il lemma 2.3 è possibile trasformare con trasformazioni di Nielsen $(v_d, \dots, v_n)$ in $(g_d, 1, \dots, 1)$. Quindi esiste una sequenza finta θ di trasformazioni di Nielsen tale che

$$(g_1, \dots, g_{d-1}, v_d, \dots, v_n) \xrightarrow{\theta} (g_1, \dots, g_d, 1, \dots, 1).$$

Abbiamo così provato che ogni $h \in V(G, n)$ è equivalente al vettore $(g_1, \dots, g_d, 1, \dots, 1)$ e quindi G ha un unico T_n-system. □

2.2 T_2-system di alcuni gruppi finiti

In questo paragrafo determineremo il numero di T_2- system di alcuni gruppi finiti. In particolare, vedremo che il gruppo dei quaternioni, il gruppo diedrale D_8, i gruppi simmetrici S_3 e S_4 e il gruppo alterno A_4 hanno un solo T_2-system, mentre il gruppo A_5 ne ha due. Concluderemo con un esempio di B.H. Neumann di un 2-gruppo avente almeno due T_2-system.

In tutti gli esempi useremo la caratterizzazione dei T-system con i vettori generatori e cercheremo quindi di determinare le classi di vettori equivalenti. A questo scopo, per prima cosa determineremo l'insieme dei vettori generatori di lunghezza 2 e gli automorfismi del gruppo, poi considereremo l'insieme Ω delle orbite prodotte dall'azione del gruppo degli automorfismi sull'insieme dei vettori generatori e infine valuteremo l'effetto delle trasformazioni di Nielsen sull'insieme Ω.

2.2.1 Gruppo dei quaternioni

Il gruppo dei quaternioni Q_8 è il gruppo generato dagli elementi i, j con le relazioni

(i) $i^4 = j^4 = 1$

(ii) $i^2 = j^2 = (ij)^2$

(iii) $jij = i$.

Q_8 ha quindi ordine 8 con insieme degli elementi

$$Q_8 = \{ 1, i, j, i^2, i^3, j^3, ij, i^3 j \}.$$

Gli elementi i, j, ij e i loro inversi $i^{-1} = i^3, j^{-1} = j^3, (ij)^{-1} = (ij)^3 = i^3 j$ hanno ordine 4, i^2 ha ordine 2.

Gli insiemi $\{ i^{\pm 1}, j^{\pm 1} \}, \{ i^{\pm 1}, (ij)^{\pm 1} \}, \{ j^{\pm 1}, (ij)^{\pm 1} \}$ generano Q_8. Inoltre Q_8 non è ciclico perché non contiene elementi di ordine 8, quindi $\langle 1, x \rangle = \langle x \rangle \lneqq Q_8$ per ogni $x \in Q_8$ e $\langle i^2, x \rangle = \langle x \rangle \lneqq Q_8$ per ogni $x \in Q_8$.

Possiamo quindi concludere che Q_8 ha 24 vettori generatori di lunghezza 2 dati da

$$V(Q_8, 2) = \{ (a^m, b^n) \mid m, n = \pm 1, a, b \in \{ i, j, ij \}, a \neq b \}.$$

Proposizione 2.1. *Il gruppo $Aut(Q_8)$ degli automorfismi di Q_8 ha ordine 24.*

Dimostrazione. Ogni automorfismo manda vettori generatori in vettori generatori rispettando l'ordine degli elementi. Considerando quindi la coppia (i, j) di generatori di Q_8 e un automorfismo $\alpha \in Aut(Q_8)$ si deve avere

$$(i, j) \xrightarrow{\alpha} (x, y)$$

con $(x, y) \in V(Q_8, 2)$ e $|x| = |i|, |y| = |j|$.

Ogni vettore generatore g_h per $h = 1, \ldots, 24$ è costituito da una coppia di elementi di ordine $4 = |i| = |j|$. Ci sono quindi al più 24 possibili automorfismi, ottenuti estendendo le mappe $\alpha_h : (i, j) \to g_h = (x_h, y_h)$. Per essere effettivamente degli automorfismi le mappe α_h devono rispettare le relazioni che definiscono il gruppo Q_8, cioè devono valere

(i) $(i^4)\alpha = (j^4)\alpha = 1\alpha = 1$

(ii) $i^2\alpha = j^2\alpha$

(iii) $(jij)\alpha = i\alpha$.

Si ha che $(i\alpha_h, j\alpha_h) = (x^m, y^n)$ per qualche $x, y \in \{ i, j, ij \}, x \neq y; m, n = \pm 1$. E' facile quindi vedere che le relazioni (i) e (ii) sono verificate per ogni h. Vediamo che vale anche la relazione (iii), cioè che vale $y^n x^m y^n = x^m$ per ogni scelta possibile di x, y, m, n.

Per $m = n = 1$ la relazione (iii) diventa $yxy = x$ ed è vera per ogni $x, y \in \{ i, j, ij \}, x \neq y$ dato che

$$\begin{aligned}
&jij = i \quad \text{per definizione} \\
&iji = j^3(jij)i = j^3i^2 = jj^2i^2 = ji^2i^2 = j \\
&j(ij)j = (jij)j = ij \\
&(ij)j(ij) = ij^2ij = ii^2ij = j \\
&(ij)i(ij) = ijj^2j = i \\
&i(ij)i = i(iji) = ij.
\end{aligned}$$

Se $m = 1, n = -1$ la relazione (iii) diventa $y^{-1}xy^{-1} = x$ che è equivalente $yxy = x$ e quindi vale per ogni $x, y \in \{ i, j, ij \}$.

Se $m = -1, n = -1$ si ha $y^{-1}x^{-1}y^{-1} = (yxy)^{-1} = x^{-1}$.

Infine se $m = -1, n = 1$ la relazione $yx^{-1}y = x^{-1}$ è verificata perché è equivalente al caso precedente.

Possiamo quindi concludere che $\alpha_h : (i, j) \to g_h$ è un automorfismo per ogni $h = 1, \ldots, 24$ e quindi $|Aut(Q_8)| = 24$. □

Osservazione 2.1. Sia G un gruppo generato da n elementi e sia $Aut(G)$ il suo gruppo degli automorfismi. Se g è un vettore generatore e $\alpha, \beta \in Aut(G)$ con $\alpha \neq \beta$ allora $g \cdot \alpha \neq g \cdot \beta$.

In particolare quindi l'orbita di g per l'azione di $Aut(G)$ sull'insieme dei vettori generatori $V(G, n)$ ha cardinalità pari a $|Aut(G)|$ e il numero di orbite è $|V(G, n)|/|Aut(G)|$.

Proposizione 2.2. *Il gruppo dei quaternioni Q_8 ha un unico T_2-system.*

Dimostrazione. Consideriamo l'azione di $Aut(Q_8)$ su $V(Q_8, 2)$. Per l'osservazione precedente il numero di orbite è pari a $|V(Q_8, 2)|/|Aut(Q_8)| = 24/24 = 1$. Quindi, tutti i vettori generatori sono equivalenti e c'è un unico T_2-system. □

2.2.2 Gruppo diedrale di ordine 8

Il gruppo diedrale di ordine 8 D_8 è il gruppo generato dagli elementi a, b con le relazioni

(i) $a^4 = 1$

(ii) $b^2 = 1$

(iii) $bab = a^{-1}$.

D_8 ha come insieme degli elementi

$$D_8 = \{ 1, a, b, a^2, a^3, ab, a^2b, a^3b \}.$$

Gli elementi b, ab, a^2b, a^3b hanno ordine 2, mentre a, a^3 hanno ordine 4.

Il gruppo D_8 ha 24 vettori generatori di lunghezza 2 dati da:

$$\begin{aligned}
g_1 &= (a, b) & g_{13} &= (b, a)\\
g_2 &= (a, ab) & g_{14} &= (ab, a)\\
g_3 &= (a, a^2b) & g_{15} &= (a^2b, a)\\
g_4 &= (a, a^3b) & g_{16} &= (a^3b, a)\\
g_5 &= (a^3, b) & g_{17} &= (b, a^3)\\
g_6 &= (a^3, ab) & g_{18} &= (ab, a^3)\\
g_7 &= (a^3, a^2b) & g_{19} &= (a^2b, a^3)\\
g_8 &= (a^3, a^3b) & g_{20} &= (a^3b, a^3)\\
g_9 &= (ab, b) & g_{21} &= (b, ab)\\
g_{10} &= (a^3b, b) & g_{22} &= (b, a^3b)\\
g_{11} &= (a^2b, ab) & g_{23} &= (ab, a^2b)\\
g_{12} &= (a^3b, a^2b) & g_{24} &= (a^2b, a^3b)
\end{aligned}$$

Infatti la coppia (a, b) genera D_8 per definizione e non è difficile vedere che per gli altri vettori generatori $g_i = (x_i, y_i)$ vale $\langle x_i, y_i\rangle = \langle a, b\rangle$.

Inoltre non ci sono altre possibili coppie di generatori perché

- $\langle 1, x\rangle = \langle x, x\rangle = \langle x\rangle$ è un sottogruppo proprio di D_8 per ogni $x \in D_8$ dato che quest'ultimo non è ciclico
- $\langle a^m, a^n\rangle = \langle a\rangle \lneqq D_8$ per ogni $m, n \in \{\, 1, 2, 3\,\}$
- $\langle a^2, a^2b\rangle = \langle a^2b, b\rangle = \langle a^2, b\rangle = H$ dove H è il sottogruppo proprio di D_8 con elementi $\{\, 1, a^2, b, a^2b\,\}$
- $\langle a^2, ab\rangle = \langle a^2, a^3b\rangle = \langle ab, a^3b\rangle = K$ dove K è il sottogruppo proprio di D_8 di elementi $\{\, 1, a^2, ab, a^3b\,\}$.

Proposizione 2.3. *Il gruppo $Aut(D_8)$ degli automorfismi di D_8 ha ordine 8.*

Dimostrazione. Consideriamo la coppia di generatori (a, b) e un automorfismo $\alpha \in Aut(D_8)$. La coppia $(a\alpha, b\alpha)$ deve essere un vettore generatore tale che $|a\alpha| = |a| = 4, |b\alpha| = |b| = 2$. Le uniche possibili immagini di (a, b) tramite un automorfismo sono allora i vettori generatori $g_1, g_2, \ldots, g_8$ e quindi $|Aut(D_8)| \leq 8$.

Vediamo che i morfismi $\alpha_i : (a, b) \to g_i$ sono ben definiti per ogni $i = 1, \ldots, 8$ e quindi sono automorfismi. Dobbiamo soltanto verificare che valga la relazione

$$(bab)\alpha_i = a^{-1}\alpha_i \qquad \forall i = 1, \ldots, 8. \tag{2.1}$$

Per $i = 1, \ldots, 8$ i vettori generatori sono della forma $(a^m, a^n b)$ con $m \in \{1, 3\}, n \in \{0, 1, 2, 3\}$. Per provare che è vera la relazione (2.1) è sufficiente verificare che valga

$$(a^n b)a^m(a^n b) = a^{-m} \quad \forall m \in \{1, 3\}, n \in \{0, 1, 2, 3\}. \tag{2.2}$$

Considerando la relazione $bab = a^{-1}$ si ha

$$\begin{aligned}(a^n b)a^m(a^n b) &= (a^n b) \underbrace{aa \ldots a}_{\text{m+n volte}} b = (a^n b)ab\, ba \ldots bab \\ &= a^n \underbrace{(bab) \ldots (bab)}_{\text{m+n volte}} = a^n a^{-m-n} = a^{-m}.\end{aligned}$$

Quindi α_i è un automorfismo per ogni $i = 1, \ldots, 8$ e $|Aut(D_8)| = 8$. □

Abbiamo provato che D_8 ha 24 vettori generatori e che $Aut(D_8)$ ha ordine 8. Per l'osservazione 2.1 ci sono $24/8 = 3$ orbite per l'azione di $Aut(D_8)$ su $V(G, 2)$ con rappresentanti

$$h_1 = (b, a) \qquad h_2 = (a, b) \qquad h_3 = (ab, b).$$

Infatti non possono esistere automorfismi che mandano h_i in h_j con $i \neq j$ perché non rispetterebbero l'ordine degli elementi.

Tuttavia i vettori h_1, h_2, h_3 sono equivalenti perché possono essere trasformati l'uno nell'altro con una sequenza finita di trasformazioni di Nielsen:

$$h_1 = (b, a) \xrightarrow{P(1,2)} h_2 = (a, b) \xrightarrow{R(1,2)} h_3 = (ab, b).$$

Abbiamo così provato che tutti i 24 vettori generatori sono equivalenti e quindi

Proposizione 2.4. *Il gruppo diedrale D_8 ha un unico T_2-system.*

2.2.3 Gruppo simmetrico di grado 3

Definizione 2.1. Dato un intero $n \geq 1$ l'insieme di tutte le permutazioni di $\{1, \ldots, n\}$ è un gruppo rispetto alla composizione di applicazioni $\circ$ definita da $(i)(f \circ g) = ((i)f)g$ per ogni $i \in \{1, \ldots, n\}$. Tale gruppo viene detto *gruppo simmetrico di grado n* e si indica con S_n.

Il gruppo S_n ha ordine $n!$ ed è generato dagli elementi $(i\ i+1)$ per $i = 1, \ldots, n-1$.

Un ciclo di lunghezza k è un elemento di S_n che può essere scritto come $(a_1\, a_2 \ldots a_k)$ con $a_i \in \{1, \ldots, n\}$; una trasposizione è un ciclo di lunghezza 2. Diremo che un elemento di S_n è di tipo $a_1.a_2.a_3 \ldots .a_k$ con k, a_i interi positivi tali che $a_1 + a_2 + \cdots + a_k \leq n, k \leq n$, se può essere scritto come il prodotto di k cicli disgiunti di lunghezze $a_1, \ldots, a_k$. Un vettore generatore $v = (v_1, \ldots, v_n)$ di S_n è di tipo $(b_1, \ldots, b_n)$ se v_i è un elemento di tipo b_i per ogni $i = 1, \ldots, n$.

Notazione 2.1. Dati due cicli $(a_1 \dots a_j), (b_1 \dots b_k) \in S_n$ rappresentanti le permutazioni f e g rispettivamente, la scrittura

$$(a_1 \dots a_j)(b_1 \dots b_k)$$

indicherà la permutazione $f \circ g$ definita da $(i)(f \circ g) = ((i)f)g \; \forall i \in \{ 1, \dots, n \}$.

Il gruppo simmetrico S_3 di grado 3 è un gruppo di ordine 6 con insieme degli elementi

$$S_3 = \{ id, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2) \}. \tag{2.3}$$

S_3 ha 18 vettori generatori di lunghezza 2 dati da

- 6 vettori di tipo $((a\,b), (b\,c))$
- 6 vettori di tipo $((a\,b), (a\,b\,c))$
- 6 vettori di tipo $((a\,b\,c), (a\,b))$

dove $a, b, c \in \{ 1, 2, 3 \}$ e $a \neq b \neq c$.

Infatti, dato che ogni permutazione si può scrivere come prodotto di trasposizioni, S_3 è generato dall'insieme $\{ (1\,2), (1\,3), (2\,3) \}$. Si ha inoltre

$$(a\,b)(b\,c)(a\,b) = (a\,c)$$
$$(a\,b)(a\,b\,c) = (a\,c) \qquad\qquad (a\,b\,c)(a\,b) = (b\,c)$$

e quindi

$$\langle (a\,b), (b\,c) \rangle = \langle (a\,b), (a\,b\,c) \rangle = \langle (a\,b), (b\,c), (a\,c) \rangle = S_3.$$

Le restanti coppie $(id, x), (x, x), (x, x^{-1})$ con $x \in S_3$ non possono essere vettori generatori perché altrimenti S_3 dovrebbe essere ciclico generato dall'elemento x.

Proposizione 2.5. *Il gruppo degli automorfismi di S_3 è isomorfo a S_3.*

Dimostrazione. Un automorfismo deve mandare il vettore $((1\,2), (2\,3))$ in un vettore generatore di tipo $((a\,b), (b\,c))$, quindi ci sono al più 6 automorfismi.

Inoltre il gruppo $Inn(S_3)$ degli automorfismi interni di S_3 è un sottogruppo di $Aut(S_3)$ isomorfo al gruppo quoziente $S_3/Z(S_3)$, dove $Z(S_3)$ indica il centro di S_3.

Dato che $(a\,b)(a\,b\,c) \neq (a\,b\,c)(a\,b)$ il centro di S_3 è banale e quindi $Inn(S_3) \simeq S_3$.

Perciò $Aut(S_3)$ ha ordine al più 6 e ha un sottogruppo di ordine 6 isomorfo a S_3, quindi

$$Aut(S_3) \simeq S_3.$$

□

Possiamo ora determinare il numero di T_2-system di S_3.

Proposizione 2.6. *Il gruppo simmetrico S_3 ha un unico T_2-system.*

Dimostrazione. Proviamo che tutti vettori generatori di lunghezza 2 sono equivalenti.

L'azione di $Aut(S_3)$ sull'insieme dei vettori generatori $V(S_3, 2)$ produce $18/6 = 3$ orbite con rappresentanti

$$h_1 = ((1\,2), (1\,3)) \qquad h_2 = ((1\,2), (1\,2\,3)) \qquad h_3 = ((1\,2\,3), (1\,2))$$

dato che non esistono automorfismi che trasformano questi vettori l'uno nell'altro.

Considerando le trasformazioni di Nielsen

$$h_1 = ((1\,2), (1\,3)) \xrightarrow{L(2,1)} h_2 = ((1\,2), (1\,2\,3)) \xrightarrow{P(1,2)} h_3 = ((1\,2\,3), (1\,2))$$

si vede che anche h_1, h_2, h_3 sono equivalenti e quindi S_3 ha un unico T_2-system. □

2.2.4 Gruppo alterno di grado 4

Definizione 2.2. L'insieme A_n delle permutazioni di $\{1, \ldots, n\}$ che sono il prodotto di un numero pari di trasposizioni è un gruppo rispetto alla composizione di applicazioni, detto gruppo alterno di grado n.

Il gruppo alterno di grado n ha ordine $n!/2$ ed è un sottogruppo normale del gruppo simmetrico di grado n.

Il gruppo alterno A_4 è un gruppo di ordine 12, formato da 8 elementi di ordine 3 e tipo 3, 3 elementi di ordine 2 e tipo 2.2 e l'identità.

$$\begin{aligned} A_4 =\{&id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3),\\ &(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}. \end{aligned}$$

Presa una coppia di elementi di A_4 di tipo $((a\,b)(c\,d), (a\,b\,c))$ con $a, b, c, d \in \{1, \ldots, 4\}, a \neq b \neq c \neq d$, si possono ottenere tutti gli elementi di A_4 di tipo 2.2 calcolando

$$\begin{aligned} (a\,b\,c)^{-1}(a\,b)(c\,d)(a\,b\,c) &= (a\,d)(b\,c)\\ (a\,b\,c)^{-2}(a\,b)(c\,d)(a\,b\,c)^2 &= (a\,c)(b\,d) \end{aligned}$$

e poi tutti gli elementi di tipo 3 prendendo i coniugati di $(a\,b\,c)^{\pm 1}$ con gli elementi di ordine 2. Quindi tutte le coppie costituite da un elemento di tipo 3 e un elemento di tipo 2.2 generano A_4.

Inoltre, data una coppia di tipo $((a\,b\,c),(a\,b\,d))$ con a,b,c,d tutti distinti si ha

$$(a\,b\,c)(a\,b\,d) = (a\,d)(b\,c)$$

quindi $\langle (a\,b\,c),(a\,b\,d)\rangle = \langle (a\,b\,c),(a\,d)(b\,c)\rangle = A_4$ e tutte le coppie costituite da due elementi x,y di tipo 3 con $x \neq y^{\pm 1}$ sono generatori.

Se, invece, x,y sono due elementi di tipo 2.2 il gruppo da essi generato $\langle x,y\rangle$ è contenuto nel sottogruppo $K = \{\, id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\,\}$ di A_4.

Infine, A_4 non è ciclico e quindi non può essere generato da insiemi del tipo $\{\,1,x\,\},\{\,x,x\,\},\{\,x,x^i\,\}$ con $x \in A_4, i \in \mathbb{Z}$.

In conclusione, A_4 ha $24 \cdot 4$ vettori generatori di cui

- 24 di tipo $((a\,b)(c\,d),(a\,b\,c))$ con $a \neq b \neq c \neq d$
- 24 di tipo $((a\,b\,c),(a\,b)(c\,d))$ con $a \neq b \neq c \neq d$
- 48 di tipo $((a\,b\,c),(x\,y\,z))$ con $(a\,b\,c) \neq (x\,y\,z)^{\pm 1}$.

Anche in questo caso,come negli esempi precedenti, determiniamo il gruppo degli automorfismi di A_4 che useremo poi per studiare i T_2-system.

Proposizione 2.7. *Il gruppo degli automorfismi di A_4 è isomorfo a S_4.*

Dimostrazione. Il vettore generatore $((1\,2)(3\,4),(1\,2\,3))$ deve essere mandato da ogni automorfismo in un distinto vettore generatore di tipo $(2.2,3)$, quindi ci sono al massimo 24 automorfismi e

$$|Aut(A_4)| \leq 24.$$

D'altra parte, dato che A_4 è un sottogruppo normale di S_4 il coniugio con un qualunque elemento di S_4 dà un automorfismo di A_4, quindi

$$S_4/C_{S_4}(A_4)$$

dove $C_{S_4}(A_4)$ indica il centralizzante in S_4 di A_4, è un sottogruppo di $Aut(A_4)$. Poiché

$$\begin{aligned}(a\,b)(c\,d)(a\,b\,c)(a\,b)(c\,d) &\neq (a\,b\,c)\\ (a\,b)(a\,b\,c)(a\,b) &\neq (a\,b\,c)\\ (a\,b\,c\,d)^{-1}(a\,b\,c)(a\,b\,c\,d) &\neq (a\,b\,c)\end{aligned}$$

il centralizzante $C_{S_4}(A_4)$ è banale. Quindi $Aut(A_4)$ contiene un sottogruppo isomorfo a S_4 e ha ordine al più 24, perciò

$$Aut(A_4) \simeq S_4.$$

□

Possiamo ora studiare l'azione di $Aut(A_4)$ sull'insieme dei vettori generatori. A_4 ha $24 \cdot 4$ vettori generatori e 24 automorfismi, quindi ci sono 4 orbite per l'azione di $Aut(A_4)$ su $V(A_4, 2)$ e queste devono avere come rappresentanti i vettori

$$h_1 = ((1\,2\,3), (1\,2)(3\,4)) \qquad h_2 = ((1\,2)(3\,4), (1\,2\,3))$$
$$h_3 = ((1\,2\,3), (1\,2\,4)) \qquad h_4 = ((1\,2\,3), (1\,4\,2)).$$

Infatti, tra h_1, h_2, h_3 non possono esserci automorfismi perché gli automorfismi rispettano l'ordine degli elementi e quindi mandano vettori di tipo (m, n) in vettori dello stesso tipo. Analogo ragionamento vale per h_1, h_2, h_4.

Tra h_3, h_4 non ci sono automorfismi perché se ci fosse un automorfismo α tale che

$$\begin{aligned} \alpha :(1\,2\,3) &\to (1\,2\,3) \\ (1\,2\,4) &\to (1\,4\,2) \end{aligned}$$

si dovrebbe avere

$$((1\,4)(2\,3))\alpha = ((1\,2\,3)(1\,2\,4))\alpha = (1\,2\,3)(1\,4\,2) = (2\,3\,4)$$

ma questo non è possibile perché α non può mandare un elemento di ordine 2 in uno di ordine 3.

Osserviamo ora che considerando le trasformazioni di Nielsen $P(i, j), \sigma(i)$ si ha

$$\begin{aligned} h_1 = ((1\,2\,3), (1\,2)(3\,4)) &\xrightarrow{P(1,2)} h_2 = ((1\,2)(3\,4), (1\,2\,3)) \\ h_3 = ((1\,2\,3), (1\,2\,4)) &\xrightarrow{\sigma(2)} h_4 = ((1\,2\,3), (1\,4\,2)) \end{aligned}$$

e quindi $h_1 \sim h_2$ e $h_3 \sim h_4$. Inoltre anche $h_1 \sim h_4$ perché

$$\begin{aligned} h_1 = ((1\,2\,3), (1\,2)(3\,4)) &\xrightarrow{L(2,1)} ((1\,2\,3), (2\,4\,3)) \\ h_4 = ((1\,2\,3), (1\,4\,2)) \xrightarrow{L(2,1)} ((1\,2\,3), (2\,3\,4)) &\xrightarrow{\sigma(2)} ((1\,2\,3), (2\,4\,3)). \end{aligned}$$

Questo prova che i vettori generatori h_1, h_2, h_3, h_4 sono equivalenti e quindi

Proposizione 2.8. *A_4 ha un unico T_2-system.*

2.2.5 Gruppo simmetrico di grado 4

Il gruppo simmetrico S_4 ha ordine 24 e contiene, oltre all'identità,

- 9 elementi di ordine 2, di cui 6 di tipo 2 e 3 di tipo 2.2

- 8 elementi di ordine 3 e tipo 3
- 6 elementi di ordine 4 e tipo 4.

Determiniamo l'insieme $V(S_4, 2)$ dei vettori generatori di lunghezza 2. Siano $a, b, c, d \in \{1, \ldots, 4\}, a \neq b \neq c \neq d$. Gli insiemi $\{(a\,b), (a\,c\,d)\}$, $\{(a\,b\,c\,d), (a\,c\,d)\}$ e $\{(a\,b), (a\,b\,c\,d)\}$ generano S_4 perché

$$(a\,b\,c\,d) = (a\,b)(a\,c\,d)$$

e calcolando

$$(a\,b\,c\,d)^{-i}(a\,b)(a\,b\,c\,d)^i \quad \text{per } i = 1, 2$$

si ottengono le trasposizioni $(b\,c), (c\,d)$ che con $(a\,b)$ generano S_4.

Inoltre osservando che

$$(a\,b\,d\,c)(a\,b\,c\,d) = (a\,c\,b)$$

si ha $\langle (a\,b\,c\,d), (a\,b\,d\,c)\rangle = \langle (a\,c\,b), (a\,b\,c\,d)\rangle = S_4$ e quindi gli insiemi $\{x, y\}$ con x, y di tipo 4 e $x \neq y^{\pm 1}$ generano S_4.

Considerando poi che S_4 non è ciclico le coppie $\{1, x\}, \{x, x\}, \{x, x^i\}$ con $x \in S_4, i = 1, \ldots, |x|$ non sono generatori. Infine, dato che il gruppo alterno A_4 e gli insiemi

$$H = \{id, (a\,b), (c\,d), (a\,b)(c\,d)\}$$
$$K = \{id, (a\,c), (b\,d), (a\,b)(c\,d), (a\,d)(b\,c), (a\,c)(b\,d), (a\,b\,c\,d), (a\,d\,c\,b)\}$$

sono sottogruppi di S_4, coppie di elementi contenute in uno di questi sottogruppi non possono generare S_4 e quindi non ci sono altre coppie di generatori.

Il gruppo S_4 ha allora $24 \cdot 9$ coppie di vettori generatori suddivise in

- 24 della forma $((a\,b), (a\,c\,d))$
- 24 della forma $((a\,c\,d), (a\,b))$
- 24 della forma $((a\,b\,c\,d), (a\,b))$
- 24 della forma $((a\,b), (a\,b\,c\,d))$
- 48 della forma (x, y) con x di tipo 3 e y di tipo 4
- 48 della forma (y, x) con x di tipo 3 e y di tipo 4
- 24 della forma (x, y) con x, y di tipo 4 e $y \neq x^{\pm 1}$

dove a, b, c, d sono elementi tutti distinti di $\{1, \ldots, 4\}$.

Determiniamo ora il gruppo degli automorfismi di S_4.

Proposizione 2.9. *Il gruppo degli automorfismi di S_4 è isomorfo a S_4.*

Dimostrazione. Il vettore generatore $((1\ 2), (1\ 3\ 4))$ viene mandato da un automorfismo in un vettore generatore di tipo $(2, 3)$, quindi

$$|Aut(S_4)| \leq 24.$$

Inoltre, dato che $(abcd)(ab) \neq (ab)(abcd)$ e $(ab)(cd)(abc) \neq (abc)(ab)(cd)$, allora $Z(S_4) = 1$ e

$$Inn(S_4) \simeq S_4/Z(S_4) = S_4.$$

$Aut(S_4)$ ha allora ordine al più 24 e contiene un sottogruppo di ordine 24 isomorfo a S_4, quindi $Aut(S_4) \simeq S_4$. □

Per l'osservazione 2.1, dall'azione di $Aut(S_4)$ sull'insieme dei vettori generatori si ottengono $24 \cdot 9/24 = 9$ orbite, che devono avere come rappresentanti

$$\begin{aligned}
h_1 &= ((1\ 2\ 3\ 4), (1\ 2\ 3)) \\
h_2 &= ((1\ 2\ 3\ 4), (1\ 2)) \\
h_3 &= ((1\ 2\ 3\ 4), (1\ 2\ 4\ 3)) \\
h_4 &= ((1\ 2\ 3\ 4), (1\ 3\ 2)) \\
h_5 &= ((2\ 3\ 4), (1\ 2)) \\
h_6 &= ((1\ 2), (2\ 3\ 4)) \\
h_7 &= ((1\ 2\ 3), (1\ 2\ 3\ 4)) \\
h_8 &= ((1\ 2), (1\ 2\ 3\ 4)) \\
h_9 &= ((1\ 3\ 2), (1\ 2\ 3\ 4)).
\end{aligned}$$

Infatti se esistesse un automorfismo α tale che

$$\begin{aligned}
\alpha : (1\ 2\ 3\ 4) &\to (1\ 2\ 3\ 4) \\
(1\ 2\ 3) &\to (1\ 3\ 2)
\end{aligned}$$

si avrebbe

$$(1\ 3\ 4\ 2)\alpha = ((1\ 2\ 3\ 4)(1\ 2\ 3))\alpha = (1\ 2\ 3\ 4)(1\ 3\ 2) = (3\ 4)$$

ma questo è impossibile perché (1342) e (34) sono elementi di ordine diverso. Quindi h_1, h_4 non appartengono alla stessa orbita e lo stesso vale per h_7, h_9.

Inoltre se $u = (u_1, u_2), v = (v_1, v_2)$ sono due vettori generatori tali che $|u_1| \neq |v_1|$ oppure $|u_2| \neq |v_2|$ allora non esistono automorfismi che mandano u in v e quindi anche tutti gli altri vettori appartengono a orbite distinte.

Considerando poi le seguenti sequenze di trasformazioni di Nielsen:

$$\begin{aligned}
h_3 \xrightarrow{R(2,1)} h_4 \xrightarrow{P(1,2)} h_9 \xrightarrow{\sigma(1)} h_7 \xrightarrow{P(1,2)} h_1 \\
h_8 \xrightarrow{P(1,2)} h_2 \xrightarrow{R(1,2)} h_5 \xrightarrow{P(1,2)} h_6
\end{aligned}$$

otteniamo

$$h_3 \sim h_4 \sim h_9 \sim h_7 \sim h_1 \qquad \text{e} \qquad h_8 \sim h_2 \sim h_5 \sim h_6.$$

Infine,

$$h_4 \xrightarrow{L(2,1)} ((1\,2\,3\,4),(3\,4)).$$

Il vettore $((1\,2\,3\,4),(3\,4))$ appartiene all'orbita di h_2 , perciò

$$h_2 \sim h_4$$

e questo prova che tutti i vettori generatori sono equivalenti e quindi

Proposizione 2.10. *Il gruppo simmetrico S_4 ha un unico T_2-system.*

2.2.6 Gruppo alterno di grado 5

Il gruppo alterno A_5 di grado 5 ha ordine 60 e contiene, oltre all'identità, 15 elementi di ordine 2 e tipo 2.2, 20 elementi di ordine 3 e tipo 3, 24 elementi di ordine 5 e tipo 5.

A_5 ha 2280 vettori generatori di lunghezza 2, suddivisi in

- 120 della forma $((a\,b\,c),(a\,d)(b\,e))$
- 120 della forma $((a\,d)(b\,e),(a\,b\,c))$
- 240 della forma (x,y) con x di tipo 2.2, $y=(a\,b\,c\,d\,e)$ di tipo 5 tale che $x \neq y^i(a\,b)(c\,e)y^{-i}$ per $i=1,\dots,5$
- 240 della forma (y,x) con x di tipo 2.2, $y=(a\,b\,c\,d\,e)$ di tipo 5 tale che $x \neq y^i(a\,b)(c\,e)y^{-i}$ per $i=1,\dots,5$
- 120 della forma $((a\,b\,c),(a\,d\,e))$
- 480 della forma (x,y) con x di tipo 3, y di tipo 5
- 480 della forma (y,x) con x di tipo 3, y di tipo 5
- 480 della forma (x,y) con x,y elementi di tipo 5, $x \neq y^i$ per $i=1,\dots,4$

dove a,b,c,d,e indicano elementi di $\{\,1,2,3,4,5\,\}$ tutti distinti.

I vettori sopra elencati sono tutti e soli i vettori generatori di lunghezza 2. Infatti, data una coppia (x,y) di tipo $(5,5)$ con $y \neq x^i$, a meno di prendere opportune potenze di x e y possiamo supporre $x=(a\,b\,c\,d\,e), y=(a\,b\,c\,e\,d)$. Calcolando le potenze i-esime per $i=1,\dots,4$ di

$$y^{-j}xy^j \quad \text{per } j=1,\dots,4$$

si ottengono tutti gli elementi di tipo 5. Considerando poi che $(abcde)(abced) = (a\,c)(b\,e)$, si possono generare tutti gli elementi di tipo 2.2 e quindi tutto A_5.

Se invece (x, y) è una coppia di tipo $(5, 3)$ allora si ha $x = (a\,b\,c\,d\,e)$ e $y = (a\,b\,c)$ oppure $y = (a\,c\,d)$. In entrambi i casi (x, yxy^{-1}) è una coppia di generatori di A_5 di tipo $(5, 5)$.

Le coppie (x, y) di tipo $(3, 2.2)$ con $x = (a\,b\,c), y = (a\,d)(b\,e)$ generano A_5 dato che $(x, xy) = ((a\,b\,c), (a\,e\,b\,c\,d))$ è una coppia di tipo $(3, 5)$ e quindi genera A_5.

Se (x, y) è di tipo $(5, 2.2)$ con $x = (a\,b\,c\,d\,e)$ e $y \neq x^i(a\,b)(c\,e)y^{-i}$ per $i = 1, \ldots, 5$ allora si ha (a meno di coniugati per x^i) $y = (a\,b)(c\,d)$ oppure $y = (a\,c)(b\,d)$ e in entrambi i casi (x, xy) è una coppia che genera A_5.

Anche le coppie $(x, y) = ((a\,b\,c), (a\,d\,e))$ generano A_5 perché (x, xy) è una coppia di generatori di tipo $(3, 5)$.

Inoltre non ci sono altri vettori generatori di lunghezza 2 perché A_5 non è ciclico e quindi le coppie $(id, x), (x, x), (x, x^i)$ con $x \in A_5$ non possono essere vettori generatori; l'insieme

$$H = \{\, (id, (a\,b\,c), (a\,c\,b), (a\,b)(d\,e), (b\,c)(d\,e), (a\,c)(d\,e)\,\}$$

è un sottogruppo e quindi le coppie di tipo $(3, 2.2)$ della forma $((abc), (ab)(de))$ e le coppie $((a\,b)(d\,e), (a\,c)(d\,e))$ non generano A_5; infine anche

$$\begin{aligned} K =\{&id, (a\,b)(c\,e), (a\,c)(d\,e), (a\,e)(b\,d), (b\,c)(a\,d), (b\,e)(c\,d),\\ &(a\,b\,c\,d\,e), (a\,c\,e\,b\,d), (a\,d\,b\,e\,c), (a\,e\,d\,c\,b)\} \end{aligned}$$

è un sottogruppo, perciò le coppie $((ab)(ce), (ac)(de))$ e $((abcde), (ab)(ce))$ non possono generare A_5.

Studiamo ora il gruppo $Aut(A_5)$ degli automorfismi di A_5, in modo da potere poi determinare le orbite della sua azione sull'insieme dei vettori generatori $V(A_5, 2)$.

Proposizione 2.11. *Il gruppo $Aut(A_5)$ degli automorfismi di A_5 è isomorfo a S_5.*

Dimostrazione. Il gruppo $Aut(A_5)$ ha ordine al massimo 120 perché ogni automorfismo deve mandare il vettore generatore $v = ((a\,b\,c), (a\,d)(b\,e))$ in un distinto vettore generatore dello stesso tipo e questi ultimi sono 120.

Inoltre, dato che A_5 è un sottogruppo normale di S_5, indicando con $C_{S_5}(A_5)$ il centralizzante in S_5 di A_5, si ha che $S_5/C_{S_5}(A_5)$ è un sottogruppo di $Aut(A_5)$. Si può vedere facilmente che $C_{S_5}(A_5) = 1$, quindi $Aut(A_5)$ contiene un sottogruppo isomorfo a S_5 e ha ordine al più 120, per cui

$$Aut(A_5) \simeq S_5.$$

□

Osservazione 2.2. Dato che $Aut(A_5) \simeq S_5$ ogni automorfismo di A_5 corrisponde al coniugio per qualche elemento di S_5, cioè

$$\forall \alpha \in Aut(A_5) \quad \exists x \in S_5 \quad \text{tale che} \quad g\alpha = x^{-1}gx \quad \forall g \in A_5.$$

Ora che conosciamo i vettori generatori e gli automorfismi di A_5, possiamo passare allo studio dei T_2-system. L'azione di $Aut(A_5)$ sull'insieme dei vettori generatori di A_5 produce $2280/120 = 19$ orbite. I vettori

$$\begin{aligned}
h_1 &= ((1\,2\,3\,4\,5), (1\,2\,3\,5\,4)) \\
h_2 &= ((1\,2\,3\,4\,5), (1\,3)(2\,5)) \\
h_3 &= ((1\,2\,3\,4\,5), (1\,5\,3\,4\,2)) \\
h_4 &= ((1\,2\,3\,4\,5), (2\,4\,3)) \\
h_5 &= ((1\,2\,3\,4\,5), (1\,4\,5)) \\
h_6 &= ((1\,2\,3), (1\,2\,3\,4\,5)) \\
h_7 &= ((1\,2\,3), (1\,3\,2\,4\,5)) \\
h_8 &= ((1\,2\,3), (1\,4\,5)) \\
h_9 &= ((1\,2)(3\,4), (1\,3\,5\,2\,4)) \\
h_{10} &= ((1\,2\,3\,4\,5), (1\,3\,4\,2\,5)) \\
h_{11} &= ((1\,2\,3\,4\,5), (1\,5\,3\,2\,4)) \\
h_{12} &= ((1\,2\,3\,4\,5), (1\,4\,3)) \\
h_{13} &= ((1\,2\,3\,4\,5), (1\,2)(4\,5)) \\
h_{14} &= ((1\,2\,3\,4\,5), (2\,3\,5)) \\
h_{15} &= ((1\,2\,3), (1\,3\,5\,2\,4)) \\
h_{16} &= ((1\,2\,3), (1\,4)(2\,5)) \\
h_{17} &= ((1\,2\,3), (1\,5\,2\,3\,4)) \\
h_{18} &= ((1\,2)(3\,4), (1\,2\,3\,4\,5)) \\
h_{19} &= ((1\,2)(3\,4), (1\,3\,5))
\end{aligned}$$

sono dei rappresentanti delle 19 orbite. Infatti, un automorfismo rispetta l'ordine degli elementi, perciò manda vettori di tipo (m, n) in vettori di tipo (m, n), quindi, posto

$$\begin{aligned}
\Omega_1 &= \{\, h_1, h_3, h_{10}, h_{11} \,\} & \Omega_5 &= \{\, h_9, h_{18} \,\} \\
\Omega_2 &= \{\, h_2, h_{13} \,\} & \Omega_6 &= \{\, h_8 \,\} \\
\Omega_3 &= \{\, h_4, h_5, h_{12}, h_{14} \,\} & \Omega_7 &= \{\, h_{16} \,\} \\
\Omega_4 &= \{\, h_6, h_7, h_{15}, h_{17} \,\} & \Omega_8 &= \{\, h_{19} \,\}
\end{aligned}$$

non esistono automorfismi che trasformano vettori di Ω_i in vettori di Ω_j per $i \neq j$. Inoltre, consideriamo ad esempio i vettori $h_1, h_3 \in \Omega_1$, questi non possono essere trasformati l'uno nell'altro con un automorfismo di A_5 perché se esistesse un tale automorfismo allora per l'osservazione 2.2 esisterebbe un elemento $x \in S_5$ tale che

$$x^{-1}(1\,2\,3\,4\,5)x = (1\,2\,3\,4\,5) \tag{2.4}$$

$$x^{-1}(1\,2\,3\,5\,4)x = (1\,5\,3\,4\,2). \tag{2.5}$$

Per (2.4) x deve essere allora un elemento del centralizzante $C_{S_5}((12345)) = \langle(1\,2\,3\,4\,5)\rangle$, ma nessuna potenza di $(1\,2\,3\,4\,5)$ soddisfa (2.5), quindi l'automorfismo cercato non esiste. Con un ragionamento analogo si può provare che non esistono automorfismi tra vettori distinti appartenenti allo stesso insieme Ω_i per $i = 1, 2, 3, 4$. Infine, anche tra i vettori dell'insieme Ω_5 non esistono automorfismi perché se esistesse un automorfismo α tra h_9 e h_{18} si dovrebbe avere

$$(1\,4\,5\,2\,3)\alpha = ((1\,2)(3\,4)(1\,3\,5\,2\,4))\alpha = (1\,2)(3\,4)(1\,2\,3\,4\,5) = (1\,3\,5)$$

e ciò è impossibile. I vettori $h_1, \ldots, h_{19}$ appartengono allora a orbite distinte.

Applicando poi la trasformazione di Nielsen $L(2,1) : (x, y) \to (x, xy)$ all'insieme $\{ h_1, \ldots, h_{19} \}$ delle $Aut(A_5)$ orbite di $V(A_5, 2)$, si ottengono le orbite

$$\begin{aligned} &\{ h_1, h_2, h_3, h_4, h_5 \}, \{ h_6, h_7, h_8 \}, \{ h_{10}, h_{11}, h_{12}, h_{13}, h_{14} \}, \\ &\{ h_{15}, h_{16}, h_{17} \}, \{ h_{18}, h_{19} \}, \end{aligned} \tag{2.6}$$

mentre applicando la trasformazione $P(1,2) : (x, y) \to (y, x)$ si ottengono le orbite

$$\begin{aligned} &\{ h_2, h_9 \}, \{ h_4, h_7 \}, \{ h_5, h_6 \}, \{ h_{12}, h_{15} \}, \\ &\{ h_{13}, h_{18} \}, \{ h_{14}, h_{17} \}, \{ h_{16}, h_{19} \}. \end{aligned} \tag{2.7}$$

Considerando (2.6) e (2.7) si vede che ci sono due classi di vettori equivalenti date da

$$h_1 \sim h_2 \cdots \sim h_9 \qquad \text{e} \qquad h_{10} \sim h_{11} \cdots \sim h_{19}. \tag{2.8}$$

Ora, per provare che A_5 ha due T_2-system è sufficiente provare che due vettori qualsiasi non appartenenti alla stessa classe non sono equivalenti. Possiamo usare il seguente criterio, noto come lemma di Higman [2].

Lemma 2.4 (Lemma di Higman)**.** *Dato un gruppo G, per ogni vettore generatore $g = (g_1, g_2) \in V(G, 2)$ indichiamo con $[g]$ il commutatore*

$$[g] = g_1^{-1} g_2^{-1} g_1 g_2.$$

Allora per ogni coppia g, g' di vettori generatori equivalenti si ha che

$$|\,[g]\,| = |\,[g']\,|.$$

Dimostrazione. Due vettori sono equivalenti se e solo se possono essere trasformati l'uno nell'altro con una sequenza finita di trasformazioni di Nielsen e/o automorfismi di G. Se α è un automorfismo di G e $g = (g_1, g_2)$ è un vettore generatore, allora

$$[g\alpha] = (g_1\alpha)^{-1}(g_2\alpha)^{-1}(g_1\alpha)(g_2\alpha) = (g_1^{-1}g_2^{-1}g_1g_2)\alpha = [g]\alpha$$

e quindi, vale

$$|\,[g]\,| = |\,[g\alpha]\,|.$$

Inoltre, osservando che

$$[g_2, g_1] = g_2^{-1}g_1^{-1}g_2g_1 = (g_1^{-1}g_2^{-1}g_1g_2)^{-1} = [g]^{-1}$$
$$[g_1^{-1}, g_2] = g_1g_2^{-1}g_1^{-1}g_2 = g_1[g_2, g_1]g_1^{-1} = g_1[g_1, g_2]^{-1}g_1^{-1} = g_1[g]^{-1}g_1^{-1}$$
$$[g_2g_1, g_2] = g_1^{-1}g_2^{-1}g_2^{-1}g_2g_1g_2 = [g]$$
$$[g_1g_2, g_2] = g_2^{-1}g_1^{-1}g_2^{-1}g_1g_2g_2 = g_2^{-1}[g]g_2$$

si ha

$$[gP(1,2)] = [g]^{-1}$$
$$[g\sigma(i)] = g_i[g]^{-1}g_i^{-1}$$
$$[gL(i,j)] = [g]$$
$$[gR(i,j)] = g_j^{-1}[g]g_j$$

e quindi anche le trasformazioni di Nielsen lasciano invariato l'ordine di $[g]$.

Allora, applicando a g una sequenza finita γ di trasformazioni di Nielsen e/o automorfismi si ottiene un elemento $g\gamma$ tale che

$$|\,[g\gamma]\,| = |\,[g]\,|$$

e questo prova che i commutatori di vettori generatori equivalenti hanno lo stesso ordine. □

Nel caso di A_5, considerando ad esempio i commutatori dei vettori h_2 e h_{16}

$$[h_2] = (1\,5\,4\,3\,2)(1\,3)(2\,5)(1\,2\,3\,4\,5)(1\,3)(2\,5) = (2\,4\,5)$$
$$[h_{16}] = (1\,3\,2)(1\,4)(2\,5)(1\,2\,3)(1\,4)(2\,5) = (1\,4\,5\,3\,2),$$

si ha che

$$|\,[h_2]\,| \neq |\,[h_{16}]\,|,$$

perciò per il lemma di Higman i due vettori non possono essere equivalenti. L'azione di $Aut(F_2) \times Aut(A_5)$ sull'insieme dei vettori generatori di lunghezza 2 di A_5 ha allora 2 orbite e quindi

Proposizione 2.12. *Il gruppo alterno di grado 5 ha due T_2-system.*

2.2.7 Un gruppo di ordine 2^{15}

Sia D un gruppo diedrale di ordine 8

$$D = \langle b, c : b^2 = c^2 = (bc)^4 = 1 \rangle.$$

Il gruppo D ammette un automorfismo α di ordine 2, che scambia tra loro b e c.

Consideriamo ora il prodotto diretto H di quattro copie di D:

$$H = D_1 \times D_2 \times D_3 \times D_4 \qquad \text{dove } D_i \simeq D \text{ per } i = 1, \ldots, 4.$$

Identificando gli elementi $b_i = b$ e $c_i = c$ di D_i con le loro copie in H, si ha che

$$H = \langle b_1, \ldots, b_4, c_1, \ldots, c_4 : {b_i}^2 = {c_i}^2 = (b_i c_i)^4 = 1 \quad \forall i = 1, \ldots, 4 \rangle$$

e quindi esiste un automorfismo β definito da

$$\begin{array}{llll} b_1\beta = b_2 & b_2\beta = b_3 & b_3\beta = b_4 & b_4\beta = c_1 \\ c_1\beta = c_2 & c_2\beta = c_3 & c_3\beta = c_4 & c_4\beta = b_1. \end{array}$$

Infatti β manda generatori in generatori e inoltre rispetta le relazioni che definiscono H, poiché si ha

$$\begin{array}{ll} ({b_i}^2)\beta = {b_{i+1}}^2 = 1 & \text{per i=1, \ldots,3} \\ ({b_4}^2)\beta = {c_1}^2 = 1 & \\ ({c_i}^2)\beta = {c_{i+1}}^2 = 1 & \text{per i=1, \ldots,3} \\ ({c_4}^2)\beta = {b_1}^2 = 1. & \end{array}$$

L'automorfismo β^4 induce in ogni D_i l'involuzione α_i che scambia b_i e c_i e di conseguenza β ha ordine 8.

Prendiamo ora l'estensione spezzante di H con l'automorfismo β, cioè il gruppo

$$G = \langle H, a : a^{-1}ha = h\beta \ \forall h \in H \rangle.$$

L'elemento a ha ordine 8 e un generico elemento x di G è dato da

$$x = a^n h \qquad \text{con } h \in H, n \in \{\, 1, 2, \ldots, |\, a| \,\},$$

quindi G ha ordine $|a| \cdot |H| = 8 \cdot 2^{12} = 2^{15}$.

Il vettore $g = (a, b_1)$ è un vettore generatore per G, perché calcolando

$$a^{-n} b_1 a^n \qquad \text{per } n = 1, 2, \ldots, 8$$

si ottengono gli elementi b_i, c_i per $i = 1, \ldots, 4$ che generano H, e il suo commutatore

$$[g] = a^{-1}{b_1}^{-1}ab_1 = b_2b_1$$

ha ordine 2.

D'altra parte anche la coppia (a, d) con $d = (a^2b_1)^3$ genera G. Infatti, dato che $|G| = 2^{15}$, si ha che $|a^2b_1| = 2^m$ per qualche intero m e quindi a^2b_1 è una potenza di $(a^2b_1)^3$. Perciò $\langle a, d\rangle$ contiene l'elemento a^2b_1 e di conseguenza la coppia di generatori a, b_1.

Osserviamo che

$$d = a^2b_1a^2b_1a^2b_1 = a^6a^{-4}b_1a^4a^{-2}b_1a^2b_1 = a^6c_1b_3b_1$$

e poniamo $g' = (a, d)$, allora

$$\begin{aligned}[g'] =& a^{-1}d^{-1}ad = a^{-1}b_1b_3c_1a^{-6}aa^6c_1b_3b_1 = \\ =& a^{-1}b_1aa^{-1}b_3aa^{-1}c_1a^{-6}aa^6c_1b_3b_1 = \\ =& b_2b_4c_2c_1b_3b_1 = c_1b_1 \times c_2 \times b_3 \times b_4.\end{aligned}$$

Dato che $|\,[g']\,| = 4$, i commutatori di g e di g' hanno ordine distinto; per il lemma di Higman 2.4 i vettori g, g' non sono equivalenti e quindi G ha almeno due T_2-system.

2.3 T-system di gruppi nilpotenti finiti

Tutti i gruppi nilpotenti finiti di classe 1, in quanto gruppi abeliani, hanno un unico sistema di transitività. Ci si può chiedere se questa proprietà resta valida per un qualsiasi gruppo nilpotente finito e, in caso contrario, qual è la minima classe di nilpotenza c di un gruppo che abbia almeno due T-system.

In questo paragrafo vedremo che già per $c = 2$ non è vero in generale che esiste un unico sistema di transitività e anzi per alcuni p-gruppi nilpotenti di classe 2 il numero di T-system può essere arbitrariamente grande. [2]

Definizione 2.3. Sia G un gruppo, $m \in \mathbb{N}$. Una *serie centrale* di lunghezza m è una collezione finita $\{\, N_i : i = 0, \ldots, m \,\}$ di sottogruppi normali di G tali che

$$\begin{aligned}&1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_m = G && \text{e} \\ &N_i/N_{i-1} \subseteq Z(G/N_{i-1}) && \forall i = 1, \ldots, m.\end{aligned}$$

Un gruppo G si dice *nilpotente* se ammette una serie centrale. Il minimo intero m per cui esiste una serie centrale di lunghezza m è detto *classe di nilpotenza* di G.

Una definizione alternativa di classe di nilpotenza di un gruppo G può essere data usando i commutatori: G è nilpotente di classe c se posto

$$\gamma_1(G) = G \qquad \gamma_{i+1}(G) = [\gamma_i(G), G] \tag{2.9}$$

si ha $\gamma_{c+1}(G) = 1, \gamma_c(G) \neq 1$ e in tal caso, la serie

$$1 = \gamma_{c+1}(G) \subseteq \gamma_c(G) \subseteq \cdots \subseteq \gamma_1(G) = G$$

è una serie centrale per G.

Esempi di gruppi nilpotenti sono i gruppi abeliani e i p-gruppi, cioè i gruppi di ordine p^n per qualche primo p e per qualche $n \in \mathbb{N}$. Infatti se G è abeliano $1 = N_0 \subseteq N_1 = G$ è una serie centrale, mentre la nilpotenza dei p-gruppi deriva dal fatto che hanno centro non banale. La serie costruita ricorsivamente ponendo $N_0 = 1, N_1 = Z$ dove Z indica il centro $Z(G)$ del p-gruppo e N_{i+1} l'unico sottogruppo normale di G tale che $Z(G/N_i) = N_{i+1}/N_i$ è infatti una serie centrale per un p-gruppo G.

Il 2-gruppo G di ordine 2^{15} costruito nel paragrafo 2.2.7 è quindi un gruppo nilpotente avente almeno due T_2-system e questo prova che in generale i gruppi nilpotenti non hanno un unico T_2-system. In realtà, vale un risultato più forte che stabilisce che per ogni primo p e per ogni intero $n > 1$ esiste un p-gruppo nilpotente con un numero arbitrariamente grande di T_n-system. Per provare questo risultato useremo una stima dal basso del numero di T_n-system, valida per alcuni particolari gruppi detti (k, n)-gruppi.

Definizione 2.4. Sia G un gruppo e siano k, n interi positivi. G è un $(k, n)-$gruppo se soddisfa le seguenti proprietà:

(*i*) G può essere generato da n elementi

(*ii*) G/V_k è il prodotto diretto di n sottogruppi ciclici di ordine k

dove V_k (che talvolta denoteremo con V) indica il sottogruppo verbale generato da tutti i commutatori e da tutte le potenze k-esime di elementi di G, cioè

$$V_k = \langle [g, h], g^k : g, h \in G \rangle.$$

Indicheremo con $\mathbb{Z}_k$ l'anello degli interi $\{ 0, 1, \ldots, k-1 \}$ con la somma e la moltiplicazione modulo k e con $\mathbb{Z}_{k,n}$ l'anello delle matrici $n \times n$ a entrate in $\mathbb{Z}_k$. Useremo invece Λ_k per denotare il gruppo degli elementi invertibili di $\mathbb{Z}_k$, cioè il sottogruppo moltiplicativo di $\mathbb{Z}_k$ formato dagli elementi coprimi con k. Analogamente, il gruppo degli elementi invertibili di $\mathbb{Z}_{k,n}$, cioè delle matrici con determinante in Λ_k, sarà indicato con $\Lambda_{k,n}$.

Siano d'ora in poi G un $(k, n)-$gruppo finito e $\{ h_1, \ldots, h_n \}$ un insieme fissato di generatori di G/V_k.

É possibile associare a ogni automorfismo τ di G/V_k una matrice di $\mathbb{Z}_{k,n}$, tramite la mappa

$$\begin{aligned} \theta : Aut(G/V_k) &\longrightarrow \mathbb{Z}_{k,n} \\ \tau &\longrightarrow (\tau_{ij}) \qquad\qquad i,j = 1,2,\ldots,n \end{aligned}$$

con τ_{ij} tali che $0 \leq \tau_{ij} \leq k-1$ e

$$h_i\tau = {h_1}^{\tau_{i1}} h_2^{\tau_{i2}} \ldots {h_n}^{\tau_{in}} \qquad i = 1,2,\ldots,n.$$

Se $g = (g_1, g_2, \ldots, g_n)$ è un vettore generatore per G, allora $gV = (g_1V, g_2V, \ldots, g_nV)$ è un vettore generatore di G/V ed esiste un unico automorfismo γ_g di G/V tale che

$$h_i\gamma_g = g_iV \qquad i = 1,2,\ldots,n. \tag{2.10}$$

Possiamo allora definire la mappa

$$\begin{aligned} D : V(G,n) &\longrightarrow \mathbb{Z}_k \\ g &\longrightarrow det(\gamma_g\theta). \end{aligned}$$

Riportiamo ora un importante lemma dovuto a W. Gaschütz [5, Lemma 17.7.2].

Lemma 2.5 (Lemma di Gaschütz)**.** *Sia $\pi : G \longrightarrow H$ un epimorfismo di gruppi finiti finitamente generati, sia $n \geq d(G)$ e sia $(h_1, h_2, \ldots, h_n)$ un vettore generatore di H. Allora esiste un vettore generatore $(g_1, g_2, \ldots, g_n)$ di G, tale che $g_i\pi = h_i$ per $i = 1,2,\ldots,n$.*

Dimostrazione. Per ogni sottogruppo C di G tale che $C\pi = H$ e per ogni vettore generatore $u = (u_1, u_2, \ldots, u_n)$ di H, indichiamo con $\phi_C(u)$ il numero di vettori generatori $c = (c_1, \ldots, c_n)$ di C tali che $c_i\pi = u_i$ per ogni $i = 1, \ldots, n$. Dato che $C\pi = H$ si ha che $|C| = |H||ker(\pi) \cap C|$. Proviamo per induzione su $|ker(\pi) \cap C|$ che il valore di $\phi_C(u)$ è indipendente da u.

Se $|ker(\pi) \cap C| = 1$, la restrizione di π a C è un isomorfismo perciò $C \simeq H$ e quindi $\phi_C(u) = 1$ per ogni $u \in V(H,n)$.

Supponiamo allora che per ogni sottogruppo C di G tale che $C\pi = H$ e $|ker(\pi) \cap C| < m$ il valore $\phi_C(u)$ sia indipendente da u. Se $|ker(\pi) \cap C| = m$, ci sono esattamente m^n elementi $c = (c_1, \ldots, c_n)$ di C^n tali che $c_i\pi = u_i$ per $i = 1,2,\ldots,n$. Ogni tale n-upla $c = (c_1, \ldots, c_n)$ genera un sottogruppo B di C tale che $B\pi = H$, perciò

$$m^n = \phi_C(u) + \sum_{B<C : B\pi = H} \phi_B(u).$$

Dato che per ogni sottogruppo proprio B di C si ha $|ker(\pi) \cap B| < m$, per ipotesi induttiva $\sum_{B<C:B\pi=H} \phi_B(u)$ è indipendente da u e allora anche $\phi_C(u)$ è indipendente da u.

Sia ora $(g'_1, \ldots, g'_n)$ un vettore generatore di G, si ha che

$$h' = (g'_1\pi, g'_2\pi, \ldots, g'_n\pi)$$

è un vettore generatore di H. Allora, per ogni vettore $h = (h_1, \ldots, h_n) \in V(H, n)$

$$\phi_G(h) = \phi_G(h') \geq 1$$

e quindi esiste un vettore $(g_1, \ldots, g_n) \in V(G, n)$ tale che $g_i\pi = h_i$ per ogni $i = 1, 2, \ldots, n$. □

Lemma 2.6. *L'immagine di $V(G, n)$ tramite D è Λ_k.*

Dimostrazione. Se τ, σ sono automorfismi di G/V si ha che $(\tau\sigma)\theta = (\tau\theta)(\sigma\theta)$ e inoltre l'automorfismo identità viene mappato nella matrice identità di $\mathbb{Z}_{k,n}$. Ogni elemento A dell'immagine di θ è allora una matrice invertibile perché se $A = \alpha\theta$ per qualche $\alpha \in Aut(G/V)$ si ha che $\alpha^{-1}\theta$ è l'inversa di A. Quindi l'immagine di θ è contenuta in $\Lambda_{k,n}$ e di conseguenza l'immagine di D è contenuta in Λ_k.

D'altra parte, per ogni $\lambda \in \Lambda_k$ il vettore $(h_1, h_2, \ldots, {h_n}^{\lambda})$ è un vettore generatore di G/V e grazie al lemma 2.5 è uguale a gV per qualche $g \in V(G, n)$, quindi l'immagine di D è Λ_k. □

Nei prossimi lemmi, indicheremo con $R(\Lambda_k)$ la rappresentazione regolare destra di Λ_k, cioè il gruppo S_{Λ_k} delle permutazioni di Λ_k con l'omomorfismo

$$\begin{aligned} \rho : \Lambda_k &\longrightarrow S_{\Lambda_k} \\ g &\longrightarrow (g)\rho \end{aligned} \tag{2.11}$$

dove $(h)(g)\rho = hg \qquad \forall g, h \in \Lambda_k$.

Dato α un automorfismo del gruppo libero F_n con generatori $x_1, x_2, \ldots, x_n$ tale che $x_i\alpha = w_i(x_1, \ldots, x_n)$, denoteremo con α_G la permutazione

$$\begin{aligned} \alpha_G : V(G, n) &\longrightarrow V(G, n) \\ (g_1, \ldots, g_n) &\longrightarrow (w_1(g_1, \ldots, g_n), \ldots, w_n(g_1, \ldots, g_n)). \end{aligned} \tag{2.12}$$

Dato β un automorfismo di G, indicheremo con β_G la permutazione di $V(G, n)$ indotta da β:

$$\begin{aligned} \beta_G : V(G, n) &\longrightarrow V(G, n) \\ (g_1, \ldots, g_n) &\longrightarrow (g_1\beta, \ldots, g_n\beta). \end{aligned} \tag{2.13}$$

Lemma 2.7. *Sia F_n il gruppo libero di rango n e sia $Aut(F_n)$ il suo gruppo degli automorfismi. Esiste una mappa $D_F : Aut(F_n) \longrightarrow R(\Lambda_k)$ tale che per ogni $\alpha \in Aut(F_n)$ e per ogni $g \in V(G, n)$ si ha*

$$D(g)D_F(\alpha) = D(g\alpha_G).$$

Inoltre, l'immagine di D_F è costituita da due elementi: l'identità e la mappa che manda ogni elemento nel suo opposto.

Dimostrazione. Siano $x_1, x_2, \ldots, x_n$ dei generatori di F_n e sia α un automorfismo di F_n tale che $x_i\alpha = w_i(x_1, \ldots, x_n)$ per $i = 1, 2, \ldots, n$. Il vettore $(w_1(h_1, \ldots, h_n), w_2(h_1, \ldots, h_n), \ldots, w_n(h_1, \ldots, h_n))$ è un vettore generatore di G/V, perciò esiste un unico automorfismo α^V di G/V tale che

$$h_i\alpha^V = w_i(h_1, \ldots, h_n) \qquad \text{per } i = 1, 2, \ldots, n.$$

Considerando poi il vettore generatore $g = (g_1, g_2, \ldots, g_n)$ e l'automorfismo γ_g definito in (2.10) si ha

$$(h_i\alpha^V)\gamma_g = w_i(g_1V, \ldots, g_nV) \qquad \text{per } i = 1, 2, \ldots, n.$$

Inoltre

$$g\alpha_G V = (g_1'V, g_2'V, \ldots, g_n'V)$$

dove $g_i'V = w_i(g_1, g_2, \ldots, g_n)V = w_i(g_1V, g_2V, \ldots, g_nV)$ per $i = 1, 2, \ldots, n$. Perciò

$$(h_1\gamma_{g\alpha_G}, h_2\gamma_{g\alpha_G}, \ldots, h_n\gamma_{g\alpha_G}) = g\alpha_G V = (h_1\alpha^V\gamma_g, h_2\alpha^V\gamma_g, \ldots, h_n\alpha^V\gamma_g)$$

e

$$\gamma_{g\alpha_G} = \alpha^V\gamma_g.$$

Quindi

$$\begin{aligned} D(g\alpha_G) = det(\gamma_{g\alpha_G}\theta) = det((\alpha^V\gamma_g)\theta) = det((\alpha^V\theta)(\gamma_g\theta)) = \\ = det(\alpha^V\theta)det(\gamma_g\theta) = D(g)det(\alpha^V\theta). \end{aligned}$$

Definendo allora $D_F(\alpha)$ come l'elemento di $R(\Lambda_k)$ corrispondente a $det(\alpha^V\theta)$, cioè $D_F(\alpha) = (det(\alpha^V\theta))\rho$ si ha che vale

$$D(g\alpha_G) = D(g)D_F(\alpha).$$

Inoltre D_F è un omomorfismo perché per ogni $\alpha, \beta \in Aut(F_n)$

$$\begin{aligned} D_F(\alpha\beta) = (det((\alpha\beta)^V\theta))\rho = & (det((\alpha^V\beta^V)\theta))\rho \\ = & (det(\alpha^V\theta)det(\beta^V\theta))\rho = D_F(\alpha)D_F(\beta). \end{aligned}$$

Per provare che l'immagine di D_F è data dall'identità e dalla mappa che manda ogni elemento nel suo opposto, è allora sufficiente determinare l'immagine di un insieme di generatori di $Aut(F_n)$. Consideriamo l'insieme di generatori[1, §6] di $Aut(F_n)$ formato dagli automorfismi μ, ν, π, σ definiti da

$$\begin{array}{llll} x_1\mu = x_2, & x_2\mu = x_1, & x_i\mu = x_i & \text{per } i = 3, \ldots, n \\ x_1\nu = x_1, & x_n\nu = x_2, & x_{i-1}\nu = x_i & \text{per } i = 3, \ldots, n \\ x_1\pi = x_1, & x_2\pi = x_1x_2, & x_i\pi = x_i & \text{per } i = 3, \ldots, n \\ x_1\sigma = x_1, & x_2\sigma = x_2^{-1}, & x_i\sigma = x_i & \text{per } i = 3, \ldots, n. \end{array}$$

Si ha che

$$\mu^V\theta = \left(\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline & 0 & I_{n-2} \end{array}\right)$$

$$\nu^V\theta = \left(\begin{array}{cc|c} 1 & 0 & 0 \\ \hline & 0 & I_{n-2} \\ \hline 0 & 1 & 0 \end{array}\right)$$

$$\pi^V\theta = \left(\begin{array}{cc|c} 1 & 0 & \\ 1 & 1 & 0 \\ \hline & 0 & I_{n-2} \end{array}\right)$$

$$\sigma^V\theta = \left(\begin{array}{cc|c} 1 & 0 & \\ 0 & -1 & 0 \\ \hline & 0 & I_{n-2} \end{array}\right)$$

dove I_{n-2} indica la matrice identità di $\mathbb{Z}_{k,n-2}$ e quindi

$$\begin{aligned} det(\mu^V\theta) &= -1 \\ det(\nu^V\theta) &= (-1)^n \\ det(\pi^V\theta) &= 1 \\ det(\sigma^V\theta) &= -1. \end{aligned}$$

L'immagine di D_F è allora il sottogruppo di $R(\Lambda_k)$ generato dalle permutazioni corrispondenti agli elementi 1 e -1 di Λ_k, cioè è il gruppo formato dalla mappa identità e dalla mappa che manda ogni elemento nel suo opposto. □

Lemma 2.8. *Sia $Aut(G)$ il gruppo degli automorfismi di G. Esiste una mappa $D_G : Aut(G) \longrightarrow R(\Lambda_k)$ tale che per ogni $\beta \in Aut(G)$ e per ogni $g \in V(G,n)$ si ha*

$$D(g)D_G(\beta) = D(g\beta_G).$$

Dimostrazione. Dato che V è un sottogruppo caratteristico di G, ogni automorfismo β di G induce un automorfismo β^V di G/V definito da

$$(gV)\beta^V = g\beta V \qquad \forall g \in G.$$

Inoltre, se $g = (g_1, g_2, \ldots, g_n)$ è un vettore generatore si ha

$$\begin{aligned} g\beta_G V =& (g_1\beta V, g_2\beta V, \ldots, g_n\beta V) = \\ =& (g_1 V\beta^V, g_2 V\beta^V, \ldots, g_n V\beta^V) = (h_1\gamma_g\beta^V, h_2\gamma_g\beta^V, \ldots, h_n\gamma_g\beta^V) \end{aligned}$$

dove γ_g è l'automorfismo di G/V definito in (2.10). Perciò

$$\gamma_{g\beta_G} = \gamma_g\beta^V$$

e quindi

$$\begin{aligned} D(g\beta_G) =& det(\gamma_{g\beta_G}) = det((\gamma_g\beta^V)\theta) \\ =& det(\gamma_g\theta)det(\beta^V\theta) = D(g)det(\beta^V\theta). \end{aligned}$$

Definendo $D_G(\beta)$ come l'elemento di $R(\Lambda_k)$ corrispondente a $det(\beta^V\theta)$, cioè $D_G(\beta) = (det(\beta^V\theta))\rho$ si ha

$$D(g\beta_G) = D(g)D_G(\beta) \qquad \forall \beta \in Aut(G)$$

come voluto. □

Consideriamo il sottogruppo P_k di $R(\Lambda_k)$ generato dall'insieme

$$\{\, D_F(\alpha), D_G(\beta) : \alpha \in Aut(F_n), \beta \in Aut(G) \,\}$$

e la sua azione su Λ_k indotta dall'azione di $R(\Lambda_k)$.

Definizione 2.5. Sia G un (k,n)-gruppo finito. Le orbite dell'azione di P_k su Λ_k sono dette $T_{n,k}$-system di G.

Denotando con $t_{n,k}(G)$ il numero di $T_{n,k}$-system del (k,n)-gruppo G e con $t_n(G)$ il numero di T_n-system di G, si ha

Teorema 2.3. *Se G è un (k,n)-gruppo finito allora*

$$t_n(G) \geq t_{n,k}(G).$$

Dimostrazione. Proviamo che se g, g' sono vettori generatori di G appartenenti allo stesso T_n-system allora $D(g), D(g')$ appartengono allo stesso $T_{n,k}$-system.

Dato che g, g' appartengono allo stesso T_n-system, allora esiste una sequenza finita di automorfismi di F_n e/o automorfismi di G che trasformano g in g'.

Sia $\alpha \in Aut(F_n)$ tale che $x_i\alpha^{-1} = w_i(x_1, x_2, \ldots, x_n)$, dove $x_1, \ldots, x_n$ è un insieme di generatori del gruppo libero F_n. Per la proposizione 1.4 l'azione di α su $g = (g_1, g_2, \ldots, g_n)$ è data da

$$g\alpha = (w_1(g_1, g_2, \ldots, g_n), w_2(g_1, g_2, \ldots, g_n), \ldots, w_n(g_1, g_2, \ldots, g_n)).$$

Quindi

$$g\alpha = g{\alpha^{-1}}_G$$

dove α_G è la permutazione definita in (2.12). Se $g' = g\alpha$ si ha allora

$$D(g') = D(g{\alpha^{-1}}_G) = D(g)D_F(\alpha^{-1})$$

e quindi $D(g), D(g')$ appartengono allo stesso $T_{n,k}$-system.

Analogamente, se $\beta \in Aut(G)$ per la proposizione 1.3 si ha che

$$g\beta = (g_1\beta, g_2\beta, \ldots, g_n\beta) = g\beta_G$$

dove β_G è la permutazione definita in (2.13). Posto $g' = g\beta$ si ha allora

$$D(g') = D(g\beta_G) = D(g)D_G(\beta)$$

e quindi $D(g), D(g')$ appartengono allo stesso $T_{n,k}$-system.

Vettori appartenenti allo stesso T_n-system vengono allora mandati da D in elementi dello stesso $T_{n,k}$-system e quindi

$$t_n(G) \geq t_{n,k}(G).$$

□

Un (q, n)-gruppo nilpotente di classe 2

Sia p un primo e siano $n \geq 2, r \geq 1$ interi; poniamo $q = p^r$.

Consideriamo il gruppo abeliano $A_{q,n}$ generato dagli elementi $a_2, a_3, \ldots, a_n$ dato da

$$\begin{aligned} A_{q,n} = \langle a_2, a_3, \ldots, a_n : [a_i, a_j] = 1 \text{ per } i, j = 2, \ldots, n, \\ {a_i}^{q^{2(i-1)}} = {a_n}^{q^{3n-2-i}} \text{ per } i = 2, \ldots, n-1,\ {a_n}^{q^{3n-2}} = 1 \rangle. \end{aligned}$$

Poiché $|a_i| = q^{3i-2}$ per $i = 2, 3, \ldots, n$ si ha che

$$\begin{aligned} ({a_i}^{1+q^{2(i-1)}})^{q^{2(i-1)}} &= {a_i}^{q^{2(i-1)}} && \text{per } i = 2, \ldots, n-1 \\ ({a_n}^{1+q^{2(n-1)}})^{q^{3n-2-i}} &= {a_n}^{q^{3n-2-i}} && \text{per } i = 2, \ldots, n-1 \end{aligned}$$

e quindi possiamo definire un automorfismo ψ di $A_{q,n}$ di ordine q^n ponendo

$$a_i\psi = {a_i}^{1+q^{2(i-1)}} \qquad \text{per } i = 2, \ldots, n.$$

Sia $B_{q,n}$ l'estensione spezzante di $A_{q,n}$ con un gruppo ciclico di ordine q^{3n-1} generato da un elemento b che induce ψ in $A_{q,n}$, cioè

$$\begin{aligned} B_{q,n} = \langle a_2, \ldots, a_n, b : \text{relazioni di } A_{q,n}, \\ b^{-1}a_ib = {a_i}^{1+q^{2(i-1)}} \text{ per } i = 2, \ldots, n,\ b^{q^{3n-1}} = 1 \rangle \end{aligned}$$

e ogni elemento di $B_{q,n}$ si scrive in modo unico nella forma

$${a_2}^{h_1}{a_3}^{h_3} \ldots {a_n}^{h_n}b^k$$

con $0 \leq h_i < q^{2(i-1)}$ per $i = 2, 3, \ldots, n-1$, $0 \leq h_n < q^{3n-2}$ e $0 \leq k < q^{3n-1}$.

Gli elementi b^{q^n} e ${a_n}^{q^{3(n-1)}}$ sono elementi del centro di $B_{q,n}$, quindi il sottogruppo H generato dall'elemento ${a_n}^{q^{3(n-1)}} b^{-q^{3n-2}}$ è normale in $B_{q,n}$ e contenuto nel centro. Si può allora considerare il gruppo quoziente $G_{q,n} = B_{q,n}/H$ che è dato da

$$G_{q,n} = \langle a_2, \ldots, a_n, b : \text{relazioni di } A_{q,n}$$
$$b^{-1}a_i b = {a_i}^{1+q^{2(i-1)}} \text{ per } i = 2, \ldots, n, b^{q^{3n-2}} = {a_n}^{q^{3(n-1)}} \rangle.$$

Il sottogruppo derivato $[G_{q,n}, G_{q,n}]$ corrisponde al gruppo $[B_{q,n}, B_{q,n}]H/H$, si può provare che $[B_{q,n}, B_{q,n}] = \langle [a_n, b] \rangle$ e quindi

$$G'_{q,n} = [G_{q,n}, G_{q,n}] = \langle [a_n, b] \rangle H/H.$$

Inoltre

$$[G'_{q,n}, G_{q,n}] = [B'_{q,n}, B_{q,n}]H/H = 1,$$

dato che $[a_n, b]$ è un elemento del centro di $B_{q,n}$.

Il gruppo $G_{q,n}$ è allora nilpotente di classe 2 e ogni elemento si può scrivere in modo unico nella forma

$${a_2}^{\beta_2} {a_3}^{\beta_3} \ldots {a_n}^{\beta_n} b^{\eta} [a_n, b]^{\mu}$$

con $0 \leq \beta_i < q^{2(i-1)}$ per $i = 2, \ldots, n$, $0 \leq \eta < q^{3n-2}$, $0 \leq \mu < q^n$.

Inoltre, $G_{q,n}$ è un (q, n)-gruppo e $\{ a_2 V_q, a_3 V_q, \ldots, a_n V_q, b V_q \}$ è un insieme di generatori per $G_{q,n}/V_q$. Cerchiamo allora di determinare il gruppo P_q associato a $G_{q,n}$, per poter poi calcolare $t_{n,q}(G_{q,n})$.

Sia allora β un automorfismo di $G_{q,n}$ definito da

$$a_i \beta = {a_2}^{\alpha_{i2}} \ldots {a_n}^{\alpha_{in}} b^{\delta_i} [a_n, b]^{\epsilon_i}$$
$$b\beta = {a_2}^{\alpha_2} \ldots {a_n}^{\alpha_n} b^{\delta} [a_n, b]^{\epsilon}$$

con $0 \leq \alpha_{ij}, \alpha_i < q^{2(i-1)}$, $0 \leq \delta_i, \delta < q^{3n-2}$, $0 \leq \epsilon_i, \epsilon < q^n$ per $i, j = 2, \ldots, n$.

Dato che ${a_i}^{q^{2(i-1)}} = [a_i, b]$ appartiene al gruppo derivato $G'_{q,n}$ per ogni $i = 2, \ldots, n$, la sua immagine tramite β

$$(a_i \beta)^{q^{2(i-1)}} = {a_2}^{\alpha_{i2} q^{2(i-1)}} \ldots {a_n}^{\alpha_{in} q^{2(i-1)}} b^{\delta_i q^{2(i-1)}} [a_n, b]^{\tilde{\epsilon_i}}$$

con $0 \leq \tilde{\epsilon_i} < q^n$, deve essere ancora un elemento di $G'_{q,n}$, quindi

$$q^{2(j-1)} | \alpha_{ij} q^{2(i-1)} \qquad \text{per ogni } j = 2, \ldots, n$$
$$q^{3n-2} | \delta_i q^{2(i-1)}$$

da cui

$$q^{2(j-i)} | \alpha_{ij} \qquad \text{per ogni } i < j \qquad (2.14)$$
$$q^{3n-2i} | \delta_i \qquad \text{per ogni i.} \qquad (2.15)$$

Rispetto alla base $a_2V_q, a_3V_q, \ldots, a_nV_q, bV_q$, si ha allora che

$$\beta^V\theta = \begin{pmatrix} \bar{\alpha}_{2,2} & 0 & \ldots & \ldots & 0 \\ \bar{\alpha}_{3,2} & \bar{\alpha}_{3,3} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ \bar{\alpha}_{n2} & \ldots & \ldots & \bar{\alpha}_{nn} & 0 \\ \bar{\alpha}_2 & \ldots & \ldots & \bar{\alpha}_n & \bar{\delta} \end{pmatrix}$$

dove $\bar{x} = x \bmod q$ e quindi

$$det(\beta^V\theta) = \delta \prod_{j=2}^{n} \alpha_{jj} \bmod q.$$

Gli automorfismi devono poi rispettare le relazioni che definiscono $G_{q,n}$, perciò devono valere

$$[a_i\beta, b\beta] = (a_n\beta)^{q^{3n-2-i}} \qquad \text{per } i = 2, \ldots, n \tag{2.16}$$

$$(b\beta)^{q^{3n-2}} = (a_n\beta)^{q^{3(n-1)}}. \tag{2.17}$$

Si ha

$$\begin{aligned}
&[a_i\beta,b\beta] = \\
&=[a_n,b]^{-\epsilon_i} b^{-\delta_i} \prod_{j=2}^{n} {a_j}^{-\alpha_{ij}} [a_n,b]^{-\epsilon} b^{-\delta} \prod_{j=2}^{n} {a_j}^{-\alpha_j} \prod_{j=2}^{n} {a_j}^{\alpha_{ij}} b^{\delta_i} [a_n,b]^{\epsilon_i} \\
&\quad \prod_{j=2}^{n} {a_j}^{\alpha_j} b^{\delta} [a_n,b]^{\epsilon} = \\
&=[a_n,b]^{-\epsilon_i} (b^{-\delta_i} \prod_{j=2}^{n} {a_j}^{-\alpha_{ij}} [a_n,b]^{-\epsilon} b^{\delta_i}) (b^{-(\delta+\delta_i)} \prod_{j=2}^{n} {a_j}^{-\alpha_j} \prod_{j=2}^{n} {a_j}^{\alpha_{ij}} b^{(\delta_i+\delta)}) \\
&\quad (b^{-\delta} [a_n,b]^{\epsilon_i} \prod_{j=2}^{n} {a_j}^{\alpha_j} b^{\delta}) [a_n,b]^{\epsilon} = \\
&=[a_n,b]^{-\epsilon_i} \prod_{j=2}^{n} {a_j}^{-\alpha_{ij}(1+q^{2(j-1)})^{\delta_i}} [a_n,b]^{-\epsilon(1+q^{2(n-1)})^{\delta_i}} \prod_{j=2}^{n} {a_j}^{(\alpha_{ij}-\alpha_j)(1+q^{2(j-1)})^{(\delta_i+\delta)}} \\
&\quad [a_n,b]^{\epsilon_i(1+q^{2(n-1)})^{\delta}} \prod_{j=2}^{n} {a_j}^{\alpha_j(1+q^{2(j-1)})^{\delta}} [a_n,b]^{\epsilon} = \\
&=\prod_{j=2}^{n} {a_j}^{-\alpha_{ij}(1+\delta_i q^{2(j-1)})+(\alpha_{ij}-\alpha_j)(1+(\delta_i+\delta)q^{2(j-1)}+\alpha_j(1+\delta q^{2(j-1)})} \\
&\quad \underbrace{[a_n,b]^{\epsilon_i\delta q^{2(n-1)}-\epsilon\delta_i q^{2(n-1)}}}_{=1} = \\
&=\prod_{j=2}^{n} {a_j}^{q^{2(j-1)}(\alpha_{ij}\delta-\alpha_j\delta_i)} = \prod_{j=2}^{n} [a_j,b]^{(\alpha_{ij}\delta-\alpha_j\delta_i)} = [a_n,b]^{\sum_{j=2}^{n}(\alpha_{ij}\delta-\alpha_j\delta_i)q^{(n-j)}}
\end{aligned}$$

e, grazie alle relazioni (2.14) e (2.15)

$$\sum_{j=2}^{n}(\alpha_{ij}\delta-\alpha_j\delta_i)q^{(n-j)}\equiv\alpha_{ii}\delta q^{n-i}\bmod q^{(n-i+1)}. \tag{2.18}$$

Inoltre,

$$\begin{aligned}(a_n\beta)^{q^{3n-2-i}} =& b^{\delta_n q^{3n-2-i}}{a_2}^{\alpha_{n2}q^{3n-2-i}}\dots{a_n}^{\alpha_{nn}q^{3n-2-i}}\underbrace{[a_n,b]^{\epsilon_n q^{3n-2-i}}}_{=1}\\ &\underbrace{[a_n,b]^{(\sum_{j=2}^{n}\sum_{h=1}^{q^{3n-2-i}}h\delta_n\alpha_{nj}q^{n-j})}}_{=1\text{ perché }q^n|\delta_n}\\ =&(b^{q^{3n-2}})^{\delta_n q^{-i}}\prod_{j=2}^{n-1}({a_j}^{q^{2(j-1)}})^{\alpha_{nj}q^{3n-2j-i}}{a_n}^{\alpha_{nn}q^{3n-2-i}}=\end{aligned}$$

$$\begin{aligned}=&({a_n}^{q^{3(n-1)}})^{\delta_n q^{-i}}\prod_{j=2}^{n-1}({a_n}^{q^{3n-2-i}})^{\alpha_{nj}q^{3n-2j-i}}{a_n}^{\alpha_{nn}q^{3n-2-i}}=\\ =&{a_n}^{cq^{3n-1-i}}{a_n}^{\alpha_{nn}q^{3n-2-i}}=[a_n,b]^{cq^{(n+1-i)}+\alpha_{nn}q^{(n-i)}}\end{aligned}$$

per qualche $0\le c<q^{(i-1)}$.

Affinché valga (2.16) deve essere

$$(\alpha_{ij}\delta-\alpha_j\delta_i)q^{(n-j)}\equiv\alpha_{nn}q^{(n-i)}+cq^{(n+1-i)}\bmod q^n$$

che implica, considerando (2.18)

$$\alpha_{ii}\delta\equiv\alpha_{nn}\bmod q\qquad\qquad\text{per i= 2, \dots, n.} \tag{2.19}$$

Analogamente,

$$\begin{aligned}(b\beta)^{q^{3n-2}} =& b^{\delta q^{3n-2}}\prod_{j=2}^{n}\underbrace{{a_j}^{\alpha_j q^{3n-2}}}_{=1}\underbrace{[a_n,b]^{\epsilon q^{3n-2}}}_{=1}\underbrace{[a_n,b]^{(\sum_{j=2}^{n}\sum_{h=1}^{q^{3n-2}}\alpha_j h\delta q^{2(j-1)})}}_{=1\text{ perché }q^n\text{ divide l'esponente}}=\\ =&{a_n}^{\delta q^{3(n-1)}}=[a_n,b]^{\delta q^{(n-1)}}\end{aligned}$$

e

$$\begin{aligned}(a_n\beta)^{q^{3(n-1)}} =& \underbrace{b^{\delta_n q^{3(n-1)}}}_{=1}\prod_{j=2}^{n-1}\underbrace{{a_j}^{\alpha_{nj}q^{3(n-1)}}}_{=1}{a_n}^{\alpha_{nn}q^{3(n-1)}}\underbrace{[a_n,b]^{\epsilon_n q^{3(n-1)}}}_{=1}\\ &\underbrace{[a_n,b]^{(\sum_{j=2}^{n}\sum_{h=1}^{q^{3(n-1)}}\alpha_{nj}h\delta_n q^{2(j-1)})}}_{=1}=\\ =&{a_n}^{\alpha_{nn}q^{3(n-1)}}=[a_n,b]^{\alpha_{nn}q^{(n-1)}}.\end{aligned}$$

Per la relazione (2.17) vale allora

$$\delta q^{(n-1)} \equiv \alpha_{nn} q^{(n-1)} \bmod q^n$$

e quindi

$$\alpha_{nn} \equiv \delta \bmod q. \tag{2.20}$$

Da (2.19) e (2.20) segue che

$$\alpha_{ii} \equiv \delta \bmod q \equiv 1 \bmod q \qquad \text{per } i = 2, \ldots, n$$

e quindi

$$det(\beta^V \theta) = 1$$

per ogni β automorfismo di $G_{q,n}$. Il P_q gruppo associato a $G_{q,n}$ è allora formato soltanto dalla mappa identità di Λ_q e dalla mappa che manda ogni elemento nel suo opposto, quindi

$$t_{n,k}(G_{q,n}) = |\Lambda_q|/|P_q| = \frac{1}{2} p^{r-1}(p-1).$$

Allora per il gruppo $G_{q,n}$ per ogni $N > 0$, prendendo r sufficientemente grande si ha

$$t_n(G_{q,n}) \geq t_{n,q}(G_{q,n}) \geq N$$

e così abbiamo dimostrato

Teorema 2.4. *Per ogni coppia di interi n, N con $n > 1, N > 0$ e per ogni primo p esiste un p-gruppo nilpotente di classe 2 che ha almeno N T_n-system.*

2.4 Generalizzazione del Lemma di Higman

Il lemma di Higman (lemma 2.4), che afferma che commutatori di vettori appartenenti allo stesso T_2-system di un gruppo finito hanno lo stesso ordine, si è rivelato essere uno strumento molto utile nello studio dei T_n-system di un gruppo per $n = 2$: nel caso del gruppo A_5 (sez. 2.2.6) e del gruppo di ordine 2^{15} (sez. 2.2.7) proprio il fatto che esistevano vettori generatori di lunghezza 2 i cui commutatori avevano ordini distinti ci ha permesso di concludere che non poteva esistere un unico T_2-system. Più in generale, se in un gruppo finito G l'ordine dei commutatori degli elementi di $V(G, 2)$ assume k valori distinti, allora G avrà almeno k distinti T_2-system.

Vista l'utilità di questo lemma, lo stesso Neumann ha posto la questione se fosse possibile generalizzare il lemma di Higman a vettori generatori di lunghezza $n > 2$.

Più precisamente, dati un gruppo finito G, un intero $n \geq d(G)$ e una parola $w = w(x_1, \ldots, x_n)$ del gruppo libero F_n con generatori $x_1, \ldots, x_n$, è ben definita la mappa

$$\begin{aligned} \varphi_w : V(G,n) &\longrightarrow G \\ (g_1, \ldots, g_n) &\longrightarrow w(g_1, \ldots, g_n). \end{aligned}$$

Indichiamo con $w^{-1}(g_1, \ldots, g_n)$ l'inverso di $w(g_1, \ldots, g_n)$ in G e diciamo che due elementi g, h di G sono $Aut(G)$- coniugati se esiste un automorfismo $\alpha \in Aut(G)$ tale che $g\alpha = h$.

Definizione 2.6. La parola $w(x_1, \ldots, x_n) \in F_n$ è invariante sui T_n-system di G se l'insieme

$$S_g = \{\, w^{\pm 1}(g_1, \ldots, g_n)\alpha : \alpha \in Aut(G) \,\}$$

degli $Aut(G)$ coniugati di $\{\, w^{\pm 1}(g_1, \ldots, g_n) \,\}$, dove $g = (g_1, \ldots, g_n) \in V(G,n)$, è invariante sui T_n-system di G, cioè se per ogni vettore generatore $h = (h_1, \ldots, h_n)$ appartenente allo stesso T_n-system di g si ha che $S_h = S_g$.

Con questa terminologia, il lemma di Higman può essere riformulato dicendo che il commutatore $[x_1, x_2] = {x_1}^{-1}{x_2}^{-1}x_1x_2$ è invariante sui T_n-system per $n = 2$. Ci si è chiesti allora se è possibile generalizzare questo lemma trovando per $n > 2$ una parola w del gruppo libero F_n invariante sui T_n-system di ogni gruppo finito G tale che $d(G) \leq n$. R. Guralnick e I. Pak hanno dimostrato con il seguente teorema che una tale parola w per $n > 2$ non esiste [6]:

Teorema 2.5. *Per ogni parola non triviale $w \in F_n$ con $n \geq 3$ esiste un gruppo finito G tale che w non è invariante sui T_n-system di G.*

Nella dimostrazione di questo teorema viene utilizzato il gruppo proiettivo lineare speciale $PSL(2,p) = SL(2,p)/Z(SL(2,p))$ dove $SL(2,p)$ indica il gruppo delle matrici 2×2 invertibili con determinate 1 a entrate nel campo con p elementi $\mathbb{F}_p$ e $Z(SL(2,p))$ indica il suo centro, cioè il sottogruppo formato dalle matrici scalari con determinante 1.

Per un risultato di R. Gilman [8] il gruppo semplice $PSL(2,p)$ ha un solo T_n-system per ogni $n \geq 3$. Inoltre vale [6]:

Lemma 2.9. *Sia w una parola non triviale in $n \geq 2$ variabili. Per ogni primo p sufficientemente grande esistono $(g_1, \ldots, g_n)$ e $(h_1, \ldots, h_n)$ vettori generatori di $G_p = PSL(2,p)$ tali che $w^{\pm 1}(h_1, \ldots, h_n)$ e $w^{\pm 1}(g_1, \ldots, g_n)$ non sono $Aut(G_p)$-coniugati.*

Possiamo ora dimostrare il teorema 2.5:

Dimostrazione teorema 2.5. Supponiamo per assurdo che esista una parola non triviale $w \in F_n$ invariante in tutti i T_n- system di ogni gruppo finito G tale che $d(G) \leq n$ con $n \geq 3$. Considerando allora il gruppo $G_p = PSL(2,p)$, poiché G_p ha un unico T_n-system per ogni $n \geq 3, p \geq 5$ si ha, per tali valori di p, che per ogni coppia di vettori generatori $g = (g_1, \ldots, g_n), h = (h_1, \ldots, h_n) \in V(G_p, n)$ vale

$$\{ w^{\pm 1}(g_1, \ldots, g_n)\alpha : \alpha \in \ Aut(G_p) \} = \{ w^{\pm 1}(h_1, \ldots, h_n)\alpha : \alpha \in \ Aut(G_p) \}.$$

In particolare quindi, per $p \geq 5$ tutti i vettori generatori sono $Aut(G_p)$ coniugati, contraddicendo così il lemma 2.9. Una parola $w \in F_n$ invariante sui T_n-system di tutti i gruppi finiti G tali che $d(G) \leq n$ non può quindi esistere per $n \geq 3$. □

Il teorema 2.5 stabilisce che non è possibile adattare il lemma di Higman per vettori generatori di lunghezza $n \geq 3$. Nel caso $n = 2$, invece, si pensa che esistano diverse parole invarianti sui T_2-system oltre al commutatore e che esistano quindi delle versioni alternative del lemma di Higman: secondo una congettura tutti i coniugati di $[x_1, x_2]^m$ con $m \in \mathbb{Z}$ possono essere utilizzati come parola invariante nel lemma di Higman per $n = 2$.

2.5 T-system di gruppi semplici finiti

In questa sezione riporteremo alcuni congetture e risultati riguardanti i sistemi di transitività dei gruppi semplici finiti. In particolare vedremo che il numero di T_2-system di un gruppo semplice finito tende a infinito se l'ordine del gruppo tende a infinito. [7]

I gruppi semplici finiti, cioè i gruppi che non hanno sottogruppi normali non banali, sono i gruppi ciclici di ordine primo, i gruppi alterni A_n con $n \geq 5$, alcuni gruppi di tipo Lie e altri 26 gruppi sporadici. Escludendo i gruppi semplici finiti ciclici, per cui i sistemi di transitività sono completamente noti in quanto rientrano nel caso dei gruppi abeliani e hanno quindi un unico T_n-system per ogni valore di $n \geq 1$, per gli altri gruppi semplici finiti la conoscenza dei sistemi di transitività è ancora frammentaria e ci sono ancora congetture aperte riguardo il numero di T_n-system.

Per ogni gruppo semplice finito non ciclico G il minimo numero di generatori $d(G)$ è pari a 2, inoltre, è stato dimostrato da Liebeck e Shalev che quasi ogni coppia $(x, y) \in G \times G$ è un vettore generatore [10]. Possiamo quindi considerare i T_n-system di un gruppo semplice finito per ogni $n \geq 2$.

Nel caso $n \geq d(G) + 1 = 3$ la congettura di Wiegold [9] afferma che il numero di T_n-system $t_n(G)$ è pari a 1. Nonostante sia stata dimostrata per alcune famiglie di gruppi semplici (ad esempio per i gruppi $PSL(2,p)$ con $p \geq 5$ primo e $n \geq 3$ e, nel caso $n = 3$, per alcuni gruppi alterni), la congettura non è ancora stata completamente risolta. Nel caso $n = 2$,

si è ottenuto qualche risultato più generale. La dimostrazione del fatto che il numero di T_2-system $t_2(G)$ tende a infinito per $|G| \longrightarrow \infty$ quando $G = PSL(2,p)$ [6] oppure $G = A_k$ [9], ha spinto I. Pak a ipotizzare che il risultato valesse per ogni gruppo semplice finito non ciclico, tesi che è stata poi confermata da un teorema di S. Garion e A. Shalev [7]:

Teorema 2.6. *Sia G un gruppo semplice finito non ciclico. Il numero $t_2(G)$ di T_2-system di G tende a infinito per $|G| \longrightarrow \infty$.*

Inoltre, $t_2(G) \geq k^{(\frac{1}{2}-\varepsilon)\log k}$ quando $G = A_k$, dove $\varepsilon > 0$ è arbitrario dato k sufficientemente grande, e $t_2(G) \geq aq^r r^{(-1)}(\log q)^{-2}$ quando G è un gruppo semplice di Lie di rango r sul campo con q elementi, dove a è una costante positiva.

La prova del teorema si basa sul seguente risultato [7]:

Teorema 2.7. *Sia G un gruppo semplice finito non ciclico e sia $g \in G$ un elemento scelto a caso. La probabilità che g possa essere rappresentato come un commutatore $g = [x,y]$ con (x,y) vettore generatore tende a 1 per $|G| \longrightarrow \infty$.*

Questo teorema permette infatti di scegliere un sottoinsieme $S \subset G$ di ordine $|S| = |G|(1 - o(1))$, dove $o(1)$ indica un numero reale dipendente da G che tende a zero per $|G| \longrightarrow \infty$, e tale che ogni elemento $g \in S$ può essere scritto come il commutatore $g = [g_1, g_2]$ di un vettore generatore (g_1, g_2) di G. Combinando questo fatto con il lemma di Higman (lemma 2.4), secondo cui l'insieme $C_g = \{\, [g_1,g_2]^{\pm 1}\alpha : \alpha \in Aut(G) \,\}$ è invariante sui T_2- system, si può stimare dal basso il valore di $t_2(G)$. Denotato infatti con $k(S)$ il numero di insiemi distinti C_g al variare di $g \in S$, si avrà

$$t_2(G) \geq k(S).$$

Stimando infine il valore di $k(S)$ nel caso dei gruppi alterni e dei gruppi semplici di Lie, si potrà provare la seconda parte dell'enunciato, che è quanto basta per dimostrare il teorema.

Abbiamo così trovato un'altra famiglia di gruppi, oltre a quella dei p-gruppi nilpotenti di classe 2, per cui il numero di sistemi di transitività può essere illimitato.

Capitolo 3

Sistemi di transitività dei gruppi profiniti

Anche per i gruppi profiniti, analogamente a quanto fatto per i gruppi astratti, è possibile definire i sistemi di transitività. In questo capitolo, vedremo che nel caso profinito, contrariamente a quanto accade per i gruppi finiti, esiste un unico T_n-system per ogni valore ammissibile di n. Questo risultato sarà una conseguenza della versione profinita del lemma di Gaschütz.

3.1 Sistemi inversi, limiti inversi e gruppi profiniti

In questo paragrafo riportiamo le principali definizioni e proprietà riguardanti gruppi profiniti, sistemi inversi e limiti inversi.

Un gruppo topologico è un insieme G che è contemporaneamente un gruppo e uno spazio topologico tale che la mappa $\mu : G \times G \longrightarrow G$ definita da $(x, y)\mu = xy^{-1}$ è continua.

Scriveremo $H \leq_O G$ per indicare che H è un sottogruppo aperto di G e $N \trianglelefteq_O G$ per indicare che N è un sottogruppo normale aperto di G. Denoteremo con $\overline{H}$ la chiusura di un sottogruppo H di G.

Un insieme diretto è un insieme I con una relazione di ordine parziale $\leq$ tale che per ogni $i_1, i_2 \in I$ esiste un elemento $j \in I$ tale che $i_1 \leq j$ e $i_2 \leq j$.

Definizione 3.1. Un *sistema inverso* di gruppi topologici (X_i, φ_{ij}) è costituito da una famiglia $\{ X_i \mid i \in I \}$ di gruppi topologici indicizzata in un insieme diretto I e una famiglia di omomorfismi continui di gruppi $\{ \varphi_{ij} : X_i \longrightarrow X_j \mid i, j \in I, j \leq i \}$ tali che $\varphi_{ii} = id$ per ogni $i \in I$ e $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ per ogni $k \leq j \leq i$.

Dato un sistema inverso (X_i, φ_{ij}) di gruppi topologici e un gruppo topologico Y, la famiglia di omomorfismi continui $\{ \sigma_i : Y \longrightarrow X_i \mid i \in I \}$ è detta compatibile se $\sigma_i\varphi_{ij} = \sigma_j$ per ogni $j \leq i$, cioè se per ogni $j \leq i$ il

diagramma

$$\begin{array}{ccc} Y & & \\ {\scriptstyle\sigma_i}\downarrow & \searrow^{\sigma_j} & \\ X_i & \xrightarrow[\varphi_{ij}]{} & X_j \end{array}$$

commuta.

Dato un sistema inverso è possibile definirne il limite inverso.

Definizione 3.2. Un *limite inverso* (X, φ_i) del sistema inverso di gruppi topologici (X_i, φ_{ij}) è un gruppo topologico X con una famiglia di omomorfismi continui compatibili $\{ \varphi_i : X \longrightarrow X_i \mid i \in I \}$ tali che soddisfano la seguente proprietà universale: per ogni gruppo topologico Y e per ogni famiglia di omomorfismi continui compatibili $\alpha_i : Y \longrightarrow X_i$, esiste un unico omomorfismo continuo $\alpha : Y \longrightarrow X$ tale che $\alpha_i = \alpha\varphi_i$ per ogni $i \in I$, cioè esiste un unico omomorfismo continuo α tale che il diagramma

$$\begin{array}{ccc} Y & \xrightarrow{\alpha} & X \\ & {\scriptstyle\alpha_i}\searrow & \downarrow{\scriptstyle\varphi_i} \\ & & X_i \end{array}$$

commuta per ogni $i \in I$.

Denoteremo con $\varprojlim_{i \in I} (X_i, \varphi_{ij})$ o semplicemente con $\varprojlim_{i \in I} X_i$ il limite inverso del sistema inverso (X_i, φ_{ij}).

Le nozioni di sistema inverso e di limite inverso sono definite per gli elementi di una qualunque categoria $\mathcal{C}$, è sufficiente infatti prendere nelle definizioni famiglie di oggetti e di morfismi appartenenti alla categoria $\mathcal{C}$. Ad esempio se nella definizione di sistema inverso si considera una famiglia $\{ X_i : i \in I \}$ di insiemi e una famiglia $\{ \varphi_{ij} : X_i \longrightarrow X_j \}$ di mappe si ottiene un sistema inverso di insiemi.

Il limite inverso di un sistema inverso esiste ed è unico a meno di isomorfismo, come ci assicura la seguente proposizione [11, Prop 1.1.4] :

Proposizione 3.1. *Sia (X_i, φ_{ij}) un sistema inverso indicizzato nell'insieme I.*

(a) *Se (X, φ_i) e (Y, ψ_i) sono due limiti del sistema inverso allora esiste un isomorfismo (o omeomorfismo se si tratta di spazi topologici) $\vartheta : X \longrightarrow Y$ tale che $\vartheta\psi_i = \varphi_i$ per ogni $i \in I$.*

(b) *Se poniamo $X = \{ x \in \prod_{i \in I} X_i \mid x\pi_j\varphi_{ji} = x\pi_i$ per ogni $i, j \in I, i \leq j \}$ e $\varphi_i = \pi_i|_X$ dove $\pi_i : \prod_{i \in I} X_i \longrightarrow X_i$ é la proiezione su X_i per ogni $i \in I$. Allora (X, φ_i) è un limite inverso di (X_i, φ_{ij}).*

Il limite inverso (X, φ_i) di un sistema inverso (X_i, φ_{ij}) di gruppi topologici indicizzato in I è quindi un sottoinsieme del prodotto cartesiano $\prod_{i\in I} X_i$. Di conseguenza, la totalità degli insiemi della forma ${\varphi_i}^{\leftarrow}(U_i)$ con U_i aperto di X_i, $i \in I$, forma una base per la topologia di X. Per sottoinsiemi di limiti inversi di gruppi (o spazi) topologici, possiamo allora usare il seguente criterio di densità:

Lemma 3.1 (Criterio di densità)**.** *Sia (X, φ_i) il limite inverso del sistema inverso di gruppi topologici (X_i, φ_{ij}) e sia Y un sottoinsieme di X. Se $Y\varphi_i = X_i$ per ogni $i \in I$, allora Y è denso in X.*

Dimostrazione. È sufficiente osservare che se $Y\varphi_i = X_i$ per ogni $i \in I$, allora per ogni aperto di base ${\varphi_i}^{\leftarrow}(U_i)$ con U_i aperto di X_i, $i \in I$ si ha

$$ {\varphi_i}^{\leftarrow}(U_i) \cap Y \neq \emptyset. $$

□

Inoltre vale [5, Corollario 1.1.4]:

Proposizione 3.2. *Il limite inverso di un sistema inverso di insiemi finiti non vuoti è non vuoto.*

Possiamo ora dare la definizione di gruppo profinito:

Definizione 3.3. Un *gruppo profinito* G è il limite inverso di un sistema inverso (G_i, φ_{ij}) di gruppi topologici finiti.

Un gruppo profinito è isomorfo a un sottogruppo chiuso di un prodotto cartesiano di gruppi finiti ed è compatto, totalmente disconesso e Hausdorff. Di conseguenza ogni epimorfismo continuo di gruppi profiniti $\rho : G \longrightarrow H$ è una mappa aperta.

Poiché in un gruppo topologico tutti i sottogruppi aperti sono chiusi e tutti i sottogruppi aperti di un gruppo compatto hanno indice finito, allora tutti i sottogruppi aperti di un gruppo profinito sono chiusi e di indice finito. Inoltre, indicando con $\mathcal{N}$ l'insieme dei sottogruppi normali e aperti di un gruppo profinito G, si ha che ogni sottoinsieme aperto di G contenente l'identità contiene un elemento di $\mathcal{N}$, ogni aperto di G è unione di classi laterali di elementi di $\mathcal{N}$ e

$$ \bigcap_{N\in\mathcal{N}} N = 1. $$

Osservazione 3.1. Dato un gruppo profinito G sia $\mathcal{N} = \{\, N : N \trianglelefteq_O G \,\}$. Ponendo su $\mathcal{N}$ la relazione d'ordine parziale $\preceq$ data da

$$ U \preceq V \Leftrightarrow V \leq U \quad \text{per ogni } U, V \in \mathcal{N} $$

si ottiene un insieme diretto. Se poi definiamo per ogni $U \preceq V$

$$\begin{aligned} q_{VU} : G/V &\longrightarrow G/U \\ gV &\longrightarrow gU \end{aligned}$$

si ottiene una famiglia di epimorfismi continui (rispetto alla topologia quoziente) tale che $(G/U, q_{UV})$ è un sistema inverso di gruppi topologici.

La seguente proposizione, in cui usiamo la stessa notazione dell'osservazione precedente, ci dice, dato un gruppo profinito, come rappresentarlo come limite inverso di un sistema inverso di gruppi finiti [11, Th. 1.2.5]:

Proposizione 3.3. *Sia G un gruppo profinito e sia $\mathcal{N} = \{ N : N \trianglelefteq_O G \}$. Allora*

$$(G, q_N) \simeq \varprojlim_{\leftarrow N \in \mathcal{N}} (G/N, q_{NN'}).$$

3.2 Gruppi liberi profiniti e generatori di gruppi profiniti

Le definizioni di generatore e di gruppo libero per i gruppi profiniti non coincidono con le corrispondenti definizioni per i gruppi finiti.

Definizione 3.4. Sia G un gruppo profinito. Un sottoinsieme $X \subseteq G$ è un *insieme di generatori* per G se il gruppo generato da X è denso in G, cioè se $\overline{\langle X \rangle} = G$. Un gruppo profinito G è finitamente generato se ammette un insieme finito di generatori.

Indicheremo con $d(G)$ la minima cardinalità di un insieme di generatori per un gruppo profinito G.

Siano G un gruppo astratto e I una base filtrante non vuota di sottogruppi normali di indice finito, cioè un insieme I di sottogruppi normali di G di indice finito con la proprietà che per ogni $U, V \in I$ esiste un elemento $W \in I$ tale che $W \subseteq U \cap V$. Il gruppo G è un gruppo topologico rispetto alla topologia i cui aperti sono unioni di classi laterali di elementi di I.

Definiremo completamento di G rispetto a I, una coppia costituita da un gruppo profinito $\hat{G}$ e un omomorfismo continuo $j : G \longrightarrow \hat{G}$ con la seguente proprietà: per ogni gruppo finito H e per ogni omomorfismo continuo $\vartheta : G \longrightarrow H$ esiste un unico omomorfismo continuo $\hat{\vartheta} : \hat{G} \longrightarrow H$ tale che $j\hat{\vartheta} = \vartheta$.

$$\begin{array}{ccc} G & \xrightarrow{\ j\ } & \hat{G} \\ & \searrow^{\vartheta} & \downarrow{\scriptstyle \hat{\vartheta}} \\ & & H \end{array}$$

Il completamento di un gruppo G rispetto alla base I risulta essere univocamente determinato e vale [11, Prop. 1.4.1]

Proposizione 3.4. *Sia* $\hat{G} = \lim_{\leftarrow N \in I} G/N$ *e* $j : G \longrightarrow \hat{G}$ *la mappa definita da* $gj = (gN)_{N \in I}$ *per ogni* $g \in G$. *La coppia* $(\hat{G}, j)$ *ha le proprietà di un completamento di* G *rispetto a* I.

Dato poi un insieme X e un gruppo profinito G una mappa $\rho : X \longrightarrow G$ è detta convergente a 1 se ogni sottogruppo normale aperto di G contiene quasi ogni elemento $x\rho$ con $x \in X$, cioè se l'insieme $\{ x \in X \mid x\rho \notin N \}$ è finito per ogni $N \trianglelefteq_O G$.

Definizione 3.5. Sia X un insieme. Un *gruppo libero profinito su* X è un gruppo profinito F con una mappa $j : X \longrightarrow F$ convergente a 1 che soddisfa la seguente proprietà universale: per ogni gruppo profinito G e per ogni mappa $\varphi : X \longrightarrow G$ convergente a 1, esiste un unico omomorfismo continuo di gruppi $\overline{\varphi} : F \longrightarrow G$ tale che $j\overline{\varphi} = \varphi$. La cardinalità di X è detta rango del gruppo libero profinito F.

Per ogni insieme X esiste un gruppo profinito libero su X ed è unico a meno di isomorfismo. Inoltre, vale [11, Prop. 5.1.3']

Proposizione 3.5. *Siano* X *un insieme e* F *il gruppo libero astratto generato da* X. *Sia* $\mathcal{N} = \{ N \trianglelefteq F \mid F/N$ *finito*, $X \setminus N$ *finito* $\}$. *Allora il completamento* $(\hat{F}, j)$ *di* F *rispetto a* $\mathcal{N}$ *è il gruppo libero profinito su* X.

Se l'insieme $X = \{ x_1, \ldots, x_n \}$ è finito, allora ogni mappa $\varphi : X \longrightarrow G$ con G gruppo profinito è convergente a 1. Inoltre, ogni sottogruppo normale del gruppo libero astratto F_n generato da X contiene quasi ogni elemento di X, perciò il gruppo libero profinito su X è il completamento $\hat{F_n}$ di F_n rispetto alla base formata dai sottogruppi normali di indice finito di F_n e ogni mappa da X a un gruppo profinito G può essere estesa a un omomorfismo continuo di gruppi da $\hat{F_n}$ a G.

Di conseguenza ogni gruppo profinito G finitamente generato da n elementi è immagine epimorfa (tramite un epimorfismo continuo) del gruppo libero profinito di rango n. Infatti se $y_1, y_2, \ldots, y_n$ sono dei generatori di G, per la proprietà universale dei gruppi liberi profiniti è possibile estendere a un omomorfismo continuo di $\hat{F_n}$ la mappa $\varphi : X \longrightarrow G$ definita da $x_i\varphi = y_i$, ottenendo in questo modo un epimorfismo continuo $\overline{\varphi} : \hat{F_n} \longrightarrow G$.

3.3 T- system di gruppi profiniti

Abbiamo visto che se G è un gruppo profinito finitamente generato e $n \geq d(G)$ allora esiste un epimorfismo continuo ρ da $\hat{F_n}$ a G, dove $\hat{F_n}$ è un gruppo libero profinito di rango n e di conseguenza $G \simeq \hat{F_n}/ker(\rho)$ tramite un isomorfismo di gruppi profiniti.

Se G è un gruppo profinito finitamente generato, analogamente a quanto fatto per i gruppi astratti, possiamo allora definire per ogni $n \geq d(G)$

l'insieme

$$\Sigma(G,n) = \{\, N \trianglelefteq \hat{F}_n \mid \hat{F}_n/N \simeq G \,\},$$

dove $\hat{F}_n$ indica il gruppo libero profinito sull'insieme $X = \{\, x_1, \ldots, x_n \,\}$.

Denotiamo con $Aut(\hat{F}_n)$ il gruppo degli automorfismi del gruppo profinito $\hat{F}_n$, ovvero

$$Aut(\hat{F}_n) = \{\, \sigma : \hat{F}_n \longrightarrow \hat{F}_n \mid \sigma \text{ isomorfismo e omeomorfismo} \,\}$$

e, analogamente, con $Aut(G)$ il gruppo degli automorfismi del gruppo profinito G, ovvero

$$Aut(G) = \{\, \alpha : G \longrightarrow G \mid \alpha \text{ isomorfismo e omeomorfismo} \,\}.$$

Il gruppo $Aut(\hat{F}_n)$ degli automorfismi di $\hat{F}_n$ agisce sull'insieme $\Sigma(G,n)$ tramite l'azione

$$\begin{aligned} \Sigma(G,n) \times Aut(\hat{F}_n) &\longrightarrow \Sigma(G,n) \\ (N,\sigma) &\longrightarrow N\sigma. \end{aligned} \tag{3.1}$$

Le orbite dell'azione di $Aut(\hat{F}_n)$ su $\Sigma(G,n)$ sono dette sistemi di transitività o T_n-system di G.

Ripercorrendo quanto fatto per i gruppi astratti, possiamo poi definire un'azione di $Aut(\hat{F}_n) \times Aut(G)$ sull'insieme E degli epimorfismi continui da $\hat{F}_n$ a G ponendo

$$\begin{aligned} E \times (Aut(\hat{F}_n) \times Aut(G)) &\longrightarrow E \\ (\rho, (\sigma, \alpha)) &\longrightarrow \sigma^{-1}\rho\alpha. \end{aligned}$$

Vale allora il seguente lemma:

Lemma 3.2. *Siano $\rho_1, \rho_2 \in E$. Allora ρ_1, ρ_2 appartengono alla stessa $Aut(G)$ orbita , i.e. $\exists \alpha \in Aut(G)$ tale che $\rho_1 = \rho_2\alpha$, se e solo se $ker(\rho_1) = ker(\rho_2)$.*

Dimostrazione. "$\Rightarrow$" Siano $\rho_1, \rho_2 \in E$ tali che $\rho_1 = \rho_2\alpha$ per qualche $\alpha \in Aut(G)$. Allora

$$ker(\rho_1) = ker(\rho_2\alpha) = \{x \in F_n | x\rho_2 \in \ker(\alpha)\} = \{x \in F_n | x\rho_2 = 1\} = ker(\rho_2).$$

"$\Leftarrow$" Siano $\rho_1, \rho_2 \in E$ tali che $ker(\rho_1) = ker(\rho_2)$. Per quanto visto nella dimostrazione del lemma 1.1, scegliendo per ogni $g \in G$ un elemento x_g nell'antimmagine $\rho_2{}^{\leftarrow}(g)$ di g tramite ρ_2 e definendo $g\alpha = x_g\rho_1$ si ottiene un automorfismo α del gruppo astratto G tale che $\rho_1 = \rho_2\alpha$. Proviamo che α è un automorfismo del gruppo profinito G, cioè che α è un omeomorfismo. A questo scopo, è sufficiente far vedere che α è continuo, dato che tutti gli

epimorfismi continui di gruppi profiniti sono mappe aperte e tutte le mappe aperte, continue e biunivoche sono omeomorfismi.

Sia allora N un sottogruppo normale e aperto di G, dobbiamo provare che l'antimmagine $\alpha^{\leftarrow}(N)$ è un aperto di G. Si ha che

$$\alpha^{\leftarrow}(N) = \{\, g \in G \mid \rho_2{}^{\leftarrow}(g) \in \rho_1{}^{\leftarrow}(N) \,\} = (\rho_1{}^{\leftarrow}(N))\rho_2$$

e quindi $\alpha^{\leftarrow}(N)$ è un aperto di G perché ρ_2 è una mappa aperta e $\rho_1{}^{\leftarrow}(N)$ è aperto dato che ρ_1 è continua.

Poiché i sottogruppi normali aperti di G formano un sistema fondamentale di intorni di 1, questo prova che α è continua e quindi $\alpha \in Aut(G)$. □

Esiste allora una corrispondenza biunivoca tra l'insieme $\hat{E}$ delle $Aut(G)$-orbite di E e l'insieme $\Sigma(G, n)$:

Lemma 3.3. *La mappa $\Lambda : \hat{E} \longrightarrow \Sigma(G, n)$ definita da $\hat{\rho}\Lambda = ker(\rho)$, dove $\hat{\rho}$ indica l'orbita in $\hat{E}$ contenente ρ, è una biezione.*

Dimostrazione. Per quanto dimostrato nel lemma 1.2 la mappa Λ è ben definita e iniettiva. Inoltre per ogni N in $\Sigma(G, n)$ esiste un isomorfismo di gruppi profiniti $\bar{\rho}_N : \hat{F_n}/N \longrightarrow G$ e definendo per ogni $x \in \hat{F_n}$ $x\rho_N = (xN)\overline{\rho}_N$ si ottiene un epimorfismo ρ_N da $\hat{F_n}$ a G. Indicando poi la proiezione sul quoziente con $\pi_N : \hat{F_n} \longrightarrow \hat{F_n}/N$, si ha che $\rho_N = \pi_N\bar{\rho}_N$, perciò ρ_N è continua in quanto composizione di funzioni continue.

Questo prova che ρ_N è un epimorfismo continuo, perciò la mappa Λ è anche suriettiva e quindi è una biezione. □

Consideriamo ora l'azione indotta di $Aut(\hat{F_n})$ sull'insieme $\hat{E}$ delle $Aut(G)$-orbite di E:

$$\begin{aligned} \hat{E} \times Aut(\hat{F_n}) &\longrightarrow \hat{E} \\ (\hat{\rho}, \sigma) &\longrightarrow \widehat{\sigma^{-1}\rho} \end{aligned} \tag{3.2}$$

dove $\hat{\rho}$ indica la $Aut(G)$-orbita di E contenente ρ.

Seguendo la stessa dimostrazione della proposizione 1.1, si dimostra che

Proposizione 3.6. *L'azione di $Aut(\hat{F_n})$ su $\hat{E}$ è equivalente all'azione di $Aut(\hat{F_n})$ su $\Sigma(G, n)$.*

In particolare quindi il numero di T_n-system di G sarà uguale al numero di orbite di $\hat{E}$ per l'azione di $Aut(\hat{F_n})$ definita in (3.2).

Anche il lemma di Gaschütz (lemma 2.5) si può estendere al caso profinito [5, lemma 17.7.2]:

Lemma 3.4 (Lemma di Gaschütz profinito)**.** *Sia $\pi : G \longrightarrow H$ un epimorfismo continuo di gruppi profiniti finitamente generati, sia $n \geq d(G)$ e sia $(h_1, h_2, \ldots, h_n)$ un vettore generatore di H. Allora esiste un vettore generatore $(g_1, g_2, \ldots, g_n)$ di G tale che $g_i\pi = h_i$ per $i = 1, 2, \ldots, n$.*

Dimostrazione. Se G è un gruppo finito allora la tesi è vera per il lemma 2.5.

Se G è infinito, consideriamo l'insieme diretto $\mathcal{N}$ costituito dai sottogruppi normali aperti di G con l'ordine parziale $\preceq$ dato da $N \preceq N' \Leftrightarrow N' \leq N$.

Poiché π è un epimorfismo continuo di gruppi profiniti, e quindi è una mappa aperta, l'insieme $\mathcal{K}$ dei sottogruppi normali aperti di H è dato da

$$\mathcal{K} = \{\, N\pi \mid N \in \mathcal{N} \,\}.$$

Possiamo allora scrivere i gruppi profiniti G e H come limiti di sistemi inversi indicizzati in $\mathcal{N}$. Infatti si ha

$$(G, \xi_N) = \varprojlim_{N \in \mathcal{N}} (G/N, \xi_{NN'})$$

dove $\xi_N, \xi_{NN'}$ sono gli epimorfismi

$$\begin{array}{lll} \xi_N : G \longrightarrow G/N & \xi_{NN'} : G/N \longrightarrow G/N' & \text{per } N, N' \in \mathcal{N}, \\ \quad g \longrightarrow gN & \quad gN \longrightarrow gN' & \quad N \leq N', \end{array}$$

e, analogamente,

$$(H, \eta_N) = \varprojlim_{N \in \mathcal{N}} (H/N\pi, \eta_{NN'})$$

dove $\eta_N, \eta_{NN'}$ sono gli epimorfismi

$$\begin{array}{lll} \eta_N : H \longrightarrow H/N & \eta_{NN'} : H/N\pi \longrightarrow H/N'\pi & \text{per } N, N' \in \mathcal{N}, \\ \quad h \longrightarrow hN\pi & \quad hN\pi \longrightarrow hN'\pi & \quad N \leq N'. \end{array}$$

L'epimorfismo π induce per ogni $N \in \mathcal{N}$ un epimorfismo di gruppi finiti π_N definito da:

$$\begin{aligned} \pi_N : G/N &\longrightarrow H/N\pi \\ gN &\longrightarrow g\pi N\pi. \end{aligned}$$

Inoltre per ogni $N \leq N'$ con $N, N' \in \mathcal{N}$ si ha che $\pi_N \eta_{NN'} = \xi_{NN'} \pi_{N'}$ e

$$\pi\eta_N = \xi_N \pi_N \tag{3.3}$$

per ogni $N \in \mathcal{N}$.

Sia ora

$$A_N = \{\, (g_1N, \ldots, g_nN) \in V(G/N, n) \mid g_iN\pi_N = h_i\eta_N \text{ per ogni } i = 1, \ldots, n \,\}.$$

Dato che per ogni $N \in \mathcal{N}$ il gruppo G/N è finito, $\pi_N : G/N \longrightarrow H/N\pi$ è un epimorfismo e $(h_1\eta_N, h_2\eta_N, \ldots, h_n\eta_N)$ è un vettore generatore di $H/N\pi$, allora per il lemma di Gaschütz per gruppi finiti esiste almeno un vettore

generatore $(g_1N, g_2N, \ldots, g_nN)$ di G/N tale che $(g_iN)\pi_N = h_i\eta_N$ per ogni $i = 1, \ldots, n$ e quindi $A_N \neq \emptyset$. Si ha poi che $(A_N, \theta_{NN'})$ con

$$\begin{aligned} \theta_{NN'} : A_N &\longrightarrow A_{N'} && \text{per ogni } N \leq N' \\ (g_1N, \ldots, g_nN) &\longrightarrow (g_1N', \ldots, g_nN') && N, N' \in \mathcal{N} \end{aligned}$$

è un sistema inverso di insiemi finiti e non vuoti, quindi per la proposizione 3.2 l'insieme $A = \lim_{\leftarrow N \in \mathcal{N}} A_N$ è non vuoto e inoltre $A \subseteq G \times \cdots \times G$.

Sia allora $g = (g_1, \ldots, g_d) \in A \subseteq G \times \cdots \times G$. Proviamo che g è il vettore cercato.

Ricordando la relazione 3.3 si ha che per ogni $N \in \mathcal{N}$

$$(g_i\pi)N\pi = g_i\pi\eta_N = g_i\xi_N\pi_N = g_iN\pi_N = h_iN\pi,$$

quindi $g_i\pi = h_in$ per qualche $n \in \bigcap_{N \in \mathcal{N}} N\pi = 1$ perciò $g_i\pi = h_i$ per ogni $i = 1, \ldots, n$. Inoltre, considerando che

$$(\langle g_1, \ldots, g_n \rangle)\pi_N = \langle g_1\pi_N, \ldots, g_n\pi_N \rangle = \langle g_1N, \ldots, g_nN \rangle = G/N$$

allora π_N è suriettivo per ogni $N \in \mathcal{N}$ e quindi per il lemma 3.1 $\langle g_1, \ldots, g_n \rangle$ è denso in G, cioè $(g_1, \ldots, g_n)$ è un generatore di G. □

Applicando il lemma di Gaschütz proveremo che i gruppi profiniti hanno un unico T_n-system per ogni valore di $n \geq d(G)$.

Vediamo prima alcune proprietà dei gruppi profiniti finitamente generati che ci torneranno utili.

Lemma 3.5. *Sia G un gruppo profinito e sia $a_n(G)$ il numero di sottogruppi aperti di G di indice n. Se G è finitamente generato allora $a_n(G) < \infty$ per ogni $n \in \mathbb{N}$.*

Dimostrazione. Sia G un gruppo profinito finitamente generato e sia $d(G) = d$. Indichiamo con $b_n(G)$ il numero di sottogruppi normali e aperti di indice n di G. Se $N \trianglelefteq_O G$ e $|G : N| = n$, allora possiamo associare a N un omomorfismo da G al gruppo simmetrico S_n di grado n con nucleo N. Infatti, G/N è un gruppo finito di ordine n e per il teorema di Cayley è isomorfo a un sottogruppo del gruppo simmetrico S_n. Esiste quindi un monomorfismo $\theta : G/N \longrightarrow S_n$. Ponendo $\alpha = \pi_N\theta$ dove $\pi_N : G \longrightarrow G/N$ è la proiezione sul quoziente, si ottiene un omomorfismo $\alpha : G \longrightarrow S_n$ con nucleo N.

Il numero $b_n(G)$ sarà quindi minore o uguale alla cardinalità dell'insieme B degli omomorfismi da G a S_n. Preso un insieme di generatori $\{ g_1, \ldots, g_d \}$ ogni omomorfismo dell'insieme B è univocamente determinato dalle immagini dei generatori, perciò si ha che

$$b_n(G) \leq |B| \leq (n!)^d.$$

Ora, dato un qualunque sottogruppo aperto H di G di indice n, il suo cuore normale $H_G = \bigcap_{x\in G} x^{-1}Hx$ è un sottogruppo normale aperto di indice m tale che $m|n!$ e inoltre

$$H = \bigcup_{x\in H} H_G x = \overset{\circ}{\bigcup_{i\in\{\,1,\ldots,k\,\}}} H_G x_i \quad \text{per qualche } k \leq m.$$

Quindi ogni sottogruppo aperto di indice n è unione finita di classi laterali di un sottogruppo normale aperto di indice m che divide $n!$. Perciò, indicando con X_m l'insieme $\{\,1, 2, \ldots, m\,\}$ si ha

$$a_n(G) \leq \sum_{m|n!} b_m(G)\mathcal{P}(X_m) \leq \sum_{m|n!} (m!)^d 2^m$$

e quindi $a_n(G) < \infty$ per ogni $n \in \mathbb{N}$. □

Lemma 3.6. *Sia G un gruppo profinito finitamente generato. Allora ogni epimorfismo continuo $\alpha : G \longrightarrow G$ è un isomorfismo di gruppi profiniti (cioè un isomorfismo di gruppi con inversa continua).*

Dimostrazione. Sia G un gruppo profinito finitamente generato e sia $\alpha : G \longrightarrow G$ un epimorfismo continuo. Dato che ogni epimorfismo continuo di gruppi profiniti è una mappa aperta e ogni mappa aperta e biettiva ha inversa continua, per provare la tesi è sufficiente verificare che α sia iniettivo. Poniamo $N = ker(\alpha)$, allora G è isomorfo come gruppo profinito a G/N.

Per ogni $n \in \mathbb{N}$ si ha che $a_n(G) = a_n(G/N)$, cioè il numero di sottogruppi aperti di G di indice n è pari al numero di sottogruppi aperti di G di indice n che contengono N. Dato che G e G/N sono finitamente generati, per il lemma 3.5 $a_n(G), a_n(G/N)$ sono entrambi finiti e quindi l'insieme dei sottogruppi aperti di indice n e quello dei sottogruppi aperti di indice n che contengono N coincidono per ogni $n \in \mathbb{N}$. In particolare N è contenuto in ogni insieme normale aperto di G, perciò

$$N \subseteq \bigcap_{K\trianglelefteq_O G} K = 1.$$

Questo prova che $N = ker(\alpha) = 1$, e quindi α è un isomorfismo di gruppi profiniti. □

Possiamo ora provare che i gruppi profiniti hanno un unico sistema di transitività:

Lemma 3.7. *Siano G un gruppo profinito finitamente generato, $n \geq d(G)$ e $\hat{F}_n$ il gruppo libero profinito di rango n. Siano π_1, π_2 due epimorfismi continui*

da $\hat{F}_n$ a G. Allora esiste un automorfismo α del gruppo profinito $\hat{F}_n$ tale che $\pi_2 = \alpha\pi_1$, cioè tale che il diagramma

$$\begin{array}{ccc} \hat{F}_n & & \\ {\scriptstyle\alpha}\uparrow & \searrow^{\pi_1} & \\ \hat{F}_n & \xrightarrow[\pi_2]{} & G \end{array}$$

è commutativo.

Dimostrazione. Sia $\hat{F}_n$ il gruppo libero profinito su $\{ x_1, x_2, \ldots, x_n \}$. Poniamo $z_i = x_i\pi_2$ per $i = 1, \ldots, n$. Il vettore $(z_1, z_2, \ldots, z_n)$ genera il gruppo profinito G e quindi per il lemma 3.4 esiste un vettore generatore $(y_1, y_2, \ldots, y_n)$ tale che $y_i\pi_1 = z_i$ per ogni $i = 1, \ldots, n$. Per la proprietà universale dei gruppi liberi profiniti, esiste allora un omomorfismo continuo $\alpha : \hat{F}_n \longrightarrow \hat{F}_n$ tale che $x_i\alpha = y_i$ per ogni $i = 1, 2, \ldots, n$. Dato che $\{ y_1, \ldots, y_n \}$ è un insieme di generatori di $\hat{F}_n$, α è un epimorfismo continuo e quindi per il lemma 3.6 α è un automorfismo di $\hat{F}_n$. Inoltre vale $\alpha\pi_1 = \pi_2$ e quindi la tesi è verificata. □

Dal lemma 3.7 segue immediatamente che l'azione di $Aut(\hat{F}_n)$ sull'insieme $\hat{E}$ definita in (3.2) produce una unica orbita. Di conseguenza, vista l'equivalenza tra questa azione e tra l'azione di $Aut(\hat{F}_n)$ su $\Sigma(G, n)$ definita in (3.1), il lemma 3.7 prova che ogni gruppo profinito G ha un unico T_n-system per ogni intero $n \geq d(G)$.

Bibliografia

[1] B.H. Neumann und H. Neumann, Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen, *Math. Nachr.* 4 (1951), pp 106-125

[2] B.H. Neumann, On a question of Gaschütz, *Archiv der Mathematik* 7 (1956), pp 87-90

[3] C.David, T_3-systems of finite simple groups, *Rendiconti del seminario matematico dell'università di Padova* 89 (1993), pp 19-27

[4] M.J. Dunwoody, On T-systems of groups, *Journal of the Australian Mathematical Society* 3 (1963), pp 172-179

[5] M.D. Fried e M. Jarden, *Field Arithmetic*, ed 3, Springer (2008)

[6] R. Guralnick e I. Pak, On a question of B. H. Neumann, *Proceedings of the American Mathematical Society*, vol 131, n 7 (July 2003), pp 2021-2025

[7] S. Garion e A. Shalev, Commutator maps, measure preservation, and T-systems, *Transactions of the American Mathematical Society*, vol 361, n 9 (September 2009), pp 4631-4651

[8] R. Gilman, Finite quotients of the automorphism group of a free group, *Canad J. Math* vol 29, n 3 (1977), pp 541-555

[9] I. Pak, What do we know about the product replacement algorithm? *Groups and computation*, III (Columbus, OH, 1999), pp 301-347, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001

[10] M.W. Liebeck e A.Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra*, vol 184, n 1 (1996), pp 31-57

[11] J. Wilson, *Profinite groups*, Oxford, Clarendon Press (1988)

[12] A. Lubotzky, Pro-finite presentation, *Journal of algebra*, vol 242 (2001), pp 672-690