Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea [Triennale] in Matematica

GENERATORI DI GRUPPI

Tesi di Laurea in Algebra

Relatrice:
Chiar.ma Prof.ssa
MARTA MORIGI

Presentata da:
MARIA TINARI

VI Sessione
Anno Accademico 2017-2018

Indice

Introduzione

Un ruolo molto importante, nello studio di un gruppo G, è svolto dagli insiemi dei suoi generatori, dai quali è possibile ricavare molte informazioni.

Gli insiemi di generatori di G possono avere un numero di elementi e proprietà molto diversi tra loro. Ad esempio, gli insiemi minimali di generatori rivestono una particolare importanza; non sempre, però, essi sono i più adatti per studiare le proprietà del gruppo.

Nel primo capitolo è fornita la definizione iniziale di insieme di generatori di un gruppo ed è analizzata l'azione di un gruppo su un insieme. Tali argomenti saranno il punto di partenza per lo sviluppo del nostro discorso.

Nel secondo capitolo ci si sofferma sullo studio degli insiemi di generatori del gruppo simmetrico. In particolare, utilizzando risultati della teoria dei grafi, dimostreremo che un insieme minimale di generatori di S_n è costituito da $n-1$ trasposizioni.

Il terzo capitolo è ancora dedicato allo studio degli insiemi di generatori di gruppi di permutazioni sull'insieme $X = \{1, 2, \ldots, n\}$, ma analizzati sotto un altro punto di vista. Infatti, se siamo interessati a studiare l'appartenenza di un elemento ad un gruppo di permutazioni G, a calcolare l'ordine di G, a creare una lista di elementi di G oppure a generare elementi casuali di G, conviene utilizzare particolari insiemi di generatori, che rispettino una opportuna catena di stabilizzatori di elementi di X. Per fare ciò introdurremo il concetto di base di un gruppo di permutazioni e descriveremo l'algoritmo di Schreier-Sims. Successivamente, descriveremo il Filtro di Jerrum, che risponde all'esigenza di limitare il numero di generatori di un gruppo di permutazioni.

Nel quarto capitolo, ci occupiamo di insiemi minimali di generatori. Si può osservare che differenti insiemi di generatori minimali di G possono non avere lo stesso numero di elementi: un esempio è fornito dal gruppo additivo $\mathbb{Z}$ dei numeri interi.

Infatti, $\{1\}$ è un insieme minimale di generatori di $\mathbb{Z}$, ma lo è anche $\{m, n\}$, dove m ed n sono due qualsiasi interi primi tra loro. Infatti, per il Teorema di Bézout, esistono $a, b \in \mathbb{Z}$ tali che $1 = am + bn$ e quindi 1 appartiene al sottogruppo generato da a e b.

Consideriamo un gruppo finito G e denotiamo con $d(G)$ la cardinalità più piccola possibile di un insieme di generatori di G. Si può osservare come in algebra lineare il concetto di *base di uno spazio vettoriale* coincida con quello di insieme minimale di generatori. Seguendo questo parallelismo con l'algebra lineare, si pongono i seguenti tre quesiti:

- Tutti gli insiemi minimali di G hanno $d(G)$ elementi?
- Ciascun insieme di generatori di G contiene un sottoinsieme con $d(G)$ che a sua volta genera G?
- Se H è un sottogruppo di G, allora è vero che $d(H) \leq d(G)$?

Nel contesto dei gruppi finiti la risposta a queste domande è negativa. Infatti, consideriamo il gruppo simmetrico S_4: si ha che due insiemi minimali di generatori sono $\{(1\ 2), (2\ 3), (3\ 4)\}$ e $\{(1\ 2), (1\ 2\ 3\ 4)\}$. Questo esempio fornisce una risposta negativa alle prime due domande. Per quanto riguarda la terza domanda, consideriamo il sottogruppo H di S_n generato dalle trasposizioni $(1\ 2)(3\ 4)\ldots(2j-1\ 2j)\ldots$. Si può dimostrare che $d(H) = [n/2]$; $d(S_n) = 2$ e quindi per $n \geq 6$ si ha $d(H) \geq d(G)$.

Tuttavia, se si considerano gruppi finiti con ordine una potenza di un numero primo, la risposta alle tre domande diventa affermativa. In questo ambito, il principale risultato è il Teorema della Base di Burnside, descritto nel capitolo 4.

Capitolo 1

Risultati preliminari

1.1 Insiemi di generatori

Definizione 1.1. In un gruppo G, il sottoinsieme S di G è un insieme di generatori di G se ogni elemento $g \in G$ può essere scritto come prodotto di potenze di elementi appartenenti ad S:

$$g = x_1^{a_1} x_2^{a_2} \dots x_r^{a_r},$$

dove $x_i \in S$ e $a_i \in \mathbb{Z}$. In tal caso diciamo che S genera G e scriviamo $G = \langle S \rangle$.

Se G ha un insieme finito di generatori diciamo che G è un gruppo finitamente generato.

Possiamo scrivere le potenze che compaiono nella definizione precedente come copie ripetute dello stesso fattore o del suo inverso. Quindi:

Osservazione 1.2. *Un sottoinsieme S di G è un insieme di generatori di G quando ogni elemento di G è prodotto di elementi di S e di inversi di elementi di S.*

Definizione 1.3. Un gruppo G si dice ciclico se esiste un suo elemento g tale che $G = \langle g \rangle$.

Teorema 1.4. *Sia $H \leq G$ tale che $H = \langle S \rangle$, con S sottoinsieme di $H \subseteq G$. Allora H è l'intersezione di tutti i sottogruppi di G che contengono S.*

Dimostrazione. Sia L l'intersezione di tutti i sottogruppi di G che contengono S e sia $H = \langle S \rangle$. Dobbiamo mostrare che $H = L$. Se H è un sottogruppo di G che contiene S, allora si ha $L \subseteq H$. Sia K un generico sottogruppo di G che contiene S. Allora K contiene tutti gli elementi che si scrivono come prodotto di elementi di S e dei loro inversi. Quindi, $H \subseteq K$. Questa osservazione vale per un qualsiasi sottogruppo K di G che contiene S, dunque si può concludere che $H \subseteq L$ e segue la tesi. □

In altre parole $\langle S \rangle$ è il più piccolo sottogruppo di G che contiene il sottoinsieme S.

1.2 Azione di un gruppo su un insieme

Definizione 1.5. Dati un insieme $\Omega = \{\alpha, \beta, \ldots\}$ e un gruppo G, si dice che G agisce su Ω, o che Ω è un G-insieme, se esiste una funzione $\Omega \times G \longrightarrow \Omega$, tale che, denotando con α^g l'immagine della coppia (α, g), si abbia:

1. $\alpha^{gh} = (\alpha^g)^h$ per ogni $\alpha \in \Omega$; $g, h \in G$;
2. $\alpha^1 = \alpha$, dove 1 è l'elemento neutro di G.

Tale funzione si chiama azione di G su Ω e la cardinalità di Ω è detta grado dell'azione.

Utilizzando un linguaggio geometrico, chiameremo *punti* gli elementi di Ω.

Osservazione 1.6. *Sia $H \leq G$ e supponiamo che G agisca su Ω, allora anche H agisce su Ω tramite la restrizione a H dell'azione di G.*

Teorema 1.7. *Supponiamo che G agisca su Ω. La funzione $\varphi_g : \Omega \longrightarrow \Omega$ data da $\varphi_g(\alpha) = \alpha^g$ è, per ogni fissato $g \in G$, una permutazione di Ω.*

Dimostrazione.

- Mostriamo l'iniettività: $\alpha^g = \beta^g \Rightarrow (\alpha^g)^{g^{-1}} = (\beta^g)^{g^{-1}} \Rightarrow \alpha^{gg^{-1}} = \beta^{gg^{-1}} \Rightarrow \alpha^1 = \beta^1 \Rightarrow \alpha = \beta$. Si noti come abbiamo utilizzato entrambi i punti della definizione precedente.
- Mostriamo la suriettività: sia $\alpha \in \Omega$ e $\beta = \alpha^{g^{-1}}$; allora $\beta^g = \left(\alpha^{g^{-1}}\right)^g = \alpha^{g^{-1}g} = \alpha^1 = \alpha$.

□

Quindi, in base a questo teorema, se G è un gruppo che agisce su Ω, possiamo considerare l'applicazione $\varphi : G \longrightarrow S^\Omega$ ottenuta associando a ogni $g \in G$ la permutazione φ_g che essa induce.

Osservazione 1.8. *Tale corrispondenza è un omomorfismo di gruppi: al prodotto di due elementi di G, corrisponde il prodotto delle due permutazioni ad essi associate.*

Osservazione 1.9. *Il nucleo di φ è dato da:*

$$K = \{g \in G |\ \alpha^g = \alpha\ \forall \alpha \in\ \Omega\}$$

cioè dagli elementi di G, le cui permutazioni associate lasciano fisso ogni elemento di Ω.

È immediato verificare che K è un sottogruppo di G. Possiamo quindi dare la seguente definizione:

Definizione 1.10. Il sottogruppo $K = \{g \in G \mid \alpha^g = \alpha\ \forall \alpha \in \Omega\}$ si chiama nucleo dell'azione.

Definizione 1.11. Se $K = 1$, con 1 elemento neutro di G, l'azione è detta fedele.

Osservazione 1.12. *Se l'azione sul gruppo G è fedele, per il Primo Teorema di Omomorfismo, si ha che G è isomorfo ad un sottogruppo di S^Ω e pertanto G sarà detto un gruppo di permutazioni su Ω.*

Osservazione 1.13. *Se $K = G$, gli elementi di G fissano tutti gli elementi di Ω: l'azione è banale.*

Un elemento α di Ω determina due sottoinsiemi molto importanti: uno in Ω, detto *orbita* di α; l'altro in G, detto *stabilizzatore* di α.

1.2.1 Orbita

Definizione 1.14. L'orbita di α sotto l'azione di G si indica con α^G oppure con O_α, ed è il sottoinsieme:

$$\alpha^G = O_\alpha = \{\alpha^g |\ g \in G\}.$$

Ovvero è l'insieme degli elementi di Ω che sono immagine di α tramite l'azione di G.

La cardinalità di $|O_\alpha|$ è detta lunghezza dell'orbita.

Teorema 1.15. *Due orbite coincidono oppure sono disgiunte.*

Dimostrazione.

- Mostriamo che se $\beta \in O_\alpha$, allora $O_\beta = O_\alpha$.

  Per definizione esiste un elemento $g \in G$ tale che $\beta = \alpha^g$. Sia $h \in G$, allora: $\beta^h = (\alpha^g)^h = \alpha^{gh}$, quindi $O_\beta \subseteq O_\alpha$. Viceversa, sia $\alpha^k \in O_\alpha$ con $k \in G$ e posto $l = g^{-1}k$ si ha $\alpha^k = \alpha^{gl} = (\alpha^g)^l = \beta^l$. Dunque $O_\alpha \subseteq O_\beta$. Vale la doppia inclusione e quindi possiamo concludere che $O_\alpha = O_\beta$.

- Mostriamo che se O_β è diversa da O_α, allora $O_\alpha \cap O_\beta = \emptyset$. Per assurdo supponiamo che $\gamma \in O_\alpha \cap O_\beta$; allora, per quanto dimostrato nel punto precedente, $O_\gamma = O_\alpha$ e $O_\gamma = O_\beta$. In particolare si ha: $O_\alpha = O_\beta$, contro le ipotesi.

□

Infatti, le orbite altro non sono che le classi della relazione di equivalenza così definita:

$$\alpha \approx \beta \text{ se e solo se esiste } g \in G \text{ tale che } \alpha^g = \beta.$$

Se indichiamo con T l'insieme dei rappresentanti delle orbite, abbiamo che Ω è unione disgiunta di orbite:

$$\Omega = \bigcup_{\alpha \in T} O_\alpha.$$

In particolare, se Ω è finito, si ha:

$$|\Omega| = \sum_{\alpha \in T} |O_\alpha|.$$

1.2.2 Stabilizzatore

Definizione 1.16. Lo stabilizzatore di α si indica con $S_G(\alpha)$ oppure con G_α, ed è il sottoinsieme di G tale che:

$$S_G(\alpha) = G_\alpha = \{g \in G |\ \alpha^g = \alpha\}.$$

In altre parole lo stabilizzatore di α è l'insieme degli elementi di G che lasciano fisso α.

Lemma 1.17. *$S_G(\alpha)$ è un sottogruppo di G.*

Dimostrazione.

- Sia 1 l'elemento neutro di G; $\alpha^1 = \alpha$, quindi $\alpha \in S_G(\alpha)$;
- Se $x, y \in S_G(\alpha)$, allora $\alpha^{xy} = (\alpha^x)^y = \alpha^y = \alpha$, e dunque $xy \in S_G(\alpha)$;
- Sia $x \in S_G(\alpha)$, allora $\alpha = \alpha^1 = \alpha^{xx^{-1}} = (\alpha^x)^{x^{-1}} = \alpha^{x^{-1}}$, e dunque $x^{-1} \in S_G(\alpha)$.

□

Osservazione 1.18. *Se un elemento di G appartiene allo stabilizzatore di ogni elemento di Ω, allora appartiene al nucleo dell'azione e viceversa. Pertanto, il nucleo K dell'azione è l'intersezione degli stabilizzatori di tutti gli elementi di Ω:*

$$K = \bigcap_{\alpha \in \Omega} S_G(\alpha).$$

1.2.3 Relazione tra orbite e stabilizzatori

La relazione tra orbite e stabilizzatori è messa in evidenza dai seguenti due teoremi.

Teorema 1.19. *La cardinalità dell'orbita di un elemento α è uguale all'indice dello stabilizzatore di α:*

$$|O_\alpha| = [G : S_G(\alpha)].$$

In particolare, se G è finito:

$$|G| = |O_\alpha| \cdot |S_G(\alpha)|$$

quindi, la cardinalità di un orbita divide l'ordine del gruppo.

Dimostrazione. Dimostriamo che la seguente mappa

$$\begin{array}{rcl} \gamma : O_\alpha & \longrightarrow & \{S_G(\alpha)\, g \mid g \in G\} \\ \alpha^g & \longmapsto & S_G(\alpha)\, g \end{array}$$

è ben definita ed è una biezione. Consideriamo due elementi $g_1,\ g_2$ di G, si ha:

$$\alpha^{g_1} = \alpha^{g_2} \Leftrightarrow \alpha^{g_1 g_2^{-1}} = \alpha \Leftrightarrow g_1 g_2^{-1} \in\ S_G(\alpha) \Leftrightarrow g_1 \in S_G(\alpha)\, g_2.$$

Cioè $\alpha^{g_1} = \alpha^{g_2} \Leftrightarrow S_G(\alpha) g_1 = S_G(\alpha) g_2$. L'implicazione da sinistra dimostra che γ è ben posta; l'implicazione da destra che γ è iniettiva. Inoltre la funzione γ è suriettiva per costruzione, dunque è biettiva. Nel caso in cui G è un gruppo finito, applicando il Teorema di Lagrange, si ottiene $|G| = |O_\alpha| \cdot |S_G(\alpha)|$. □

Teorema 1.20. *Se β appartiene all'orbita di α, allora gli stabilizzatori di β e α sono coniugati, cioè se $\beta = \alpha^g$ allora $S_G(\beta) = (S_G(\alpha))^g$. In particolare si ha:*

$$S_G(\alpha^g) = (S_G(\alpha))^g$$

Dimostrazione. Sia $x \in S_G(\alpha)$, allora $(\alpha^g)^{g^{-1}xg} = (\alpha^x)^g = \alpha^g$, cioè $g^{-1}xg$ stabilizza $\alpha^g = \beta$. Pertanto $(S_G(\alpha))^g \subseteq S_G(\alpha^g) = S_G(\beta)$.

Viceversa, se $x \in S_G(\alpha^g)$, allora $(\alpha^g)^x = \alpha^g$, ovvero $gxg^{-1} \in S_G(\alpha)$ e quindi $x \in (S_G(\alpha))^g$ e $S_G(\alpha^g) = S_G(\beta) \subseteq (S_G(\alpha))^g$. □

Se α e β appartengono alla stessa orbita, allora per quanto osservato precedentemente $O_\alpha = O_\beta$, e dunque per il Teorema 1.19 si ha $[G : S_G(\alpha)] = |O_\alpha| = |O_\beta| = [G : S_G(\beta)]$. In altri termini i due stabilizzatori hanno lo stesso indice.

Corollario 1.21. *Supponiamo che Ω sia un insieme finito sul quale agisce il gruppo G. Sia Ω l'unione disgiunta delle orbite $O_1, O_2, \ldots, O_m$:*

$$\Omega = O_1 \cup O_2 \cup \ldots \cup O_m \text{ con } O_i \cap O_j = \emptyset \ \forall i \neq j.$$

Se $x_i \in O_i$ per $i = 1, 2, \ldots m$, allora $|\Omega| = \sum_{i=1}^{m} [G : S_G(x_i)]$.

1.2.4 Formula delle classi

L'esempio piú importante di automorfismo di gruppi è il coniugio. Sia $g \in G$ un elemento fissato. Allora il coniugio tramite g è l'applicazione $\varphi : G \to G$ definita da:

$$\varphi(x) = g^{-1}xg.$$

Essa è un automorfismo perchè è compatibile con l'operazione di G:

$$\varphi(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \varphi(x)\varphi(y).$$

Inoltre è una applicazione biettiva perchè ha una funzione inversa: il coniugio mediante g^{-1}.

Se il gruppo è abeliano, allora il coniugio è l'applicazione identica :

$$g^{-1}ag = ag^{-1}g = a.$$

Invece, se il gruppo non è commutativo, allora esiste qualche coniugio non banale.

Adesso applichiamo tutti i risultati analizzati fino ad ora al caso dell'azione di un gruppo finito su se stesso tramite coniugio. Più precisamente consideriamo l'azione:

$$G \times G \longrightarrow G$$
$$(g, \alpha) \longmapsto \alpha^g = g\alpha g^{-1}$$

Nel caso di questa azione particolare, le orbite e gli stabilizzatori degli elementi di G assumono dei nomi particolari:

Definizione 1.22. Si definisce classe di coniugio di α in G, l'orbita di α in G quando G agisce su se stesso tramite coniugio. La classe di coniugio di α si indica con $Cl(\alpha)$. Se S è un sottoinsieme di G e g un suo elemento si definisce il coniugato di S tramite g:

$$S^g = g^{-1}Sg = \{g^{-1}sg |\ s \in S\}\ .$$

In altri termini la classe di coniugio di α è l'insieme di tutti gli elementi della forma $g^{-1}\alpha g$. Tali elementi si dicono *coniugati* di α.

Definizione 1.23. Si definisce centralizzante di α in G, lo stabilizzatore di α quando G agisce su se stesso tramite coniugio. Il centralizzante di α si indica con $C_G(\alpha)$.

Scriviamo esplicitamente l'insieme $C_G(\alpha)$:

$$C_G(\alpha) = \{g \in G |\ \alpha^g = \alpha\} = \{g \in G |\ g\alpha g^{-1} = \alpha\} = \{g \in G |\ g\alpha = \alpha g\}.$$

Osservazione 1.24. *Dai risultati fin qui analizzati, segue immediatamente:*

$$|Cl(\alpha)| = [G : C_G(\alpha)].$$

Definizione 1.25. Sia S un sottoinsieme di G. Si definisce centralizzante di S in G, e si indica con $C_G(S)$, il sottogruppo $\{g \in G \mid gs = sg \text{ per ogni } s \in S\}$.

Definizione 1.26. Il centralizzante in G del gruppo G stesso è detto centro di G e si indica con $Z(G) = C_G(G)$.

Definizione 1.27. Sia S un sottoinsieme di G. Si definisce normalizzante di S in G e si indica con $N_G(S)$, il sottogruppo:

$$N_G(S) = \{g \in G |\ S^g = S\}.$$

Il corollario 1.21, nel caso dell'azione di un gruppo finito su se stesso tramite coniugio si traduce in :

Teorema 1.28. *Sia G un gruppo finito. Allora*

$$|G| = \textstyle\sum_{i=1}^{m} [G : C_G x_i]$$

dove gli x_i con $i = 1, 2, \ldots m$ sono i rappresentanti delle classi di coniugio (uno per ogni classe).

Tale teorema è noto come *equazione delle classi*.

Capitolo 2

Generatori del gruppo simmetrico

Definizione 2.1. Sia k un intero positivo, $2 \leq k \leq n$ e siano dati k elementi distinti $i_1, i_2 \dots i_k \in \{1, 2, \dots n\}$. Con la notazione $\alpha = (i_1\ i_2\ \dots\ i_k)$ si indica la permutazione $\alpha \in S_n$ tale che:

- $\alpha(i_r) = i_r$ se $i_r \notin \{i_1,\ i_2\ \dots,\ i_k\}$;
- $\alpha(i_r) = i_{r+1}$ se $1 \leq r \leq k-1$;
- $\alpha(i_k) = i_1$.

Tale permutazione è detta ciclo di lunghezza k.

Sia X l'insieme $\{1, 2 \dots, n\}$ e fissiamo una permutazione $\sigma \in S_n$. $\mathbb{Z}$ agisce su X nel seguente modo:

$$\begin{gathered} X \times \mathbb{Z} \longrightarrow X \\ (a, i) \mapsto a^i := \sigma^i(a) \end{gathered}$$

In particolare l'orbita di $a \in X$ è: $O_a = \{\sigma^i(a) \mid i \in \mathbb{Z}\}$.
Indicheremo la permutazione identica con σ^0.

Teorema 2.2. *Esiste un intero l tale che $O_a = \left\{\sigma^0(a), \sigma^1(a), \dots, \sigma^{l-1}(a)\right\}$.*

Dimostrazione. Per prima cosa osserviamo che O_a è contenuta in X, quindi ha un numero finito di elementi. Di conseguenza, esistono $i, j \in \mathbb{Z}$, $i > j$ tali che $\sigma^i(a) = \sigma^j(a)$. Pertanto:

$$\sigma^{-j+i}(a) = \sigma^{-j}(\sigma^i(a)) = a.$$

Poichè $i - j > 0$, l'insieme $\{n \in \mathbb{Z},\ n > 0 |\ \sigma^n(a) = a\}$ è non vuoto e possiede un minimo l. Dividiamo $i \in \mathbb{Z}$ per l: $i = lq + r$, dove q e r sono rispettivamente il quoziente e il resto della divisione. Dunque si ha:

$$\sigma^i(a) = \sigma^{ql+r}(a) = \sigma^r\left(\left(\sigma^l\right)^q(a)\right) = \sigma^r(a),$$

poichè $\sigma^l(a) = a$. Siccome $0 \leq r \leq l-1$, ciò prova che $O_a \subseteq \left\{\sigma^0(a), \dots, \sigma^{l-1}(a)\right\}$. L'altra inclusione è ovvia, quindi possiamo concludere la dimostrazione. □

Definizione 2.3. Il ciclo $\left(\sigma^0(a), \sigma^1(a), \ldots, \sigma^{l-1}(a)\right)$ si dice ciclo associato all'orbita di a sotto l'azione di σ. Al variare di a in X, i cicli associati alle orbite di a sotto l'azione di σ sono detti cicli di σ.

Definizione 2.4. Si dice supporto di una permutazione l'insieme degli elementi che essa non lascia fissi.

Teorema 2.5. *Ogni permutazione è uguale al prodotto dei suoi cicli, in qualsiasi ordine.*

Dimostrazione. Sia $\sigma \in S_n$. Scriviamo $X = \{1, 2, \ldots, n\}$ come unione disgiunta delle orbite $\Omega_1, \ldots, \Omega_k$ associate all'azione di $\mathbb{Z}$ su X tramite σ. Supponiamo che $\Omega_1, \ldots \Omega_r$ siano orbite costituite da più di un elemento e siano $\gamma_1, \ldots, \gamma_r$ i cicli corrispondenti a tali orbite. Osserviamo che nel prodotto $\gamma_1 \ldots \gamma_r$ è indifferente l'ordine dei fattori perchè i cicli sono disgiunti. Sia $a \in X$.

- Se a è lasciato fisso da σ, allora non appartiene al suo supporto e quindi non appartiene a nessuna orbita $\Omega_1, \ldots, \Omega_r$. Pertanto a è lasciato fisso da ciascun ciclo $\gamma_1, \ldots, \gamma_r$:

$$(\gamma_1 \gamma_2 \ldots \gamma_r)(a) = a = \sigma(a).$$

- Supponiamo che a appartenga al supporto di σ. Allora a è in una delle orbite $\Omega_1, \ldots, \Omega_r$. Poichè l'ordine dei fattori è indifferente, possiamo supporre $a \in \Omega_r$, quindi, $\gamma_r(a) = \sigma(a)$. Inoltre, $a \notin \Omega_1, \Omega_2, \ldots, \Omega_{r-1}$, cioè $\gamma_i(a) = a$ per ogni $i = 1, 2, \ldots, r-1$. Pertanto:

$$(\gamma_1 \ldots \gamma_r)(a) = ((\gamma_1 \ldots \gamma_{r-1})\gamma_r)(a) = \gamma_r(a) = \sigma(a).$$

Abbiamo così provato che, per ogni $a \in X$, $\gamma_1 \ldots \gamma_r(a) = \sigma(a)$, cioè:

$$\sigma = \gamma_1 \ldots \gamma_r.$$

□

Teorema 2.6. *Per $n \geq 2$, S_n è generato dalle sue trasposizioni (cicli di lunghezza 2).*

Dimostrazione. È ovvio per $n = 2$. Per $n \geq 3$, osserviamo che $(1) = (1\ 2)^2$ e ogni ciclo di lunghezza maggiore di 2 è prodotto di trasposizioni:

$$(i_1\ i_2 \ldots i_k) = (i_1\ i_2)(i_2\ i_3) \ldots (i_{k-1}\ i_k).$$

Inoltre, per il Teorema 2.5 ogni permutazione in S_n è prodotto di cicli, quindi i cicli generano S_n e poichè i prodotti di trasposizioni producono cicli, possiamo concludere che le trasposizioni generano S_n. □

Il numero totale delle trasposizioni di S_n è : $\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$, quindi S_n ha un insieme di generatori con un numero di elementi che è dell'ordine di grandezza di n^2. Mostreremo come tale numero possa essere ridotto a $n-1$.

Teorema 2.7. *Per $n \geq 2$, S_n è generato dalle n-1 trasposizioni* $(1\ 2)\,(1\ 3)\ldots(1\ n)$.

Dimostrazione. Il teorema è ovvio per $n = 2$. Occorre mostrare che ogni trasposizione in S_n si può scrivere come prodotto di trasposizioni che coinvolgono 1. Per la trasposizione $(i\ j)$ con $i,\ j \neq 1$, si ottiene : $(i\ j) = (1\ i)\,(1\ j)\,(1\ i)$. □

Teorema 2.8. *Per $n \geq 2$, S_n è generato dalle n-1 trasposizioni:*

$$(1\ 2)\,(2\ 3)\,(3\ 4)\ldots\ (n-1\ n).$$

Dimostrazione. È sufficiente mostrare che ogni trasposizione $(a\ b)$ in S_n è prodotto di trasposizioni della forma $(i\ i+1)$ con $i < n$. Poichè $(a\ b) = (b\ a)$, senza perdere di generalità possiamo supporre $a < b$.
Procediamo per induzione su $b-a$: se $b-a = 1$ allora $(a\ b) = (a\ a+1)$; se $b-a = k > 1$ e supponiamo vero il teorema per tutte le trasposizioni i cui elementi differiscono per meno di k elementi, allora $(a\ b) = (a\ a+1)\,(a+1\ b)\,(a\ a+1)$. La prima e la terza trasposizione sono della forma desiderata; la seconda trasposizione permuta una coppia di interi con differenza $b-(a+1) = k-1 < k$. Per ipotesi induttiva $(a+1\ b)$ è prodotto di trasposizioni della forma $(i\ i+1)$ e dunque segue il risultato. □

Lemma 2.9. *Per un k-ciclo $(i_1\ i_2\ldots i_k)$ in S_n e per ogni $\sigma \in S_n$ si ha:*

$$\sigma^{-1}\,(i_1\ i_2\ldots i_k)\,\sigma = (\sigma\,(i_1)\ \ \sigma\,(i_2)\ldots\sigma\,(i_k))\ .$$

Dimostrazione. Occorre mostrare che entrambi i membri dell'equazione hanno lo stesso effetto sui numeri interi da 1 a n. Per un intero da 1 a n della forma $\sigma\,(i_r)$, con $1 \leq r < k$, il membro a sinistra dell'equazione agisce nel seguente modo:

$$\sigma\,(i_r) \mapsto i_r \mapsto i\,(r+1) \mapsto \sigma\,(i_{r+1}).$$

Il membro a destra dell'equazione manda $\sigma\,(i_r)$ in $\sigma\,(i_{r+1})$. Lo stesso ragionamento mostra che entrambi i membri del'equazione mandano $\sigma\,(i_k)$ in $\sigma\,(i_1)$:

$$\sigma\,(i_k) \mapsto i_k \mapsto i_1 \mapsto \sigma\,(i_1)$$

$$\sigma\,(i_k) \mapsto \sigma\,(i_1).$$

Un intero l con $1 \leq l \leq n$ che non appartiene a $\{\sigma\,(i_1)\ldots\sigma\,(i_k)\}$ non fa parte del ciclo a destra e quindi è un punto fisso di tale ciclo. Dimostriamo che l è un punto fisso anche del ciclo $\sigma^{-1}\,(i_1\ i_2\ldots i_k)\,\sigma$. Poichè $l \notin \{\sigma\,(i_1)\ldots\sigma\,(i_k)\}$, si ha che $\sigma^{-1}\,(l) \notin \{i_1,\ldots,i_k\}$; quindi il ciclo $(i_1\ldots i_k)$ fissa $\sigma^{-1}\,(l)$; infine applicando σ a $\sigma^{-1}\,(l)$ otteniamo l. □

Teorema 2.10. *Per $n \geq 2$, S_n è generato da $(1\ 2)$ e dall' n-ciclo $(1\ 2\ 3 \dots n)$.*

Dimostrazione. È sufficiente mostrare che $(1\ 2)\,(1\ 2\ 3 \dots n)$ può essere scritto sotto forma di prodotto di trasposizioni del tipo $(i\ i+1)$. Dimostriamolo per $n \geq 3$. Poniamo $\sigma = (1\ 2\ 3 \dots n)$ e applichiamo il Lemma 2.9: $\sigma^{-1}\,(1\ 2)\,\sigma = (\sigma\,(1)\ \sigma\,(2)) = (2\ 3)$ e più generalmente per $k = 1, 2, 3, \dots n-2$ si ottiene $\sigma^{-k}\,(1\ 2)\,\sigma^k = \left(\sigma^k\,(1)\ \sigma^k\,(2)\right) = (k+1\ k+2)$. □

Corollario 2.11. *Per $n \geq 2$, S_n è generato da $(1\ 2)$ e dall' $(n-1)$-ciclo $(2\ 3 \dots n)$.*

Dimostrazione. Dopo aver osservato che $(1\ 2\ \dots n) = (1\ 2)\,(2\ 3 \dots n)$, il risultato segue immediatamente dal teorema precedente. □

Studiamo con maggiore attenzione il caso in cui un sistema di generatori di S_n è costituito da trasposizioni (Teorema 2.6). Abbiamo bisogno di alcune definizioni preliminari della teoria dei grafi.

2.1 Grafi

In questo elaborato, considereremo solo grafi non orientati privi di cappi, che chiameremo semplicemente *grafi*.

Definizione 2.12. Un grafo Γ è una coppia di insiemi (V, E):

- V è l'insieme dei vertici;
- E è l'insieme dei lati che connettono i vertici e i suoi elementi sono sottoinsiemi di V di cardinalità 2.

Usiamo la seguente terminologia:

- due vertici u e v sono gli *estremi* del lato $\{u, v\}$;
- due lati sono *adiacenti* se hanno un estremo in comune;
- due vertici u e v sono *adiacenti* se connessi da un lato, cioè se $\{u, v\}$ appartiene ad E;
- un vertice v è *isolato* se non ci sono lati che hanno v come vertice;
- un vertice è *finale* se appartiene ad un solo lato.

Definizione 2.13. Un cammino nel grafo $\Gamma = (V, E)$ è una sequenza finita di vertici alternati a lati di Γ:

$$v_{i_0}, e_{j_1}, v_{i_1}, e_{j_2}, \ldots, e_{j_k}, v_{i_k}.$$

Un cammino inizia con un vertice. I vertici $v_{i_{t-1}}$ e v_{i_t} sono i vertici di e_{j_t} per $t = 1, 2, \ldots k$; v_{i_0} è il vertice iniziale, v_{i_k} è il vertice finale; k è la lunghezza del cammino. Un cammino di lunghezza 0 è costituito da un solo vertice v_{i_0}.

Definizione 2.14. Un cammino è aperto se $v_{i_0} \neq v_{i_k}$, altrimenti è un ciclo.

Il cammino che inizia in u e termina in v è detto *cammino u-v*.

Definizione 2.15. I vertici u e v sono connessi se c'è un cammino u-v nel grafo. Un grafo è connesso se tutti i suoi vertici sono connessi tra loro.

Definizione 2.16. Il sottografo Γ_1 di Γ è una componente connessa di Γ se: Γ_1 è connesso e nessun vertice di Γ_1 è connesso a vertici di Γ che non sono in Γ_1.

Definizione 2.17. Una foresta è un grafo senza cicli.

Definizione 2.18. Un albero è una foresta connessa.

2.2 Relazione tra grafi e gruppo simmetrico

Consideriamo il gruppo simmetrico S_n e sia S un insieme di trasposizioni, $S \subseteq S_n$.

Indichiamo con $\Gamma(S) = (V, E)$ il grafo associato ad S costruito nel seguente modo:

- l'insieme dei vertici V è $\{1, 2, \ldots n\}$;
- $\{i, j\}$, con i, j appartenenti a V, è un lato del grafo se e solo se la trasposizione $(i\ j)$ è in S.

Teorema 2.19. *Se S genera S_n, allora il grafo associato $\Gamma(S)$ è connesso.*

Dimostrazione. Siano i e j due vertici di $\Gamma(S)$. Poichè S genera S_n, esiste una permutazione α appartenente a $\langle S \rangle$ tale che $\alpha(i) = j$. Inoltre, α può essere scritta come prodotto di trasposizioni: $\alpha = \tau_1 \ldots \tau_k$, con $k \in \mathbb{N}$. Se $(i\ j) \in \{\tau_1, \ldots \tau_k\}$, allora esiste un lato di $\Gamma(S)$ che connette i e j. Se $(i\ j) \notin \{\tau_1, \ldots, \tau_k\}$, poichè $\tau_1 \ldots \tau_k(i) = j$, nell'insieme $\{\tau_1, \ldots \tau_k\}$ ci devono essere necessariamente trasposizioni della forma:

$$(i\ a), (a\ b), (b\ c), \ldots, (s\ v), (v\ j).$$

Ciò equivale a dire che in $\Gamma(S)$ c'è un cammino che connette i e j. Quest'ultimi sono vertici arbitrari, dunque, si ha che $\Gamma(S)$ è connesso. □

Teorema 2.20. *Sia Γ un grafo privo di cicli, con n vertici. Allora Γ ha al più $n - 1$ lati.*

Dimostrazione. Dimostriamo il teorema per induzione su n. Per $n = 2$, si può costruire al più un lato, quindi il teorema è verificato. Supponiamo il teorema vero per un grafo privo di cicli con n vertici e dimostriamolo per un grafo con $n+1$ vertici. Poichè il grafo non ha cicli, ci sarà almeno un lato $\{a, b\}$ che costituisce il lato finale di un cammino massimale. Eliminiamo il vertice b e il lato $\{a, b\}$. Otteniamo un grafo senza cicli su n vertici, che per ipotesi induttiva ha al più $n-1$ lati. Pertanto il nostro grafo originario ha al più n lati, perchè bisogna aggiungere agli $n-1$ lati, il lato $\{a, b\}$, che avevamo eliminato in precedenza. □

Corollario 2.21. *Se Γ è un albero con n vertici, allora Γ ha $n-1$ lati.*

Dimostrazione. Poichè Γ non ha cicli, per il Teorema 2.20, ha al più $n-1$ lati. Inoltre, Γ è connesso, pertanto, deve avere almeno $n-1$ lati che collegano gli n vertici. □

Teorema 2.22. *Se $\Gamma(S)$ è un albero, allora il prodotto degli elementi di S, in qualsiasi ordine, è un ciclo.*

Dimostrazione. Procediamo per induzione su n. Se $n = 2$ il risultato è ovvio. Supponiamo vera la tesi per n. Sia $S = \{t_1, t_2, \ldots, t_{n-1}\}$ con t_i trasposizioni sull'insieme $\{1, 2, \ldots, n\}$ e sia $\alpha = t_1 \ldots t_{n-1}$ con $t_{n-1} = (a\ b)$. Rimuovendo il lato $\{a, b\}$ da $\Gamma(S)$, otteniamo due componenti connesse di $\Gamma(S)$ che indichiamo con A e B. Possiamo scrivere $t_1 \ldots t_{n-1}$ come prodotto del tipo $\alpha_1 \ldots \alpha_r \beta_{r+1} \ldots \beta_{n-2} t_{n-1}$, con α_i lati di A e β_i lati di B, poichè $\alpha_i \beta_j = \beta_j \alpha_i$ per ogni i e j. Per ipotesi induttiva $\alpha_1 \ldots \alpha_r$ è un ciclo $(i_1\ \ldots\ i_{r+1})$ e possiamo supporre $a = i_{r+1}$. Analogamente, $\beta_{r+1} \ldots \beta_{n-2}$ è un ciclo $(j_1\ \ldots\ j_{k-1})$ e possiamo supporre $b = j_{k-1}$. Si può notare, inoltre, che i due cicli $(i_1\ \ldots\ i_{r+1})$ e $(j_1\ \ldots\ j_{k-1})$ sono disgiunti. Allora, si ottiene :

$$(i_1\ \ldots\ i_r\ a)\,(j_1\ \ldots\ j_{k-2}\ b)\,(a\ b) = (i_1\ \ldots\ i_r\ b\ j_1\ \ldots\ j_{k-2}\ a),$$

che è un ciclo di lunghezza n. □

Teorema 2.23. *Se $\Gamma(S)$ è un albero, allora S genera S_n.*

Dimostrazione. Procediamo per induzione su n. Se $n = 2$, allora la permutazione $(1\ 2)$ è in S e $S_2 = \langle (1\ 2) \rangle$. Supponiamo la tesi vera per $n-1$. Rinominiamo i vertici dell'albero in modo che n sia un vertice finale e sia $\{n, i\}$ il lato che contiene n. Eliminiamo da S la trasposizione $(i\ n)$. Ciò equivale ad eliminare da $\Gamma(S)$ il lato $\{i, n\}$: otteniamo, così, un albero Γ_1 (con insieme dei vertici $\{1, 2, \ldots, n-1\}$) ed un vertice isolato n. Per ipotesi induttiva, il sottogruppo U generato da $S \setminus \{(i\ n)\}$ è S_{n-1}. Quindi, $(1\ 2)\,(1\ 3) \ldots (1\ n-1) \in U \subseteq \langle S \rangle$. Inoltre, $(1\ n) \in \langle S \rangle$ e pertanto $(1\ i)\,(i\ n) = (1\ n)$ è in S. Per il Teorema 2.7, si ha che S genera S_n. □

Lemma 2.24. *Se Γ è un grafo connesso con insieme finito di vertici V, allora ha almeno un sottografo che è un albero ed il cui insieme di vertici coincide con V.*

Dimostrazione. Se Γ è un albero, il teorema è verificato. Se Γ non è un albero, allora ha almeno un ciclo. Consideriamo un ciclo ed elimiamo un suo lato: si ottiene un grafo connesso Γ_1 che ha gli stessi vertici di Γ e un lato in meno. Se Γ_1 è un albero il teorema è verificato; altrimenti, ripetendo il procedimento, dopo un numero finito di passi, si ottiene un sottografo che è un albero. □

Teorema 2.25. *Se $\Gamma(S)$ è connesso, allora S genera S_n.*

Dimostrazione. Se $\Gamma(S)$ è connesso, allora, per il Lemma 2.24, contiene un albero. Siano $t_1, t_2, \ldots, t_{n-1}$ i lati dell'albero. Per il Teorema 2.23, $t_1, t_2, \ldots, t_{n-1}$ generano S_n. In particolare, si ha che S_n è contenuto in $\langle S \rangle$, da cui segue che $\langle S \rangle = S_n$. □

Teorema 2.26. *Se $\Gamma(S)$ è un albero, allora S è un insieme di generatori minimale di S_n.*

Dimostrazione. Se $\Gamma(S)$ è un albero, in particolare è connesso e quindi per il teorema precedente si ha $S_n = \langle S \rangle$. Inoltre, $\Gamma(S)$ non ha cicli, il che equivale a dire che se si elimina un solo lato si creano due componenti connesse e dunque, per il Teorema 2.19, non abbiamo un sistema di generatori di S_n. Pertanto, S è un insieme minimale di generatori. □

Teorema 2.27. *Se S è un insieme minimale di generatori per S_n, allora $\Gamma(S)$ è un albero.*

Dimostrazione. Poichè S genera S_n, per il Teorema 2.19, $\Gamma(S)$ è connesso. Quindi, se per assurdo $\Gamma(S)$ non è un albero, allora contiene un sottografo che è un albero, con insieme dei lati $\{t_1, t_2, \ldots, t_{n-1}\}$. Per il Teorema 2.23, $S_n = \langle t_1, \ldots, t_{n-1} \rangle$, cioè S non è un insieme minimale di generatori. □

Combinando il Corollario 2.21 e il Teorema 2.27, si ottiene che un insieme minimale di generatori di S_n è costituito da $n-1$ trasposizioni.

Capitolo 3

Basi di gruppi di permutazioni

Per risolvere problemi computazionali con i gruppi di permutazioni, occorre prestare molta attenzione alla giusta scelta della rappresentazione di tali gruppi. In particolare, in molti casi è utile costruire una catena decrescente di sottogruppi, nella quale ogni sottogruppo è lo stabilizzatore di un punto nel precedente.

Un insieme contenente generatori per ogni sottogruppo della catena è detto insieme forte di generatori e una particolare sequenza di punti dell'insieme sul quale agisce il gruppo è detta base. Questi concetti sono stati utilizzati per la prima volta dal matematico Charles Sims (1938-2017).

Dato un gruppo descritto dalle permutazioni che lo generano, l'algoritmo di Schreier-Sims costruisce una sua base e un suo insieme forte di generatori. L'algoritmo è stato descritto da Sims nel 1970 e utilizza il Lemma di Schreier per calcolare un insieme di generatori per gli stabilizzatori (da qui deriva il nome dell'algoritmo).

Nel corso degli anni sono state realizzate diverse varianti per rendere l'algoritmo più efficiente.

3.1 Catene di sottogruppi

Sia G un gruppo finito.

Definizione 3.1. Una catena di sottogruppi di G è una sequenza della forma:

$$G = G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(k)} \geq G^{(k+1)} = 1.$$

Se abbiamo una catena di sottogruppi, allora consideriamo per $i = 1, 2, \ldots, k$ un insieme $U^{(i)}$ formato dai rappresentanti delle classi laterali destre di $G^{(i+1)}$ in $G^{(i)}$. Mostriamo per induzione su $k - i$ che ogni elemento di G può essere scritto come prodotto di elementi u_i in $U^{(i)}$, con $i = 1, \ldots, k$. Un elemento g di G è contenuto in esattamente un laterale di $G^{(2)}$ in $G^{(1)}$, quindi $g = h \cdot u_1$ con h appartenente a $G^{(2)}$ e u_1 in $U^{(1)}$.

Per induzione abbiamo:

$$h = u_k \dots u_2,$$

dove ciascun u_i appartenente a $U^{(i)}$ è univocamente determinato da g, quindi $g = u_k \cdot u_{k-1} \cdot \ldots \cdot u_1$.

Scrivere ogni elemento di un gruppo in modo unico come prodotto di fattori della forma appena descritta, permette di risolvere molti problemi computazionali della teoria dei gruppi. I più importanti sono:

- trovare l'ordine di un gruppo;
- fare una lista degli elementi del gruppo senza ripetizioni;
- generare elementi casuali del gruppo;
- testare l'appartenenza di un elemento ad un gruppo.

Infatti, l'ordine di G è il prodotto delle cardinalità degli insiemi dei rappresentanti dei laterali. Possiamo creare una lista di elementi del gruppo senza ripetizioni, considerando tutti i termini della forma $u_k \cdot u_{k-1} \cdot \ldots \cdot u_1$, con $u_i \in U^{(i)}$. Un elemento casuale del gruppo può essere costruito prendendo un elemento casuale u_i da ogni $U^{(i)}$, per $i = 1, \dots, k$ e moltiplicando tali elementi in modo che l'ordine degli indici sia decrescente. Infine, se una permutazione può essere riscritta nella forma $u_k \cdot u_{k-1} \cdot \ldots \cdot u_1$, allora appartiene al gruppo; altrimento no.

3.2 Basi ed insiemi forti di generatori

Sia G un gruppo di permutazioni su un insieme Ω. Consideriamo l'azione di G su Ω e sia β un elemento di Ω. Nel Capitolo 1 abbiamo definito lo stabilizzatore di β in G nel seguente modo:

$$G_\beta = \{g \in G \,|\, \beta^g = \beta\}.$$

Allora, per induzione possiamo dare la seguente definizione:

Definizione 3.2. Siano $\beta_1, \beta_2, \dots, \beta_i$ elementi di Ω. Poniamo:

$$G_{\beta_1,\beta_2,\dots,\beta_i} = \left(G_{\beta_1,\beta_2,\dots,\beta_{i-1}}\right)_{\beta_i} = \left\{g \in G \mid \beta_j^g = \beta_j \text{ per } j = 1, 2, \dots, i\right\}$$

Possiamo ora definire il concetto di base e quello di catena di sottogruppi ad essa associata:

Definizione 3.3. Una base di G è una sequenza finita $B = [\beta_1, \beta_2, \dots, \beta_k]$ di punti distinti di Ω tali che $G_{\beta_1,\beta_2,\dots,\beta_k} = 1$.

Dunque, l'unico elemento di G che fissa tutti i punti $\beta_1, \beta_2, \dots, \beta_k$ è l'identità.

Osservazione 3.4. *Ogni gruppo di permutazioni ha una base, ma non tutte le basi di un dato gruppo hanno la stessa cardinalità. Ad esempio,* $G = \langle (1\ 2), (3\ 4) \rangle$ *ha come base* $[2, 4]$ *oppure* $[1, 3, 4]$.

Se poniamo $G = G^{(1)}$ e $G^{(i)} = G_{\beta_1,\beta_2,\ldots,\beta_{i-1}}$, allora abbiamo una catena di stabilizzatori:

$$G = G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(k)} \geq G^{(k+1)} = 1.$$

Spesso è richiesto che una base abbia la seguente proprietà addizionale: $G^{(i)} \neq G^{(i+1)}$.

È utile avere un insieme di generatori di G per ogni sottogruppo della catena di stabilizzatori.

Definizione 3.5. Un insieme forte di generatori di un gruppo di permutazioni G che rispetta la base $B = [\beta_1, \beta_2, \ldots, \beta_k]$ è un insieme S di elementi del gruppo tali che per $i = 1, 2, 3, \ldots, k$ si ha:

$$G^{(i)} = \left\langle S \cap G^{(i)} \right\rangle.$$

Si può notare che $S \cap G^{(i)}$ è l'insieme degli elementi in S che fissano $\beta_1, \beta_2, \ldots \beta_{i-1}$. Per allegerire la notazione scriveremo $S^{(i)}$ al posto di $S \cap G^{(i)}$.

Esempio 3.6. Il gruppo simmetrico S_n ha per base $[1, 2, \ldots, n-1]$ ed insieme forte di generatori $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$.

Esempio 3.7. Consideriamo il gruppo $G = S_4$ che agisce sull'insieme $\{1, 2, 3, 4\}$. Una sua base è $B = [1, 2, 3]$; la corrispondente catena è :

$$G^{(1)} = \mathrm{Sym}(\{1, 2, 3, 4\}) \geq G^{(2)} = \mathrm{Sym}(\{2, 3, 4\}) \geq G^{(3)} = \mathrm{Sym}(\{3, 4\}) \geq G^{(4)} = 1.$$

Gli insiemi $S = \{(1, 2, 3, 4), (3, 4)\}$ e $T = \{(1, 2, 3, 4), (2, 3, 4), (3, 4)\}$ generano G, ma S non è un insieme forte di generatori relativo a B, perchè $\left\langle S \cap G^{(2)} \right\rangle = \mathrm{Sym}(\{3, 4\})$ che è diverso da $G^{(2)} = \mathrm{Sym}(\{2, 3, 4\})$. Invece, T è un insieme forte di generatori rispetto a B.

3.3 Orbite di base e funzione di rappresentazione

Sia G un gruppo che agisce sull'insieme Ω, sia β un elemento di Ω e sia β^G la sua orbita. Nel Capitolo 1 abbiamo mostrato che $\left|\beta^G\right| = [G\ :\ G_\beta]$.

Si può osservare che se abbiamo una funzione u definita da β^G in G tale che:

$$\beta^{u(\gamma)} = \gamma \text{ e } u(\beta) = e,$$

allora la sua immagine è un insieme dei rappresentanti delle classi laterali di G_β. Chiamiamo l'applicazione u così definita *funzione di rappresentazione*. Si può notare che il rappresentante di $G_\beta h$ è $u\left(\beta^h\right)$.

Supponiamo che G abbia per base $B = [\beta_1, \beta_2, \ldots, \beta_k]$.

Definizione 3.8. Per $i = 1, 2, \ldots, k$, l' i-esima orbita di base, denotata con $\Delta^{(i)}$, è $\beta_i^{G^{(i)}}$ e l'i-esimo indice di base è la lunghezza dell'orbita i-esima.

Dai risultati sulla relazione tra orbite e stabilizzatori analizzati nel Capitolo 1, segue che c'è una corrispondenza biunivoca tra i-esima orbita di base e l'insieme dei rappresentanti di $G^{(i+1)}$ in $G^{(i)}$. In particolare:

$$\left|\Delta^{(i)}\right| = \left[G^{(i)} \ : \ G^{(i+1)}\right].$$

3.4 Algoritmo di Schreier-Sims

Sia G un gruppo di permutazioni su un insieme finito $\Omega = \{1, 2, \ldots, n\}$ e sia $\{g_1, g_2 \ldots, g_n\}$ un insieme di generatori di G. Descriviamo l'algoritmo di Schreier-Sims che ci permetterà di calcolare una base e un insieme forte di generatori di G. Una componente chiave di tale algoritmo è il seguente teorema, noto come *Lemma di Schreier*.

Teorema 3.9. *Siano G un gruppo e $X = \{g_1, g_2, \ldots, g_r\}$ un insieme di generatori di G. Sia H un sottogruppo di G di ordine n e sia $U = \{x_1, x_2, \ldots, x_n\}$ un insieme dei rappresentanti delle classi laterali di H in G, con $x_1 = 1$ in quanto rappresentante di H. Sia $\overline{g}$ il rappresentante del laterale Hg. Allora:*

$$H = \left\langle x_i g_j \left(\overline{x_i g_j}\right)^{-1} \ \textit{con} \ 1 \leq i \leq n, \ 1 \leq j \leq r \right\rangle.$$

Dimostrazione. Riportiamo la dimostrazione di Hall (1959).

Ogni elemento h di H può essere scritto nella forma $y_1 \cdot y_2 \cdot \ldots y_l$, dove ogni y_i, o il suo inverso, è in X. Sia $u_0 = e$ e $u_i = \overline{y_1 \cdot y_2 \cdot \ldots \cdot y_i}$ per $i = 1, 2, \ldots, l$. Allora $u_l = \overline{h} = e$, dunque:

$$h = u_0 \cdot h \cdot u_l^{-1} =$$
$$= \left(u_0 \cdot y_1 \cdot u_1^{-1}\right) \cdot \left(u_1 \cdot y_2 \cdot u_2^{-1}\right) \cdot \ldots \cdot \left(u_{l-1} \cdot y_l \cdot u_l^{-1}\right).$$

Consideriamo $u_{i-1} \cdot y_i \cdot u_i^{-1}$, per $i = 1, 2, \ldots, l$. Poichè $Hy_1y_2 \ldots y_i = Hu_{i-1}y_i$, si ha:

$$u_i = \overline{y_1 \cdot y_2 \cdot \ldots y_i} = \overline{u_{i-1} \cdot y_i}.$$

Sia $u = u_{i-1} \in U$ e $y = y_i$. Possiamo scrivere:

$$u_{i-1} \cdot y_i \cdot u_i^{-1} = u \cdot y \cdot \left(\overline{u \cdot y}\right)^{-1}.$$

Abbiamo ottenuto la forma desiderata se y appartiene ad X; altrimenti sia $y = x^{-1}$ per qualche x appartenente ad X e sia $v = \overline{u \cdot x^{-1}}$ appartenente ad U. Poichè $Hvx = Hux^{-1}x$, abbiamo che $\overline{v \cdot x} = u$ e dunque, l'inverso di $u \cdot y \cdot (\overline{u \cdot y})^{-1}$ può essere scritto come:

$$\overline{u \cdot x^{-1}} \cdot x \cdot u^{-1} = v \cdot x \cdot (\overline{v \cdot x})^{-1},$$

che ha la forma desiderata. □

I generatori di H dati da questo teorema sono chiamati *generatori di Schreier*. L'algoritmo di Schreier-Sims può essere esposto attraverso due passi.

Passo 1:

Sia α_1 un elemento di Ω. Calcoliamo la sua orbita applicando ad α_1 ripetutamente i generatori $g_1, g_2, \ldots, g_n$. Ad esempio, se $n = 4$ e $G = \langle g_1, g_2 \rangle$, con $g_1 = (1,2)(3,4)$ e $g_2 = (1,2,3)$. Prendiamo $\alpha_1 = 1$ ed otteniamo: $2 = 1^{g_1}$, $3 = 2^{g_2}$, $4 = 3^{g_1}$. Dunque, $1^G = \{1,2,3,4\}$.

Possiamo memorizzare l'orbita di α_1 attraverso un vettore che costruiamo nel modo seguente:

- nella posizione α_1 del vettore inseriamo il marcatore $*$;
- se β appartiene all'orbita di α_1, allora $\beta = \alpha^g$ con $g \in G$. Poichè $\{g_1, g_2, \ldots, g_n\}$ è un sistema di generatori di G, scriviamo g come prodotto di elementi di $\{g_1, g_2, \ldots, g_n\}$ e inseriamo tale prodotto nella posizione β del vettore;
- se β non appartiene all'orbita di α_1, in posizione β del vettore inseriamo il marcatore $\circ$.

Ad esempio, nel caso precedente otteniamo: $(*,\ g_1,\ g_1g_2,\ g_1g_2g_1)$. Il vettore così costruito prende il nome di *vettore di Schreier* e contiene informazioni complete riguardanti l'orbita di un elemento di Ω.

Passo 2:

Dopo aver calcolato l'orbita $\Delta^{(1)}$ di α_1 in G, costruiamo l'insieme U_1 dei rappresentanti delle classi laterali di $G^{(1)} := G_{\alpha_1}$ in G. Applichiamo il Teorema 3.9, con $U = U_1$, $X = \{g_1, \ldots, g_n\}$, $H = G^{(1)}$: troviamo un insieme di generatori di $G^{(1)}$ che chiamiamo W_1. Scegliamo $\alpha_2 \in \Omega$ che non è fissato dagli elementi di W_1 e ripetiamo i due passi.

L'algoritmo, quindi, procede ricorsivamente: analizziamo un generico passo della procedura. Supponiamo di aver costruito una base parziale $\alpha_1, \ldots, \alpha_{i-1}$ con le corrispondenti catene di sottogruppi $G = G^{(0)} \geq G^{(1)} \geq \ldots \geq G^{(i-1)}$, le orbite di base $\Delta^{(1)}, \ldots, \Delta^{(i-1)}$, gli insiemi di rappresentanti delle classi laterali $U_1, \ldots, U_{i-1}$ e un insieme di generatori W_{i-1} di $G^{(i-1)}$. Se $W_{i-1} = \emptyset$, allora l'algoritmo termina; se $W_{i-1} \neq \emptyset$, scegliamo $\alpha_i \in \Omega$ che non è fissato dagli elementi di W_{i-1}. Seguendo quanto descritto dal passo

1, calcoliamo l'orbita $\Delta^{(i)}$ di α_i in $G^{(i-1)}$. Costruiamo l'insieme U_i dei rappresentanti di $G^{(i)} := \left(G^{(i-1)}\right)_{\alpha_i}$ in $G^{(i-1)}$. Procediamo con il passo 2 e calcoliamo l'insieme di generatori W_i di $G^{(i)}$.

Quando l'algoritmo termina, dunque, fornisce :

1. una base $[\alpha_1, \ldots, \alpha_m]$;
2. un insieme forte di generatori $U = U_1 \cup \ldots \cup U_m$.

3.4.1 Applicazioni

Utilizzando i dati ottenuti applicando l'algoritmo di Schreier-Sims ad un gruppo G, riusciamo a ricavare diverse informazioni:

1. **Ordine di G**

   Per costruzione, si ha $G = G^{(0)}$, $G^{(m)} = 1$ e $|U_i| = \left[G^{(i-1)} : G^{(i)}\right]$, dunque:

$$\begin{aligned} |G| &= \left[G^{(0)} : G^{(1)}\right] \cdot \left|G^{(1)}\right| = \\ &= \left[G^{(0)} : G^{(1)}\right] \cdot \left[G^{(1)} : G^{(2)}\right] \cdot \left|G^{(2)}\right| = \\ &= \left[G^{(0)} : G^{(1)}\right] \cdot \left[G^{(1)} : G^{(2)}\right] \cdot \ldots \left[G^{(m-1\}} : G^{(m)}\right] = \\ &= |U_1| \cdot \ldots \cdot |U_m|. \end{aligned}$$

2. **Test per l'appartenenza di un elemento a G**

   Sia G un gruppo di permutazioni su Ω con base $[\beta_1, \beta_2, \ldots, \beta_m]$ e insieme forte di generatori U. Supponiamo di conoscere le orbite di base Δ_i e le funzioni di rappresentazione u_i che rispettano tale base. Una permutazione arbitraria g di Ω è un elemento di G se e solo se può essere espresso nella forma :

$$g = u_m(\gamma_m) \cdot u_{m-1}(\gamma_{m-1}) \cdot \ldots \cdot u_1(\gamma_1),$$

   dove ogni γ_i appartiene a $\Delta^{(i)}$.

   Teorema 3.10. *Sia G un gruppo di permutazioni su Ω e sia β un elemento di Ω. Sia $u : \beta^G \longrightarrow G$ una fuzione di rappresentazione. Se g appartiene a G, allora esiste $h \in G_\beta$ tale che :*

$$g = h \cdot u(\beta^g).$$

   Dimostrazione. $\beta^g = \beta^{u(\beta^g)}$, dunque $\beta^{g \cdot u(\beta^g)^{-1}} = \beta$.

   Quindi $h = g \cdot u(\beta^g)^{-1}$ appartiene a G_β. □

Questo teorema consente di ricavare un algoritmo per testare se una permutazione è un elemento di G.

Se g è una permutazione di Ω e β_1^g non appartiene a $\Delta^{(1)}$, allora g non è in G. Altrimenti, possiamo scrivere $g = h \cdot u_1(\beta_1^g)$ e allora g appartiene a G se e solo se h appartiene a $G^{(2)}$.

Il problema si riduce, dunque, a calcolare se h è in $G^{(2)}$. Iterando questo processo, troviamo che g può essere scritto nella forma:

$$g = \widetilde{g} \cdot u_{l-1}(\gamma_{l-1}) \cdot u_{l-2}(\gamma_{l-2}) \cdot \ldots \cdot u_1(\gamma_1),$$

dove $\beta_l^{\widetilde{g}}$ non appartiene a $\Delta^{(l)}$ oppure $l = k+1$. Quindi g è in G se e solo se $\widetilde{g} = e$.

3. **Generare elementi casuali di G**

   Troviamo un metodo che consente di generare un elemento casuale di G, nel quale ogni elemento ha la stessa probabiltà degli altri di essere scelto. Bisogna scegliere un elemento da ogni insieme $U_m, U_{m-1}, \ldots, U_1$ e moltiplicarli tra loro:

$$u_m u_{m-1} \ldots u_1 \text{ con } u_i \in U_i \text{ per } i = 1, 2, \ldots, m.$$

3.5 Filtro di Jerrum

L'algoritmo di Schreier-Sims può causare ad un calcolatore problemi di memoria. Supponiamo di avere un insieme G presentato attraverso r generatori che agisce sull'insieme $S = \{1, 2, \ldots, n\}$, l'algoritmo di Schreier-Sims produce circa rn generatori di $G^{(1)}$, rn^2 generatori per $G^{(2)}$ e così via. Dunque, incorriamo in problemi di memoria se n è molto grande.

Il *Filtro di Jerrum* fornisce una dimostrazione del seguente teorema e, di conseguenza, una soluzione a tale problema.

Indicheremo con e la permutazione identica.

Teorema 3.11. *Ogni sottogruppo di S_n può essere generato al più da $n-1$ elementi.*

Prima di descrivere l'algoritmo, enunciamo la seguente definizione:

Definizione 3.12. Sia T un insieme di permutazioni su $\Omega = \{1, 2, \ldots, n\}$; definiamo:

$$m(T) = \textstyle\sum_{g \in T} i(g),$$

dove $i(g)$ indica il più piccolo elemento j di Ω tale che $g(j) \neq j$.

Osservazione 3.13. *$m(T)$ è limitato superiormente. Ad esempio, è maggiorato da n^2 perchè ci sono al massimo n permutazioni e $i(g) \leq n$ per ogni $g \neq e$.*

Supponiamo di avere un gruppo $G \leq S_n$, con insieme di generatori A. Indichiamo con S l'insieme $\{1, 2, \ldots, n\}$. Costruiamo il grafo $\Gamma(A)$ associato ad A: S è l'insieme dei vertici; due vertici in S sono collegati da un lato se e solo se c'è un elemento in A che manda l'uno nell'altro. Lo scopo è quello di costruire un insieme B di generatori di G il cui grafo associato è privo di cicli.

Sia $B = \emptyset$ e $\mathcal{X}$ un grafo privo di lati il cui insieme di vertici è S.

L'algoritmo procede ricorsivamente: analizziamo un singolo passo. Supponiamo che all'inizio dello step il sottogruppo generato da B sia uguale a quello generato da un sottoinsieme A_0 di A e il grafo associato $\mathcal{X}$ è stato costruito in modo tale che per ogni elemento b di B, $\{i(b), b(i(b))\}$ è un lato di $\mathcal{X}$. Inoltre, supponiamo $\mathcal{X}$ privo di cicli e che B abbia s elementi. Sia a un elemento di $A \setminus A_0$ e poniamo $A_1 := A_0 \cup \{a\}$. Lo step ha lo scopo di modificare B e di conseguenza $\mathcal{X}$, in modo che $\langle B \rangle = \langle A_1 \rangle$ ed $\mathcal{X}$ sia ancora privo di cicli.

Se $a = e$ oppure $a \in B$ oppure $a^{-1} \in B$, non occorre modificare B. In caso contrario, sostituiamo B con $B \cup \{a\}$ e troviamo il più piccolo elemento di S spostato da a (denotiamolo con r). Quindi, aggiungiamo ad $\mathcal{X}$ il lato che ha per vertici r e la sua immagine tramite a. A questo punto dell'algoritmo si ha che:

- $\langle A_1 \rangle = \langle B \rangle$;
- la cardinalità di B è uguale $s + 1$.

Possiamo notare, inoltre, che $\mathcal{X}$ ha al più un ciclo e, nel caso tale ciclo esista, deve contenere necessariamente il nuovo lato aggiunto.

1. Se $\mathcal{X}$ è privo di cicli, lo step termina e la cardinalità di B è pari a $s + 1$.
2. Se $\mathcal{X}$ ha un ciclo: il nostro obiettivo è quello di trasformare $\mathcal{X}$ in un grafo privo di cicli. Per prima cosa, troviamo il più piccolo elemento di S che è un vertice del ciclo e lo denotiamo con m. Troviamo in $\mathcal{X}$ il lato che ha per vertice iniziale m e sia g il corrispondente elemento di B, cioè l'elemento tale che $i(g) = m$. Percorriamo il ciclo partendo dal lato relativo a g e moltiplichiamo nell'ordine le permutazioni corrispondenti ai lati del ciclo (denominiamo queste permutazioni $\tau_1, \ldots, \tau_r$). Chiamiamo tale prodotto h. Poichè il più piccolo vertice del ciclo è m, si ha che h fissa $1, 2, \ldots, m-1$. Inoltre, h fissa m perchè ad h possiamo associare il ciclo che inizia e termina con m, quindi $i(h) > m = i(g)$.
3. Se $h = e$, possiamo cancellare g da B e il relativo lato in $\mathcal{X}$: eliminiamo, quindi, il ciclo in $\mathcal{X}$ e la cardinalità di B diventa s. Inoltre $\langle B \rangle = \langle A_1 \rangle$ perchè, se $h = e$, allora $e = g\tau_1 \ldots \tau_r$. Dunque, $g = (\tau_1 \ldots \tau_r)^{-1}$; g è un elemento ridondante nel sistema di generatori B.

4. Se h è diverso dall'identità, cancelliamo g da B e vi aggiungiamo h. Di conseguenza, eliminiamo il lato di $\mathcal{X}$ corrispondente a g e aggiungiamo quello relativo a h. Così facendo, la cardinalità di B rimane uguale a $s+1$, $\langle B\rangle = \langle A_1\rangle$ e $\mathcal{X}$ ha al più un ciclo. Sostituendo g con h non cambia il sottogruppo generato da B. Infatti $h = g\tau_1 \dots \tau_r$ e $g = h\left(\tau_1 \dots \tau_r\right)^{-1}$; pertanto $\langle B \setminus \{g\} \cup \{h\}\rangle = \langle B\rangle$.

   - Se $\mathcal{X}$ non ha cicli, lo step termina.
   - Se $\mathcal{X}$ ha un ciclo, osserviamo che $m(B)$ assume un valore maggiore rispetto a quello che aveva all'inizio dello step, perchè in B abbiamo sostituito g con h e $i(h) > i(g)$. Torniamo al punto 2 e ripetiamo il procedimento con questo nuovo ciclo.

   Poichè $m(B)$ è sicuramente minore o uguale di n^2, la seconda alternativa può verificarsi solo un numero finito di volte. Pertanto, dopo un numero finito di passi si trasforma $\mathcal{X}$ in un grafo privo di cicli.

Si conclude lo step dell'algoritmo e lo si ripete di nuovo considerando un elemento di A non appartenente a A_1.

Dopo un numero finito di passi, otteniamo $G = \langle B\rangle$ e $\mathcal{X}$ è un grafo senza cicli con n vertici. Dunque, applicando il Teorema 2.20, concludiamo la dimostrazione.

Capitolo 4

Teorema della base di Burnside

4.1 Sottogruppi normali massimali

Definizione 4.1. Un sottogruppo normale H di G è detto sottogruppo normale massimale di G se soddisfa le seguenti due condizioni:

- $H \neq G$;
- $H \subseteq K \subseteq G$, dove K è un sottogruppo normale di G implica che $K = G$ o $H = K$.

Analogamente, si può dare la definizione di sottogruppo normale minimale M di G: $M \neq \{1\}$ e se N è un sottogruppo normale di G con $M \supseteq N \supseteq \{1\}$, allora $N = \{1\}$ oppure $N = M$.

Un gruppo finito contiene almeno un sottogruppo normale minimale e un sottogruppo normale massimale.

Definizione 4.2. Un gruppo G è detto semplice se $G \neq 1$ e se i suoi unici sottogruppi normali sono quelli banali.

Richiamiamo il Teorema di Corrispondenza di un gruppo perchè lo utilizzeremo nella prossima dimostrazione:

Teorema 4.3. *Sia H un sottogruppo normale di un gruppo G e sia $\overline{G} = G/H$. Per ogni sottogruppo $\overline{V}$ di $\overline{G}$ esiste un unico sottogruppo V di G tale che:*

$$H \subseteq V \ e \ \overline{V} = V/H.$$

Quindi, tra l'insieme $\overline{X}$ dei sottogruppi di $\overline{G}$ e l'insieme X dei sottogruppi di G che contengono H, esiste una corrispondenza biunivoca: $\overline{V} \leftrightarrow V$.

Teorema 4.4. *Sia H un sottogruppo normale di un gruppo G. Se H è un sottogruppo normale massimale di G, il gruppo quoziente G/H è un gruppo semplice. Viceversa, se il gruppo quoziente G/H è semplice, allora H è un sottogruppo normale massimale di G.*

Dimostrazione. Per assurdo, supponiamo che esista un sottogruppo normale massimale H di G tale che il gruppo quoziente $\bar{G} = G/H$ non è semplice, allora $\bar{G}$ contiene un sottogruppo normale $\bar{N}$ non banale. Per il Teorema di Corrispondenza , esiste un sottogruppo N di G tale che $H \subset N$ e $\bar{N} = N/H$. Dunque N è normale in G ed abbiamo $H \subset N \subset G$, perchè $\bar{N}$ non è banale. Da qui otteniamo che H non è un sottogruppo normale massimale di G.

Viceversa, se H non è un sottogruppo normale massimale, allora esiste un sottogruppo normale N di G tale che $H \subseteq N$ e $H \neq N \neq G$. Inoltre $\bar{N} = N/H$, è un sottogruppo normale di $\bar{G}$ che non è banale perchè $H \neq N \neq G$. Dunque $\bar{G}$ non è semplice. □

4.2 p-gruppi

Definizione 4.5. Sia p un numero primo fissato. Un gruppo finito è detto p-gruppo se il suo ordine è una potenza di p.

Teorema 4.6. *Sia G un p-gruppo. Ogni sottogruppo di G è ancora un p-gruppo. Se H è un sottogruppo normale di G, il gruppo quoziente G/H è un p-gruppo.*

Dimostrazione. Per il Teorema di Lagrange sappiamo che $|G| = |H| \cdot [G : H]$. Quindi l'ordine di H è un divisore dell'ordine di G e poichè quest'ultimo è una potenza di p con p primo , l'ordine di H deve essere necessariamente una potenza di p.

Inoltre, poiché l'ordine del gruppo quoziente $|G/H| = [G : H]$, si ha che anche G/H è un p-gruppo. □

Teorema 4.7. *Sia G un p-gruppo e X un G-insieme non vuoto finito. Se $|X| \not\equiv 0 \,(\ mod\ p)$, allora X contiene un elemento G-invariante, cioè un punto fisso dell'azione di G su X.*

Dimostrazione. Per il Corollario 1.21, l'insieme X è partizionato in un'unione disgiunta di orbite:

$$X = O_1 \cup O_2 \cup \ldots O_m.$$

Per ogni $i = 1, \ldots, m$, per il Teorema 1.19 la dimensione dell'orbita O_i è uguale all'indice dello stabilizzatore $S_G(x_i)$, con $x_i \in O_i$. Per ipotesi, G è un p-gruppo, quindi per il Teorema 4.6 , $|G : S_G(x_i)|$ è una potenza di p. Poichè per ipotesi $|X| \not\equiv 0 \,(mod\ p)$, allora $\sum_{i=1}^{m} |G : S_G(x_i)| \not\equiv 0 \,(mod\ p)$. Questo equivale a dire che almeno per un indice i la quantità $|G : S_G(x_i)|$ non è divisibile per p. Una potenza p^n di p non è divisibile per p se e soltanto se $n = 0$; quindi abbiamo $|O_i| = p^0 = 1$. Quindi, l'orbita O_i è formata da un singolo elemento G-invariante. □

Corollario 4.8. *Supponiamo che un p-gruppo Q agisca su un altro p-gruppo G. Se $G \neq \{1\}$, allora esiste un elemento Q-invariante di G oltre all'elemento neutro.*

Dimostrazione. Sia $X = G \setminus \{1\}$. Per ipotesi , X è un insieme non vuoto sul quale agisce Q tale che $|X| \not\equiv 0 \ (mod\ p)$. Quindi, per il teorema precedente, esiste un elemento Q-invariante di X. □

Dal teorema precedente e da quest'ultimo corollario, possiamo derivare diverse proprietà sugli p-gruppi.

Teorema 4.9. *Sia G un p-gruppo e sia H un sottogruppo normale di G. Se $H \neq \{1\}$, allora $H \cap Z(G) \neq \{1\}$. In particolare se $G \neq \{1\}$, allora il centro di G contiene un elemento diverso da 1.*

Dimostrazione. Per il Teorema 4.6, H è un p-gruppo. Poichè H è un sottogruppo normale di G, il p-gruppo G agisce sul p-gruppo $H \neq \{1\}$ tramite coniugio. Per il corollario precedente H contiene un elemento z G-invariante oltre all'elemento neutro 1. Per definizione di azione, si ha $z = z^g = g^{-1}zg$ per ogni $g \in G$. Quindi, z è contenuto nel centro di G:

$$z \in H \cap Z(G) \neq \{1\}.$$

Questo ragionamento prova la prima parte del teorema; il resto segue immediatamente ponendo $G = H$. □

Ora, utilizzando il Teorema 4.9 e il teorema seguente, dimostreremo la commutatività di gruppi di ordine p^2.

Teorema 4.10. *Il centro $Z(G)$ di un gruppo G è un sottogruppo commutativo di G. Sia H un sottogruppo di $Z(G)$. Allora il sottogruppo $\langle H, x\rangle$ generato da H e da un elemento x di G è abeliano.*

Dimostrazione. Dimostriamo il teorema in due fasi:

- Sia $K = \langle H, x\rangle$ e sia $k \in K$. Mostriamo che k può essere scritto nella forma hx^m con $h \in H$ e $m \in \mathbb{Z}$. Per definizione di sottogruppo generato , k può essere espresso come un prodotto della forma $u_1 \cdot u_2 \cdot \ldots u_n$ con $u_i \in H$, oppure $u_i = x$ oppure $u_i = x^{-1}$. Poichè H è contenuto nel centro di G, $u_1, u_2, \ldots u_n$ commutano l'uno con l'altro. Dunque tutti i fattori di k contenuti in H possono essere spostati a sinistra: i rimanenti fattori sono x o x^{-1}. Chiamo h il prodotto di tutti i fattori in H di k; allora $k = hx^m$ per qualche intero m.

- Mostriamo che se $h_1, h_2 \in H$, allora $(h_1x^m)(h_2x^n) = (h_2x^n)(h_1x^m)$. Usando la proprietà associativa e il fatto che $H \leq Z(G)$ si ha

$$(h_1x^m)(h_2x^n) = ((h_1x^m)h_2)x^n = (h_2(h_1x^m))x^n = h_2(h_1(x^mx^n)) = h_2(h_1(x^nx^m)) = h_2(x^n(h_1x^m)) = (h_2x^n)(h_1x^m).$$

Da entrambi i punti segue che K è un sottogruppo abeliano. □

Teorema 4.11. *Se G ha ordine p^2, allora G è abeliano.*

Dimostrazione. Per i due teoremi precedenti si ha che il centro di G non è banale, quindi per il suo ordine, utilizzando il Teorema di Lagrange, ci sono due possibiltà: o è p o è p^2. Per assurdo supponiamo che l'ordine di $Z(G)$ sia p, allora esisterebbe $a \in G \setminus Z(G)$. Per definizione di centro e centralizzante si ha che $C_G(a) \supseteq Z(G)$ e anzi l'inclusione è stretta perchè $a \in C_G(a)$ ma $a \notin Z(G)$. Allora $C_G(a)$ è un sottogruppo con un numero di elementi maggiore di p e dunque ne deve avere p^2. Dunque $C_G(a) = G$. Da questo segue che $a \in Z(G)$, il che è assurdo, pertanto $Z(G)$ ha ordine p^2, cioè $Z(G) = G$. □

Teorema 4.12. *Sia H un sottogruppo di un p-gruppo G. Allora H è normale in G oppure un sottogruppo coniugato $H^x = x^{-1}Hx$ diverso da H è contenuto in $N_G(H)$.*

Dimostrazione. Supponiamo che H non sia normale e sia X l'insieme dei coniugati H^x diversi da H. Allora, X è un insieme non vuoto sul quale H agisce tramite coniugio. Poichè il numero dei coniugati di H è uguale all'indice $|G : N_G(H)|$, per ipotesi e per il Teorema 4.6, abbiamo:

$$|X| = |G : N_G(H)| - 1 \not\equiv 0 \pmod{p}.$$

Dunque, per il Teorema 4.7, X contiene un elemento H-invariante, detto H^y. Poichè H^y è H-invariante, abbiamo che $H \subset N_G(H^y)$. Ponendo $x = y^{-1}$, otteniamo $H \neq H^x \subset N_G(H)$. □

Il prossimo teorema segue facilmente da quello precedente.

Teorema 4.13. *Se H è un sottogruppo proprio di un p-gruppo G, allora abbiamo $N_G(H) \neq H$. Dunque, il normalizzante di un sottogruppo proprio H contiene propriamente H.*

Dimostrazione. Se H è normale in G, allora $N_G(H) = G \neq H$, quindi il teorema è verificato. Se H non è normale, per il teorema precedente, $N_G(H)$ contiene un coniugato H^x di H che è diverso da H. Quindi $N_G(H) \neq H$ anche in questo caso. □

Corollario 4.14. *Ogni sottogruppo massimale M di un p-gruppo G è normale ed il gruppo quoziente G/M è un gruppo ciclico di ordine p. In particolare, $[G : M] = p$.*

Dimostrazione. Per il teorema precedente, il normalizzante di M è strettamente più grande di M, quindi M è normale in G. Per il Teorema di Corrispondenza , il gruppo quoziente G/M non contiene sottogruppi non banali. Quindi G/M è un grupppo ciclico di ordine un numero primo. Dal Teorema 4.6 otteniamo che $[G : M] = p$. □

4.3 Gruppi Nilpotenti

Definizione 4.15. Per ogni gruppo G, definiamo il sottogruppo $Z_i(G)$ per $i = 0, 1, 2, 3 \ldots$ come segue. (Per abbreviare la notazione, poniamo $Z_i(G) = Z_i$. Definiamo $Z_0 = 1$ e per $i \geq 1$ Z_i è il sottogruppo di G corrispondente a $Z(G/Z_{i-1})$ nel Teorema di Corrispondenza:

$$Z_i/Z_{i-1} = Z(G/Z_{i-1}).$$

Definizione 4.16. La sequenza di sottogruppi $Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \ldots$ è detta serie centrale crescente; il suo i-esimo termine Z_i è detto centro i-esimo di G. Un gruppo G è detto nilpotente se $Z_m(G) = G$ per qualche intero m. In tal caso il più piccolo intero c tale che $Z_c(G) = G$ è detto classe di G.

Il gruppo banale $\{1\}$ è l'unico gruppo nilpotente di classe 0. I gruppi abeliani diversi da $\{1\}$ sono gruppi nilpotenti di classe 1. Quindi il concetto di gruppo nilpotente è una generalizzazione di gruppo abeliano.

Teorema 4.17. *Consideriamo la serie centrale di un p-gruppo G. C'è un intero m tale che $Z_m(G) = G$. Quindi ogni p-gruppo è nilpotente.*

Dimostrazione. Il Teorema segue applicando ripetutamente il Teorema 4.9. □

4.4 Teorema della base di Burnside

Definizione 4.18. Sia G un gruppo e $\mathcal{M}$ l'insieme di tutti i sottogruppi massimali di G. L'intersezione di tutti i sottogruppi appartenenti a $\mathcal{M}$ è chiamata sottogruppo di Frattini o Φ-sottogruppo di G; lo denotiamo con $\Phi(G)$.

Definizione 4.19. Sia H un sottogruppo di G. Diciamo che H è un sottogruppo caratteristico di G se ogni automorfismo di G manda H in sé stesso. Scriviamo: H *char* G.

Teorema 4.20. *Sia $\Phi = \Phi(G)$ il sottogruppo di Frattini del gruppo G. Allora Φ char G.*

Dimostrazione. Ogni automorfismo di G manda un sottogruppo massimale in un sottogruppo massimale. Quindi l'insieme $\mathcal{M}$ è invariante per ogni automorfismo e di conseguenza anche Φ. □

Teorema 4.21. *Per un sottoinsieme X del gruppo G,*

$$\langle X, \Phi \rangle = G \Rightarrow \langle X \rangle = G.$$

Dimostrazione. Per assurdo supponiamo che $\langle X \rangle$ sia un sottogruppo proprio di G, allora esiste un sottogruppo massimale M che contiene X. Ma allora $\langle \Phi, X \rangle \subseteq M$, contrariamente all'ipotesi. □

Teorema 4.22. *Sia G un p-gruppo. Il gruppo quoziente G/Φ è un gruppo abeliano tale che ogni suo elemento x soddisfa $x^p = 1$.*

Dimostrazione. Per il corollario 4.14, $M \triangleleft G$ per ogni $M \in \mathcal{M}$ e il gruppo quoziente G/M è un gruppo ciclico di ordine p. Dunque, presi due elementi x e y di G, si ha che $x^p \in M$ e $x^{-1}y^{-1}xy \in M$ per tutti gli $M \in \mathcal{M}$. Quindi x^p e $x^{-1}y^{-1}xy$ sono contenuti nell'intersezione di questi sottogruppi, cioè $x^p \in \Phi$ e $x^{-1}y^{-1}xy \in \Phi$. Abbiamo $(x\Phi)^p = 1$ e $x\Phi y\Phi = y\Phi x\Phi$. Questo prova il teorema. □

Teorema 4.23. *Sia p un numero primo fissato. Se un gruppo abeliano E è tale che per ogni suo elemento x si ha $x^p = 1$, allora E è isomorfo a uno spazio vettoriale sul campo con p elementi $\boldsymbol{F}_p$.*

Dimostrazione. Per semplicità supponiamo che E sia un gruppo additivo ed utilizziamo la notazione additiva. Per ipotesi si ha che ogni elemento x di E soddisfa $px = 0$. Il gruppo degli interi $\mathbb{Z}$ agisce su E tramite la funzione ξ definita nel seguente modo:

siano $x \in E$, $z \in \mathbb{Z}$, $\xi : \mathbb{Z} \times E \longrightarrow E$;

- se $z = 0$, allora $\xi(0, x) = 0$;
- se $z > 0$, allora $\xi(z, x) = \underbrace{x + \ldots + x}_{z \text{ volte}}$
- se $z < 0$, posto $n = -z > 0$, si ha $\xi(z, x) = -\xi(n, x)$.

In particolare, si può osservare:

$$(m + n)\, x = mx + nx,$$
$$(mn)\, x = m\,(nx)$$

con $n, m \in \mathbb{Z}$. Poichè $px = 0$ per tutti $x \in E$, allora l'azione di $\mathbb{Z}$ induce un'azione sull'anello quoziente $\mathbb{Z}/(p)$, dove (p) è l'ideale generato da p. Identifichiamo $\mathbb{Z}/(p)$ con il campo $\mathbf{F}_p$ di p elementi. In questo modo $\mathbf{F}_p$ agisce su E, ed è facile verificare che E è uno spazio vettoriale su $\mathbf{F}_p$. Un automorfismo f di E soddisfa:

$$f(nx) = nf(x) \quad \textit{con } n \in \mathbb{Z}.$$

Quindi f è una trasformazione lineare su $\mathbf{F}_p$. □

Per questo teorema e per il Teorema 4.22, si ha che il gruppo quoziente G/Φ è isomorfo ad uno spazio vettoriale su un campo con p elementi $\mathbf{F}_p$. Sia $V = G/\Phi$. Consideriamo V come spazio vettoriale su $\mathbf{F}_p$. Possiamo adesso enunciare il **Teorema della base di Burnside**.

Teorema 4.24. *Sia Φ il sottogruppo di Frattini di un p-gruppo G, e consideriamo $V = G/\Phi$ come uno spazio vettoriale su $\boldsymbol{F}_p$. Sia $[G : \Phi] = p^d$. Siano $x_1, x_2, \ldots, x_n$ elementi di G e $v_i = \Phi x_i$ per $i = 1, 2, \ldots n$. Allora:*

1. *La dimensione di V su $\boldsymbol{F}_p$ è d;*
2. *$G = \langle x_1, x_2, \ldots x_n \rangle$ se e soltanto se V coincide con lo spazio generato da $v_1, v_2, \ldots, v_n$. In particolare, se $G = \langle x_1, x_2, \ldots x_n \rangle$, allora $n \geq d$.*
3. *Il gruppo G è generato da esattamente d elementi. Il sottoinsieme $\{x_1, x_2, \ldots x_n\}$ genera G se e soltanto se $\{v_1, v_2, \ldots v_d\}$ è una base per lo spazio vettoriale V su $\boldsymbol{F}_p$.*

Dimostrazione. 1. Uno spazio vettoriale di dimensione m su $\mathbf{F}_p$ contiene esattamente p^m elementi. Quindi la prima affermazione è ovvia.

2. Se $G = \langle x_1, x_2, \ldots x_n \rangle$, allora V è generato da $v_1, \ldots v_n$. Un teorema dell'algebra lineare afferma che uno spazio vettoriale di dimensione d non può essere generato da meno di d elementi. Dunque $n \geq d$.

   Viceversa, supponiamo che $V = \langle v_1, v_2 \ldots v_n \rangle$. Prendendo $X = \{x_1, x_2, \ldots x_n\}$, abbiamo $\langle X, \Phi \rangle = G$, quindi per il Teorema 4.21 otteniamo $G = \langle X \rangle$.

3. Se $\{v_1, v_2, \ldots v_d\}$ è una base di V su $\mathbf{F}_p$, allora per il punto precedente abbiamo $G = \langle x_1, \ldots, x_d \rangle$. Viceversa, se $G = \langle x_1, \ldots, x_d \rangle$, allora sempre per il punto precedente abbiamo che $V = \langle v_1, \ldots, v_d \rangle$. In questo caso $v_1, \ldots, v_d$ sono linearmente indipendenti e quindi $\{v_1, \ldots, v_d\}$ è una base di V.

□

Quindi, grazie al Teorema della base di Burnside, possiamo osservare che due insiemi minimali di generatori di un p-gruppo hanno sempre lo stesso numero di elementi.

Bibliografia

[1] M. Bóna, *Combinatorics of permutations*, Chapman & Hall/ CRC, 2004.

[2] P. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999.

[3] K. Conrad, *Generating Sets*, materiale didattico:
https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf.

[4] J. Dixon, B. Mortimer, *Permutation Groups*, Springer, New York, 1996.

[5] A. Machì, *Gruppi. Una introduzione a idee e metodi della teoria dei gruppi*, Springer, Milano, 2007.

[6] S. Murray, *The Schreier-Sims algorithm*, 2013,
https://www.maths.usyd.edu.au/u/murray/research/essay.pdf.

[7] M. Suzuki, *Group Theory*, Springer, Berlino, 1982.