

PARTE PRIMA

RICHIAMI

E

ARGOMENTI PRELIMINARI

Questa parte é da considerarsi introduttiva e propedeutica alle successive. Molti degli argomenti in essa contenuti rivestono un ruolo fondamentale nella matematica e per essere trattati compiutamente avrebbero bisogno di ben altro spazio. Noi ci limiteremo ad esporre, spesso sommariamente, soltanto i risultati utili per un'agevole lettura di queste note.

Capitolo 1

Il gruppo simmetrico

1.1 Generalità

Se $f : A \rightarrow B$ e $g : B \rightarrow C$ sono due applicazioni, useremo la notazione fg per denotare l'applicazione composta $g \circ f$ di A in C , porremo cioè

$$(fg)(a) := g(f(a))¹,$$

per ogni $a \in A$.

Sia X un insieme non vuoto.

DEFINIZIONE 1.1.1. Una funzione biunivoca di X su se stesso prende il nome di *permutazione* su X . Se σ e τ sono permutazioni su X , la funzione

$$\tau \circ \sigma : x \in X \rightarrow \tau(\sigma(x)) \in X \tag{1.1}$$

é ancora una permutazione e l'operazione definita dalla (1.1) induce una struttura di gruppo sull'insieme di tutte le permutazioni su X . Tale gruppo prende il nome di *gruppo simmetrico* su X e si denota con $S(X)$. \square

Ovviamente, l'unitá di $S(X)$ é la permutazione identica, cioè la funzione identitá su X , che denoteremo col simbolo 1 .

DEFINIZIONE 1.1.2. Un gruppo G prende il nome di *gruppo di permutazioni* (su X) se é sottogruppo di $S(X)$, per un opportuno insieme X . \square

La teoria dei gruppi di permutazioni é equivalente all'intera teoria dei gruppi nel senso precisato dal seguente teorema.

¹La notazione $:=$ indica che il simbolo scritto alla sua sinistra é definito da ciò che é scritto alla sua destra.

PROPOSIZIONE 1.1.3. (Teorema di Cayley) *Ogni gruppo G è isomorfo ad un gruppo di permutazioni sull'insieme degli elementi di G .*

DIMOSTRAZIONE. Per ogni elemento $g \in G$, la traslazione destra individuata da g

$$\tau_g : x \in G \rightarrow xg \in G$$

è una funzione biunivoca e quindi una permutazione sugli elementi di G . Si verifica facilmente che l'applicazione

$$\tau : g \in G \rightarrow \tau_g \in S(G)$$

è un monomorfismo di G in $S(G)$. Ne segue che G è isomorfo a $\tau(G)$, cioè l'asserto. \square

OSSERVAZIONE 1.1.4. Se X e Y sono insiemi non vuoti ed equipotenti e f è una funzione biunivoca di X su Y , è facile verificare che l'applicazione

$$\sigma \in S(X) \rightarrow f^{-1}\sigma f \in S(Y)$$

è un isomorfismo di gruppi. Pertanto, il gruppo $S(X)$, a meno di isomorfismi, dipende solo dalla cardinalità X . \square

Nel seguito del presente capitolo prenderemo in considerazione solo gruppi simmetrici su insiemi finiti e quindi, se X è finito e contiene esattamente n elementi, il gruppo $S(X)$ dipende solo da n ; esso prende il nome di *gruppo simmetrico* su n oggetti, o *di grado n* , e si denota con S_n . Allo scopo di evitare complicazioni nelle notazioni penseremo sempre S_n come il gruppo simmetrico sull'insieme $N_n := \{1, 2, \dots, n\}$ dei primi n interi positivi. In questo caso può essere talvolta conveniente rappresentare una permutazione σ su N_n mediante la matrice

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

che ha nella prima riga gli interi da 1 ad n disposti in ordine crescente e sotto ognuno di essi l'intero corrispondente in σ . Ovviamente, con questa notazione, la matrice

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{bmatrix}$$

rappresenta la permutazione identica.

ESEMPIO 1.1.5. Le permutazioni σ e τ di $N_4 = \{1, 2, 3, 4\}$ definite da

$$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 1; \tau(1) = 3, \tau(2) = 4, \tau(3) = 1, \tau(4) = 2$$

si scrivono

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}.$$

In questo modo se, per esempio, vogliamo calcolare l'immagine di 2 nel prodotto $\sigma\tau$, basta leggere l'intero sotto 2 nella tabella di σ , nel nostro caso 3, e poi l'intero sotto 3 nella tabella di τ ; abbiamo così $\sigma\tau(2) = \tau(\sigma(2)) = 1$. \square

Talvolta, nello scrivere la matrice di una permutazione σ , può essere conveniente riportare nella prima riga gli interi da 1 ad n in un ordine che non sia quello crescente. In questo caso, ovviamente, sotto ognuno di essi va riportata la propria immagine in σ . Per esempio, abbiamo

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 1 & 3 & 2 \\ 1 & 2 & 4 & 3 \end{bmatrix}.$$

Osserviamo che, se m ed n sono interi positivi con $m < n$, ad ogni permutazione $\sigma \in S_m$ possiamo associare la permutazione $\sigma' \in S_n$ che opera come σ sugli interi $1, 2, \dots, m$ e trasforma in se stesso ogni altro elemento di N_n . Si prova subito che l'applicazione

$$f : \sigma \in S_m \rightarrow \sigma' \in S_n$$

è un monomorfismo di gruppi e quindi l'immagine $f(S_m)$ è un sottogruppo di S_n isomorfo a S_m . Nel seguito spesso identificheremo S_m con $f(S_m)$ in modo da considerare S_m come sottogruppo di S_n e, con abuso di notazione, denoteremo ancora con σ la permutazione $\sigma' = f(\sigma)$. Con questa convenzione gli elementi j di N_n che non compaiono nella matrice che rappresenta una fissata permutazione σ sono tali che $\sigma(j) = j$. Per esempio, la permutazione

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

considerata come elemento di S_6 , è la permutazione

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{bmatrix}.$$

Osserviamo ancora che, se σ e τ sono le due permutazioni su N_3 definite da

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix},$$

risulta $\sigma\tau \neq \tau\sigma$ e si ha così la seguente proposizione.

PROPOSIZIONE 1.1.6. *Il gruppo simmetrico S_n non è abeliano per ogni intero n maggiore di 2.*

ESERCIZIO 1.1.7. *Provare che S_3 (che è non abeliano) possiede solo sottogruppi propri abeliani.*

DEFINIZIONE 1.1.8. Una matrice quadrata ad elementi 0, 1 prende il nome di *matrice di permutazione* se ciascuna delle sue righe e colonne contiene un unico elemento uguale ad 1. L'insieme delle matrici di permutazione d'ordine n , rispetto al prodotto righe per colonne, forma un gruppo che denoteremo con $MP(n)$. \square

ESERCIZIO 1.1.9. *Provare che, per ogni permutazione $\sigma \in S_n$, la matrice $P_\sigma = (\sigma_{ij})$, definita da*

$$\sigma_{ij} = \begin{cases} 1, & \text{se } \sigma(i) = j \\ 0, & \text{se } \sigma(i) \neq j \end{cases}, \quad (1.2)$$

è una matrice di permutazione (la matrice associata a σ). Provare, inoltre, che l'applicazione

$$\sigma \in S_n \rightarrow P_\sigma \in MP(n)$$

è un isomorfismo di gruppi.

Calcolare l'ordine di S_n è un facile esercizio. Abbiamo infatti che, se si vuole costruire una permutazione σ su N_n , vi sono n possibili scelte per $\sigma(1)$, $n-1$ per $\sigma(2)$, $n-3$ per $\sigma(3)$ e così via. Ne segue per induzione che

$$|S_n| = n!. \quad (1.3)$$

DEFINIZIONE 1.1.10. Diciamo che un elemento j di N_n è *unito* o *fisso* in una permutazione σ se risulta $\sigma(j) = j$ e denotiamo con $F(\sigma)$ l'insieme degli elementi uniti di σ , cioè

$$F(\sigma) = \{x \in N_n : \sigma(x) = x\}.$$

Due permutazioni σ e τ si dicono *disgiunte* se i rispettivi insiemi di elementi non uniti, $N_n \setminus F(\sigma)$ e $N_n \setminus F(\tau)$, sono ad intersezione vuota. \square

ESERCIZIO 1.1.11. *Provare che due permutazioni disgiunte sono elementi permutabili di S_n .*

DEFINIZIONE 1.1.12. Una permutazione σ si dice *k-ciclo* o *ciclo di lunghezza k* se, detto j un elemento di N_n non unito in σ , risulta

$$N_n \setminus F(\sigma) = \{j, \sigma(j), \sigma^2(j), \dots, \sigma^{k-1}(j)\}$$

e, in questo caso, si usa per σ la seguente notazione

$$\sigma = (j, \sigma(j), \sigma^2(j), \dots, \sigma^{k-1}(j)).$$

\square

OSSERVAZIONE 1.1.13. Nella k -pla $(j, \sigma(j), \sigma^2(j), \dots, \sigma^{k-1}(j))$, che denota il k -ciclo σ , compaiono soltanto gli elementi di N_n spostati da σ e questi sono ordinati in modo che, tranne che per l'ultimo, l'immagine in σ di ciascuno di essi è data dal successivo, mentre l'ultimo elemento ha per immagine il primo. Inoltre, se t è un qualsiasi elemento di N_n diverso da j e spostato da σ , risulta anche $\sigma = (t, \sigma(t), \sigma^2(t), \dots, \sigma^{k-1}(t))$. Per esempio, il 5-ciclo $\sigma = (2, 1, 3, 4, 7)$ di S_7 è la permutazione su N_7 definita da

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 7 & 5 & 6 & 2 \end{bmatrix};$$

in questo caso è $F(\sigma) = \{5, 6\}$ e si ha anche

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

\square

ESERCIZIO 1.1.14. *Provare che*

$$(i_1, i_2, \dots, i_k)^{-1} = (i_k, i_{k-1}, \dots, i_1),$$

per ogni k -ciclo (i_1, i_2, \dots, i_k) di S_n .

DEFINIZIONE 1.1.15. La permutazione identica, che é l'unico ciclo di lunghezza 1, si chiama *ciclo banale*. I cicli di lunghezza 2 prendono il nome di *trasposizioni* ed é chiaro che, per ogni trasposizione σ , risulta $\sigma = \sigma^{-1}$. Un n -ciclo $\sigma \in S_n$ prende il nome di *permutazione ciclica* di N_n . \square

ESERCIZIO 1.1.16. *Provare che un k -ciclo é un elemento di periodo k in S_n .*

Nello studio del gruppo simmetrico S_n i cicli sono di fondamentale importanza. Essi infatti generano S_n e giocano in qualche modo un ruolo simile a quello dei numeri primi nella fattorizzazione degli interi, nel senso precisato dal seguente teorema.

PROPOSIZIONE 1.1.17. *Ogni permutazione $\sigma \in S_n$ può decomporre in un prodotto di cicli non banali e disgiunti. Tale decomposizione é unica a meno dell'ordine dei cicli nella fattorizzazione.*

DIMOSTRAZIONE. Essendo l'asserto ovvio nei casi $n = 1, 2$, possiamo supporre $n > 2$ e procedere per induzione su n . Siano, dunque, j un elemento di N_n non unito in σ ed m il piú piccolo intero positivo tale che $\sigma^m(j) = j$. Osserviamo che, nel caso $m = n$, σ é un ciclo di lunghezza n e non abbiamo nulla da provare. Se é $m < n$, detta τ la permutazione che fissa $j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j)$ e opera come σ sui rimanenti $n - m$ elementi di N_n , risulta

$$\sigma = (j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j))\tau = \tau(j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j)).$$

Si noti che, per costruzione, il ciclo $(j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j))$ e la permutazione τ sono disgiunti. Inoltre, in forza della legge di cancellazione, τ é l'unica permutazione in S_n che verifica l'uguaglianza precedente. Allora, potendosi τ riguardare come una permutazione su $n - m$ oggetti, dall'ipotesi di induzione su n segue senza difficoltà l'asserto. \square

Nel seguito, quando parleremo di *fattorizzazione di una permutazione in cicli disgiunti*, sottintenderemo sempre che tali cicli sono non banali. La scrittura di una permutazione σ come prodotto di cicli disgiunti prende il nome di *notazione ciclica* di σ ed é chiaro che, se un elemento $j \in N_n$ non compare in nessuno dei cicli che fattorizzano σ , allora j é unito in σ .

PROPOSIZIONE 1.1.18. *L'ordine di un elemento $\sigma \in S_n$ é uguale al minimo comune multiplo delle lunghezze dei cicli che fattorizzano σ .*

DIMOSTRAZIONE. Sia $\sigma_1\sigma_2 \cdots \sigma_k$ una fattorizzazione in cicli disgiunti di σ e, denotato con s_j l'ordine di σ_j , sia

$$m = \text{mcm}(s_1, s_2, \dots, s_k) \quad \text{e} \quad m = s_j m_j,$$

per ogni $j = 1, 2, \dots, k$. Osserviamo che i cicli $\sigma_1, \sigma_2, \dots, \sigma_k$ sono a due a due disgiunti e quindi a due a due permutabili; ne segue che

$$\sigma^t = \sigma_1^t \sigma_2^t \cdots \sigma_k^t,$$

per ogni intero t . Allora risulta

$$\sigma^m = \sigma_1^m \sigma_2^m \cdots \sigma_k^m = (\sigma_1^{s_1})^{m_1} (\sigma_2^{s_2})^{m_2} \cdots (\sigma_k^{s_k})^{m_k} = 1.$$

Inoltre, se t é un intero positivo minore di m , esiste un indice j tale che t non é multiplo di s_j . Ne segue che $\sigma_j^t \neq 1$ e, essendo $\sigma_1^t, \sigma_2^t, \dots, \sigma_k^t$ permutazioni a due a due disgiunte, risulta

$$\sigma^t = \sigma_1^t \sigma_2^t \cdots \sigma_k^t \neq 1.$$

L'asserto é cosí completamente provato. \square

1.2 Coniugio in S_n

Una permutazione $\sigma \in S_n$ si dice di *tipo* $1^{t_1} 2^{t_2} \cdots n^{t_n}$ se, per ogni $j = 2, \dots, n$, l'intero t_j é il numero di cicli di lunghezza j che compaiono in una qualsiasi fattorizzazione di σ in cicli disgiunti e non banali e l'intero t_1 é il numero di punti fissi di σ . Naturalmente risulta

$$t_1 + 2t_2 + 3t_3 + \cdots + nt_n = n.$$

Due permutazioni dello stesso tipo si dicono anche *simili*. Quando scriviamo il tipo $1^{t_1} 2^{t_2} \cdots n^{t_n}$ di una permutazione puó essere conveniente omettere i termini del tipo j^{t_j} per i quali é $t_j = 0$. Per esempio, possiamo dire che la permutazione $(1, 3)(2, 5) \in S_7$, che é prodotto di due cicli di lunghezza 2 e ha tre punti fissi, é di tipo $1^3 2^2$ invece di $1^3 2^2 3^0 4^0 5^0 6^0 7^0$.

PROPOSIZIONE 1.2.1. Se $\sigma = (i_1, i_2, \dots, i_k)$ é un k -ciclo e τ una permutazione, risulta

$$\tau^{-1} \sigma \tau = (\tau(i_1), \tau(i_2), \dots, \tau(i_k)),$$

cioé in S_n ogni elemento coniugato di un k -ciclo é ancora un k -ciclo.

DIMOSTRAZIONE. Per ogni $j = 1, 2, \dots, k$ risulta

$$\begin{aligned} (\tau^{-1} \sigma \tau)(\tau(i_j)) &= \sigma \tau(\tau^{-1}(\tau(i_j))) = \\ \tau(\sigma(i_j)) &= \begin{cases} \tau(i_{j+1}), & \text{se } j = 1, 2, \dots, k-1 \\ \tau(i_1), & \text{se } j = k \end{cases}. \end{aligned}$$

Inoltre, se un elemento $s \in N_n$ non appartiene a $\{\tau(i_1), \tau(i_2), \dots, \tau(i_k)\}$, allora $\tau^{-1}(s)$ non appartiene a $\{i_1, i_2, \dots, i_k\}$ e quindi

$$\tau^{-1} \sigma \tau(s) = \tau(\sigma(\tau^{-1}(s))) = \tau \tau^{-1}(s) = s.$$

Ne segue l'asserto. \square

PROPOSIZIONE 1.2.2. Due permutazioni $\sigma, \tau \in S_n$ sono coniugate se, e solo se, sono simili.

DIMOSTRAZIONE. Supponiamo $\tau = \mu^{-1} \sigma \mu$ e sia

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_h$$

la fattorizzazione di σ in cicli disgiunti. Allora

$$\tau = \mu^{-1}\sigma\mu = \mu^{-1}\sigma_1\sigma_2 \cdots \sigma_h\mu = (\mu^{-1}\sigma_1\mu)(\mu^{-1}\sigma_2\mu) \cdots (\mu^{-1}\sigma_h\mu)$$

e, essendo ogni $\mu^{-1}\sigma_j\mu$ un ciclo della stessa lunghezza di σ_j , abbiamo che σ e τ sono simili.

Viceversa, se σ e τ sono simili e le fattorizziamo in cicli disgiunti

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_h \text{ e } \tau = \tau_1\tau_2 \cdots \tau_h,$$

possiamo assumere che, per ogni $j = 1, 2, \dots, h$, si abbia

$$\sigma_j = (s_1^j, s_2^j, \dots, s_{\nu(j)}^j), \quad \tau_j = (t_1^j, t_2^j, \dots, t_{\nu(j)}^j).$$

Allora, detta μ la permutazione definita da

$$\mu(s_k^j) = t_k^j, \quad \text{per ogni } j = 1, 2, \dots, h, \quad k = 1, 2, \dots, \nu(j),$$

risulta

$$\mu^{-1}\sigma_j\mu = \tau_j, \quad \text{per ogni } j = 1, 2, \dots, h;$$

quindi é

$$\mu^{-1}\sigma\mu = (\mu^{-1}\sigma_1\mu)(\mu^{-1}\sigma_2\mu) \cdots (\mu^{-1}\sigma_h\mu) = \tau_1\tau_2 \cdots \tau_h = \tau$$

e l'asserto é provato. □

ESERCIZIO 1.2.3. Siano σ e τ due permutazioni in S_n . Provare che $\sigma\tau$ e $\tau\sigma$ sono simili.

PROPOSIZIONE 1.2.4. Il numero delle permutazioni di tipo $1^{t_1}2^{t_2} \cdots n^{t_n}$ in S_n é dato da

$$\frac{n!}{1^{t_1}2^{t_2} \cdots n^{t_n}(t_1!)(t_2!) \cdots (t_n!)}.$$

DIMOSTRAZIONE. Se σ é una permutazione di tipo $1^{t_1}2^{t_2} \cdots n^{t_n}$, scriviamo una sua fattorizzazione in cicli disgiunti disponendo tali cicli in ordine crescente rispetto alle lunghezze e sia $\sigma = \tau_1\tau_2 \cdots \tau_k$. Se t_1 é diverso da zero, diciamo i_1, i_2, \dots, i_{t_1} , i punti uniti di σ , e scriviamo σ nella seguente forma:

$$\sigma = \begin{cases} \tau_1\tau_2 \cdots \tau_k, & \text{se } t_1 = 0 \\ (i_1)(i_2) \cdots (i_{t_1})\tau_1\tau_2 \cdots \tau_k, & \text{se } t_1 \neq 0 \end{cases} \quad (1.4)$$

con

$$1 < |\tau_1| \leq |\tau_2| \leq \cdots \leq |\tau_k|.$$

Adesso contiamo il numero $n(\sigma)$ dei modi possibili di scrivere σ nella forma precedente. A tale scopo osserviamo che ogni ciclo (s_1, s_2, \dots, s_j) di lunghezza j della fattorizzazione può essere scritto in esattamente j modi diversi e, precisamente

$$(s_1, s_2, \dots, s_j) = (s_2, s_3, \dots, s_j, s_1) = (s_3, s_4, \dots, s_1, s_2) = \cdots = (s_j, s_1, \dots, s_{j-1}).$$

Abbiamo, così $1^{t_1}2^{t_2} \cdots n^{t_n}$ modi diversi di disporre gli elementi di N_n nella scrittura dei cicli che fattorizzano σ . Inoltre, senza alterare la forma della scrittura di σ nella 1.4, possiamo scambiare

l'ordine dei cicli della stessa lunghezza e ciò può essere fatto in esattamente $(t_1!)(t_2!) \cdots (t_n!)$ modi diversi. Ne segue che

$$n(\sigma) = 1^{t_1} 2^{t_2} \cdots n^{t_n} (t_1!)(t_2!) \cdots (t_n!)$$

e, quindi, tale numero dipende soltanto dal tipo di σ . Da tale osservazione segue facilmente l'asserto. \square

E' facile rendersi conto che per $n > 2$ l'unica classe di coniugio di S_n contenente un solo elemento é quella individuata dalla permutazione identica. Da questa osservazione, ricordando che un elemento g di un gruppo é centrale se, e soltanto se, la sua classe di coniugio si riduce al singleton $\{g\}$, abbiamo la seguente proposizione.

PROPOSIZIONE 1.2.5. *Per ogni intero $n > 2$ la permutazione identica é l'unico elemento centrale di S_n , cioè $Z(S_n) = \{1\}$.*

Fissato un intero $n > 0$, denotiamo con $P(n)$ l'insieme di tutte le successioni

$$(j_1, j_2, \dots, j_k)$$

di interi positivi tali che

$$j_1 \leq j_2 \leq \cdots \leq j_k \quad \text{e} \quad j_1 + j_2 + \cdots + j_k = n.$$

Gli elementi di $P(n)$ si chiamano *partizioni* dell'intero n .

Sia (j_1, j_2, \dots, j_k) una partizione di n . Se $\{i_1, i_2, \dots, i_s\}$, con $i_1 < \cdots < i_s$, é l'insieme di tutti gli interi che compaiono nella partizione (j_1, j_2, \dots, j_k) e se l'intero i_h compare esattamente t_h volte in (j_1, j_2, \dots, j_k) , poniamo

$$(j_1, j_2, \dots, j_k) = [i_1^{t_1} i_2^{t_2} \cdots i_s^{t_s}].$$

La notazione appena introdotta per le partizioni di un intero prende il nome di *notazione standard*. La seguente tabella riporta tutte le partizioni dei primi cinque interi positivi.

n	Partizioni di n
1	(1)
2	(1, 1), (2)
3	(1, 1, 1), (1, 2), (3)
4	(1, 1, 1, 1), (1, 1, 2), (1, 3), (2, 2), (4)
5	$[1^5], [1^3 2^1], [1^2 3^1], [1^4 1^1], [1^1 2^2], [2^1 3^1], [5^1]$

PROPOSIZIONE 1.2.6. *Il numero delle classi di coniugio di S_n é uguale al numero delle partizioni di n .*

DIMOSTRAZIONE. Denotiamo con Γ_n l'insieme delle classi di coniugio di S_n e ricordiamo che due permutazioni sono coniugate se, e soltanto se, sono dello stesso tipo. Se γ é una classe di coniugio e se le permutazioni contenute in γ sono quelle di tipo $j_1^{t_1} j_2^{t_2} \dots j_s^{t_s}$, denotiamo con $f(\gamma)$ la partizione $[j_1^{t_1} j_2^{t_2} \dots j_s^{t_s}]$ di n . Possiamo allora considerare la funzione

$$f : \gamma \in \Gamma \rightarrow f(\gamma) \in P(n),$$

la quale, per quanto ricordato, risulta iniettiva.

D'altra parte, se $[j_1^{t_1} j_2^{t_2} \dots j_s^{t_s}]$ é una partizione di n , é possibile trovare una permutazione di tipo $j_1^{t_1} j_2^{t_2} \dots j_s^{t_s}$ e quindi la f é anche suriettiva.

La f é dunque biunivoca e l'asserto é provato. \square

Avvertiamo il lettore che per il calcolo esplicito del numero $p(n)$ di tutte le partizioni di un intero n esistono procedimenti ricorsivi, che non riportiamo perché esulano dallo scopo di queste note. A tale proposito, osserviamo soltanto che $p(n)$ é una funzione crescente di n e, giusto per dare un'idea di come varia, riportiamo nella tabella che segue alcuni suoi valori.

n	$p(n)$	n	$p(n)$	n	$p(n)$
1	1	10	42	19	490
2	2	11	56	20	627
3	3	12	77	50	204.226
4	5	13	101	100	190.569.292
5	7	14	135	150	40.853.235.313
6	11	15	176	200	3.972.999.029.388
7	15	16	231	250	230.793.554.364.681
8	22	18	385	400	6.727.090.051.741.041.926

1.3 Il gruppo alterno

Ogni ciclo $\sigma = (j_1, j_2, \dots, j_k)$ del gruppo simmetrico S_n può scriversi come prodotto di trasposizioni, risultando

$$(j_1, j_2, \dots, j_k) = (j_1, j_2)(j_1, j_3) \dots (j_1, j_{k-1})(j_1, j_k)$$

e quindi, in forza della prop.1.1.17, la stessa proprietà é vera per una qualsiasi permutazione. Si vede facilmente che, in generale, una permutazione σ può fattorizzarsi in modi diversi mediante trasposizioni, nel senso che le trasposizioni che compaiono in una tale fattorizzazione e il loro numero non risultano degli invarianti di σ . Le possibili diverse fattorizzazioni in trasposizioni di una stessa permutazione σ possiedono però un importante invariante che prende il nome di *segno* di σ e che adesso andiamo a definire.

Sia dunque σ una permutazione e consideriamo una coppia (i, j) , ove i, j sono elementi di N_n con $i < j$. Diciamo che σ presenta una *inversione* sulla coppia (i, j) se risulta $\sigma(i) > \sigma(j)$. Ciò premesso, diciamo che σ é una permutazione *pari* se presenta un numero pari di inversioni,

dispari nel caso contrario. A questo punto, definiamo *segno* di σ , e lo denotiamo con $sgn(\sigma)$, l'intero 1 o -1 a seconda che σ sia rispettivamente pari o dispari. Per esempio, ogni trasposizione é una permutazione dispari e quindi ha segno -1 . La permutazione identica é ovviamente una permutazione pari.

Osserviamo che, per una permutazione σ , risulta

$$sgn(\sigma) = \prod_{\{i,j\} \subseteq N_n} \frac{i-j}{\sigma(i) - \sigma(j)} = \prod_{i < j} \frac{i-j}{\sigma(i) - \sigma(j)}$$

e, per ogni due permutazioni σ e τ , abbiamo

$$\begin{aligned} sgn(\sigma\tau) &= \prod_{i < j} \frac{i-j}{(\sigma\tau)(i) - (\sigma\tau)(j)} = \\ &= \left(\prod_{i < j} \frac{i-j}{\sigma(i) - \sigma(j)} \right) \left(\prod_{i < j} \frac{\sigma(i) - \sigma(j)}{\tau(\sigma(i)) - \tau(\sigma(j))} \right) = \\ &= \left(\prod_{i < j} \frac{i-j}{\sigma(i) - \sigma(j)} \right) \left(\prod_{\sigma(i) < \sigma(j)} \frac{\sigma(i) - \sigma(j)}{\tau(\sigma(i)) - \tau(\sigma(j))} \right) = \\ &= \left(\prod_{i < j} \frac{i-j}{\sigma(i) - \sigma(j)} \right) \left(\prod_{i < j} \frac{i-j}{\tau(i) - \tau(j)} \right) = sgn(\sigma)sgn(\tau). \end{aligned}$$

Ne segue che *il prodotto di due permutazioni dello stesso segno é pari, mentre il prodotto di due permutazioni di segno diverso é dispari.*

DEFINIZIONE 1.3.1. L'insieme di tutte le permutazioni pari di S_n costituisce un sottogruppo di S_n , che si denota con A_n e si chiama *gruppo alterno* su n oggetti o di grado n . \square

ESERCIZIO 1.3.2. Consideriamo la prima tabella delle due seguenti, formata da 15 quadrati numerati e da uno spazio libero.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Supponiamo che i quadrati numerati possano scorrere orizzontalmente e verticalmente usando lo spazio libero senza fuoriuscire dalla tabella stessa. Provare che, muovendo i quadrati nel modo anzidetto, non esiste alcun modo per trasformare la prima tabella nella seconda.

ESERCIZIO 1.3.3. Sia G un sottogruppo di S_n . Provare che, se G non é un sottogruppo di A_n , allora metà dei suoi elementi sono permutazioni pari e metà dispari.

ESERCIZIO 1.3.4. Provare che risulta

$$|A_n| = \frac{1}{2}n!. \quad (1.5)$$

OSSERVAZIONE 1.3.5. L'applicazione

$$\text{sgn} : \sigma \in S_n \rightarrow \text{sgn}(\sigma) \in \{1, -1\}$$

di S_n nel gruppo $(\{1, -1\}, \cdot)$ é un omomorfismo. \square

PROPOSIZIONE 1.3.6. Se $\alpha_1\alpha_2\cdots\alpha_s$ e $\beta_1\beta_2\cdots\beta_t$ sono due fattorizzazioni in trasposizioni di una stessa permutazione σ , allora gli interi s e t hanno la stessa parità; essi sono cioè o entrambi pari o entrambi dispari.

DIMOSTRAZIONE. Ogni trasposizione é una permutazione dispari. Allora il prodotto di un numero pari di trasposizioni é pari, mentre il prodotto di un numero dispari di trasposizioni é dispari. Da questa osservazione segue subito l'asserto. \square

ESERCIZIO 1.3.7. Provare che un ciclo é una permutazione pari o dispari a seconda che la sua lunghezza sia rispettivamente dispari o pari.

PROPOSIZIONE 1.3.8. Per ogni intero $n > 4$, tutti i 3-cicli sono coniugati nel gruppo alterno A_n .

DIMOSTRAZIONE. Sappiamo che ogni 3-ciclo é una permutazione pari e quindi appartiene ad A_n . Siano dunque (j_1, j_2, j_3) un 3-ciclo e σ una permutazione tale che $\sigma(1) = j_1, \sigma(2) = j_2, \sigma(3) = j_3$, onde

$$(j_1, j_2, j_3) = \sigma^{-1}(1, 2, 3)\sigma.$$

Se σ non appartiene ad A_n , posto

$$\tau = (s, t)\sigma, \quad s, t \in N_n \setminus \{1, 2, 3\},$$

abbiamo

$$\begin{aligned} \tau^{-1}(1, 2, 3)\tau &= \sigma^{-1}(s, t)(1, 2, 3)(s, t)\sigma = \\ \sigma^{-1}(1, 2, 3)(s, t)(s, t)\sigma &= \sigma^{-1}(1, 2, 3)\sigma = (j_1, j_2, j_3) \end{aligned}$$

e, poiché τ é una permutazione pari, ricaviamo che ogni 3-ciclo é coniugato di $(1, 2, 3)$ in A_n . Ne segue l'asserto. \square

PROPOSIZIONE 1.3.9. Per ogni intero $n > 2$, il gruppo alterno A_n é generato dai 3-cicli.

DIMOSTRAZIONE. Basta far vedere che il prodotto di due trasposizioni può fattorizzarsi in 3-cicli. Allora, poiché abbiamo

$$(i, j)(i, t) = (i, j, t) \text{ e } (i, j)(t, s) = (i, j, t)(t, i, s),$$

per ogni sottoinsieme $\{i, j, s, t\}$ di N_n , l'asserto é provato. \square

PROPOSIZIONE 1.3.10. *Per ogni intero positivo $n \neq 4$, il gruppo alterno A_n é semplice.*

DIMOSTRAZIONE. Assumiamo $n > 4$ perché i gruppi A_1 e A_2 sono di ordine 1 e A_3 é di ordine 3 e quindi sono senz'altro semplici. In queste ipotesi, detto H un sottogruppo normale non identico di A_n , cominciamo col provare che H contiene almeno un 3-ciclo. A tale scopo, detto p un divisore primo dell'ordine di H , il teorema di Cauchy assicura l'esistenza di un elemento $\sigma \in H$ di periodo p e questo deve ammettere una fattorizzazione in p -cicli disgiunti

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_h.$$

Se é $p > 3$ e $\sigma_1 = (i_1, i_2, \dots, i_p)$, la permutazione $(i_1, i_2, i_3)^{-1} \sigma^{-1} (i_1, i_2, i_3)$ appartiene ad H perché coniugata di $\sigma^{-1} \in H$ e H é normale in A_n . Ne segue che

$$\begin{aligned} H \ni ((i_1, i_2, i_3)^{-1} \sigma^{-1} (i_1, i_2, i_3)) \sigma &= (i_1, i_2, i_3)^{-1} (\sigma^{-1} (i_1, i_2, i_3) \sigma) = \\ &= (i_3, i_2, i_1) (\sigma(i_1), \sigma(i_2), \sigma(i_3)) = (i_3, i_2, i_1) (i_2, i_3, i_4) = (i_1, i_4, i_2) \end{aligned}$$

e cosí (i_1, i_4, i_2) é un 3-ciclo appartenente ad H .

Se é $p = 3$, possiamo supporre $h > 1$, altrimenti σ é il 3-ciclo cercato. In questo caso, posto $\sigma_1 = (i_1, i_2, i_3)$ e $\sigma_2 = (i_4, i_5, i_6)$, abbiamo

$$\begin{aligned} H \ni ((i_1, i_2, i_4)^{-1} \sigma^{-1} (i_1, i_2, i_4)) \sigma &= (i_1, i_2, i_4)^{-1} (\sigma^{-1} (i_1, i_2, i_4) \sigma) = \\ &= (i_4, i_2, i_1) (\sigma(i_1), \sigma(i_2), \sigma(i_4)) = (i_4, i_2, i_1) (i_2, i_3, i_5) = (i_1, i_4, i_3, i_5, i_2). \end{aligned}$$

H contiene dunque un 5-ciclo e, per quanto detto prima, deve contenere anche un 3-ciclo.

Se é $p = 2$, essendo σ una permutazione pari, h deve essere pari. In questo caso, nell'ipotesi che σ possega un elemento fisso, possiamo supporre $\sigma_1 = (i_1, i_2)$, $\sigma_2 = (i_3, i_4)$, $\sigma(i_5) = i_5$ e abbiamo

$$\begin{aligned} H \ni ((i_1, i_2, i_5)^{-1} \sigma^{-1} (i_1, i_2, i_5)) \sigma &= (i_1, i_2, i_5)^{-1} (\sigma^{-1} (i_1, i_2, i_5) \sigma) = \\ &= (i_5, i_2, i_1) (\sigma(i_1), \sigma(i_2), \sigma(i_5)) = (i_5, i_2, i_1) (i_2, i_1, i_5) = (i_1, i_2, i_5); \end{aligned}$$

cióé H contiene un 3-ciclo. Se invece σ non ha elementi fissi, allora é $n > 5$ e possiamo supporre $\sigma_1 = (i_1, i_2)$, $\sigma_2 = (i_3, i_4)$, $\sigma_3 = (i_5, i_6)$. Ne segue che

$$\begin{aligned} H \ni ((i_1, i_2, i_5)^{-1} \sigma^{-1} (i_1, i_2, i_5)) \sigma &= (i_1, i_2, i_5)^{-1} (\sigma^{-1} (i_1, i_2, i_5) \sigma) = \\ &= (i_5, i_2, i_1) (\sigma(i_1), \sigma(i_2), \sigma(i_5)) = (i_5, i_2, i_1) (i_2, i_1, i_6) = (i_1, i_5) (i_2, i_6) \end{aligned}$$

e, riportandoci al caso precedente, abbiamo subito che H contiene un 3-ciclo.

Resta cosí provato che in ogni caso H contiene almeno un 3-ciclo. A questo punto, la 1.3.8 e l'essere H normale in A_n , assicurano che H contiene tutti i 3-cicli. Dalla 1.3.9 segue allora che é $H = A_n$ e cióé l'asserto. \square

OSSERVAZIONE 1.3.11. Il gruppo alterno A_4 non é semplice. É infatti possibile verificare che A_4 possiede un solo sottogruppo normale non banale dato dal sottogruppo d'ordine 4

$$H = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

\square

PROPOSIZIONE 1.3.12. *Per ogni intero $n > 4$, il gruppo alterno A_n é l'unico sottogruppo normale non banale di S_n .*

DIMOSTRAZIONE. Se H é un sottogruppo normale non banale di S_n , $H \cap A_n$ é normale in S_n e quindi anche in A_n . Poiché A_n é semplice, abbiamo $H \cap A_n = \{1\}$ o $H \cap A_n = \{A_n\}$.

Nell'ipotesi $H \cap A_n = \{1\}$, abbiamo

$$HA_n = \langle H, A_n \rangle = S_n, \quad H \sim H/(H \cap A_n) \sim \langle H, A_n \rangle / A_n = S_n/A_n,$$

da cui segue che H ha ordine due, cioè é del tipo $H = \{1, \sigma\}$, ove σ é una trasposizione. Ora, essendo H normale in S_n , la classe di coniugio $cl(\sigma)$ di σ deve essere contenuta in H , cioè $cl(\sigma) = \{\sigma\}$ e σ risulta centrale. Ciò é assurdo in forza della 1.2.5.

Resta cosí provato che $H \cap A_n = A_n$ e quindi $A_n \leq H$. Allora, poiché A_n ha indice due in S_n e $H \neq S_n$, deve essere $H = A_n$ e l'asserto é completamente provato. \square

ESERCIZIO 1.3.13. *Provare che, per $n > 4$, il gruppo alterno A_n é l'unico sottogruppo di indice due in S_n .* \square