1

Capitolo D25
gruppi finiti di permutazioni

Contenuti delle sezioni

a. gruppi finiti di permutazioni [1] p. 2
b. permutazioni cicliche p. 5
c. fattorizzazioni mediante scambi e parità delle permutazioni p. 9
d. algoritmi di base per le permutazioni p. 12
e. gruppi di permutazioni p. 13
f. orbite di un gruppo di permutazioni p. 16
g. cicli di una permutazione p. 18
h. gruppo simmetrico p. 20

22 pagine

D25 0.01 In questo capitolo viene approfondito l'esame delle permutazioni di un insieme finito introdotte già in B16d e B16e.

Alberto Marini

D25 a. gruppi finiti di permutazioni [1]

D25 a.01 Consideriamo le permutazioni di un insieme finito di n elementi $X = \{x_1, x_2, ..., x_n\}$, cioè le biiezioni entro l'insieme X.
Una permutazione di X si individua naturalmente con una matrice di profilo $2 \times n$ come

$$\left\downarrow \begin{matrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{matrix} \right\downarrow , \tag{1}$$

la quale significa che la permutazione associa all'elemento $x_1 \in X$ l'elemento y_1, a x_2 l'elemento y_2, ..., a x_n l'elemento y_n.
Questa **notazione matriciale delle permutazioni** è in stretta corrispondenza con la raffigurazione sagittale della funzione $P : \lceil X \triangleleft\!\longrightarrow\!\triangleright X \rceil$

D25 a.02 Si dice genericamente **permutazione di grado** n una permutazione di un insieme avente cardinale n.

Un modello tangibile delle permutazioni di grado n considera n scatole che etichettiamo con gli interi da 1 a n in ciascuna delle quali si trova uno degli oggetti costituenti un insieme X di n elementi mutuamente distinguibili; ogni permutazione P viene descritta come un meccanismo che sposta il contenuto di ogni particolare scatola in un'altra determinata scatola (con la possibilità di lasciarlo nella stessa scatola) in modo da ottenere una configurazione che che presenta in ogni scatola uno e un solo oggetto.
Lo spostamento dell'oggetto dalla scatola i corrisponde a una freccia della raffigurazione sagittale della P intesa come funzione di X su X.
Le scatole si possono presentare allineate e quindi etichettate dagli interi da 1 ad n, in modo che gli oggetti prima della azione della permutazione risultano disposti in modo ordinato, ovvero etichettati dai suddetti interi. Una permutazione può quindi descriversi come un riordinamento di una sequenza di oggetti distinguibili.
Una permutazione infine può essere presentata mediante la sua **raffigurazione mediante il digrafo** equivalente alla sua raffigurazione sagittale.

D25 a.03 Vi sono considerazioni sulle permutazioni, tendenzialmente applicative, che tengono conto di come sono individuati o costruiti gli oggetti che vengono permutati; per altre considerazioni, tendenzialmente più astratte, non serve tenere conto delle caratteristiche genetiche degli oggetti, ma occorre solo poterli individuare distintamente.
Nel secondo caso risulta conveniente ricondursi al caso canonico delle permutazioni degli interi di **(**n **]** $= \{1, 2, ..., n\}$; in tal modo si considerano oggetti naturalmente ordinati e gli oggetti si possono confondere con le posizioni delle scatole allineate, ciascuna in grado di contenerne uno in ogni istante.
Per le considerazioni generali sulle permutazioni ci limiteremo a considerare trasformazioni dei primi n interi positivi. Una permutazione P corrisponde allora a un riordinamento della sequenza $\langle 1, 2, ..., n\rangle$ nella sequenza che scriviamo $\langle 1P, 2P, ..., nP\rangle$.
In questa scrittura consideriamo una permutazione come un operatore la cui applicazione a un intero $i \in$ **(**n **]** fornisce l'intero che individuiamo con la scrittura suffissa iP.

D25 a.04 Una permutazione P di **(**n **]**, quindi, quando si pone l'accento sulla sua natura di trasformazione, può essere rappresentata con la notazione matriciale

$$P = \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1P & 2P & \dots & nP \end{matrix} \right\downarrow .$$

Nella precedente matrice, l'ordine delle colonne è inessenziale; queste possono essere riordinate arbitrariamente: quindi se T denota una arbitraria permutazione di (n], si può scrivere equivalentemente:

$$P = \left\downarrow \begin{matrix} 1T & 2T & \dots & nT \\ 1TP & 2TP & \dots & nTP \end{matrix} \right\downarrow ,$$

dove si intende che $i\,T\,P \;:=\; (i\,T)P = i_{,}(T \circ_{lr} P)$.

Se in particolare $T = P^{-\mathbf{1}}$ si ha:

$$P = \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1P & 2P & \dots & nP \end{matrix} \right\downarrow = \left\downarrow \begin{matrix} 1P^{-\mathbf{1}} & 2P^{-\mathbf{1}} & \dots & nP^{-\mathbf{1}} \\ 1 & 2 & \dots & n \end{matrix} \right\downarrow .$$

La precedente uguaglianza chiarisce il rapporto tra una permutazione e la sua inversa.

Oltre alle notazioni matriciali, per presentare P si può usare l'equivalente più concisa rappresentazione sequenziale formata dalla seconda riga della prima rappresentazione matriciale $P = \langle 1P, 2P, ..., nP\rangle$.

D25 a.05 Il prodotto di composizione di due permutazioni di (n] P e Q si può definire con

$$P \circ_{lr} Q \;:=\; \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1\,P & 2\,P & \dots & n\,P \end{matrix} \right\downarrow \circ_{lr} \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1\,Q & 2\,Q & \dots & n\,Q \end{matrix} \right\downarrow := \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1\,P\,Q & 2\,P\,Q & \dots & n\,P\,Q \end{matrix} \right\downarrow .$$

Denotiamo con Sym_n l'insieme di tutte le permutazioni di (n] e più in generale scriviamo Sym_X l'insieme di tutte le permutazioni di un insieme generico X.

Con la scrittura matriciale è semplice verificare che Sym_X munito del prodotto di composizione, dell'inversione (composizionale) e dell'identità $\boldsymbol{Id}_X$ costituisce un gruppo.
È sufficiente verificare che per $X =$ (n] valgono i quattro assiomi della specie strutturale dei gruppi.

(1) $\forall P, Q \in \mathsf{Sym}_X \;:\; P \circ Q \in \mathsf{Sym}_n$: scende dalla uguaglianza precedente.

(2) Il prodotto di composizione è associativo: questo vale per ogni prodotto di trasformazioni.

(3) Sym_n contiene un elemento neutro per il prodotto: si tratta della trasformazione identica di (n] che qui denotiamo con $\boldsymbol{Id}_n$:

$$I = \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{matrix} \right\downarrow .$$

(4) $\forall P \in \mathsf{Sym}_n \,:\, \mathsf{Sym}_n \ni P^{-\mathbf{1}}$: si tratta di

$$P^{-\mathbf{1}} = \left\downarrow \begin{matrix} 1\,P & 2\,P & \dots & n\,P \\ 1 & 2 & \dots & n \end{matrix} \right\downarrow \;=\; \left\downarrow \begin{matrix} 1 & 2 & \dots & n \\ 1(P^{-\mathbf{1}}) & 2(P^{-\mathbf{1}}) & \dots & n(P^{-\mathbf{1}}) \end{matrix} \right\downarrow ,$$

permutazione inversa funzionale della P per la quale si ha: $P \circ P^{-\mathbf{1}} \;=\; P^{-\mathbf{1}} \circ P = \mathsf{Id}_n$.

Quindi l'insieme delle permutazioni di (n] costituisce un gruppo chiamato **gruppo simmetrico** di (n] o **gruppo totale delle permutazioni** di (n].

In generale per un insieme qualsiasi X denotiamo con Sym_X il gruppo simmetrico dell'insieme X.

D25 a.06 Sappiamo che dati n oggetti, e in particolare dato (n], il numero delle loro permutazioni è $n!$: questo dice che l'ordine del gruppo Sym_n è $n!$, cioè che $|\mathsf{Sym}_n| \;=\; n!$.

Per esempio il gruppo Sym_3 delle permutazioni su $\{1, 2, 3\}$ è formato da $3! = 3 \cdot 2 \cdot 1 = 6$ elementi:

$$e = \left\downarrow \begin{matrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{matrix} \right\downarrow \quad a = \left\downarrow \begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix} \right\downarrow \quad b = \left\downarrow \begin{matrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{matrix} \right\downarrow$$

$$c = \left\downarrow \begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix} \right\downarrow \quad d = \left\downarrow \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix} \right\downarrow \quad f = \left\downarrow \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix} \right\downarrow$$

Invece l'ordine di Sym_4 è 24, e gli ordini dei gruppi Sym_k per $k = 5, 6, 7, 8, 9, 10$ sono, risp., 120, 720, 5040, 40 320, 362 880 e 628 800.

D25 a.07 I gruppi simmetrici sono oggetti matematici di importanza primaria, in quanto su di essi e sui loro sottogruppi si basa lo studio delle simmetrie di tutte le entità di interesse matematico, scientifico o tecnologico individuate da un numero finito di oggetti.

Il loro studio è molto avanzato e si collega a una vastissima varietà di argomenti e problemi che si trovano nella matematica (combinatorica, geometria, teoria delle funzioni speciali, ...), in discipline come la fisica, la chimica, la statistica, la biologia, la ricerca operativa, l'ingegneria strutturale, ...

Alle elaborazioni sul gruppo simmetrico sono dedicati anche sofisticati pacchetti software.

D25 b. permutazioni cicliche

D25 b.01 Consideriamo una permutazione della forma

$$C = \left\downarrow \begin{matrix} i_1 & i_2 & \dots & i_{m-1} & i_m & i_{m+1} & \dots & i_n \\ i_2 & i_3 & \dots & i_m & i_1 & i_{m+1} & \dots & i_n \end{matrix} \right\downarrow ,$$

dove $\langle i_1, i_2, \dots, i_n \rangle$ è una qualsiasi permutazione dei primi n interi; questa permutazione presenta $n - m$ punti fissi, $i_{m+1}, ..., i_n$, e viene detta **permutazione circolare**, **permutazione ciclica** o anche, sbrigativamente, ciclo di lunghezza m.

Per una permutazione ciclica come la precedente adottiamo la notazione $(i_1\ i_2\ \dots\ i_m) := C$.

Per questa notazione la scelta dell'elemento che si pone nella prima posizione tra le parentesi è irrilevante, conta solo il succedersi ciclico degli oggetti tra le parentesi. Si ha cioè: $C = (i_r\ i_{r+1}\ \dots\ i_m\ i_1\ \dots\ i_{r-1})$ per $r = 1, 2, ..., m$, ovvero $(i_1, ..., i_r, j_1, ..., j_s) = (j_1, ..., j_s, i_1, ..., i_r)$.

D25 b.02 Denotiamo con $\boldsymbol{Cycl}_n$ il sottoinsieme di Sym_n costituito dalle permutazioni cicliche e con $\boldsymbol{Cycl}_{n,m}$ l'insieme delle permutazioni cicliche di (n] aventi lunghezza m.
Evidentemente $\boldsymbol{Cycl}_n$ si ripartisce negli insiemi delle permutazioni cicliche delle diverse lunghezze ammissibili e queste vanno da 1 a n:

(1) Prop.: $\boldsymbol{Cycl}_n = \dot\cup_{m=1}^{n} \boldsymbol{Cycl}_{n,m}$ ∎

Si osserva subito che la sola permutazione riconducibile ad un ciclo a un solo elemento è l'identità, $\boldsymbol{Cycl}_{n,1} = \{\boldsymbol{Id}_n\}$ e che $\boldsymbol{Cycl}_{n,2} = \{i = 1, ..., n-1 \wedge j = i+1, ..., n :| (i\ j)\}$.

Quindi in termini di cardinali $|\boldsymbol{Cycl}_{n,1}| = 1$ e $|\boldsymbol{Cycl}_{n,2}| = \dfrac{n(n-1)}{2}$.
I cicli di lunghezza n sono rappresentati dalle scritture $(i_1, ..., i_n)$; queste sono in biiezione con le permutazioni di (n], cioè sono $n!$; accade però che le n scritture ottenibili l'una dall'altra per permutazione circolare individuano lo stesso ciclo; quindi: $|\boldsymbol{Cycl}_{n,n}| = (n-1)!$.

D25 b.03 Esaminiamo ora i cicli costituenti $\boldsymbol{Cycl}_{n,m}$.
Ogni scrittura $(i_1, ..., i_m)$ individua uno di questi cicli; queste scritture sono in biiezione con le disposizioni senza ripetizioni di lunghezza m e quindi sono $n(n-1)\cdots(n-m+1) = n^{\underline{m}}$; accade però che queste scritture si ripartiscono in classi, ciascuna di m elementi ottenibili da uno di essi per permutazioni circolari e che tutte le scritture di una classe individuano la stessa permutazione ciclica.
Quindi $|\boldsymbol{Cycl}_{n,m}| = \dfrac{n(n-1)\cdots(n-m+1)}{m}$.

Tenendo conto di b.02(1), si ottiene quindi:

(1) Prop.: $|\boldsymbol{Cycl}_n| = 1 + \sum_{m=2}^{n} \frac{n(n-1)\cdots(n-m+1)}{m}$ ∎

Per esempio tra le 3!=6 permutazioni di $\{1,2,3\}$ si trovano 1 ciclo di lunghezza 1, 3 di lunghezza 2 e 2 di lunghezza 3.
Per trovare permutazioni non cicliche occorre cercarle nei Sym_n con $n \geq 4$.

D25 b.04 (1) Eserc. Verificare che $\langle m = 1, ..., 4 :| \, |\boldsymbol{Cycl}_{4,m}| \rangle = \langle 1, 6, 8, 6 \rangle$ e che vi sono $3 = 24 - 21$ permutazioni di **(**4**]** non cicliche.

(2) Eserc. Verificare che $\langle m = 1, ..., 5 :| \, |\boldsymbol{Cycl}_{5,m}| \rangle = \langle 1, 10, 20, 30, 24 \rangle$ e che vi sono $35 = 120 - 85$ permutazioni di **(**5**]** non cicliche.

(3) Eserc. Determinare le 3 sequenze $\langle m = 1, ..., n :| \, |\boldsymbol{Cycl}_{n,m}| \rangle$ e le corrispondenti sequenze $|\mathsf{Sym}_n \setminus \boldsymbol{Cycl}_n|$ per $n = 6, 7, 8$.

D25 b.05 Prop. Ogni permutazione può essere espressa come prodotto di cicli disgiunti.

Dim.: Presa una permutazione P di **(**n **]** e un qualsiasi intero di questo insieme i_{11}, si osserva che questo viene trasformato in $i_{11}P =: i_{12}$, che questo a sua volta va in $i_{11}P^2 =: i_{13}$, e così via finchè si ottiene di nuovo l'elemento i_{11} come $i_{11} = i_{11}P^{m_1}$. A questo punto, o si sono esauriti tutti gli interi di **(**n **]** in quanto la P è ciclica, oppure $n - m$ di essi non sono stati incontrati.

In quest'ultimo caso si riprende il procedimento precedente a partire da uno qualsiasi degli interi rimanenti; chiamatolo i_{21}, si ottiene il ciclo **(**$i_{21}\ i_{21}P$ ... $i_{21}P^{m_2} = i_{21}$**)**. Questo procedimento si può portare avanti fino a quando si sono inseriti in qualche ciclo tutti gli interi di **(**n **]**.

La generica permutazione di **(**n **]** si può quindi scrivere:

$$P = \left\downarrow \begin{matrix} 1 & \dots & n \\ 1P & \dots & nP \end{matrix} \right\downarrow = \left\downarrow \begin{matrix} i_{11} & i_{12} & \dots & i_{1m_1} & i_{21} & i_{22} & \dots & i_{2m_2} & \dots & i_{r1} & i_{r2} & \dots & i_{rm_r} \\ i_{12} & i_{13} & \dots & i_{11} & i_{22} & i_{23} & \dots & i_{21} & \dots & i_{r2} & i_{r3} & \dots & i_{r1} \end{matrix} \right\downarrow$$

$$= \mathbf{(}i_{11}\ i_{11}P\ i_{11}P^2\ ...\ i_{11}P^{m_1-1}\mathbf{)} \circ \mathbf{(}i_{21}\ i_{21}P\ i_{21}P^2\ ...\ i_{21}P^{m_2-1}\mathbf{)} \circ \ldots \circ \mathbf{(}i_{r1}\ i_{r1}P\ i_{r1}P^2\ ...\ i_{r1}P^{m_r-1}\mathbf{)}\ .$$

D25 b.06 Due permutazioni di un insieme si dicono **permutazioni disgiunte-t** sse i due insiemi di oggetti che esse non lasciano fissi sono disgiunti. Evidentemente due permutazioni disgiunte-t commutano; in particolare commutano due cicli disgiunti.

La precedente espressione per P costituisce una **fattorizzazione di una permutazione mediante cicli disgiunti**. Quindi è possibile cambiare ad arbitrio l'ordine dei suoi fattori (in accordo con le arbitrarietà delle scelte nel procedimento in b.05 .

La fattorizzazione in cicli disgiunti di una permutazione è unica a meno di permutazioni dei cicli fattori. Una permutazione quindi può essere significativamente caratterizzata dal multiinsieme delle lunghezze dei suoi fattori ciclici; equivalentemente viene caratterizzata da una partizione dell'intero n o da una forma di Ferrers di area n. Questa caratterizzazione risulta evidente dalla rappresentazione mediante digrafo della permutazione.

Per ogni permutazione $\boldsymbol{P}$ di grado n denotiamo con *prti*($\boldsymbol{P}$) la corrispondente partizione di n e con *frrs*($\boldsymbol{P}$) la forma di Ferrers associata.

Solitamente le scritture delle fattorizzazioni come la precedente si semplificano omettono i cicli di lunghezza 1 e i segni "∘". Inoltre usiamo la scrittura **(**1**)** per denotare l'identità di **(**n **]**.

D25 b.07 Consideriamo l'esempio della permutazione

$$\rho = \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 3 & 5 & 9 & 6 & 8 & 7 \end{matrix} \right\downarrow .$$

La sua fattorizzazione mediante cicli è:

$$\rho = (1\ 2\ 4\ 3)(5)(6\ 9\ 7)(8) = (1\ 2\ 4\ 3)(6\ 9\ 7)$$

D25 b.08 La rappresentazione delle permutazioni mediante cicli può risultare conveniente nel calcolo del prodotto di più permutazioni. Per esempio consideriamo le permutazioni:

$$f = (1\ 3\ 4)(2\ 6) \qquad g = (1\ 5\ 2)(3\ 6\ 4) \qquad h = (1\ 4\ 5\ 6)$$

e calcoliamo il prodotto $p = f \cdot g \cdot h = (1\ 3\ 4)(2\ 6)(1\ 5\ 2)(3\ 6\ 4)(1\ 4\ 5\ 6)$.

In genere conviene determinare la rappresentazione ciclica del prodotto iniziando dal numero 1 e individuando le modifiche alle quali viene sottoposto dai fattori ciclici considerati da destra a sinistra; dai cicli si ricava la sequenza delle trasformazioni:

$$1 \to 4 \to 3 \to 3 \to 3 \to 4$$

Considerati tutti i fattori otteniamo $1\,p = 4$. Si individuano poi le trasformazioni subite dal numero 4:

$$4 \to 5 \to 5 \to 2 \to 6 \to 6$$

ottenendo $4\,p = 6$; ricominciando dal numero 6 e poi dal 5 si trova:

$$6 \to 1 \to 1 \to 5 \to 5 \to 5$$

$$5 \to 6 \to 4 \to 4 \to 4 \to 1$$

Avendo ottenuto di nuovo il numero 1 da cui siamo partiti, risulta concluso il ciclo $(1\ 4\ 6\ 5)$. Dato che non si sono incontrati tutti gli interi di $(6]$, si può ripartire dal più piccolo intero non incluso nel ciclo, il numero 2, e costruire con lo stesso procedimento il secondo ciclo; si trova allora che:

$$2 \to 2 \to 2 \to 1 \to 1 \to 3$$

$$3 \to 3 \to 6 \to 6 \to 2 \to 2$$

Con il secondo ciclo si esaurisce $(6]$; quindi:

$$f \circ g \circ h = (1\ 3\ 4)(2\ 6)\ (1\ 5\ 2)(3\ 6\ 4)\ (1\ 4\ 5\ 6) = (1\ 4\ 6\ 5)(2\ 3)$$

D25 b.09 La scrittura mediante cicli di una permutazione di n oggetti, ovvero le corrispondenti partizione di n e forma di Ferrers di peso n, permettono di caratterizzare completamente ed efficacemente la classe di coniugio del gruppo Sym_n cui essa appartiene.

(1) Prop.: Consideriamo due permutazioni di grado n $\boldsymbol{P}$ e $\boldsymbol{Q}$. $P \sim Q \iff prti(P) = prti(Q)$.

Dim.: "$\Longrightarrow$" Per la permutazione P scriviamo

$$P = \left\downarrow \begin{matrix} i_1 & i_1P & \dots & i_1P^{m_1-1} & \dots & i_r & i_rP & \dots & i_rP^{m_r-1} \\ i_1P & i_1P^2 & \dots & i_1 & \dots & i_rP & i_rP^2 & \dots & i_r \end{matrix} \right\downarrow .$$

Se Q appartiene alla sua stessa classe di coniugio possiamo scrivere per qualche permutazione T:

$$Q = T^{-1} \circ P \circ T = \left\downarrow \begin{matrix} iT \\ i \end{matrix} \right\downarrow \ \circ\ P\ \circ\ \left\downarrow \begin{matrix} i \\ iT \end{matrix} \right\downarrow =$$

$$\left\downarrow \begin{matrix} i_1T & i_1PT & \cdots & i_1P^{m_1-1}T & \cdots & i_rT & i_rPT & \cdots & i_rP^{m_r-1}T \\ i_1PT & i_1P^2T & \cdots & i_1T & \cdots & i_rPT & i_rP^2T & \cdots & i_rT \end{matrix} \right\downarrow =$$

$$\left\downarrow \begin{matrix} i_1 & i_1T^{-1}PT & \cdots & i_1T^{-1}P^{m_1-1}T & \cdots & i_r & i_rT^{-1}PT & \cdots & i_rT^{-1}P^{m_r-1}T \\ i_1T^{-1}PT & i_1T^{-1}P^2T & \cdots & i_1 & \cdots & i_rT^{-1}PT & i_rT^{-1}P^2T & \cdots & i_r \end{matrix} \right\downarrow =$$

$$(i_1\ i_1Q\ i_1Q^2\ \cdots\ i_1Q^{m_1-1})\cdots(i_r\ i_rQ\ i_rQ^2\ \cdots\ i_rQ^{m_r-1})\ .$$

Quindi per Q si è trovata una struttura ciclica uguale a quella di P.

"$\Longleftarrow$" Se P e Q hanno la stessa struttura ciclica:

$$P = (i_1\ i_1P\ i_1P^2\ \cdots\ i_1P^{m_1-1})\cdots(i_r\ i_rP\ i_rP^2\ \cdots\ i_rP^{m_r-1})$$
$$Q = (j_1\ j_1Q\ j_1Q^2\ \cdots\ j_1Q^{m_1-1})\cdots(j_r\ j_rQ\ j_rQ^2\ \cdots\ j_rQ^{m_r-1})$$

Si trova un'altra permutazione T tale che $Q = T^{-1} \circ P \circ T$ e precisamente:

$$Q = \left\downarrow \begin{matrix} j_1 & j_1Q & \cdots & j_1Q^{m_1-1} & \cdots & j_r & j_rQ & \cdots & j_rQ^{m_r-1} \\ i_1 & i_1P & \cdots & i_1P^{m_1-1} & \cdots & i_r & i_rP & \cdots & i_rP^{m_r-1} \end{matrix} \right\downarrow .$$

$$\left\downarrow \begin{matrix} i_1 & i_1P & \cdots & i_1P^{m_1-1} & \cdots & i_r & i_rP & \cdots & i_rP^{m_r-1} \\ i_1P & i_1P^2 & \cdots & i_1 & \cdots & i_rP & i_rP^2 & \cdots & i_r \end{matrix} \right\downarrow .$$

$$\left\downarrow \begin{matrix} i_1P & \cdots & i_1P^{m_1-1} & i_1 & \cdots & i_rP & \cdots & i_rP^{m_r-1} & i_r \\ j_1Q & \cdots & j_1Q^{m_1-1} & j_1 & \cdots & j_rQ & \cdots & j_rQ^{m_r-1} & j_r \end{matrix} \right\downarrow$$

Quindi P eQ appartengono alla stessa classe di coniugio ∎

D25 b.10 Le permutazioni di Sym_n costituenti una classe di coniugio sono caratterizzate dall'avere una stessa struttura ciclica, cioè contengono lo stesso numero α_1 di cicli a un elemento, lo stesso numero α_2 di cicli a due elementi (cicli binari), ... , lo stesso numero α_n di cicli ad n elementi. Questi α_i sono numeri interi positivi o nulli caratterizzati dal soddisfare l'equazione:

$$\sum_{i=1}^{n} i\,\alpha_i \ = \ n\ . \tag{1}$$

Una classe di Sym_n risulta completamente definita fornendo una sequenza $\underline{\alpha} = \langle \alpha_1, ..., \alpha_n \rangle \in \mathbb{N}^n$ che verifica l'equazione precedente. Riferendosi a tale sequenza la classe di coniugio viene denotata con $\mathcal{C}^{(\underline{\alpha})}$.

D25 b.11 Le permutazioni cicliche di lunghezza 2 si dicono **scambi** o **trasposizioni**.
L'insieme $\boldsymbol{Cycl}_{n,2}$ degli scambi di Sym_n si denota anche con $\boldsymbol{Excgs}_n$; si è visto che $|\boldsymbol{Excgs}_n| = \frac{n(n-1)}{2}$.

Evidentemente uno scambio coincide con il proprio inverso, $\langle_{cy} i, j\rangle^{-1} = \langle_{cy} Ii, j\rangle$; gli scambi quindi sono permutazioni involutorie e sono involutori anche i prodotto di scambi disgiunti.

La permutazione inversa di una ciclica è anch'essa ciclica e può esprimersi con la riflessa della notazione sequenziale: $\left\langle_{cy} i_1, i_2, ..., i_{r-1}, i_r\right\rangle^{-1} = \left\langle_{cy} i_r, i_{r-1}, ..., i_2, i_1\right\rangle$. Questa formula è ben chiarita dalla raffigurazione dei cicli mediante digrafi.

(1) Prop.: L'inversa di una permutazione P^{-1} appartiene alla stessa classe di cui fa parte P.

Dim.: Infatti da una espressione di P come prodotto di cicli disgiunti

$$P = (i_{11}\ i_{12}\ \cdots\ i_{1m_1}) \circ (i_{21}\ i_{22}\ \cdots\ i_{2m_2}) \circ \ldots \circ (i_{r1}\ i_{r2}\ \cdots\ i_{rm_r})\ ,$$

si ricava l'espressione analoga

$$P^{-1} = (i_{1m_1} \ \cdots \ i_{12} \ i_{11}) \circ (i_{2m_2} \ \cdots \ i_{22} \ i_{21}) \circ \ldots \circ (i_{rm_r} \ \cdots \ i_{r2} \ i_{r1}) \ ,$$

caratterizzata dalla stessa partizione di n ∎

D25 b.12 Prop. Il numero delle classi di coniugio di Sym_n è dunque uguale al numero delle partizioni di n ottenuto in D23:

$$p(n) = \sum_{1 \leq \frac{3k^2 \pm k}{2} \leq n} (-)^{k-1} p\left(n - \frac{3k^2 \pm k}{2}\right) \ .$$

dove si è posto $p(0) = 1$.

D25 b.13 Si pone naturalmente il problema di determinare il cardinale di ciascuna classe di coniugio: più precisamente si vuole determinare il numero di permutazioni che contengono α_1 cicli di lunghezza uno, α_2 cicli binari, ..., α_n cicli di lunghezza n. Questo problema è risolto dal seguente enunciato.

(1) Prop.: formula di Cauchy per le classi di coniugio

$$|\mathcal{C}^{(\underline{\alpha})}| = \frac{n!}{\prod_{i=1}^{n} i^{\alpha_i} \alpha_i!},$$

. . . . ∎

Per esempio, per $n = 3$ e $\alpha = (1, 1, 0)$, il numero di permutazioni con un ciclo di lunghezza 1 e un ciclo binario sono:

$$|\mathcal{C}^{(1,1,0)}| = \frac{3!}{1 \cdot 1! \cdot 2 \cdot 1!} = 3,$$

Queste permutazioni sono:

$$a = (1\ 2)(3) \qquad b = (1\ 3)(2) \qquad c = (3\ 2)(1).$$

D25 b.14 Prop. Ogni permutazione f di un insieme finito X di n elementi può essere associata a un digrafo i cui nodi che scriviamo 1,2,...n rappresentano gli elementi di X e i cui archi sono le n coppie $\langle i, f(i)\rangle$, ciascuna raffigurata da un segmento orientato da i a $f(i)$ (la direzione viene presentata con una freccia). Per esempio, per

$$f = \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{matrix} \right\downarrow = (1\ 3\ 4\ 2)$$

abbiamo la seguente raffigurazione:

Poiché f è una biiezione, in ogni vertice i esiste uno e uno solo arco entrante e uno e uno solo arco uscente.

Un altro esempio è dato dalla seguente permutazione:

$$g = \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{matrix} \right\downarrow = (1\ 3\ 2)(4)(5)(6)$$

che è una permutazione circolare sugli elementi 1,2,3. La sua rappresentazione mediante un grafo è:

D25 c. fattorizzazioni mediante scambi e parità delle permutazioni

D25 c.01 Dopo aver visto che ogni permutazione di Sym_n si può fattorizzare mediante elementi di $\boldsymbol{Cycl}_n$, vediamo come i cicli a loro volta si possono esprimere mediante prodotti di scambi.

Poiché $(i_1\ i_2\ \cdots\ i_m) = (j\ i_1\ i_2\ \cdots\ i_k)(j\ i_{k+1}\ \cdots\ i_m\ i_1) \qquad j = 1, ..., n$, si ha allora:

$(i_1\ i_2\ \cdots\ i_m) = (j\ i_m)(j\ i_1)(j\ i_2)\cdots(j\ i_m)$

$(i_1\ i_2\ i_3\ \cdots\ i_{m-1}\ i_m) = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_{m-1})(i_1\ i_m)$

ossia:

$(*c*) = (i_r\ i_{r+1})(i_r\ i_{r+2})\cdots(i_r\ i_m)(i_r\ i_1)\cdots(i_r\ i_{r-1}) \qquad r = 1, ..., m$

ed anche che:

$= (i_m\ i_{m-1})(i_{m-1}\ i_{m-2})\cdots(i_3\ i_2)(i_2\ i_1)$

ossia:

$= (i_r\ i_{r-1})(i_{r-1}\ i_{r-2})\cdots(i_2\ i_1)(i_1\ i_r)(i_r\ i_{r-1})(i_{r+2}\ i_{r+1}) \qquad r = 1, ..., m$

In particolare si deve tener presente che:

$(i\ j\ k) = (j\ k)(i\ j) = (i\ j)(i\ k) = (k\ i)(k\ j)$.

D25 c.02 A loro volta ogni elemento di Sym_n può essere fattorizzato come prodotto degli $n-1$ scambi di interi successivi $\boldsymbol{(i\ i+1)}$, $\quad i = 1, ..., n-1$, il cui insieme denotiamo con $\boldsymbol{Excgs}_n$. Un qualsiasi scambio si può scrivere come $(i\ i+r) \quad r \geq 1$ e si ha:

$(i\ i+r) = (i\ i+1)(i+1, i+2)\cdots(i+r-1, i+r)(i+r-2, i+r-1)\cdots(i+1, i+2)(i\ i+1) =$

$(!) = (i+r-1, i+r-2)\cdots(i+1, i+2)(i\ i+1)(i+1, i+2)\cdots(i+r-1, i+r-2)$

D25 c.03 $\boldsymbol{Excgs}_n$ è un insieme di generatori di Sym_n. Le formule precedenti evidenziano come si possa ottenere la fattorizzazione di una permutazione qualsiasi mediante scambi di interi successivi.

Per ottenere questo non si ha un procedimento univoco; in particolare si ha ampia arbitrarietà quando si esprime un elemento di $\boldsymbol{Cycl}_n$ con fattori di $\boldsymbol{Excgs}_n$.
Si possono quindi ottenere diverse espressioni di una permutazione mediante scambi di interi successivi, nelle quali il numero dei fattori può essere sensibilmente diverso.

D25 c.04 Non si conosce un criterio univoco per ottenere per qualsiasi permutazione la fattorizzazione di lunghezza minima. Si può notare che nella espressione degli elementi di $\boldsymbol{Cycl}_n$ in trasposizione, conviene utilizzare per ogni ciclo la formula $(*c*)$ partendo dall'intero i_r il cui valore si avvicina maggiormente alla media aritmetica degli interi costituenti il ciclo stesso.
Strettamente potrebbero influire anche la scelta dell'ordine dei fattori nella fattorizzazione della permutazione in elementi di $\boldsymbol{Cycl}_n$ e la scelta delle due possibili fattorizzazioni presentate nella (!).

D25 c.05 Accade che per una fissata permutazione il numero di tali trasposizioni deve essere sempre pari o dispari. Le permutazioni del primo tipo si chiamano **permutazioni pari**, quelle del secondo **permutazioni dispari**. Le prime, nel loro insieme, costituiscono il cosiddetto **gruppo alternante** denotato con $\mathcal{A}_n$, sottogruppo invariante di Sym_n, cioè tale che $P^{-1}\mathcal{A}_n P = \mathcal{A}_n$, e unico almeno per $n \neq 4$. $\mathcal{A}_n$ è l'insieme delle classi Sym_n caratterizzate dall'avere un numero pari di cicli di lunghezza pari.

D25 c.06 Per poter parlare di parità di una permutazione dobbiamo introdurre alcuni parametri numerici.

Consideriamo la generica permutazione P di $\{1, ..., n\}$ e per ogni intero $i \in$ (n] diciamo **insieme delle inversioni apportate alla permutazione** P da i, l'insieme degli interi maggiori di i che nella rappresentazione sequenziale di P precedono i e sono maggiori di i; denotiamo tale insieme con $I(P, i)$.
Ad esempio per la permutazione

$$\overline{P} := \left\downarrow \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{matrix} \right\downarrow = \langle 4\ 5\ 1\ 2\ 3 \rangle \ .$$

abbiamo:

$I(\overline{P}, 1) = \{4, 5\}$, $I(\overline{P}, 2) = \{4, 5\}$, $I(\overline{P}, 3) = \{4, 5\}$ $\quad I(\overline{P}, 4) = \emptyset$, $\ I(\overline{P}, 5) = \emptyset$.

Definiamo come **numero totale di inversioni della permutazione** P l'intero naturale che denotiamo con $\mathsf{perminvN}(P)$ dato dalla somma sugli $i \in$ (n] dei cardinali degli $I(P, i)$; ad esempio:

$$\mathsf{perminvN}(\overline{P}) = 2 + 2 + 2 = 6.$$

D25 c.07 Definiamo **segnatura della permutazione** P la quantità $\ \mathrm{sign}(P) \ := \ (-1)^{\mathsf{perminvN}(P)}$.
La segnatura permette di fare una importante distinzione tra le permutazioni: definiamo **permutazione pari** una permutazione P con $\mathrm{sign}(P) = +1$; e definiamo **permutazione dispari** una permutazione P con $\mathrm{sign}(P) = -1$.

La parità di una permutazione può essere determinata anche facendo riferimento alla fattorizzazione delle permutazioni mediante scambi di interi successivi.

D25 c.08 Prop. Se una permutazione P può essere espressa come prodotto di q scambi, allora q e $\mathsf{perminvN}(P)$ hanno la stessa parità ∎

In altre parole, se una permutazione P può essere espressa come prodotto di un numero pari di scambi, allora è pari, mentre se è esprimibile come prodotto di un numero dispari di scambi, allora è dispari.

Per ottenere una fattorizzazione mediante scambi di interi successivi non si ha un procedimento univoco; in particolare si ha ampia arbitrarietà quando si esprime un elemento di $\boldsymbol{Cycl}_n$ con fattori di $\boldsymbol{Excgs}_n$. Si possono quindi ottenere diverse espressioni di una permutazione mediante trasposizioni di elementi successivi, nelle quali il numero dei fattori può essere sensibilmente diverso.

D25 c.09 Prop. In ogni gruppo di permutazioni $G \subseteq \mathsf{Sym}_n$, o tutte le permutazioni sono pari, oppure ci sono tante permutazioni dispari quante sono le pari.

Dim.: Supponiamo che G contenga una permutazione dispari Q, cioè tale che $\mathrm{sign}(Q) = -1$. Dato che la mappa $\ulcorner P \in G \mapsto QP \urcorner$ di G in se stesso è una biiezione, si ha

$$\sum_{P \in G} \mathrm{sign}(P) = \sum_{P \in G} \mathrm{sign}(QP) = \sum_{P \in G} \mathrm{sign}(Q)\mathrm{sign}(P) = -\sum_{P \in G} \mathrm{sign}(P) \ .$$

Quindi

$$\sum_{P \in G} \mathrm{sign}(P) = 0 \ .$$

Questo ci dice che il numero delle permutazioni P con $\mathrm{sign}(P) = +1$ è uguale al numero delle permutazioni P con $\mathrm{sign}(P) = -1$ ∎

D25 c.10 Prop. L'insieme di tutte le permutazioni pari di (n]

$$\mathcal{A}_n \ := \ \{g \in \mathsf{Sym}_n \ ST \ \mathrm{sign}(g) = +1\}$$

è un sottogruppo normale di Sym_n chiamato **gruppo alternante**. Esso contiene $\frac{1}{2}n!$ elementi ∎

D25 c.11 Prop. Il gruppo alternante $\mathcal{A}_n$ è generato da $n - 2$ permutazioni circolari

$$t_3 = (1\ 2\ 3) \quad t_4 = (1\ 2\ 4) \quad \dots \quad t_n = (1\ 2\ n)\ .$$

Dim.: . . . ∎

D25 d. algoritmi di base per le permutazioni

D25 d.01 Nella pratica delle elaborazioni discrete si pone il problema di generare tutte le permutazioni di una Sym_n secondo qualche opportuno ordinamento totale.

Il problema dell'ordinamento e della generazione automatica secondo l'ordinamento totale, si pone anche per altri allineamenti di interi, ad ese. per le partizioni di interi rappresentate dagli allineamenti $(\underline{\alpha})$ oppure dagli $\big[m\big]$.

Per ogni insieme di allineamenti di interi, e più in generale per ogni insieme di allineamenti di oggetti sui quali è definito un ordinamento totale, si possono definire quattro tipi di ordinamenti canonici che denoteremo, risp., con Ω, $\Omega^{\leftarrow}$, $\overset{\sim}{\Omega}$, $\overset{\sim}{\Omega}^{\leftarrow}$.

Secondo Ω, detto **ordinamento lessicografico crescente**, dati due allineamenti $i_1, i_2, ..., i_r$ e $j_1, j_2, ..., j_r$, il primo precede il secondo sse accade che la prima delle differenze $i_k - j_k$, per $k = 1, ..., min(r, s)$, nonnulla, è negativa, oppure se $i_k = j_k$ per $k = 1, ..., r$ ed $r < s$.
L'ordinamento riflesso del precedente $\Omega^{\leftarrow}$ è chiamato **ordinamento lessicografico decrescente**.

Secondo l'ordinamento $\overset{\sim}{\Omega}$, detto **ordinamento antilessicografico crescente**, si dice che dei suddetti allineamenti, il primo precede il secondo se $r < s$, oppure, nel caso $r = s$, se l'ultima tra le differenze $i_k - j_k$ è negativa.
L'ordinamento riflesso del precedente $\overset{\sim}{\Omega}^{\leftarrow}$ viene chiamato **ordinamento antilessicografico decrescente**.

D25 e. gruppi di permutazioni

D25 e.01 Consideriamo un insieme finito X e un insieme G di permutazioni entro X. Consideriamo in particolare il caso in cui le permutazioni costituenti G formano gruppo, cioè il caso in cui:

(1) G contiene $\boldsymbol{Id}_X$;
(2) accanto a una $P \in \lceil X \lhd\!\!\rightarrow\!\!\rhd X \rceil$, G contiene anche la sua inversa P^{-1};
(3) accanto a due permutazioni P e Q, G contiene anche la loro composizione $P \circ Q$.

In questo caso G si dice **gruppo di permutazioni dell'insieme** X. Si dice anche che il gruppo G "agisce" su X e si esaminano le **azioni del gruppo sull'insieme** $\lceil x \in X \mapsto g(x) \rceil$ per i vari $g \in G$.

Evidentemente G è un gruppo di permutazioni di X sse G munito di prodotto di composizione, passaggio all'inverso e identità di X è un sottogruppo di Sym_X, il gruppo di tutte le permutazioni entro X.

Per assicurarsi che un insieme G di permutazioni di X sia un gruppo, basta dimostrare che:

$$\forall\ P,\ Q\ \in G\ :\qquad P \circ Q^{-1} \in G,$$

D25 e.02 I gruppi di permutazione più significativi si ottengono munendo gli elementi di X di peculiarità diverse dalla loro semplice indistinguibilità e chiedendo che le permutazioni le rispettino. È infatti evidente che se due permutazioni rispettano una certa proprietà degli elementi di X, anche le loro inverse, la loro composizione e la identità di X, la rispettano.

Gli elementi di X possono essere caratterizzati in modo utile e interessante in termini geometrici. Si tratta di considerare gli elementi di X come componenti di una configurazione geometrica o combinatorica (tipicamente i vertici, i lati o le facce di una figura geometrica) e di richiedere che le permutazioni da individuare e studiare trasformino la configurazione in una indistinguibile.
Procedendo in questo modo, si individuano numerosi gruppi di trasformazioni, ciascuno dei quali viene chiamato **gruppo di simmetria** o **gruppo degli automorfismi** del proprio campo d'azione.

D25 e.03 Per esempio se scriviamo $X = \{1, 2, 3, 4, 5\}$ per linsieme dei vertici di un pentagono regolare, il sottogruppo di Sym_5 delle simmetrie di tale poligono è costituito dalle seguenti permutazioni:

Identità	$Id_{(5]}$
Rotazione antioraria di 72°	(12345)
Rotazione antioraria di 144°	(13524)
Rotazione antioraria di 216°	(14253)
Rotazione antioraria di 288°	(15432)
Riflessione rispetto all'asse passante per 1	(25) (34)
Riflessione rispetto all'asse passante per 2	(13) (54)
Riflessione rispetto all'asse passante per 3	(24) (15)
Riflessione rispetto all'asse passante per 4	(12) (35)
Riflessione rispetto all'asse passante per 5	(14) (23)

Abbiamo quindi un sottogruppo di ordine 10 del gruppo Sym_5 avente ordine $120 = 5!$.

D25 e.04 Molti gruppi di permutazioni si individuano a partire da grafi dei vari generi [D35] .
Si osservi che il gruppo di simmetria del pentagono è più complesso del pentagono, nel senso che la sua descrizione è notevolmente più lunga di quella del poligono. Questo è un fatto piuttosto generale

e può essere facilmente verificato su molte altre configurazioni geometriche. Quindi con semplici configurazioni geometriche, si possono individuare gruppi di permutazioni piuttosto complessi.

È importante osservare che per la nozione di gruppo di permutazioni o di simmetria, non è essenziale che X sia un insieme finito.
Quanto detto sul carattere gruppale dell'insieme delle permutazioni che trasformano una configurazione in una forma indistinguibile, valgono quale che sia l'insieme X (finito, numerabile o altro). Nel caso di insieme non finito, naturalmente, si pongono i problemi della effettiva costruzione del gruppo e della verifica delle sue proprietà.

D25 e.05 Consideriamo dunque un generico gruppo G di permutazioni di un insieme X ed associamogli una relazione di equivalenza su X "$\sim_G$" , ponendo:

$$x \sim_G y \quad \text{sse} \quad G \text{ contiene una permutazione } g \text{ tale che } g(x) = y \ .$$

Si verifica facilmente che $\sim_G$ è riflessiva (in quanto $\forall x \in X \ : \ Id_X(x) = x$), simmetrica (se $g(x) = y$ $g^{-1}(y) = x$ e quindi $x \sim_G y \Longrightarrow y \sim_G x$) e transitiva (se $g(x) = y$ e $h(y) = z$, allora $h\big(g(x)\big) = g \circ h(x) = z$ e quindi $x \sim_G y,\ y \sim_G z \Longrightarrow x \sim_G z$).

La classi della relazione $\sim_G$ si chiamano **orbite del gruppo** G agente su X.
Ogni orbita di G si può porre nella forma $G(x) = \{g \in G |\ g(x)\}$.
In un'orbita $G(x)$ si trovano gli elementi di X che non sono distinguibili da x, quando si perde la percezione delle loro singole individualità e rimane solo la percezione delle loro mutue relazioni.

D25 e.06 L'insieme degli elementi di G che trasformano un elemento $x \in X$ in se stesso è detto **stabilizzatore entro** G **dell'elemento** x. Esso si denota con $\boldsymbol{Stabr}_G(x)$.

Chiaramente lo stabilizzatore di ogni elemento di X costituisce un sottogruppo di G: infatti la composizione di due permutazioni che lasciano fisso un elemento di X, non può modificare tale elemento.

Passare da un gruppo di permutazioni G a un suo sottogruppo stabilizzatore $\boldsymbol{Stabr}_G(x)$, corrisponde ad aggiungere una caratterizzazione distintiva all'elemento x che non gli consenta di essere trasformato in alcun altro elemento di X; in modo intuitivo si può pensare di caratterizzare x con una informazione peculiare, con una etichetta.

D25 e.07 Altri insiemi interessanti di permutazioni di G sono quelli degli elementi che trasformano un dato $x \in X$ in un determinato y e che denoteremo con $\boldsymbol{Trsf}_G(x, y)$.

Questi insiemi e gli stabilizzatori sono collegati da una relazione assai utile.

D25 e.08 Prop. Se $t \in \boldsymbol{Trsf}_G(x, y)$, questo insieme è dato da $\boldsymbol{Trsf}_G(x, y) = t \cdot \boldsymbol{Stabr}_G(x)$, cioè da un laterale sinistro del sottogruppo stabilizzatore.

Dim.: Se $u \in t \cdot \boldsymbol{Stabr}_G(x)$, $u = t \cdot s$ con s elemento dello stabilizzatore e quindi $u(x) = t\big(s(x)\big) = t(x) = y$, cioè $t \cdot \boldsymbol{Stabr}_G(x) \subseteq \boldsymbol{Trsf}_G(x, y)$.
Se viceversa $u \in \boldsymbol{Trsf}_G(x, y)$, $t^{-1}\big(u(x)\big) = t^{-1}(y) = x$ cioè $t^{-1} \cdot u \in \boldsymbol{Stabr}_G(x)$ e quindi $u \in t \cdot \boldsymbol{Stabr}_G(x)$, ovvero $\boldsymbol{Trsf}_G(x, y) \subseteq \boldsymbol{Stabr}_G(x)$ ∎

D25 e.09 Dimostriamo ora una importante relazione riguardante le orbite e gli stabilizzatori per i gruppi di permutazioni.

(1) Prop.: Se G è un gruppo di permutazioni di un insieme X ed $x \in X$, si ha:

$$|\ G(x)\ | \times |\ \boldsymbol{Stabr}_G(x)\ | \ = \ |\ G\ |$$

Dim.: Consideriamo la collezione di coppie associata ad x: $C = \{\langle g, y\rangle \in G \times X \ \mathbb{[} \ g(x) = y\}$. Per ogni $g \in G$, dato che si tratta di una funzione, si ha una sola coppia $\langle g, y\rangle \in C$: quindi il cardinale di C è $|\ G\ |$. Per ogni $y \notin G(x)$ non si ha alcuna coppia $\langle g, y\rangle \in C$. Per ogni $y \in G(x)$, invece, il numero di coppie $\langle g, y\rangle \in C$, è dato da $|\ \boldsymbol{Trsf}_G(x, y)\ |$ uguale come si è visto a $|\ \boldsymbol{Stabr}_G(x)\ |$; quindi segue l'uguaglianza precedente ∎

D25 f. orbite di un gruppo di permutazioni

D25 f.01 Se G è un gruppo di permutazioni agente su un insieme finito X, ossia un sottogruppo di Sym_X, e se $|X| = n$ e $x, y \in X$, scriviamo

$$x \equiv_{\mathsf{G}} y$$

sse esiste $g \in G$ tale che $y = g(x)$. In questo caso diciamo che x **è equivalente a** y **relativamente al gruppo** G. La relazione $\equiv_G$ è una equivalenza, in quanto è

riflessiva: $x \equiv_G x$, poiché $x = e\,x\,e^{-1}$;

simmetrica: $x \equiv_G y \implies y := g(x) \implies x = g^{-1}(y) \implies y \equiv_G x$;

transitiva: $x \equiv_G y \Longrightarrow y := g(x)\ ,\ y \equiv_G z \Longrightarrow z =: g'(y)$ da cui segue che
$z = g' \cdot g(x) \Longrightarrow x \equiv_G z$.

Le classi di equivalenza di $\equiv_G$ costituiscono le **orbite del gruppo** G; l'insieme delle orbite di un gruppo sono una estensione dell'insieme dei suoi cicli; infatti se G è il sottogruppo $\langle f \rangle = \{e, f, f^2, f^3, ...\}$ generato dalla permutazione f, le orbite di G sono i cicli di f.

D25 f.02 Consideriamo, quindi, il problema di determinare il numero di orbite di un gruppo G: per tutti i $k \in X$ sia

$$G_k = \{g \ :\ g \in G,\ g(k) = k\}$$

cioè G_k sia il sottogruppo di G formato dalle permutazioni che fissano k.

D25 f.03 Teorema Se $\mathcal{O}_k$ è l'orbita di G contenente k e se G_k è il sottogruppo di G che lascia k invariato, allora

$$|G_k| \times |\mathcal{O}_k| = |G|\blacksquare$$

D25 f.04 Teorema (**lemma di Burnside**)
Se $\lambda_1(g)$ è il numero di elementi di X fissati dalla permutazione g, cioè se è il numero di cicli di lunghezza 1, allora il numero di orbite di un gruppo $G \subseteq \mathsf{Sym}_n$ è

$$|\mathcal{O}_G| \ = \ \frac{1}{|G|} \sum_{g \in G} \lambda_1(g)\blacksquare$$

D25 f.05 Consideriamo il seguente esempio: sia G il sottogruppo di Sym_5 generato da $a = (1\ 2\ 3)(4\ 5)$. Gli elementi di G sono:

$$\begin{aligned} a &= (1\ 2\ 3)(4\ 5) \\ a^2 &= (1\ 3\ 2)(4)(5) \\ a^3 &= (1)(2)(3)(4\ 5) \\ a^4 &= (1\ 2\ 3)(4)(5) \\ a^5 &= (1\ 3\ 2)(4\ 5) \\ a^6 &= (1)(2)(3)(4)(5) = e \end{aligned}$$

Le orbite sono

$$\mathcal{O} = \{1, 2, 3\} \qquad \text{e} \qquad \mathcal{O}' = \{4, 5\}$$

Allora, $\mathcal{O}_1 = \{1, 2, 3\}$, $G_1 = \{a^3, a^6\}$ e $G = \{a, a^2, a^3, a^4, a^5, a^6\}$. Il primo teorema presentato è immediatamente verificato, infatti

$$|G_1| \times |\mathcal{O}_1| = 3 \times 2 = 6 = |G|.$$

Per quanto riguarda il secondo teorema abbiamo:

$$\lambda_1(a) = 0 \quad \lambda_1(a^2) = 2 \quad \lambda_1(a^3) = 3$$
$$\lambda_1(a^4) = 2 \quad \lambda_1(a^5) = 0 \quad \lambda_1(a^6) = 5$$

da cui si ottiene:

$$|\mathcal{O}_G| = \frac{1}{6}(2 + 3 + 2 + 5) = 2,$$

Le permutazioni di Sym_n possono essere generate secondo un certo ordinamento totale.

Il problema dell'ordinamento e della generazione automatica secondo l'ordinamento totale, si pone anche per altri allineamenti di interi, e precisamente per le partizioni.
Per ogni insieme di allineamenti di interi, si possono definire quattro tipi di ordinamenti che denoteremo con Ω, Ω^{-1}, $\overset{\sim}{\Omega}$, $\overset{\sim}{\Omega}^{-1}$.

Secondo Ω, noto come **ordinamento lessicografico crescente**, dati due allineamenti $i_1, i_2, ..., i_r$ e $j_1, j_2, ..., j_s$, il primo precede il secondo se la prima delle differenze $i_k - j_k$, per $k = 1, ..., min(r, s)$, nonnulla, è negativa, oppure se $i_k = j_k$ per $k = 1, ..., r$ ed $r < s$.
L'ordinamento lessicografico decrescente Ω^{-1} è l'inverso del precedente.

Secondo l'ordinamento $\overset{\sim}{\Omega}$, detto **ordinamento antilessicografico crescente**, si dice che dei suddetti allineamenti, il primo precede il secondo se $r < s$, ovvero, essendo $r = s$, se l'ultima tra le differenze $i_k - j_k$ è negativa.
L'ordinamento antilessicografico decrescente $\overset{\sim}{\Omega}^{-1}$ è l'inverso del precedente.

D25 g. cicli di una permutazione

D25 g.01 Ogni permutazione può essere espressa anche come prodotto di cicli disgiunti: presa una permutazione f, si ha che essa trasforma l'elemento i_{11} in $f(i_{11}) = i_{12}$, questo a sua volta va in $f^2(i_{11}) = i_{13}$, e via dicendo finchè non si ottiene di nuovo l'elemento i_{11} come $i_{11} = f^{m_1}(i_{11})$. A questo punto, o si saranno esauriti tutti gli interi di Sym_n, oppure un certo numero di essi non sarà stato toccato. In quest'ultimo caso si riprende il procedimento precedente a partire dal più piccolo dei numeri rimanenti, chiamiamolo i_{21}, ottenendo la sequenza ciclica $i_{21}, f(i_{21}), ..., f^{m_2}(i_{21}) = i_{21}$. Questo procedimento si può procedere fino a esaurire Sym_n.

Per esempio se consideriamo la permutazione

$$C = \left| \begin{matrix} i_1 & i_2 & i_3 & \dots & i_{m-1} & i_m & i_{m+1} & i_{m+2} & \dots & i_n \\ \downarrow & & & & & & & & & \downarrow \\ i_2 & i_3 & \dots & i_{m-1} & i_m & i_1 & i_{m+1} & i_{m+2} & \dots & i_n \end{matrix} \right|$$

$i_1, i_2, ..., i_n$ è una qualsiasi permutazione dei primi n interi che viene detta **ciclo di lunghezza** m e viene denotata con:

$$\text{C}=(i_1\ i_2\ ...\ i_m)$$

Poiché abbiamo a che fare con un ciclo, in C non è importante il primo scritto tra gli elementi.
Una permutazione costituita da un unico ciclo di lunghezza maggiore di uno è detta **permutazione circolare**.
Se denotiamo con $\boldsymbol{Cycl}_n$ il sottoinsieme di Sym_n formato dalle sole permutazioni circolari possiamo dire che:

$$|\boldsymbol{Cycl}_n| = 1 + \sum_{m=2}^{n} \frac{n(n-1)\cdots(n-m+1)}{m},$$

Gli elementi su cui opera un ciclo sono tutti distinti; si hanno cicli a un solo elemento, o di lunghezza 1, (che in genere vengono omessi nella rappresentazione della permutazione), cicli di lunghezza 2 detti "cicli binari", "cicli ternari", "cicli quaternari" etc.
La scrittura di una permutazione attraverso i suoi cicli viene chiamata **fattorizzazione di una permutazione in cicli**.

D25 g.02 L'importanza della fattorizzazione in cicli per lo studio di Sym_n proviene anche dal fatto che essa permette di caratterizzare completamente la classe di coniugio a cui appartiene un elemento qualunque.
Se G è un sottogruppo di Sym_n diciamo che due permutazioni s e t sono **permutazioni coniugate** per G sse esiste un elemento $g \in G$ tale che $s = g\,t\,g^{-1}$. L'operazione di coniugio è una relazione di equivalenza su G, infatti è

riflessiva: $\forall s \in G \ : \ s = ese^{-1}$;

simmetrica: $\forall s, t \in G \ : \ s = gtg^{-1} \Longrightarrow t = g^{-1}sg$;

transitiva: $\forall s, t, u \in G \ : \ s = gtg^{-1} \wedge t = huh^{-1} \implies s = g(huh^{-1})g^{-1} = (gh)u(gh)^{-1}$.

Il gruppo Sym_n viene quindi suddiviso in classi di coniugio: tutte le permutazioni che hanno la stessa struttura ciclica, cioè che contengono lo stesso numero α_1 di cicli di lunghezza uno, lo stesso numero α_2

di cicli binari,..., lo stesso numero α_n di cicli di lunghezza n appartengono alla stessa classe di coniugio di Sym_n. Questi α_i sono numeri interi positivi o nulli e verificano l'equazione

$$\sum_{i=1}^{n} i\alpha_i = n \qquad (**),$$

Vale infatti il seguente teorema:

Teorema Due permutazioni s e t sono coniugate in Sym_n sse hanno lo stesso numero di cicli di uguale lunghezza ∎

Da questo segue che ogni permutazione e la sua inversa (o reciproca) appartengono alla stessa classe. Una classe di Sym_n sarà completamente definita dando l'allineamento dei numeri positivi o nulli α_i che verificano l'equazione $(**)$ appena vista. Denotando tale allineamento con (α), la classe associata verrà denotata con $\mathcal{C}^{(\alpha)}$.

D25 h. gruppo simmetrico

D25 h.01 Si prenda in considerazione il gruppo delle permutazioni di un insieme finito di oggetti. In molte considerazioni non è necessario tenere conto della precisa individualità degli oggetti, ma occorre solo distinguerli; in questo caso ci si può limitare a considerare il gruppo simmetrico Sym_n, gruppo delle permutazioni degli interi 1,2,...,n. Quando è necessario precisare la individualità degli oggetti permutati si considera un gruppo Sym_X, dove X denota l'insieme degli oggetti.

D25 h.02 Consideriamo una sequenza di interi nonnegativi distinti α_i che soddisfano l'equazione $(**)$ e poniamo:

$m_1 = \alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_n$
$m_2 = \alpha_2 + \alpha_3 + \cdots + \alpha_n$
$m_1 = \alpha_3 + \cdots + \alpha_n$
.....
$m_n = \alpha_n$

L'equazione $(**)$ implica $\sum_{i=1}^{n} m_i = n$, dove $m_i \geq m_{i+1} \geq 0, \quad i = 1, ..., n-1$. Gli m_i formano, per definizione, una partizione dell'intero n.

Una tale partizione costituita dagli interi $m_1, ..., m_n$, che si suppongono allineati in ordine noncrescente, si denoterà con $\big[m_1, ...m_n\big]$, o più brevemente con $\big[m\big]$.
Di solito si omettono gli zeri che possono trovarsi alla fine e si può usare una notazione ad esponenti, per indicare la presenza ripetuta di uno stesso numero, notazione della forma

$$\big[{\mu_1}^{m_1}, ...{\mu_h}^{m_h}\big] \ ,$$

dove $\mu_1 > \mu_2 > \cdots > \mu_h, \quad m_i > 0$ e con $\sum_{i=1}^{n} m_i \mu_i \ = \ n$.

Dalle equazioni precedenti si può dedurre che la corrispondenza tra allineamenti (α) e allineamenti $\big[m\big]$ è biunivoca.

D25 h.03 Se consideriamo X come una sequenza di n oggetti posti in posizioni successive, l'effetto della permutazione ϕ è la sostituzione dell'oggetto i con l'oggetto $k_i = \phi(i)$.
La risultante n-upla $k_1, k_2, ..., k_n$ viene chiamata **riordinamento della sequenza** $\langle 1, 2, ..., n\rangle$ dovuto alla permutazione ϕ.

Agli elementi di un insieme si possono applicare più permutazioni successive: se consideriamo due permutazioni f e g sull'insieme $X = \{1, 2, ..., n\}$ possiamo definire prodotto $f \circ_{rl} g$ di f e g la permutazione fornita da:

$$f \cdot g(i) \ := \ f(g(i)) \ .$$

Per esempio, se

$$f \ = \ \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ k_1 & k_2 & k_3 & k_4 & k_5 \end{vmatrix} \qquad \text{e} \qquad g \ = \ \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 5 & 3 & 4 \end{vmatrix} \ ,$$

dalla definizione di prodotto di composizione si constata che:

$$\begin{aligned} f \circ_{rl} g \ &= \ \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ k_1 & k_2 & k_3 & k_4 & k_5 \end{vmatrix} \circ_{rl} \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 5 & 3 & 4 \end{vmatrix} \\ &= \ \begin{vmatrix} 2 & 1 & 5 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ k_2 & k_1 & k_5 & k_3 & k_4 \end{vmatrix} \circ_{rl} \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 5 & 3 & 4 \end{vmatrix} \\ &= \ \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ k_2 & k_1 & k_5 & k_3 & k_4 \end{vmatrix} \end{aligned}$$

cioè :

$$f \cdot g(1) = f(g(1)) = f(2) = k_2 \quad , \quad f \cdot g(2) = f(g(2)) = f(1) = k_1, \quad \text{etc.}$$

Si verifica che in generale $(f \circ g) \neq (g \circ f)$. Basta per questo considerare permutazioni di tre oggetti.

Se consideriamo il prodotto di permutazioni come legge di composizione possiamo dimostrare il seguente fatto.

Teorema Le permutazioni di grado n formano un gruppo chiamato **gruppo simmetrico di grado** n, gruppo denotato con Sym_n.

Dim.: Per dimostrare il teorema dobbiamo verificare i quattro seguenti assiomi della specie di struttura gruppo:

[Grp 1]: La composizione di due permitazioni è una permutazione.
[Grp 2]: (*i*) *Associatività*: $\forall\ f, g, h \in \mathsf{Sym}_n\ :$

$$f \cdot (g \cdot h) = (f \cdot g) \cdot h = f \cdot g \cdot h$$

Questo assioma è ovviamente soddisfatto, infatti

$$[f \cdot (g \cdot h)](i) = f\{g[h(i)]\} = [(f \cdot g) \cdot h](i).$$

[Grp 3]: (*ii*) *Esistenza dell'identità*: Esiste $e \in \mathsf{Sym}_n$ tale che:

$$f \cdot e = e \cdot f = f$$

[Grp 4]: $\forall\ f \in \mathsf{Sym}_n\ :\ \mathsf{Sym}_n \ni \overline{f}\ ST\ f \circ \overline{f} = fol \circ f = e\ .$

L'elemento e è la permutazione che tiene fisso ogni elemento, infatti:

$$e = \begin{vmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{vmatrix}$$

e si ha: $f \cdot e(i) = f(i)$ e $e \cdot f(i) = e[f(i)] = f(i)$.

[Grp 4]: (*iii*) *Esistenza dell'inverso*: Se $f \in \mathsf{Sym}_n$, esiste un elemento inverso $f^{-1} \in \mathsf{Sym}_n$ tale che:

$$f \cdot f^{-1} = f^{-1} \cdot f = e.$$

Data una permutazione f in forma matriciale la sua inversa è quella ottenuta scambiando le due righe di f:

$$f = \begin{vmatrix} k_1 & k_2 & \dots & k_n \\ p_1 & p_2 & \dots & p_n \end{vmatrix}$$
$$f^{-1} = \begin{vmatrix} p_1 & p_2 & \dots & p_n \\ k_1 & k_2 & \dots & k_n \end{vmatrix}$$

Infatti:

$$\forall i \in (\mathrm{n}\ ]\ :\ (f \circ_{rl} f^{-1})(p_i) = f(k_i) = p_i \qquad , \qquad (f^{-1} \circ_{rl} f)(k_i) = f^{-1}(p_i) = k_i\ ,$$

ossia $f \cdot f^{-1} = f^{-1} \cdot f = e$ ∎

Dato un intero m nonnegativo e una permutazione f definiamo m-esima **potenza della permutazione** f la permutazione f^m data dal prodotto di f per se stessa m volte e definita in questo modo:

$$f^m(i) \ := \ \underbrace{f \cdot f \cdots f(i)}_{m}$$

Un caso particolare è quello in cui $m = 0$: in questo caso si pone $f^0 := \mathsf{Id}_n$.
Similmente definiamo la m-esima **potenza inversa della permutazione** f:

$$f^{-m}(i) := \underbrace{f^{-1} \cdot f^{-1} \cdots f^{-1}(i)}_{m}.$$

Testo fruibile in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php