

# DETERMINANTI (PRIMA PARTE). NOTE DI ALGEBRA LINEARE 2010-11

MARCO MANETTI: 10 DICEMBRE 2010

## 1. UNA FORMULA PER IL DETERMINANTE

Iniziamo con il definire, per ogni  $n \geq 0$  e per ogni matrice  $A \in M_{n,n}(\mathbb{K})$  un scalare  $|A| \in \mathbb{K}$  detto **determinante** di  $A$ ; scriveremo talvolta  $\det(A)$  per indicare  $|A|$ .

Se  $n = 0$  e  $A \in M_{0,0}(\mathbb{K})$  è la matrice vuota poniamo per convenzione  $|A| = 1$ . Se  $n = 1$  ed  $A = (a)$ , con  $a \in \mathbb{K}$  poniamo  $|A| = a$ . Se  $n > 1$  definiamo  $|A|$  in maniera ricorsiva, come una funzione polinomiale dei coefficienti di  $A$  e dei determinanti di opportune sottomatrici di  $A$  di ordine minore di  $n$ . Data una matrice  $A = (a_{ij}) \in M_{n,n}(\mathbb{K})$  indichiamo con  $A_{ij} \in M_{n-1,n-1}(\mathbb{K})$  la sottomatrice ottenuta cancellando la riga  $i$  e la colonna  $j$ ; definiamo poi

$$(1.1) \quad |A| = a_{11}|A_{11}| - a_{12}|A_{12}| + a_{13}|A_{13}| - \cdots = \sum_{j=1}^n (-1)^{j+1} a_{1j}|A_{1j}|.$$

**Esempio 1.1.** Per  $n = 2$  si ha

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

**Esempio 1.2.**

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} - 2 \begin{vmatrix} 4 & 6 \\ 7 & 9 \end{vmatrix} + 3 \begin{vmatrix} 4 & 5 \\ 7 & 8 \end{vmatrix} = (45 - 48) - 2(36 - 42) + 3(32 - 35) = 0.$$

**Definizione 1.3.** Sia  $V$  uno spazio vettoriale sul campo  $\mathbb{K}$ , un'applicazione

$$\Phi: \underbrace{V \times \cdots \times V}_{n \text{ fattori}} \rightarrow \mathbb{K}$$

si dice **multilineare**, o anche **separatamente lineare**, se è lineare in ognuna delle  $n$  variabili, quando le rimanenti  $n - 1$  sono lasciate fisse.

In altri termini,  $\Phi$  è multilineare se per ogni indice  $i$  vale

$$\begin{aligned} \Phi(v_1, \dots, \lambda v_i, \dots, v_n) &= \lambda \Phi(v_1, \dots, v_i, \dots, v_n), \\ \Phi(v_1, \dots, v_i + w_i, \dots, v_n) &= \Phi(v_1, \dots, v_i, \dots, v_n) + \Phi(v_1, \dots, w_i, \dots, v_n). \end{aligned}$$

**Esempio 1.4.** Se  $f, g: V \rightarrow \mathbb{K}$  sono due applicazioni lineari, allora

$$\Phi: V \times V \rightarrow \mathbb{K}, \quad \Phi(v, w) = f(v)g(w),$$

è multilineare. Infatti

$$\begin{aligned} \Phi(\lambda v, w) &= f(\lambda v)g(w) = \lambda f(v)g(w) = \lambda \Phi(v, w), & \Phi(v, \lambda w) &= f(v)g(\lambda w) = \lambda f(v)g(w) = \lambda \Phi(v, w), \\ \Phi(u + v, w) &= f(u + v)g(w) = (f(u) + f(v))g(w) = f(u)g(w) + f(v)g(w) = \Phi(u, w) + \Phi(v, w), \\ \Phi(v, w + z) &= f(v)g(w + z) = f(v)(g(w) + g(z)) = f(v)g(w) + f(v)g(z) = \Phi(v, w) + \Phi(v, z). \end{aligned}$$

**Teorema 1.5.** L'applicazione  $A \mapsto |A|$  definita in (1.1) ha le seguenti proprietà:

- (1) L'applicazione  $A \mapsto |A|$  è multilineare sulle colonne.
- (2) Se la matrice  $A$  ha due colonne adiacenti uguali, allora  $|A| = 0$ .
- (3)  $|I| = 1$ , dove  $I$  è la matrice identità.

Per essere precisi, la condizione (1) equivale a dire che l'applicazione

$$\underbrace{\mathbb{K}^n \times \cdots \times \mathbb{K}^n}_{n \text{ fattori}} \rightarrow \mathbb{K}, \quad (A^1, \dots, A^n) \mapsto |A^1, \dots, A^n|,$$

è multilineare, dove ogni  $A^i$  è un vettore colonna e  $|A^1, \dots, A^n|$  è il determinante della matrice che ha come colonne  $A^1, \dots, A^n$ .

*Dimostrazione.* Dimostriamo la multilinearità per induzione sull'ordine delle matrici. Per semplicità espositiva mostriamo che il determinante è lineare rispetto alla prima colonna: la linearità rispetto alle altre colonne è del tutto simile. Consideriamo quindi una matrice  $A = (A^1, \dots, A^n) = (a_{ij})$ , uno scalare  $\lambda \in \mathbb{K}$  ed un vettore colonna  $B^1 = (b_{11}, \dots, b_{n1})^T$ . Considerando le matrici

$$C = (\lambda A^1, A^2, \dots, A^n), \quad D = (B^1, A^2, \dots, A^n), \quad E = (A^1 + B^1, A^2, \dots, A^n),$$

occorre dimostrare che

$$|C| = \lambda|A|, \quad |E| = |A| + |D|.$$

Si ha  $C_{11} = A_{11}$ , mentre per ogni  $j > 1$  la matrice  $C_{1j}$  è ottenuta da  $A_{1j}$  moltiplicando la prima riga per  $\lambda$ ; per l'ipotesi induttiva  $|C_{1j}| = \lambda|A_{1j}|$  per ogni  $j > 1$  e quindi per la formula (1.1) si ha

$$|C| = \lambda a_{11}|C_{11}| - a_{12}|C_{12}| + \cdots = \lambda a_{11}|A_{11}| - a_{12}\lambda|A_{12}| + \cdots = \lambda|A|.$$

Similmente si ha  $E_{11} = A_{11} + D_{11}$  e per induzione  $|E_{1j}| = |A_{1j}| + |D_{1j}|$  per ogni  $j > 1$ . Quindi

$$\begin{aligned} |E| &= (a_{11} + b_{11})|E_{11}| - a_{12}|E_{12}| + \cdots \\ &= (a_{11}|A_{11}| + b_{11}|A_{11}| - a_{12}|A_{12}| + \cdots) + (b_{11}|D_{11}| - a_{12}|D_{12}| + \cdots) = |A| + |D|. \end{aligned}$$

Supponiamo adesso che la matrice  $A = (A^1, \dots, A^n)$  abbia due colonne adiacenti uguali, diciamo  $A^i = A^{i+1}$ . Allora per ogni  $j \neq i, i+1$  la matrice  $A_{1j}$  ha due colonne adiacenti uguali. Per induzione  $|A_{1j}| = 0$  per ogni  $j \neq i, i+1$  e quindi la formula (1.1) si riduce a

$$|A| = (-1)^{i+1} a_{1,i} |A_{1,i}| + (-1)^{i+2} a_{1,i+1} |A_{1,i+1}|$$

e basta osservare che  $a_{1,i} = a_{1,i+1}$  e  $A_{1,i} = A_{1,i+1}$  per avere  $|A| = 0$ . Il determinante della matrice identità si calcola facilmente per induzione. Infatti  $|I| = |I_{11}|$  e la sottomatrice  $I_{11}$  è ancora una matrice identità.  $\square$

*Osservazione 1.6.* Per calcolare il determinante di una matrice abbiamo usato solo le operazioni di somma e prodotto: non abbiamo mai dovuto dividere per alcun coefficiente. Se  $A = (a_{ij}(x))$  è una matrice i cui coefficienti sono polinomi  $a_{ij}(x) \in \mathbb{K}[x]$  possiamo ancora calcolare il determinante, che continuerà ad essere un polinomio. Ad esempio

$$\begin{vmatrix} x & 2 \\ x^2 - x & x + 1 \end{vmatrix} = x(x+1) - 2(x^2 - x) = -x^2 + 3x \in \mathbb{K}[x].$$

Inoltre per ogni  $\alpha \in \mathbb{K}$  il valore del determinante di  $A$  calcolato per  $x = \alpha$  coincide con il determinante della matrice  $(a_{ij}(\alpha)) \in M_{n,n}(\mathbb{K})$ .

## Esercizi.

**1.1.** Calcolare i determinanti:

$$\begin{vmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 3 & 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 2 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{vmatrix}.$$

**1.2.** Dimostrare per induzione su  $n$  che il determinante di una matrice diagonale  $n \times n$  è uguale al prodotto degli elementi sulla diagonale.

**1.3.** Dimostrare che il determinante di una matrice triangolare inferiore è uguale al prodotto degli elementi sulla diagonale.

**1.4.** Dimostrare per induzione su  $n$  che il determinante di una matrice  $n \times n$  con una colonna nulla è uguale a 0. Provare anche che lo stessa conclusione vale se la matrice ha una riga nulla.

**1.5.** Sia

$$p(x) = \begin{vmatrix} x & x^2 & 2x & 3x \\ 1 & x^2 & 4 & x^3 \\ 1 & x^3 & 4x & 5 \\ 1 & x^4 & 16 & x^9 \end{vmatrix} \in \mathbb{K}[x].$$

Calcolare  $p(0)$ ,  $p(1)$  e  $p(2)$ .

**1.6.** Calcolare il determinante

$$\begin{vmatrix} 1 & a & a^2 & a^3 \\ 0 & 1 & a & a^2 \\ b & 0 & 1 & a \\ c & d & 0 & 1 \end{vmatrix}$$

dove  $a$  = gli anni del rettore,  $b$  = le sorelle di Antani,  $c$  = il peso atomico del Cirillio e  $d$  = il numero di emeriti.

## 2. PERMUTAZIONI, SEGNAURA ED UNICITÀ DEL DETERMINANTE

**Definizione 2.1.** Diremo che un'applicazione  $d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}$  è **multilineare alternante sulle colonne** se soddisfa le seguenti due condizioni:

**D1:** L'applicazione  $d$  è multilineare sulle colonne.

**D2:** Se la matrice  $A$  ha due colonne adiacenti uguali, allora  $d(A) = 0$ .

**Esempio 2.2.** Per il Teorema 1.5 il determinante è multilineare alternante sulle colonne. Lo stesso vale per l'applicazione  $d(A) = \lambda|A|$ , dove  $\lambda \in \mathbb{K}$  è uno scalare qualsiasi.

**Esempio 2.3.** Fissata una matrice  $B \in M_{n,n}(\mathbb{K})$  l'applicazione

$$d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}, \quad d(A) = |BA|,$$

è multilineare alternante sulle colonne. Questo segue facilmente dal fatto che la  $i$ -esima colonna di  $BA$  è uguale a  $BA^i$ , dove  $A^i$  è la  $i$ -esima colonna di  $A$ .

**Lemma 2.4.** Sia  $d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}$  multilineare alternante sulle colonne. Allora si ha:

**D3:** Se una matrice  $B$  è ottenuta da  $A$  scambiando tra loro le posizioni di due colonne vale  $d(B) = -d(A)$ .

**D4:** Se la matrice  $A$  ha due colonne uguali, allora  $d(A) = 0$ .

**D5:** Se  $A$  contiene una colonna nulla allora  $d(A) = 0$ .

**D6:** Se le colonne di  $A$  sono linearmente dipendenti allora  $d(A) = 0$ .

*Dimostrazione.* Sia  $B$  la matrice ottenuta da  $A$  scambiando tra di loro due colonne adiacenti, diciamo

$$A = (\dots, A^i, A^{i+1}, \dots), \quad B = (\dots, A^{i+1}, A^i, \dots).$$

Per la proprietà D1 si ha l'uguaglianza

$$\begin{aligned} d(\dots, A^i + A^{i+1}, A^i + A^{i+1}, \dots) &= d(\dots, A^i, A^i + A^{i+1}, \dots) + d(\dots, A^{i+1}, A^i + A^{i+1}, \dots) = \\ &= d(\dots, A^i, A^i, \dots) + d(\dots, A^i, A^{i+1}, \dots) + d(\dots, A^{i+1}, A^i, \dots) + d(\dots, A^{i+1}, A^{i+1}, \dots). \end{aligned}$$

che per la proprietà D2 si riduce a

$$0 = d(\dots, A^i, A^{i+1}, \dots) + d(\dots, A^{i+1}, A^i, \dots),$$

e cioè  $d(B) = -d(A)$ .

Se adesso la matrice  $A$  ha due colonne uguali, diciamo  $A^i$  ed  $A^j$  con  $i < j$  possiamo scambiare la colonna  $i$  con la colonna  $i + 1$ , poi la colonna  $i + 1$  con la  $i + 2$  e si prosegue fino a quando la colonna  $i$  si trova nella posizione  $j - 1$ . Si ha quindi  $d(A) = (-1)^{j-i-1}d(B)$  dove  $B$  è una matrice con le colonne  $j - 1$  e  $j$  uguali. Dunque  $d(B) = 0$ ,  $d(A) = 0$  e questo prova D4.

Chiamiamo scambio elementare lo scambio di due colonne adiacenti; per provare D3 è sufficiente dimostrare che ogni scambio di due colonne si può ottenere come composizione di un numero dispari di scambi elementari. Indichiamo con

$$\tau_i: M_{n,n}(\mathbb{K}) \rightarrow M_{n,n}(\mathbb{K})$$

l'applicazione che scambia la colonna  $i$  con la colonna  $i + 1$ . Se  $i < j$  si vede facilmente che la composizione di  $2(j - i) - 1$  scambi elementari

$$\underbrace{\tau_i \circ \tau_{i+1} \circ \cdots \circ \tau_{j-2}}_{\text{indici crescenti}} \circ \tau_{j-1} \circ \underbrace{\tau_{j-2} \circ \tau_{j-3} \circ \cdots \circ \tau_i}_{\text{indici decrescenti}}$$

scambia le colonne  $i, j$  e lascia le altre al loro posto.

Sia adesso  $A = (A^1, \dots, A^n)$  una matrice con una colonna nulla, che per semplicità notazionale supporremo essere la prima. Allora  $0 = A^1 = 0A^1$  e quindi

$$d(A) = d(A^1, \dots, A^n) = d(0A^1, \dots, A^n) = 0d(A^1, \dots, A^n) = 0.$$

Resta da dimostrare la proprietà D6: supponiamo che le colonne  $A^1, \dots, A^n$  siano linearmente dipendenti e, per fissare le idee che l'ultima colonna sia combinazione lineare delle precedenti:  $A^n = a_1A^1 + \cdots + a_{n-1}A^{n-1}$ . Allora si ha

$$d(A^1, \dots, A^n) = d\left(A^1, \dots, A^{n-1}, \sum_{i=1}^{n-1} a_i A^i\right) = \sum_{i=1}^{n-1} a_i d(A^1, \dots, A^{n-1}, A^i) = 0.$$

□

**Esempio 2.5.** Consideriamo una matrice  $A \in M_{n,n}(\mathbb{K})$  che sia della forma

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

con  $B \in M_{r,s}(\mathbb{K})$ ,  $C \in M_{r,n-s}(\mathbb{K})$  e  $D \in M_{n-r,n-s}(\mathbb{K})$ . Se  $r < s$  allora  $|A| = 0$  in quanto le prime  $s$  colonne di  $A$  sono linearmente dipendenti.

Indichiamo con  $\Sigma_n$  l'insieme di tutte le **permutazioni** di  $\{1, \dots, n\}$ , ossia l'insieme di tutte le applicazioni bigettive  $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ . Una **trasposizione** è una permutazione che scambia due elementi e lascia fissi i rimanenti: è facile vedere, oltre che intuitivo, che ogni permutazione si può scrivere come composizione di trasposizioni. Va osservato che non c'è un modo unico di scrivere una permutazione come composizione di trasposizioni: ad esempio se  $\sigma, \tau$  sono due trasposizioni allora  $\tau = \tau \circ \sigma \circ \sigma$

Data una matrice  $A \in M_{n,n}(\mathbb{K})$  ed una permutazione  $\sigma \in \Sigma_n$  denotiamo con  $A^\sigma$  la matrice ottenuta da  $A$  permutando le colonne secondo quanto dettato da  $\sigma$ : più precisamente se  $A = (A^1, \dots, A^n)$  si definisce  $A^\sigma = (A^{\sigma(1)}, \dots, A^{\sigma(n)})$ . Si noti che se  $\sigma, \tau$  sono due permutazioni, allora vale la formula  $A^{\sigma \circ \tau} = (A^\sigma)^\tau$ .<sup>1</sup>

**Definizione 2.6.** La **segnatura**  $(-1)^\sigma$  di una permutazione  $\sigma \in \Sigma_n$  è definita tramite la formula

$$(-1)^\sigma = |I^\sigma|,$$

dove  $I \in M_{n,n}(\mathbb{Q})$  è la matrice identità.

Se la permutazione  $\sigma$  è ottenuta come composizione di  $k$  trasposizioni, allora la matrice  $I^\sigma$  è ottenuta dall'identità con  $k$  scambi di colonne e quindi

$$(-1)^\sigma = |I^\sigma| = (-1)^k |I| = (-1)^k.$$

Ne consegue in particolare che se una permutazione  $\sigma$  è scritta come composizione di  $k$  trasposizioni, allora  $(-1)^k$  dipende solo da  $\sigma$  e non dalla scelta delle trasposizioni. Una permutazione si dice **pari** se ha segnatura 1, o equivalentemente se può essere scritta come composizione di un numero pari di trasposizioni. Si dice **dispari** se ha segnatura  $-1$ .

<sup>1</sup>Se pensiamo una matrice  $A = (A^1, \dots, A^n)$  come l'applicazione  $A: \{1, \dots, n\} \rightarrow \mathbb{K}^n$ ,  $i \mapsto A^i$ , allora  $A^\sigma$  equivale alla composizione  $A \circ \sigma$  e quindi  $A^{\sigma \circ \tau} = A \circ (\sigma \circ \tau) = (A \circ \sigma) \circ \tau = (A^\sigma)^\tau$ .

**Lemma 2.7.** *Sia  $d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}$  multilineare alternante sulle colonne. Allora si ha:*

**D7:** *Per ogni matrice  $A$  ed ogni permutazione  $\sigma$  vale  $d(A^\sigma) = (-1)^\sigma d(A)$ .*

*Dimostrazione.* Scriviamo  $\sigma$  come composizione di  $k$  trasposizioni. Per D3 ogni trasposizione fa cambiare segno e quindi  $d(A^\sigma) = (-1)^k d(A) = (-1)^\sigma d(A)$ .  $\square$

Siamo adesso in grado di dimostrare il teorema di unicit  del determinante.

**Teorema 2.8.** *Sia  $d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}$  multilineare alternante sulle colonne. Allora per ogni matrice  $A$  si ha*

$$d(A) = |A|d(I).$$

*In particolare se  $d(I) = 1$  allora  $d$    uguale al determinante.*

*Dimostrazione.* Se  $A = (A^1, \dots, A^n) = (a_{ij})$  allora per ogni  $i$  vale  $A^i = \sum_{j=1}^n a_{ji}e_j$ , dove  $e_1, \dots, e_n$    la base canonica di  $\mathbb{K}^n$ . Per linearit  rispetto alla prima colonna si ha

$$d(A) = d\left(\sum_{j=1}^n a_{j1}e_j, A^2, \dots, A^n\right) = \sum_{j=1}^n a_{j1}d(e_j, A^2, \dots, A^n).$$

Ripetendo la procedura per la seconda colonna

$$d(A) = \sum_{j=1}^n a_{j1}d\left(e_j, \sum_{k=1}^n a_{k2}e_k, A^3, \dots, A^n\right) = \sum_{j=1}^n \sum_{k=1}^n a_{j1}a_{k2}d(e_j, e_k, A^3, \dots, A^n)$$

e procedendo fino alla  $n$ -esima si ottiene

$$d(A) = \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n a_{j_1 1} \cdots a_{j_n n} d(e_{j_1}, \dots, e_{j_n}).$$

Siccome  $d(e_{j_1}, \dots, e_{j_n}) = 0$  quando due indici  $j_h$  coincidono la precedente formula si riduce a

$$d(A) = \sum_{\sigma \in \Sigma_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} d(e_{\sigma(1)}, \dots, e_{\sigma(n)}).$$

e tenendo presente che

$$d(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = d(I^\sigma) = (-1)^\sigma d(I)$$

arriviamo alla formula

$$(2.1) \quad d(A) = \sum_{\sigma \in \Sigma_n} (-1)^\sigma a_{\sigma(1),1} \cdots a_{\sigma(n),n} d(I),$$

che per  $d$  uguale al determinante diventa

$$(2.2) \quad |A| = \sum_{\sigma \in \Sigma_n} (-1)^\sigma a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

dal confronto delle equazioni (2.1) e (2.2) si arriva alla conclusione.  $\square$

**Teorema 2.9** (Binet). *Date due matrici  $A, B \in M_{n,n}(\mathbb{K})$  si ha*

$$|AB| = |BA| = |A||B|.$$

*Dimostrazione.* Abbiamo gi  osservato che l'applicazione

$$d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}, \quad d(A) = |BA|,$$

  multilineare alternante sulle colonne e quindi vale

$$|BA| = d(A) = |A|d(I) = |A||BI| = |A||B|.$$

Per simmetria  $|AB| = |B||A| = |A||B| = |BA|$ .  $\square$

**Esercizi.**

**2.1.** Provare che

$$\begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 6 \\ 1 & 0 & 0 & 0 & 5 \\ 2 & 0 & 0 & 0 & 5 \\ 1 & 0 & 0 & 0 & 2 \end{vmatrix} = 0.$$

**2.2.** Siano  $f_1, \dots, f_n: \mathbb{K}^n \rightarrow \mathbb{K}$  applicazioni lineari. Provare che l'applicazione

$$d: M_{n,n}(\mathbb{K}) \rightarrow \mathbb{K}, \quad d(A^1, \dots, A^n) = \sum_{\sigma \in \Sigma_n} (-1)^\sigma f_{\sigma(1)}(A^1) f_{\sigma(2)}(A^2) \cdots f_{\sigma(n)}(A^n),$$

è multilineare alternante sulle colonne.

**3. PERMUTAZIONI ED INCROCI**

Un modo conveniente di rappresentare una permutazione  $\sigma$  di  $\{1, \dots, n\}$  elementi è mediante una matrice  $2 \times n$  in cui la prima riga contiene i numeri da 1 a  $n$  e la seconda riga le rispettive immagini, ossia

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

Ricordiamo che le trasposizioni sono permutazioni che scambiano di posizione due elementi e lasciano invariati i rimanenti. Ad esempio, la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

è una trasposizione. Per ogni  $i < n$ , denotiamo con  $\tau_i \in \Sigma_n$  la trasposizione che scambia  $i$  con  $i+1$ :

$$\tau_i(i) = i+1, \quad \tau_i(i+1) = i, \quad \tau_i(a) = a \quad \forall a \neq i, i+1.$$

**Definizione 3.1.** Diremo che un sottoinsieme  $A \subset \{1, \dots, n\}$  di **due** elementi è un **incrocio** della permutazione  $\sigma$  se la restrizione di  $\sigma$  ad  $A$  è decrescente; in altri termini, un sottoinsieme

$$A = \{i, j\}, \quad \text{con } i < j,$$

è un incrocio di  $\sigma$  se  $\sigma(i) > \sigma(j)$ .

Indichiamo con  $\delta(\sigma)$  il numero di incroci di  $\sigma$ . Ad esempio, l'identità ha zero incroci, le trasposizioni  $\tau_i$  hanno un solo incrocio, mentre la permutazione

$$\sigma(i) = n+1-i$$

ha  $n(n-1)/2$  incroci. In un certo senso, il numero di incroci è una misura della complessità della permutazione.

*Osservazione 3.2.* Una maniera di contare il numero di incroci di  $\sigma$  è la seguente. Per ogni  $i = 1, \dots, n$  si disegna nel piano il segmento che unisce il punto di coordinate  $(i, 0)$  con il punto di coordinate  $(\sigma(i), 1)$  e poi si conta il numero di punti di intersezione dei vari segmenti. Bisogna però fare attenzione al fatto che, se per un punto passano  $h$  segmenti, con  $h > 2$ , allora ci troviamo di fronte ad una intersezione multipla ed a tale punto corrispondono  $h(h-1)/2$  incroci. Ad esempio, le due permutazioni

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \quad \begin{array}{c} \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\ \diagdown \quad \diagup \quad \diagdown \quad \diagup \quad \diagdown \\ \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \end{array}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \quad \begin{array}{c} \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\ \diagdown \quad \diagup \quad \diagdown \quad \diagup \quad \diagdown \\ \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \end{array}$$

hanno entrambe 4 incroci.

**Esempio 3.3.** Siano  $i < j$  e sia  $\sigma$  la trasposizione che scambia  $i$  e  $j$ . Un sottoinsieme

$$A = \{a, b\}, \quad \text{con } a < b,$$

è un incrocio se e solo se  $a = i$  e  $b \leq j$ , oppure se  $a \geq i$  e  $b = j$ ; quindi  $\delta(\sigma) = 2(j - i) - 1$ .  
Ne consegue che ogni trasposizione ha segnatura uguale a  $-1$ .

Le permutazioni, in quanto applicazioni di un insieme in sé, possono essere composte tra loro. Se  $\sigma, \eta \in \Sigma_n$  definiamo il prodotto  $\sigma\eta \in \Sigma_n$  come

$$\sigma\eta(i) = \sigma(\eta(i)), \quad i = 1, \dots, n.$$

Ad esempio

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

Notiamo che il prodotto di ogni trasposizione con sé stessa è uguale all'identità; in particolare  $\tau_i \tau_i = \text{identità}$  per ogni  $i$ .

**Teorema 3.4.** *Date due permutazioni  $\sigma, \eta \in \Sigma_n$ , indichiamo con  $a$  il numero di sottoinsiemi  $A \subseteq \{1, \dots, n\}$  di due elementi che soddisfano le due condizioni:*

- (1)  $A$  è un incrocio di  $\eta$ .
- (2)  $\eta(A)$  è un incrocio di  $\sigma$ .

Allora vale la formula

$$\delta(\sigma\eta) = \delta(\sigma) + \delta(\eta) - 2a$$

*Dimostrazione.* Per ogni insieme finito  $X$  indichiamo con  $|X|$  la sua cardinalità, ossia il numero di elementi che contiene. Indichiamo con  $\mathcal{P}$  la collezione di tutti i sottoinsiemi di  $\{1, \dots, n\}$  di cardinalità 2.

Notiamo che  $A \in \mathcal{P}$  è un incrocio di  $\sigma\eta$  se e soltanto se vale una delle seguenti due condizioni:

- (1)  $A$  è un incrocio di  $\eta$  e  $\eta(A)$  non è un incrocio di  $\sigma$ .
- (2)  $A$  non è un incrocio di  $\eta$  e  $\eta(A)$  è un incrocio di  $\sigma$ .

Indichiamo adesso con

$$\begin{aligned} \mathcal{C} &= \{A \in \mathcal{P} : A \text{ è incrocio di } \eta\}. \\ \mathcal{D} &= \{A \in \mathcal{P} : \eta(A) \text{ è incrocio di } \sigma\}. \end{aligned}$$

Chiaramente  $|\mathcal{C}| = \delta(\eta)$  e, siccome  $\eta: \mathcal{P} \rightarrow \mathcal{P}$  è bigettiva, vale anche  $|\mathcal{D}| = \delta(\sigma)$ .

Per definizione  $a$  è il numero di elementi di  $\mathcal{C} \cap \mathcal{D}$ . Denotiamo con  $c$  il numero di elementi di  $\mathcal{C}$  che non appartengono a  $\mathcal{D}$  e con  $d$  il numero di elementi di  $\mathcal{D}$  che non appartengono a  $\mathcal{C}$ .

Abbiamo visto che valgono le uguaglianze

$$a + c = \delta(\eta), \quad a + d = \delta(\sigma), \quad c + d = \delta(\sigma\eta).$$

Da tali uguaglianze segue che

$$\delta(\sigma\eta) = \delta(\sigma) + \delta(\eta) - 2a.$$

□

Definiamo l'applicazione  $\varepsilon: \Sigma_n \rightarrow \{\pm 1\}$  mediante la formula

$$\varepsilon(\sigma) = (-1)^{\delta(\sigma)}.$$

**Corollario 3.5.** *Per ogni  $\sigma, \eta \in \Sigma_n$  vale*

$$\varepsilon(\sigma\eta) = \varepsilon(\sigma)\varepsilon(\eta).$$

*In particolare  $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ .*

*Dimostrazione.* La prima uguaglianza segue immediatamente dal Teorema 3.4. Per la seconda basta osservare che

$$\varepsilon(\sigma)\varepsilon(\sigma^{-1}) = \varepsilon(\sigma\sigma^{-1}) = \varepsilon(\text{identità}) = 1.$$

□

**Corollario 3.6.** *Se una permutazione  $\sigma$  è uguale al prodotto di  $k$  trasposizioni, allora  $\varepsilon(\sigma) = (-1)^k$  e quindi  $\varepsilon(\sigma)$  è uguale alla segnatura  $(-1)^\sigma$ .*

*Dimostrazione.* Ogni trasposizione ha segnatura  $-1$ . □

**Corollario 3.7.** *Ogni permutazione  $\sigma$  si può scrivere come prodotto di  $\delta(\sigma)$  trasposizioni  $\tau_i$ .*

*Dimostrazione.* Induzione su  $\delta(\sigma)$ . Se  $\sigma$  non ha incroci, allora  $\sigma$  è l'identità. Se invece  $\sigma$  è diversa dall'identità, allora l'applicazione bigettiva

$$\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

non può essere crescente e dunque esiste almeno un indice  $h < n$  tale che  $\sigma(h) > \sigma(h+1)$ . Dimostriamo adesso che

$$\delta(\sigma\tau_h) = \delta(\sigma) - 1.$$

Infatti la trasposizione  $\tau_h$  ha un unico incrocio  $\{h, h+1\}$  che, per come abbiamo scelto  $h$ , è anche un incrocio di  $\sigma$ . Quindi per il Teorema 3.4

$$\delta(\sigma\tau_h) = \delta(\sigma) + \delta(\tau_h) - 2 = \delta(\sigma) - 1.$$

Per l'ipotesi induttiva la permutazione  $\sigma\tau_h$  è prodotto di  $\delta(\sigma) - 1$  trasposizioni  $\tau_i$  e quindi

$$\sigma = \sigma(\tau_h\tau_h) = (\sigma\tau_h)\tau_h$$

è prodotto di  $\delta(\sigma)$  trasposizioni  $\tau_i$ . □

Supponiamo adesso di avere un insieme finito  $X$  e di considerare una permutazione di  $X$ , ossia un'applicazione bigettiva  $f: X \rightarrow X$ . In questo caso non possiamo definire il numero di incroci (per fare ciò bisognerebbe che  $X$  fosse ordinato) ma possiamo ugualmente definire la segnatura nel modo seguente:

Supponiamo che  $X$  abbia esattamente  $n$  elementi e scegliamo un'applicazione bigettiva

$$h: \{1, \dots, n\} \rightarrow X.$$

Allora l'applicazione

$$h^{-1}fh: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

è bigettiva e possiamo definire la segnatura come

$$\varepsilon(f) = \varepsilon(h^{-1}fh).$$

Bisogna dimostrare che si tratta di una **buona definizione**, ossia che  $\varepsilon(f)$  non dipende dalla scelta di  $h$ . Se prendiamo un'altra applicazione bigettiva

$$k: \{1, \dots, n\} \rightarrow X,$$

allora  $\sigma = k^{-1}h$  è una permutazione di  $\{1, \dots, n\}$  con inversa  $\sigma^{-1} = h^{-1}k$  e quindi

$$\varepsilon(h^{-1}fh) = \varepsilon(\sigma^{-1}k^{-1}fk\sigma) = \varepsilon(\sigma^{-1})\varepsilon(k^{-1}fk)\varepsilon(\sigma) = \varepsilon(k^{-1}fk).$$

## Esercizi.

**3.1.** Siano  $r < n$  e  $\sigma \in \Sigma_n$  la permutazione

$$\sigma(i) = \begin{cases} i+r & \text{se } i \leq n-r \\ i-(n-r) & \text{se } i > n-r \end{cases}$$

Calcolare la segnatura di  $\sigma$ .