Nel caso in cui i due polinomi considerati sono omogenei, anche il loro risultante lo è. Più precisamente si ha il seguente teorema.

A.18 TEOREMA *Siano*

$$F = A_n + A_{n-1}X_N + \dots + A_0X_N^n,$$
$$G = B_m + B_{m-1}X_N + \dots + B_0X_N^m$$

dove, per ogni $j = 0, \dots, n$, $k = 0, \dots, m$, A_j *e* B_k *sono omogenei di grado* j *e* k *rispettivamente in* $X_1, \dots, X_{N-1}$, *e* $A_0B_0 \neq 0$. *Allora il risultante* $R(F, G)$ *di* F *e* G *rispetto a* X_N *è un polinomio in* $X_1, \dots, X_{N-1}$ *omogeneo di grado* mn, *oppure* $R(F, G) = 0$.

Dimostrazione

Ponendo $R(F, G) = R(X_1, \dots, X_{N-1})$, si ha

$$R(tX_1, \dots, tX_{N-1}) =$$
$$= \begin{pmatrix} t^nA_n & t^{n-1}A_{n-1} & \dots & A_0 & 0 & \dots & & & 0 \\ 0 & t^nA_n & t^{n-1}A_{n-1} & \dots & A_0 & 0 & \dots & & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \dots & & & t^nA_n & t^{n-1}A_{n-1} & & \dots & A_0 \\ t^mB_m & t^{m-1}B_{m-1} & \dots & B_0 & 0 & \dots & & & 0 \\ 0 & t^mB_m & t^{m-1}B_{m-1} & \dots & B_0 & 0 & \dots & & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \dots & & 0 & t^mB_m & t^{m-1}B_{m-1} & & \dots & B_0 \end{pmatrix}.$$

Moltiplichiamo la i-esima riga degli A per t^{m-i+1} e la j-esima riga dei B per t^{n-j+1}. Otteniamo

$$t^pR(tX_1, \dots, tX_{N-1}) =$$
$$= \begin{pmatrix} t^{n+m}A_n & t^{n+m-1}A_{n-1} & \dots & & t^mA_0 & 0 & \dots & 0 \\ 0 & t^{n+m-1}A_n & \dots & & t^mA_1 & t^{m-1}A_0 & 0 \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & & & t^{n+1}A_n & \dots & & tA_0 \\ t^{n+m}B_m & t^{n+m-1}B_{m-1} & \dots & t^nB_0 & 0 & \dots & & 0 \\ 0 & t^{n+m-1}B_m & \dots & t^{n-1}B_0 & 0 & \dots & & 0 \\ \vdots & & & & & & & \vdots \\ 0 & & & & 0 & t^{m+1}B_m & \dots & tB_0 \end{pmatrix} =$$
$$= t^qR(X_1, \dots, X_{N-1}),$$

dove

$$p = m + (m-1) + \dots + 1 + n + (n-1) + \dots + 1 = \binom{m+1}{2} + \binom{n+1}{2}$$

e

$$q = (n+m) + (n+m-1) + \dots + 1 = \binom{m+n+1}{2}.$$

Deduciamo

$$R(tX_1, \dots, tX_{N-1}) = t^{q-p}R(X_1, \dots, X_{N-1}) = t^{mn}R(X_1, \dots, X_{N-1})$$

e la conclusione segue dalla proposizione A.12 (1).

A.19 *Esempi*

1. Nel caso $n = m = 2$, cioè se

$$F = A_2 + A_1X_N + A_0X_N^2$$
$$G = B_2 + B_1X_N + B_0X_N^2,$$

si ha

$$4R(F, G) = (2A_0B_2 - A_1B_1 + 2A_2B_0)^2 - (4A_0A_2 - A_1^2)(4B_0B_2 - B_1^2).$$

2. Nel caso $m = 1$, cioè se

$$F = A_n + A_{n-1}X_N + \dots + A_0X_N^n,$$
$$G = B_1 + B_0X_N,$$

si ha

$$R(F, G) = (-B_0)^nF(-B_1/B_0) =$$
$$= A_0B_1^n - A_1B_0B_1^{n-1} + A_2B_0^2B_1^{n-2} + \dots + (-1)^nA_nB_0^n.$$

B Permutazioni

In quest'appendice esponiamo alcune proprietà delle permutazioni degli insiemi finiti, che vengono utilizzate nella definizione e nello studio dei determinanti.

Sia $\mathscr{J}$ un insieme finito. Una *permutazione* di $\mathscr{J}$ è una corrispondenza biunivoca p: $\mathscr{J} \to \mathscr{J}$. Supponiamo che $\mathscr{J}$ consista di n elementi. Dopo averli numerati, si può identificare $\mathscr{J}$ con l'insieme $\{1, 2, \dots, n\}$ dei primi n numeri naturali. Ci limiteremo quindi a considerare le permutazioni di $\{1, 2, \dots, n\}$. Esse costituiscono un gruppo rispetto alla composizione, consistente di $n! = 1 \cdot 2 \cdot \dots \cdot n$ elementi (la verifica è lasciata al lettore); denoteremo tale gruppo con il simbolo

σ_n. Un elemento $p \in \sigma_n$ viene spesso indicato con una tabella:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ p(1) & p(2) & \dots & p(n) \end{pmatrix}$$

in cui sotto al numero i compare la sua immagine $p(i)$. Ad esempio, la permutazione identica **1** è rappresentata da

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Questa notazione non richiede che nella riga superiore della tabella i numeri $1, 2, \dots, n$ siano disposti in ordine crescente: ad esempio, per ogni $p \in \sigma_n$ la tabella

$$\begin{pmatrix} p(1) & p(2) & \dots & p(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

rappresenta la permutazione p^{-1}.

Siano $a_1, a_2, \dots, a_r$ elementi distinti di $\{1, 2, \dots, n\}$. La permutazione k definita da

$$k(a_1) = a_2, \quad k(a_2) = a_3, \quad \dots \quad k(a_{r-1}) = a_r, \quad k(a_r) = a_1,$$
$$k(b) = b \quad \text{per ogni} \quad b \notin \{a_1, a_2, \dots, a_r\},$$

è un *ciclo di lunghezza* r, e si denota con $(a_1 \ \ a_2 \ \ \dots \ \ a_r)$. In particolare:

$$(1 \ \ 2 \ \ \dots \ \ n) = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}.$$

Ad esempio $(1 \ \ 3 \ \ 2 \ \ 6) \in \sigma_6$ è la permutazione

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

Ogni ciclo di lunghezza 1 è la permutazione identica. Un ciclo di lunghezza 2 si dice *trasposizione*. Una trasposizione scambia tra loro due elementi e lascia fissi tutti gli altri. In particolare una trasposizione è inversa di sé stessa.

Due *cicli* $(a_1 \ \ a_2 \ \ \dots \ \ a_r)$ e $(b_1 \ \ b_2 \ \ \dots \ \ b_s)$ si dicono *disgiunti* se

$$\{a_1, a_2, \dots, a_r\} \cap \{b_1, b_2, \dots, b_s\} = \emptyset.$$

B.1 Proposizione

1) *Ogni permutazione $p \in \sigma_n$ è prodotto di cicli a due a due disgiunti.*
2) *Ogni permutazione $p \in \sigma_n$ è prodotto di trasposizioni.*

Dimostrazione

1) Sia $a_1 \in \{1, \dots, n\}$ qualsiasi, e siano $a_2 = p(a_1)$ $a_3 = p(a_2)$, $a_4 = p(a_3)$, … . Nella successione

$$a_1, a_2, a_3, a_4, \dots \qquad [B.1]$$

il primo elemento che viene ripetuto è a_1, perché se la prima ripetizione fosse $a_r = a_k$, $2 \le k < r$, si avrebbe $a_{r-1} = a_{k-1}$, e la ripetizione non sarebbe la prima. La [B.1] è dunque della forma

$$a_1, a_2, \dots, a_r, a_1, a_2, \dots,$$

e quindi p permuta ciclicamente gli elementi $a_1, a_2, \dots, a_r$.

Consideriamo il ciclo $(a_1 \ \ a_2 \ \ \dots \ \ a_r)$. Se $r = n$, allora $p = (a_1 \ \ a_2 \ \ \dots \ \ a_n)$ e l'asserto è vero. Altrimenti esiste $b_1 \in \{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$. Ragionando come prima si ottiene un ciclo $(b_1 \ \ b_2 \ \ \dots \ \ b_s)$ disgiunto dal precedente. Procedendo in questo modo otterremo un numero finito di cicli disgiunti $K_1, K_2, \dots, K_i$ tali che

$$p = K_1 \circ \dots \circ K_2 \circ K_i. \qquad [B.2]$$

2) In virtù della (1), è sufficiente dimostrare l'asserto nel caso in cui $p = (a_1 \ \ a_2 \ \ \dots \ \ a_r)$ è un ciclo. A questo scopo è sufficiente osservare che

$$(a_1 \ \ a_2 \ \ \dots \ \ a_r) = (a_1 \ \ a_r) \circ (a_1 \ \ a_{r-1}) \circ \ \dots \ \circ (a_1 \ \ a_3) \circ (a_1 \ \ a_2).$$

I cicli $K_1, K_2, \dots, K_i$, essendo disgiunti, sono a due a due permutabili, cioè la scrittura [B.2] è indipendente dall'ordine in cui vengono presi. Se nella [B.2] compaiono dei cicli di lunghezza 1, questi possono essere omessi perché corrispondono alla permutazione identica. Pertanto ogni permutazione si scrive in modo irridondante come prodotto di cicli disgiunti di lunghezza almeno 2.

Si noti che l'espressione di una permutazione come prodotto di trasposizioni non è unica. Ad esempio si ha

$$(1 \ \ 2 \ \ 3) = (1 \ \ 3) \circ (1 \ \ 2) = (2 \ \ 3) \circ (1 \ \ 3).$$

B.2 Teorema *Sia $p \in \sigma_n$. Supponiamo che*

$$p = T_1 \circ T_2 \circ \dots \circ T_h = S_1 \circ S_2 \circ \dots \circ S_k,$$

dove $T_1, \dots, T_h$, $S_1, \dots, S_k$ sono trasposizioni. Allora $h \equiv k$ (mod. 2), cioè h e k hanno la stessa parità.

Dimostrazione

Poiché $\mathbf{1} = p \circ p^{-1} = S_1 \circ S_2 \circ \dots \circ S_k \circ T_h \circ \dots \circ T_2 \circ T_1$, è sufficiente dimostrare che la permutazione identica non può essere ottenuta come prodotto di un numero dispari di trasposizioni.

Sia

$$\mathbf{1} = R_1 \circ \ldots \circ R_m, \qquad [B.3]$$

con $R_1, R_2, \ldots, R_m$ trasposizioni. Supponiamo che si abbia $R_j = (1 \quad a_j)$, per ogni $j = 1, \ldots, m$. Allora, poiché $\mathbf{1}(a_j) = a_j$, la trasposizione $(1 \quad a_j) = (a_j \quad 1)$ compare un numero pari di volte in [B.3], e quindi il numero m di fattori è pari. Se per qualche j si ha $R_j = (b_j, a_j)$, con $b_j \neq 1 \neq a_j$, allora, poiché

$$(b_j, a_j) = (1 \quad b_j) \circ (1 \quad a_j) \circ (1 \quad b_j),$$

possiamo sostituire R_j con il prodotto a secondo membro senza cambiare la parità del numero di fattori della [B.3]. Ci si può quindi ridurre al caso precedente, in cui l'asserto è già stato dimostrato.

B.3 Definizione *Sia $p \in \sigma_n$. Se $p = T_1 \circ T_2 \circ \ldots \circ T_h$, con $T_1, T_2, \ldots, T_h$ trasposizioni, il* segno di p *è* $\epsilon(p) = (-1)^h$.

Dal teorema [B.2] segue che la definizione di segno di una permutazione p è ben posta, perché la parità di h dipende solo da p. Il segno $\epsilon(p)$ gode delle seguenti proprietà, che discendono immediatamente dalla definizione.

B.4 Proposizione

1) $\epsilon(\mathbf{1}) = 1$.

2) $\epsilon(p^{-1}) = \epsilon(p)$ *per ogni* $p \in \sigma_n$.

3) $\epsilon(p \circ q) = \epsilon(p)\,\epsilon(q)$.

4) $\epsilon(T) = -1$ *per ogni trasposizione* $T \in \sigma_n$.

Risoluzione degli esercizi

§ 2

1. a) $\begin{pmatrix} 24 + 9\sqrt{2} \\ -8 + 5\sqrt{2} \end{pmatrix}$ b) $\begin{pmatrix} 14 \\ -21 \end{pmatrix}$ c) $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 10 & 0 & 2 & 0 \end{pmatrix}$.

5. ${}^t(A + {}^tA) = {}^tA + A = A + {}^tA$; ${}^t(A - {}^tA) = {}^tA - A = -(A - {}^tA)$.

Si ha $A = \dfrac{1}{2}(A + {}^tA) + \dfrac{1}{2}(A - {}^tA)$ e il primo addendo è una matrice simmetrica, mentre il secondo è una matrice antisimmetrica.

6. a) $\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} + \begin{pmatrix} 0 & \frac{3}{2} \\ -\frac{3}{2} & 0 \end{pmatrix}$

b) $\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

c) $\begin{pmatrix} 1 & \frac{1}{2} & 1 \\ \frac{1}{2} & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -\frac{1}{2} & -1 \\ \frac{1}{2} & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}$.