Il teorema di Hamilton–Cayley

Sia $A \in \mathbb{K}^{n,n}$ una matrice quadrata di ordine n e $p(\lambda) = p_0 + p_1\lambda + \ldots + p_s\lambda^s$ un polinomio nell'indeterminata λ a coefficienti in $\mathbb{K}$. Definiamo come $p(A)$ la matrice di $\mathbb{K}^{n,n}$ data da

$$p(A) = p_0 + p_1 A + \ldots + p_s A^s.$$

Teorema 1 (Hamilton–Cayley). *Per ogni matrice quadrata $A \in \mathbb{K}^{n,n}$,*

$$\chi_A(A) = O_n,$$

ove con $\chi_A(\lambda)$ si intende il polinomio caratteristico di A,

$$\chi_A(\lambda) = \det(A - \lambda I_n),$$

mentre con O_n si denota la matrice nulla di $\mathbb{K}^{n,n}$.

Dimostrazione. Sia

$$\chi_a(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n.$$

Innanzi tutto, osserviamo che nella matrice B^*, aggiunta di B, compaiono termini in λ con grado al più $n-1$. Pertanto è possibile scrivere

$$B^* = B_0 + B_1\lambda + \ldots + B_{n-1}\lambda^{n-1},$$

ove le B_i sono tutte matrici $n \times n$ ad entrate in $\mathbb{K}$.

Per i due teoremi di Laplace, abbiamo

$$BB^* = (\det B)I_n;$$

in altre parole, tenuto conto della definizione di B e della scrittura di B^*,

$$(A - \lambda I_n)(B_0 + B_1\lambda + \ldots + B_{n-1}\lambda^{n-1}) = \det(A - \lambda I_n)I_n,$$

ovvero

$$(A - \lambda I_n)(B_0 + B_1\lambda + \ldots + B_{n-1}\lambda^{n-1}) = \chi_A(\lambda)I_n = (a_0 + a_1\lambda + \ldots + a_n\lambda^n)I_n.$$

Affinché la relazione sia soddisfatta tutte le matrici che moltiplicano le varie potenze di λ a destra e a sinistra del segno di uguale devono coincidere, ovvero

$$\begin{aligned} AB_0 &= a_0 I_n \\ AB_1 - B_0 &= a_1 I_n \\ AB_2 - B_1 &= a_2 I_n \\ \vdots \quad & \quad \vdots \\ AB_{n-1} - B_{n-2} &= a_{n-1} I_{n-1} \\ -B_{n-1} &= a_n I_n. \end{aligned}$$

Moltiplicando le relazioni date per I_n, A, A^2, ..., A^n nell'ordine si ottiene

$$\begin{aligned} AB_0 &= a_0 I_n \\ A^2 B_1 - AB_0 &= a_1 A \\ A^3 B_2 - A^2 B_1 &= a_2 A^2 \\ \vdots \quad & \quad \vdots \\ A^n B_{n-1} - A^{n-1} B_{n-2} &= a_{n-1} A^{n-1} \\ -A^n B_{n-1} &= a_n A^n; \end{aligned}$$

sommando ora tutte queste equazioni fra loro si ha

$$O_n = a_0 I_n + a_1 A + a_2 A^2 + \ldots + a_n A^n = \chi_A(A),$$

da cui segue il teorema. □

Corollario 1. *Data una matrice* $A \in \mathbb{K}^{n,n}$*, l'insieme*

$$\{A^0 = I, A, A^2, \ldots, A^n\}$$

è linearmente dipendente.

Indicheremo con il simbolo $\mathbb{K}[x]$ l'insieme di tutti i polinomi nell'indeterminata x a coefficienti in un campo $\mathbb{K}$. Tale insieme è dotato della struttura di spazio vettoriale ma *non* è finitamente generato.

Rammentiamo che un campo $\mathbb{K}$ è *algebricamente chiuso* se ogni polinomio $f(x) \in \mathbb{K}[x]$ con $\deg f(x) \geqslant 1$ ammette almeno una radice in $\mathbb{K}$. In particolare, questo è equivalente ad asserire che ogni polinomio di $\mathbb{K}[x]$ si può scrivere come prodotto di polinomi di grado 1, tutti appartenenti a $\mathbb{K}[x]$ stesso. Un esempio di campo algebricamente chiuso è il campo complesso $\mathbb{C}$.

Teorema 2. *Sia* $f(x) \in \mathbb{C}[x]$ *un polinomio tale che* $f(0) \neq 0$. *Allora, per ogni intero* $r > 0$ *esiste un polinomio* $g(x) \in \mathbb{C}[x]$ *tale che* $g(x)^r - x$ *è divisibile per* $f(x)$.

Corollario 2. *Sia* $A \in GL(n, \mathbb{C})$. *Allora, esiste una matrice* $T \in GL(n, \mathbb{C})$ *tale che*

$$T^2 = A.$$

Dimostrazione. Per il Teorema 2, con $f(x) = \chi_A(x)$ ed $r = 2$, esistono due polinomi $g(x), h(x) \in \mathbb{C}[x]$ tali che

$$g(x)^2 - x = \chi_A(x)h(x).$$

Sostituendo ad x la matrice A ed osservando che per il Teorema 1 $\chi_A(A) = O_n$, si ha

$$g(A)^2 - A = O_n,$$

cioè

$$A = g(A)^2.$$

Ponendo $T = g(A)$ si ottiene il risultato. □

Il corollario precedente è vero qualora si sostituisca $\mathbb{C}$ con un qualsiasi campo algebricamente chiuso di caratteristica 0.

Referenze

W.V.D Hodge, D. Pedoe, *Methods of algebraic geometry*, Volume 1, Cambridge University Press (1953).