Le théorème de Cayley-Hamilton

par Alain Prouté
Université Denis Diderot — Paris 7

Nous présentons ici une démonstration du théorème de Cayley-Hamilton qui est à la fois élémentaire et aussi peu calculatoire que possible. De plus, elle ne repose pas sur le fait (souvent utilisé dans ce genre de démonstration) que le corps de base est un sous-corps d'un corps algébriquement clos, argument utilisé pour mettre une matrice sous forme triangulaire, et imposant le plus souvent au niveau élémentaire que le corps de base soit un sous-corps de $\mathbb{C}$. Dans la démonstration ci-dessous, on utilise le fait, un endomorphisme linéaire f étant donné, qu'à tout polynôme $P(X)$ correspond un endomorphisme $P(f)$ et que cette correspondance respecte addition et multiplication (c'est un morphisme d'anneaux unitaires). De plus, comme l'anneau des polynômes est commutatif, les endomorphismes $P(f)$ et $Q(f)$ commutent quels que soient les polynômes $P(X)$ et $Q(X)$.

Théorème **1** *(Cayley-Hamilton) Soit E un espace vectoriel de dimension finie sur un corps K. Soit $f : E \to E$ un endomorphisme linéaire de E. Soit*

$$\chi_f(\lambda) = \det(f - \lambda.\mathbf{Id})$$

le polynôme caractéristique de f. Alors l'endomorphisme $\chi_f(f)$ est nul.

Notons n la dimension de E. Supposons dans un premier temps qu'il existe un vecteur non nul $x \in E$ tel que les n vecteurs :

$$x, f(x), f^2(x), \dots, f^{n-1}(x)$$

soient linéairement indépendants. Ils forment alors une base de E, et le vecteur $f^n(x)$ peut être écrit :

$$f^n(x) = a_0x + a_1f(x) + a_2f^2(x) + \cdots + a_{n-1}f^{n-1}(x)$$

On pose $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} - X^n$, et on a $P(f)(x) = 0$.

La matrice de f dans la base $(x, f(x), \dots, f^{n-1}(x)$ s'écrit alors :

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & & 0 & 0 & a_1 \\ 0 & 1 & \ddots & 0 & 0 & a_2 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & & 1 & 0 & a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & a_{n-1} \end{pmatrix}$$

puisque $x \mapsto f(x)$, $f(x) \mapsto f^2(x)$, etc... $f^{n-1}(x) \mapsto f^n(x) = a_0x + a_1f(x) + \cdots + a_{n-1}f^{n-1}(x)$.

On a donc :

$$\chi_f(\lambda) = \det \begin{pmatrix} -\lambda & 0 & \dots & 0 & 0 & a_0 \\ 1 & -\lambda & & 0 & 0 & a_1 \\ 0 & 1 & \ddots & 0 & 0 & a_2 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & & 1 & -\lambda & a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & a_{n-1}-\lambda \end{pmatrix}$$

Les lignes de cette dernière matrice étant nomées $L_0, L_1, \dots, L_{n-1}$, ajoutons à la première ligne la combinaison linéaire suivante des autres lignes : $\lambda L_1 + \lambda^2 L_2 + \cdots + \lambda^{n-1} L_{n-1}$. Ceci ne change pas le déterminant, et la première ligne de la matrice devient :

$$0 \; 0 \; \dots \; 0 \; 0 \; P(\lambda)$$

En développant le déterminant par rapport à la première ligne on obtient :

$$\chi_f(\lambda) = \pm P(\lambda)$$

Or, on sait que $P(f)(x) = 0$. Par ailleurs, comme les endomorphismes $P(f)$ et f^i commutent, on a :

$$P(f)(f^i(x)) = f^i(P(f)(x)) = f^i(0) = 0$$

ce qui donne $P(f) = 0$, donc $\chi_f(f) = 0$.

On a fait au début l'hypothèse que les vecteurs $x, f(x), f^2(x), \dots$ engendrent E. Passons-nous maintenant de cette hypothèse. Si $E = 0$ le théorème est trivial. Sinon, il existe un vecteur non nul x dans E. Soit k le plus grand entier tel que $(x, f(x), f^2(x), \dots, f^{k-1}(x))$ soit un système libre. Cet entier existe car E est de dimension finie, et il est au moins égal à 1. De plus $f^k(x)$ est combinaison linéaire de $x, f(x), \dots, f^{k-1}(x)$.

Notons F le sous-espace de E engendré par les vecteurs $x, f(x), \dots, f^{k-1}(x)$. Ce sous-espace est stable par f. Notons $f_1 : F \to F$ la restriction de f à F. Si on complète le système libre $(x, f(x), f^2(x), \dots, f^{k-1}(x))$ en une base de E, la matrice de f dans cette base prend la forme suivante :

$$\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right)$$

où A est un bloc carré $k \times k$ et B un bloc carré $(n-k) \times (n-k)$. Soustrayons $\lambda.\mathbf{Id}$ à cette matrice et prenons le déterminant. On obtient (calcul du déterminant par blocs) :

$$\chi_f(\lambda) = \chi_{f_1}(\lambda) Q(\lambda)$$

pour un certain polynôme Q.

D'après la première partie de la démonstration, on a $\chi_{f_1}(f_1)(x) = 0$. Mais comme f_1 est la restriction de f, on a aussi $\chi_{f_1}(f)(x) = 0$, donc $\chi_f(f)(x) = Q(f)(\chi_{f_1}(f)(x)) = 0$. Comme ceci est valable pour tout vecteur non nul x, on a $\chi_f(f) = 0$. ■