

DM 17 - Théorème de Cayley-Hamilton

1 Théorème de Cayley-Hamilton

1.1 Matrice compagne

1. Une simple lecture matricielle nous apprend que $C_P e_j = e_{j+1}$ si $j \in \llbracket 1, n-1 \rrbracket$ et que $C_P e_n = -\sum_{i=1}^n a_{i-1} e_i$. On en déduit (récurrence immédiate) que : $\forall k \in \llbracket 0, n-1 \rrbracket, C_P^k e_1 = e_{k+1}$ et que

$$C_P^n e_1 = C_P e_n = -\sum_{i=1}^n a_{i-1} e_i.$$

2. On calcule :

$$P(C_P) e_1 = \sum_{k=0}^{n-1} a_k C_P^k e_1 + C_P^n e_1 = \sum_{k=0}^{n-1} a_k e_{k+1} - \sum_{i=1}^n a_{i-1} e_i = 0.$$

3. Pour tout $k \in \mathbb{N}$, les matrices C_P^k et $P(C_P)$ commutent. Donc, si $k \in \llbracket 1, n \rrbracket$,

$$P(C_P) e_k = P(C_P) C_P^{k-1} e_1 = C_P^{k-1} P(C_P) e_1 = 0.$$

Comme $P(C_P)$ s'annule sur tous les vecteurs de la base canonique de \mathbb{K}^n , $P(C_P) = 0$.

4. P est un polynôme unitaire de degré n , qui annule C_P . Pour montrer que c'est le polynôme minimal de C_P , il suffit de montrer qu'aucun polynôme non nul de $\mathbb{K}_{n-1}[X]$ n'annule C_P .

Soit $Q = \sum_{k=0}^{n-1} a_k X^k$ un polynôme de $\mathbb{K}_{n-1}[X]$.

On a $Q(C_P) e_1 = \sum_{k=0}^{n-1} a_k e^{k+1}$ d'après les questions précédentes. Par liberté de la famille (e_1, \dots, e_n) , ce vecteur est nul ssi tous les a_k sont nuls. Donc, le seul polynôme de degré $\leq n-1$ annulant C_P est le polynôme nul.

Donc, P est le polynôme minimal de C_P .

1.2 Polynôme caractéristique

5. Tous les $p_{i,j}$ sont des polynômes. Comme χ_A est une combinaison linéaire de produits de $p_{i,j}$ c'est aussi un polynôme.

De plus, les $p_{i,j}$ sont de degré 1 ou 0 : 1 exactement quand $i = j$. On en déduit d'une part que chaque produit $p_{\sigma(1),1} \dots p_{\sigma(n),n}$ est de degré au plus n , et qu'il est de degré n exactement quand $\sigma = \text{id}_{\llbracket 1, n \rrbracket}$.

Ceci montre que χ_A est de degré n et que son coefficient dominant est le même que celui de $\varepsilon(\text{id}) p_{1,1} \dots p_{n,n}$, c'est-à-dire 1.

6. Soit $\lambda \in \mathbb{K}$. On a les équivalences suivantes :

$$\begin{aligned} \chi_A(\lambda) = 0 &\iff \det(\lambda I_n - A) = 0 \\ &\iff \lambda I_n - A \text{ n'est pas inversible} \\ &\iff \text{Ker}(\lambda I_n - A) \neq 0 \\ &\iff \exists X \in \mathcal{M}_{n,1}(\mathbb{K}) - \{0\} : (\lambda I_n - A)X = 0 \\ &\iff \exists X \in \mathcal{M}_{n,1}(\mathbb{K}) - \{0\} : AX = \lambda X \\ &\iff \lambda \text{ est valeur propre de } A. \end{aligned}$$

7. Si χ_A est scindé à racines simples, A a n valeurs propres distinctes $\lambda_1, \dots, \lambda_n$. On considère $v_1, \dots, v_n \in \mathbb{K}^n$ des vecteurs propres correspondants. On a alors montré dans le cours que la famille (v_1, \dots, v_n) est libre, donc c'est une base de \mathbb{K}^n , puisqu'elle est formée de n vecteurs et que \mathbb{K}^n est de dimension n .

Si on note D la matrice dans la base (v_1, \dots, v_n) de l'endomorphisme de \mathbb{K}^n canoniquement associé à A , D est la matrice diagonale $\text{Diag}(\lambda_1, \dots, \lambda_n)$ (puisque pour tout $k \in \llbracket 1, n \rrbracket$, $Av_k = \lambda_k v_k$).

Et d'après le cours, A est semblable à D . On a $A = P^{-1}DP$ si P est la matrice de passage de la base canonique (e_1, \dots, e_n) vers (v_1, \dots, v_n) .

La réciproque est fautive. La matrice nulle est semblable à une matrice diagonale (elle est elle-même diagonale) mais son polynôme caractéristique est X^n , qui n'est pas à racines simples.

8. Considérons A et B deux matrices semblables. Il existe donc $P \in \text{GL}_n(\mathbb{K})$ telle que $A = P^{-1}BP$. Soit $x \in \mathbb{K}$. On a l'égalité

$$xI_n - A = P^{-1}(xI_n - B)P,$$

car $P^{-1} \times xI_n \times P = xI_n$. En prenant les déterminants, on a donc :

$$\chi_A(x) = \det(xI_n - A) = \det(P^{-1})\det(xI_n - B)\det(P)\det(xI_n - B) = \chi_B(x),$$

car $\det(P^{-1}) = \det(P)^{-1}$. Ainsi, les applications polynomiales associées à χ_A et χ_B sont égales. Si \mathbb{K} est infini (on peut s'en contenter !), on sait que cela implique que les polynômes χ_A et χ_B sont égaux.

Si \mathbb{K} est fini, on remarque que \mathbb{K} peut être vu comme un sous-corps d'un corps infini \mathbb{L} (p. ex. $\mathbb{K}(X)$). La même preuve montre alors que les applications polynomiales associées à χ_A et χ_B , vues comme des polynômes de $\mathbb{L}[X]$, sont égales, donc χ_A et χ_B sont égaux.

Remarque : on rappelle que dans le cadre du programme, on peut toujours supposer que \mathbb{K} est égal à \mathbb{R} ou \mathbb{C} , voire exceptionnellement \mathbb{Q} . La subtilité avec les corps finis n'est donc pas très importante. Par contre, on prend garde à bien distinguer égalité entre polynômes et égalité entre fonctions polynomiales associées (même si à la fin, les deux sont équivalentes).

9. **Exemples :**

- (a) A est la matrice d'un projecteur de rang r . On a vu qu'alors, A est semblable à la matrice diagonale D avec r valeurs 1 et $n - r$ valeurs 0 sur la diagonale. Donc,

$$\chi_A = \chi_D = (X - 1)^r X^{n-r}.$$

- (b) B est la matrice d'une symétrie par rapport à un sous-espace de dimension r . Donc, B est semblable à la matrice diagonale D' avec r valeurs 1 et $n - r$ valeurs -1 sur la diagonale. Donc,

$$\chi_B = \chi_{D'} = (X - 1)^r (X + 1)^{n-r}.$$

10. On considère (f_1, \dots, f_r) une base de F , qu'on complète en une base $(f_1, \dots, f_r, g_{r+1}, \dots, g_n)$ de E . Notons A_F la matrice de f_F dans la base (f_1, \dots, f_r) et A la matrice de f dans la base $(f_1, \dots, f_r, g_{r+1}, \dots, g_n)$. Alors, A s'écrit par blocs :

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

où $C \in \mathcal{M}_{r, n-r}(\mathbb{K})$ et $D \in \mathcal{M}_{n-r}(\mathbb{K})$. Pour tout $x \in \mathbb{K}$, on a aussi :

$$xI_n - A = \begin{pmatrix} xI_r - A_F & C \\ 0 & xI_{n-r} - D \end{pmatrix}.$$

D'où l'on tire $\det(xI_n - A) = \det(xI_r - A_F) \det(xI_{n-r} - D)$. En notant P l'application polynomiale $x \mapsto \det(xI_{n-r} - D)$, on a donc :

$$\forall x \in \mathbb{K}, \chi_A(x) = \chi_{A_F}(x)P(x).$$

Comme précédemment, cette égalité entre applications polynomiales induit une égalité entre polynômes : $\chi_A = \chi_{A_F}P$. Donc χ_{A_F} divise χ_A .

1.3 Théorème de Cayley-Hamilton

11. Soit $x \in \mathbb{K}$. On considère la matrice $C_P(x) = xI_n - C_P$. On a :

$$C_P(x) = \begin{pmatrix} x & 0 & \dots & 0 & a_0 \\ -1 & x & \dots & 0 & a_1 \\ 0 & -1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & a_{n-1} + x \end{pmatrix}.$$

On calcule son déterminant en développant selon la première colonne : on a

$$\det(C_P(x)) = x \cdot \begin{vmatrix} x & \dots & 0 & a_1 \\ -1 & \ddots & \vdots & a_2 \\ 0 & \ddots & x & \vdots \\ \vdots & \ddots & -1 & a_{n-1} + x \end{vmatrix} + 1 \cdot \begin{vmatrix} 0 & \dots & 0 & a_0 \\ -1 & \ddots & \vdots & a_2 \\ 0 & \ddots & x & \vdots \\ \vdots & \ddots & -1 & a_{n-1} + x \end{vmatrix}.$$

Le deuxième déterminant se calcule en développant selon la première ligne : il vaut

$$a_0(-1)^{1+(n-1)}\det(-I_{n-2}) = a_0.$$

En notant Q le polynôme $Q = X^{n-1} + \sum_{k=0}^{n-2} a_{k+1}X^k$, on a donc :

$$\forall x \in \mathbb{K}, \det(C_P(x)) = x \times \det(C_Q(x)) + a_0.$$

On peut alors procéder par récurrence sur $n \in \mathbb{N}^*$ pour montrer que si P est un polynôme unitaire de degré n , alors $\forall x \in \mathbb{K}, \chi_{C_P}(x) = P(x)$.

Si $n = 1$ et $P = X + a_0$, $C_P(x) = (a_0 + x)$ et donc $\chi_{C_P}(x) = a_0 + x = P(x)$.

Si le résultat est montré pour tout polynôme de degré $n - 1$ et si P est de degré n , on a, avec les notations précédentes : $\chi_{C_P}(x) = x \times \chi_{C_Q}(x) + a_0$. Or, par hypothèse de récurrence, $\chi_{C_Q}(x) = Q(x)$ et on a bien $P(x) = xQ(x) + a_0$, ce qui conclut.

On a donc montré que pour tout $x \in \mathbb{K}$, $\chi_{C_P}(x) = P(x)$. Comme précédemment, on en déduit que cette égalité entre fonctions polynomiales induit une égalité polynomiale $\chi_{C_P} = P$.

On a montré précédemment que $P(C_P) = 0$, donc $\chi(C_P)(C_P) = 0$, ce qui montre le théorème de Cayley-Hamilton pour les matrices compagnes.

12. (a) Soit $n \in \mathbb{N}$. Alors $f(f^n(x)) = f^{n+1}(x) \in E_x$. Comme E_x est engendré par les $f_n(x)$, ceci montre que $f(E_x) \subset E_x$.

Comme E est de dimension finie, la famille $(f^n(x))_{n \in \mathbb{N}}$ n'est pas liée. On considère le plus grand entier $r \in \mathbb{N}^*$ tel que $(x, f(x), \dots, f^{r-1}(x))$ est libre. Alors, $f^r(x)$ est combinaison linéaire de cette famille (sinon on contredirait la maximalité de r). On peut donc trouver des scalaires a_0, \dots, a_{r-1} tels que

$$f^r(x) = \sum_{k=0}^{r-1} a_k f^k(x).$$

On note P le polynôme $X^r - \sum_{k=0}^{r-1} a_k X^k$. Soit $n \in \mathbb{N}$. On effectue la division euclidienne de X^n par P :

$$X^n = Q \times P + R,$$

avec $\deg R \leq n - 1$. On évalue cette égalité polynomiale en f :

$$f^n = Q(f) \circ P(f) + R(f),$$

puis on évalue en x :

$$f^n(x) = Q(f)(P(f)(x)) + R(f)(x) = R(f)(x),$$

car $P(f)(x) = 0$.

Or, $R(f)(x) \in \text{Vect}(x, f(x), \dots, f^{r-1}(x))$. Ceci montre que la famille $(x, f(x), \dots, f^{r-1}(x))$ est aussi génératrice de E_x ; c'en est donc une base.

(b) Pour tout $i \in \llbracket 0, r-2 \rrbracket$, on a $f(f^i(x)) = f^{i+1}(x)$. Et, $f(f^{r-1}(x)) = \sum_{k=0}^{r-1} a_k f^k(x)$, avec les notations précédentes.

La traduction matricielle de ces égalités est que, dans la base $(x, f(x), \dots, f^{r-1}(x))$, la matrice de f_{E_x} est :

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

c'est-à-dire la matrice compagne de P (avec les notations précédentes).

(c) On vient de montrer que f_{E_x} est représenté dans la base $(x, f(x), \dots, f^{r-1}(x))$ par une matrice compagne C_P , pour un certain polynôme P . On a $\chi_{C_P}(C_P) = 0$, d'après la question 11. Or, par définition, $\chi_{f_{E_x}} = \chi_{C_P}$; donc $\chi_{C_P}(C_P)$ est la représentation matricielle de $\chi_{f_{E_x}}(f_{E_x})$ (dans la même base). Donc $\chi_{f_{E_x}}(f_{E_x}) = 0$.

13. On cherche à montrer que $\chi_f(f) = 0$. Cela revient à montrer que, pour tout $x \in E$, $\chi_f(f)(x) = 0$. Soit $x \in E$.

Alors, x est dans E_x . Par la question précédente, on a donc $\chi_{f_{E_x}}(f_{E_x})(x) = 0$. Comme f et f_{E_x} coïncident sur E_x , on peut plus simplement écrire $\chi_{f_{E_x}}(f)(x) = 0$. De plus, on sait par la question 10 que $\chi_{f_{E_x}}$ divise χ_f . Notons P un polynôme tel que $\chi_f = P \times \chi_{f_{E_x}}$. En évaluant en f , puis en x , on a donc :

$$\chi_f(f)(x) = P(f)(\chi_{f_{E_x}}(f)(x)) = 0.$$

Ainsi, pour tout x dans E , $\chi_f(f)(x) = 0$.

Donc, $\chi_f(f) = 0$, ce qui conclut la démonstration du théorème de Cayley-Hamilton.