Feuille de TD n° 3

Diagonalisation, trigonalisation, polynômes d'endomorphismes

Exercice 1 : (Rotations) Soit

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

la rotation d'angle $\theta \in \mathbb{R}/2\pi\mathbb{Z}$.

(i) Déterminer les angles θ pour lesquels R_θ est diagonalisable sur $\mathbb{R}$.

(ii) Montrer que R_θ est toujours diagonalisable sur $\mathbb{C}$. Donner sa forme diagonale.

(iii) Expliciter le cas $\theta = \pi/2$. (On appelle $J = R_{\pi/2}$ *la structure complexe standard sur* $\mathbb{R}^2$.)

Solution de l'exercice 1. (i) Le polynôme caractéristique est $P_{R_\theta}(X) = X^2 - 2\cos\theta X + 1$. Celui-ci admet des racinces réelles si et seulement si $\cos\theta = \pm 1$, ou encore $\theta = 0 \bmod 2\pi$ ou $\theta = \pi \bmod 2\pi$. Dans ces cas $R_\theta = \pm I_2$ est diagonale.

(ii) Pour $|\cos\theta| < 1$ le polynôme caractéristique a deux racines complexes conjuguées simples et distinctes. Par un critère vu en cours, la matrice R_θ est diagonalisable.

(iii) Pour $\theta = \pi/2$, la matrice $R_{\pi/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ admet comme forme diagonale $D = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. L'espace propre pour la valeur propre i est $V_i = \text{Vect}\begin{pmatrix} 1 \\ -i \end{pmatrix}$, l'espace propre pour la valeur propre $-i$ est $V_{-i} = \text{Vect}\begin{pmatrix} 1 \\ i \end{pmatrix}$. On a

$$D = P^{-1}R_{\pi/2}P, \quad \text{avec } P = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \quad \text{et } P^{-1} = \frac{1}{2i}\begin{pmatrix} i & -1 \\ i & 1 \end{pmatrix}.$$

Exercice 2 : (Puissances de matrices) (i) Soit $A \in M_n(k)$ une matrice diagonalisable et $P \in \mathrm{GL}_n(k)$ telle que $P^{-1}AP = D$, où $D \in M_n(k)$ est diagonale. Montrer l'égalité

$$A^n = PD^nP^{-1}$$

pour tout $n \geq 0$. Étendre cette égalité à tout $n \in \mathbb{Z}$ lorsque A est inversible.

(ii) Calculer A^n pour $n \geq 0$ lorsque

$$A = \begin{pmatrix} 13 & -6 \\ 28 & -13 \end{pmatrix}, \quad \text{respectivement} \quad A = \begin{pmatrix} -5 & 3 \\ -14 & 8 \end{pmatrix}.$$

Solution de l'exercice 2. (i) –

(ii) Lorsque $A = \begin{pmatrix} 13 & -6 \\ 28 & -13 \end{pmatrix}$ les valeurs propres sont ± 1 et $A = P^{-1}DP$ avec $P = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Lorsque $A = \begin{pmatrix} -5 & 3 \\ -14 & 8 \end{pmatrix}$ les valeurs propres sont 1 et 2 et nous avons $A = P^{-1}DP$ avec la même matrice P que précédemment et $D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

Exercice 3 : (Diagonalisation simultanée) Soient V un k-espace vectoriel et $u, v \in \mathrm{End}_k(V)$. On dit que *$u$ et v commutent* si $uv = vu$. On dit que *u et v sont simultanément diagonalisables* s'il existe une base $\mathcal{B}$ de V telle que les matrices $M_{\mathcal{B}}(u)$ et $M_{\mathcal{B}}(v)$ soient toutes les deux diagonales.

Dans cet exercice nous supposons V de dimension finie.

1. Nous nous proposons de montrer le résultat suivant :

Soient $u, v \in \mathrm{End}_k(V)$ diagonalisables. Alors u et v commutent $\Leftrightarrow$ u et v sont simultanément diagonalisables.

(i) Montrer l'implication inverse $\Leftarrow$.

(ii) Montrer que tout espace propre de u est stable par v. Conclure en utilisant la Proposition 1.2.4 du polycopié, dont on pourra se rappeler la démonstration. (*La restriction d'un endomorphisme diagonalisable à un sous-espace stable est encore diagonalisable.*)

2. Donner des exemples d'endomorphismes u, v diagonalisables qui ne commutent pas.

3. Montrer que, si u et v sont diagonalisables et commutent, alors $u + v$ et uv sont diagonalisables.

4. Donner un exemple d'endomorphismes diagonalisables, qui ne commutent pas, tels que $u + v$ ou uv ne soient pas diagonalisables. (L'on pourra prendre V de dimension 2.)

5. Montrer que, si u et v commutent, alors

$$(u + v)^p = \sum_{i=0}^{p} \binom{p}{i} u^i v^{p-i}, \quad \text{pour tout } p \in \mathbb{N}.$$

Solution de l'exercice 3.

1.(i). Toutes deux matrices diagonales commutent.

1.(ii). Soit $\lambda \in k$ une valeur propre de u et $V_\lambda = \mathrm{Ker}(u - \lambda \mathrm{Id}_V)$ l'espace propre associé. Pour tout $x \in V_\lambda$ l'on a

$$u(v(x)) = v(u(x)) = v(\lambda x) = \lambda v(x),$$

de sorte que $v(x) \in V_\lambda$. Ainsi V_λ est stable par v. La Proposition 1.2.4 assure qu'il existe une base de V_λ constituée de vecteurs propres de v. Bien-sûr, ceux-ci sont aussi des vecteurs propres de u.

En adjoignant de telles bases pour tous les espaces propres de u nous construisons une base qui diagonalise simultanément u et v.

2. et 4. Prenons $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.

3. Si D et D' sont deux matrices diagonales, alors $D + D'$ et DD' sont diagonales.

5. Récurrence. C'est une instance de la formule binomiale de Newton.

Exercice 4 : (Approximation par des matrices inversibles) Soit A une matrice réelle de taille $n \times n$. Parmi les matrices de la forme $A_\lambda = A + \lambda I_n$, $\lambda \in \mathbb{R}$, quelles sont celles qui sont inversibles ? Montrer qu'il existe une suite (λ_k) tendant vers zéro telle que toutes les matrices A_{λ_k} sont inversibles et la suite A_{λ_k} converge vers A, au sens où les coefficients des A_{λ_k} convergent vers ceux de A.

Solution de l'exercice 4. La matrice $A + \lambda I_n$ est inversible si et seulement si λ n'est pas une valeur propre, si et seulement si λ n'est pas racine du polynôme caractéristique. Celui-ci admet au plus n

racines. Or, étant donné un nombre fini (ici au plus n) de valeurs réelles, il existe une suite $\lambda_k \to 0$, $k \to \infty$ qui les évite. Ou encore : le complémentaire d'un sous-ensemble fini de $\mathbb{R}$ est dense dans $\mathbb{R}$.

Exercice 5 : (Approximation par des matrices diagonalisables) Montrer que les matrices de $M_n(\mathbb{C})$ qui sont diagonalisables sont denses dans $M_n(\mathbb{C})$. Autrement dit, pour toute matrice $A \in M_n(\mathbb{C})$ il existe une suite $A_k \in M_n(\mathbb{C})$, $k \geq 1$ telle que $A_k \to A$ pour $k \to \infty$, au sens où, pour tous $i, j \in \{1, \ldots, n\}$, on a $A_k(i,j) \to A(i,j)$ pour $k \to \infty$. Ici $A(i,j)$ désigne le coefficient (i,j) de la matrice A.

Solution de l'exercice 5. Soit $A \in M_n(\mathbb{C})$. Puisque le corps $\mathbb{C}$ est algébriquement clôs, le polynôme caractéristique de A est scindé sur $\mathbb{C}$ et la matrice est trigonalisable. Quitte à conjuguer par une matrice inversible, nous pouvons donc supposer sans perte de généralité que A est triangulaire supérieure.

Nous pouvons alors choisir des suites $a_k^1, \ldots, a_k^n$, $k \geq 1$ telles que pour tout $i = 1, \ldots, n$ on ait $a_k^i \to 0$ pour $k \to \infty$ et telles que la matrice triangulaire supérieure $A_k = A + \mathrm{Diag}(a_k^1, \ldots, a_k^n)$ ait des coefficients distincts sur la diagonale. Alors A_k est diagonalisable et $A_k \to A$ pour $k \to \infty$.

Exercice 6 : (i) Soit u un endomorphisme d'un K-espace vectoriel vérifiant $u^3 = \mathrm{Id}$. Montrer que $E = \mathrm{Ker}(u - \mathrm{Id}) \oplus \mathrm{Ker}(u^2 + u + \mathrm{Id})$.

(ii) Soient u un endomorphisme d'un K-espace vectoriel et $P \in K[X]$ un polynôme annulateur de u. On suppose qu'on peut écrire $P = QR$, avec Q et R premiers entre eux. Montrer que $\mathrm{Im}(Q(u)) = \mathrm{Ker}(R(u))$.

Solution de l'exercice 6. 1. Il suffit de voir que les deux polynômes $x - 1$ et $x^2 + x + 1$ sont premiers entre eux.

2. On a premièrement $\forall x \in E, P(u)(x) = R(u)(Q(u)(x)) = 0$, donc $\mathrm{Im}(Q(u)) \subset \mathrm{Ker}(R(u))$. Deuxièmement, $E = \mathrm{Im}(Q(u)) \oplus \mathrm{Ker}(Q(u))$ et $E = \mathrm{Ker}(Q(u)) \oplus \mathrm{Ker}(R(u))$, donc $\dim(\mathrm{Im}(Q(u))) = \dim(\mathrm{Ker}(R(u)))$, ce qui entraîne la conclusion.

Exercice 7 : Soit $A \in M_n(\mathbb{R})$.

1. On suppose que $A^3 = A^2$.

(i) Montrer que A^2 est diagonalisable.

(ii) Trouver une telle matrice A non diagonalisable.

2. On suppose que $A^{k+1} = A^k$, avec $k > 0$ un entier. Montrer que A^k est diagonalisable.

Solution de l'exercice 7. 1. (i) On a $A^4 = (A^3)A = A^2A = A^3 = A^2$, donc A^2 est annulée par le polynôme à racines simples $X(X-1)$. Elle est donc diagonalisable.

(ii) La matrice $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ convient.

2. Si $A^k = A^{k+1}$ l'on a aussi $A^{k+1} = A^{k+2}$. On montre alors que $A^p = A^{p+1}$ pour tout $p \geq k$, ce qui entraîne $A^k = A^{2k}$, ou encore $A^k(A^k - I_n) = 0$. La matrice A^k est donc annulèe par le polynôme $X(X-1)$, scindé avec racines simples. Elle est donc diagonalisable.

Exercice 8 : Soit

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

.

(i) Déterminer le polynôme caractéristique de A ;

(ii) Déterminer le polynôme minimal de A ;

(iii) En utilisant le théorème de Cayley-Hamilton, en déduire que A est inversible et déterminer A^{-1}.

Solution de l'exercice 8. (i) $P_A(X) = (2-X)^3$. (ii) Le polynôme minimal divise le polynôme caractéristique, il peut donc être égal à $2-X$, $(2-X)^2$, ou $(2-X)^3$. Par ailleurs, le polynôme minimal annule A. On voit que $2I_3 - A \neq 0$ et $(2I_3 - A)^2 = 0$, donc le polynôme minimal est $(2-X)^2$. (iii) $A^{-1} = -\frac{1}{4}A + I_3$

Exercice 9 : Soit $A \in M_n(K)$, avec K égal à $\mathbb{R}$ ou $\mathbb{C}$. On suppose que A vérifie la relation

$$A^2 + A + I_n = 0.$$

1. On suppose $K = \mathbb{C}$. Montrer que la matrice A est diagonalisable.

2. On suppose $K = \mathbb{R}$.

(i) Montrer que la matrice A n'est pas trigonalisable.

(ii) Montrer que n est un entier pair.

(iii) On suppose que $n = 2$. Construire une telle matrice.

(iv) Trouver, à l'aide de la question précédente et pour tout entier n pair, une matrice réelle A d'ordre n vérifiant la relation $A^2 + A + I_n = 0$.

Solution de l'exercice 9. 1. La matrice est diagonalisable sur $\mathbb{C}$ puisqu'elle est annulée par le polynôme scindé sur $\mathbb{C}$ à racines simples $X^2 + X + 1$.

2.(i) Le polynôme $X^2 + X + 1$ est irreductible sur $\mathbb{R}$, la matrice n'est donc pas trigonalisable.

(ii) Le polynôme $X^2 + X + 1$ étant irréductible et annulateur de A, c'est le polynôme minimal de A. Le polynôme caractéristique est donc du type $(X^2 + X + 1)^k$, de degré pair.

(iii) Par exemple $A = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$.

(iv) On peut prendre une matrice diagonale par blocs 2×2, avec tous les blocs diagonaux égaux à la matrice A construite au point précédent.

Exercice 10 : (Endomorphismes définis par des permutations) Le but de cet exercice est d'étudier des exemples d'endomorphismes définis par une permutation des vecteurs d'une base d'un espace vectoriel. Plus précisément si E est un $k-$espace vectoriel, si $\mathcal{B} = (e_1, \dots, e_n)$ est une base de E et si $\sigma \in S_n$ est une permutation de l'ensemble $\{1, \dots, n\}$, on définit $u_{\sigma,\mathcal{B}}$ par son action sur la base :

$$\forall i \in \{1, \dots, n\}, \quad u_{\sigma,\mathcal{B}}(e_i) = e_{\sigma(n)}\,.$$

Dans la suite, on notera simplement u l'endomorphisme ainsi défini si σ et $\mathcal{B}$ sont fixés et qu'il n'y a pas de confusion possible. Si v est un endomorphisme d'un $k-$espace vectoriel V, on notera μ_v le polynôme minimal de v et χ_v son polynôme charactéristique.

a) Un exemple : la base étant fixée, on suppose que σ est la permutation circulaire $(1, \dots, n) \mapsto (n, 1, \dots, n-1)$.
   i) Montrer que le polynôme caractéristique de u est $(-1)^n(X^n - 1)$. En déduire que u est diagonalisable.
   ii) Montrer qu'un polynôme P qui annule u et tel que $deg(P) < n$ est nécessairement le polynôme nul. En déduire que le polynôme minimal de u est $X^n - 1$.
   iii) On pose $\omega = e^{\frac{2i\pi}{n}}$. Pour $1 \leq k \leq n$, soit $x_k = \sum_{i=1}^{n} (\omega^k)^{n-i+1} e_i$. Montrer que $(x_1, \dots, x_n)$ est une base de vecteurs propres et donner la matrice de u dans cette base.

b) On revient au cas général. On établit deux résultats préliminaires.
   i) On suppose que $E = \oplus_{i=1}^{k} E_i$ est somme directe de sous-espaces non nuls et stables par $v \in \mathrm{End}_k(E)$. Pour $i \in \{1, \dots, k\}$, on note v_i l'endomorphisme de E_i induit par v.
   Montrer que $\mu_v = PPCM(\mu_{v_1}, \dots, \mu_{v_k})$ et que $\chi_v = \chi_{v_1} \cdot \dots \cdot \chi_{v_k}$.
   ii) Montrer (ou rappeler) qu'une permutation $\sigma \in S_n$ est le produit d'un nombre fini de cycles de supports disjoints $\sigma = \sigma_1 \cdots \sigma_k$. On note $\mathrm{supp}(\sigma_i) \subset \{1, \dots, n\}$ le support de σ_i et m_i son cardinal.

c) Un exemple : on suppose $n = 5$ et $\sigma : (1, \dots, 5) \mapsto (3, 5, 4, 1, 2)$ alors $\sigma = (3, 4, 1) \cdot (5, 2)$, $\sigma_1 = (3, 4, 1)$, $\mathrm{supp}(\sigma_1) = \{1, 3, 4\}$, $\sigma_2 = (5, 2)$, $\mathrm{supp}(\sigma_2) = \{2, 5\}$.
   Montrer que $\mathrm{Vect}(e_1, e_3, e_4)$ et $\mathrm{Vect}(e_2, e_5)$ sont stables par u. Calculer le polynôme caractéristique et le polynôme minimal de u.

d) En général, on note $E_k = \mathrm{Vect}(e_i, i \in \mathrm{supp}(\sigma_i))$. Montrer que $E = \oplus_{i=1}^{k} E_i$, montrer que E_i est stable par u. On note u_{σ_i} l 'endomorphisme de E_i induit par u. Montrer que $\chi_u = \Pi_{i=1}^{k}(X^{m_i} - 1)$ et $\mu_u = PPCM\{X^{m_i} - 1, i = 1, \dots, k\}$. Montrer que u est d'ordre $PPCM(m_i, i = 1 \dots, k)$.

e) On suppose $n = 4$. Donner la liste des paires (μ_u, χ_u) possibles.

Solution de l'exercice 10.

a) i) On peut calculer directement le polynôme caractéristique : la matrice de l'endomorphisme u dans la base $(f_0, \dots, f_{n-1})$ est

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \text{ donc } \det(u - X\,\mathrm{Id}) = \begin{vmatrix} -X & 0 & 0 & \dots & 1 \\ 1 & -X & \dots & \dots & 0 \\ 0 & 1 & -X & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \\ 0 & \dots & 0 & 1 & -X \end{vmatrix} \text{ que l'on développe}$$

suivant la premire ligne :

$$-X \cdot \begin{vmatrix} -X & \dots & \dots & 0 \\ 1 & -X & \dots & \vdots \\ \ddots & \ddots & \ddots & \\ \dots & 0 & 1 & -X \end{vmatrix} + (-1)^{n-1} \begin{vmatrix} 1 & -X & 0 & \dots \\ 0 & 1 & -X & \dots \\ \vdots & \ddots & \ddots & \ddots \\ 0 & \dots & 0 & 1 \end{vmatrix} = (-X)^n + (-1)^{n-1} = (-1)^n(X^n - 1)\,.$$

Comme $X^n - 1 = \Pi_{k=0}^{n-1}(X - \omega^k)$ admet n racines distinctes, u est diagonalisable.

ii) Tout polynôme non nul qui annule u est de degré plus grand que $n = d$:
Si $P(X) = \sum_{k=0}^{r} a_k X^k$ est tel que $P(u) = 0$ et si $r \leq n-1$, on a

$$0 = P(u)(e_1) = \sum_{k=0}^{r} a_k u^k(e_1) = \sum_{k=0}^{r} a_k e_{k+1}\,.$$

Mais $(e_1, \ldots, e_n)$ base de V entraine $a_1 = \ldots = a_r = 0$ (car $r \leq n-1$).
Donc $X^d - 1$ est le polynôme minimal de u (voir déf 1.5.2 du cours).

iii) Pour $0 \leq k \leq n-1$, soit $x_k = \sum_{i=1}^{n} (\omega^k)^{i-1} e_i$. Posons $e_{n+1} = e_1$. Alors

$$\begin{aligned} u(x_k) = \sum_{i=1}^{n} (\omega^k)^{i-1} e_{i+1} \quad &= \omega^k \cdot \sum_{i=1}^{n} (\omega^k)^{i} e_{i+1} \quad \text{(on pose } j = i+1) \\ = \omega^k \cdot \sum_{j=2}^{n} (\omega^k)^{j-1} e_j + e_1 = \omega^k \cdot \sum_{i=1}^{n} (\omega^k)^{i-1} e_i \quad &= \omega^k \cdot x_k\,. \end{aligned}$$

car $(\omega^k)^n e_{n+1} = e_1$. Ainsi x_k est vecteur propre pour la valeur propre $\omega^k = e^{i\frac{2k\pi}{n}}$. Les valeurs propres étant distinctes, on obtient une base de vecteurs propres. La matrice de u dans cette base est $\mathrm{Diag}(1, \omega, \omega^2, \ldots, \omega^{n-1})$.

b)

c)

d) Comme le polynôme minimal et le polynôme caractéristique son invariants par conjugaison, en particulier la conjugaison induite par permutation des vecteurs d'une base, on pourra raisonner seulement sur le nombre et la longueur des cycles de la permutation σ.

i) Un unique cycle de longueur 4 : $\sigma = (4, 1, 2, 3)$, $\mu_u = \chi_u = X^4 - 1$.

ii) Un cycle de longueur 3, un de longueur 1 : $\sigma = (1)(4, 2, 3)$, $\chi_u = (X^3-1)(X-1)$, $\mu_u = X^3-1$.

iii) Un cycle de longueur 2, deux cycles de longueur 1 : $\sigma = (1)(2)(43)$, $\chi = (X^2-1)(X-1)^2$, $\mu_u = X^2 - 1$.

iv) Deux cycles de longueur 2 : $\sigma = (21)(43)$, $\chi_u = (X^2-1)^2$, $\mu_u = X^2 - 1$.

v) Uniquement des cycles de longueur 1 : σ est l'identité de $\{1, \ldots, 4\}$, u est l'identité de E, $\mu_u = X - 1$, $\chi_u = (X-1)^4$.

Exercice 11 : (Une autre démonstration de théorème de Cayley-Hamilton) Soient E un K-espace vectoriel de dimension finie égale à n et $f \in \mathrm{End}_K(E)$. On veut montrer que le polynôme caractéristique P_f est un annulateur de f, c'est-à-dire $P_f(f) = 0$.

(i) Soit $x \in E$, $x \neq 0$. Justifier qu'il existe un entier p avec $0 \leq p \leq n-1$ tel que le système $(x, f(x), ..., f^p(x))$ soit libre et le système $(x, f(x), ..., f^p(x), f^{p+1}(x))$ soit lié.

(ii) On note $G = \mathrm{Vect}(x, f(x), ..., f^p(x))$ et f_G la restriction de f à G. Écrire la matrice de f_G dans la base $(x, f(x), ..., f^p(x))$ et montrer que

$$P_{f_G}(f_G) = 0.$$

(iii) Conclure par récurrence sur $n \geq 1$.

Solution de l'exercice 11. (i) Les vecteurs $(x, f(x), ..., f^{n-1}(x), f^n(x))$ sont liés puisque l'espace E est de dimension égale à n et donc toute famille libre est constituée d'au plus n vecteurs. Soit $p_0 \in \mathbb{N}$ le plus petit entier tel que les vecteurs $(x, f(x), ..., f^p(x), f^{p+1}(x))$ soient liés. Alors $p \leq n-1$ par ce qui précède, et les vecteurs $(x, f(x), \ldots, f^p(x))$ forment une famille libre par définition de p.

(ii) Par définition de p, il existe $a_0, a_1, ..., a_p \in K$ tels que $f^{p+1}(x) = a_0 x + a_1 f(x) + ... + a_p f^p(x)$. La matrice de la restriction de f_G est alors

$$A(a_0, \dots, a_p) = \begin{pmatrix} 0 & 0 & 0 & 0 & ... & a_0 \\ 1 & 0 & 0 & 0 & ... & a_1 \\ 0 & 1 & 0 & 0 & ... & a_2 \\ 0 & 0 & 1 & 0 & ... & a_3 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & a_p \end{pmatrix}.$$

Nous affirmons que le polynôme caractéristique de cette matrice est

$$P_{f_G}(X) = P_{A(a_0,...,a_p)}(X) = (-1)^{p+1}(X^{p+1} - \sum_{i=0}^{p} a_i X^i).$$

La formule est suggérée par le cas particuliers $p = 0, 1, 2$, lorsque l'on calcule directement

$$P_{A(a_0)}(X) = a_0 - X, \qquad P_{A(a_0,a_1)}(X) = X^2 - a_1 X - a_0, \qquad P_{A(a_0,a_1,a_2)}(X) = -X^3 + a_2 X^2 + a_1 X + a_0.$$

Nous démontrons la formule par récurrence sur p. En la supposant démontrée au rang $p-1$, nous la démontrons au rang p en développant selon la première ligne :

$$\begin{aligned} P_{A(a_0,...,a_p)}(X) &= -X P_{A(a_1,...,a_p)}(X) + a_0(-1)^{p+2} \\ &= a_0(-1)^{p+2} - X(-1)^p(X^p - \sum_{i=1}^{p} a_i X^{i-1}) \\ &= (-1)^{p+1}(X^{p+1} - \sum_{i=1}^{p} a_i X^i - a_0). \end{aligned}$$

Le point crucial à remarquer est que

$$P_{f_G}(f_G) = 0.$$

En effet, pour tout $\ell \in \{0, \dots, p\}$ nous avons

$$P_{f_G}(f_G)(f^\ell(x)) = (f^{p+1} - \sum_{i=0}^{p} a_i f^i)(f^\ell(x)) = f^\ell \left(f^{p+1}(x) - \sum_{i=0}^{p} a_i f^i(x) \right) = 0.$$

(iii) Nous démontrons maintenant le théorème de Cayley-Hamilton par récurrence sur n. En le supposant démontré au rang $\leq n-1$, démontrons-le au rang n. Soit H un sous espace vectoriel supplémentaire de G. Puisque $\dim G = p+1 \geq 1$, on a $\dim H = n-p-1 \leq n-1$. Choisissons une base $\mathcal{B} = (x_{p+2}, ..., x_n)$ de H et considérons la matrice de f dans la base $\tilde{\mathcal{B}} = \{x, f(x), f^2(x), ...f^p(x), x_{p+2}, ..., x_n\}$. Celle-ci s'écrit

$$M_{\tilde{\mathcal{B}}}(f) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

où A est la matrice de la restriction de f_G et C est la matrice de l'application $f' = p \circ f|_H : H \to H$ dans la base $\mathcal{B}$, avec $p : E \to H$ la projection sur H parallèlement à G. Alors

$$P_f(X) = P_A(X) P_C(X) = P_{f_G}(X) P_{f'}(X) = P_{f'}(X) P_{f_G}(X).$$

Pour tout $v \in E$, écrivons de manière unique $v = v_G + v_H$, avec $v_G \in G$ et $v_H \in H$. Pour montrer que $P_f(f) = 0$ il suffit de montrer que $P_f(f)(v_G) = 0$ et $P_f(f)(v_H) = 0$ pour tout $v \in E$.

— Nous avons $P_f(f)(v_G) = P_{f'}(f)\left(P_{f_G}(f)(v_G)\right) = P_{f_G}(f_G)(v_G) = 0$, puisque $P_{f_G}(f_G)(v_G) = 0$ d'après (ii).

— Nous avons

$$\begin{aligned} P_f(f)(v_H) &= P_{f_G}(f)\left(P_{f'}(f)(v_H)\right) \\ &= P_{f_G}(f)\left(\left(P_{f'}(f)(v_H)\right)_G + \left(P_{f'}(f)(v_H)\right)_H\right) \\ &= P_{f_G}(f)\left(\left(P_{f'}(f)(v_H)\right)_G + \left(P_{f'}(f')(v_H)\right)_H\right) \\ &= P_{f_G}(f)\left(\left(P_{f'}(f)(v_H)\right)_G + 0\right) \\ &= P_{f_G}(f_G)\left(\left(P_{f'}(f)(v_H)\right)_G\right) \\ &= 0. \end{aligned}$$

La 3$^{\text{e}}$ égalité utilise le fait que G est stable par f, la 4$^{\text{e}}$ égalité utilise l'hypothèse de récurrence $P_{f'}(f') = 0$, et la 5$^{\text{e}}$ utilise le point (ii).