Applications linéaires et matrices

Cours de É. Bouchet – ECS1

7 mai 2021

Table des matières

Dans tout ce chapitre $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$.

1 Matrices et applications linéaires

1.1 Matrice d'une application linéaire

Définition (Matrice d'une application linéaire dans des bases)**.**

Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$, de base $B_E = (e_1, \dots, e_p)$ et F un espace vectoriel de dimension $n \in \mathbb{N}^*$, de base B_F. Soit f une application linéaire de E dans F. On appelle **matrice de l'application f dans les bases B_E et B_F**, notée $\mathrm{Mat}_{B_F,B_E}(f)$, la matrice de $M_{n,p}(\mathbb{K})$ dont la j-ième colonne est composée des coordonnées du vecteur $f(e_j)$ dans la base B_F.

Remarque. Attention ! La notation Mat_{B_E,B_F} peut être utilisée dans certains livres à la place de Mat_{B_F,B_E}. Le programme impose les notations de la définition.

Exemple 1. On considère l'application linéaire f définie de $\mathbb{R}^3$ dans $\mathbb{R}^4$ par : $\forall (x,y,z) \in \mathbb{R}^3$,

$$f\left((x,y,z)\right) = (2x+y, 4y, y+z, 6z).$$

On note $B_3 = (e_1, e_2, e_3)$ la base canonique de $\mathbb{R}^3$ et B_4 la base canonique de $\mathbb{R}^4$.

1. Déterminer la matrice de l'application f dans les bases B_3 et B_4.
2. $B_3' = (e_1, e_1+e_2, e_1-e_3)$ est une autre base de $\mathbb{R}^3$. Déterminer la matrice de l'application f dans les bases B_3' et B_4.

1. On remarque que $f(e_1) = (2,0,0,0)$, $f(e_2) = (1,4,1,0)$ et $f(e_3) = (0,0,1,6)$. Donc :

$$\mathrm{Mat}_{B_4,B_3}(f) = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 4 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 6 \end{pmatrix}.$$

2. On remarque que $f(e_1) = (2,0,0,0)$, $f(e_1+e_2) = (3,4,1,0)$ et $f(e_1-e_3) = (2,0,-1,-6)$. Donc :

$$\mathrm{Mat}_{B_4,B_3'}(f) = \begin{pmatrix} 2 & 3 & 2 \\ 0 & 4 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & -6 \end{pmatrix}.$$

Exemple 2. On considère l'endomorphisme g de $\mathbb{R}_3[X]$ qui à un polynôme $P(X)$ associe son polynôme dérivé $P'(X)$. On note B la base canonique de $\mathbb{R}_3[X]$. Déterminer $\mathrm{Mat}_{B,B}(g)$.
On remarque que $g(1) = 0$, $g(X) = 1$, $g(X^2) = 2X$ et $g(X^3) = 3X^2$. Donc :

$$\mathrm{Mat}_{B,B}(g) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Définition (Application linéaire canoniquement associée à une matrice).

Soit $(n,p) \in (\mathbb{N}^*)^2$ et $A \in M_{n,p}(\mathbb{K})$. On note B_p et B_n les bases canoniques respectives de $\mathbb{K}^p$ et $\mathbb{K}^n$. L'application linéaire f de $\mathbb{K}^p$ dans $\mathbb{K}^n$ qui vérifie $\mathrm{Mat}_{B_n,B_p}(f) = A$ est appelée **application linéaire canoniquement associée** à A et vérifie : $\forall (x_1,\dots,x_p) \in \mathbb{K}^p$,

$$f((x_1,\dots,x_p)) = (y_1,\dots,y_n) \quad \text{avec} \quad \forall i \in [\![1,n]\!], \quad y_i = \sum_{k=1}^{p} a_{ik}x_k.$$

Exemple 3. On considère la matrice $\begin{pmatrix} 2 & 5 & 2 \\ 0 & 3 & 1 \end{pmatrix}$. Donner son application linéaire canoniquement associée.

C'est l'application f de $\mathbb{R}^3$ dans $\mathbb{R}^2$ qui à $(x,y,z) \in \mathbb{R}^3$ associe $f((x,y,z)) = (2x+5y+2z, 3y+z)$. On peut le lire horizontalement sur la matrice, ou remarquer que la linéarité de f donne :

$$f((x,y,z)) = xf((1,0,0)) + yf((0,1,0)) + zf((0,0,1)) = x(2,0) + y(5,3) + z(2,1) = (2x+5y+2z, 3y+z).$$

Proposition (Matrices lignes et formes linéaires).

- Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$ et de base B_E et f une forme linéaire sur E. Alors $\mathrm{Mat}_{1,B_E}(f)$ est une matrice ligne (à p colonnes).
- Réciproquement, l'application linéaire canoniquement associée à une matrice ligne de $\mathcal{M}_{1,p}(\mathbb{K})$ est une forme linéaire sur $\mathbb{K}^p$.

Démonstration.

- Si f est une forme linéaire de E, f va d'un espace de dimension p dans un espace de dimension 1 et par définition de la matrice d'une application linéaire, sa matrice sera (quelles que soient les bases choisies, seul le cardinal de ces bases est important pour la taille de la matrice) dans $\mathcal{M}_{1,p}(\mathbb{K})$.
- Réciproquement, si A est une matrice ligne à p colonnes, son application linéaire canoniquement associée va de $\mathbb{K}^p$ dans $\mathbb{K}$, et est donc une forme linéaire.

□

1.2 Interprétations matricielles

Définition (Vecteur colonne des coordonnées dans une base B_E).

Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$, de base B_E, et $x \in E$. On appelle **vecteur colonne des coordonnées** de x dans la base B_E le vecteur colonne $X \in M_{p,1}(\mathbb{K})$ formé des coordonnées de x dans la base B_E.

Exemple 4. On considère le polynôme $P(X) = 1 + X^2 + 3X^3 \in \mathbb{R}_3[X]$. Le vecteur colonne de ses coordonnées dans la base $(1, X, X^2, X^3)$ est $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 3 \end{pmatrix}$.

Théorème (Interprétation matricielle de l'image d'un vecteur)**.**

Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$, de base B_E, et F un espace vectoriel de dimension $n \in \mathbb{N}^*$, de base B_F. Soit f une application linéaire de E dans F et $A = \operatorname{Mat}_{B_F,B_E}(f)$. Soit $x \in E$, $y \in F$ et X et Y les vecteurs colonnes de leurs coordonnées dans les bases B_E et B_F. On a :

$$y = f(x) \Longleftrightarrow Y = AX.$$

Démonstration. (démonstration à connaître) On pose $B_E = (e_1, \ldots, e_p)$ et $B_F = (f_1, \ldots, f_n)$. Comme $x \in E$ et $y \in F$, il existe des scalaires x_j et y_i tels que $x = \sum_{j=1}^{p} x_j e_j$ et $y = \sum_{i=1}^{n} y_i f_i$. On pose $A = (a_{ij})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p}$. Par linéarité de f, définition de A, puis interversion des sommes :

$$f(x) = \sum_{j=1}^{p} x_j f(e_j) = \sum_{j=1}^{p} x_j \left(\sum_{i=1}^{n} a_{ij} f_i \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{ij} x_j \right) f_i.$$

Ce qui nous donne, par identification des coefficients dans la base F puis par définition du produit matriciel :

$$y = f(x) \Longleftrightarrow \forall i \in [\![1, n]\!], y_i = \sum_{j=1}^{p} a_{ij} x_j \Longleftrightarrow Y = AX.$$

$\square$

Exemple 5. On réutilise l'application g de l'exemple 2 et le polynôme $P(X) = 1 + X^2 + 3X^3$ de l'exemple 4. Alors,

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 9 \\ 0 \end{pmatrix}.$$

On en déduit que $g(P(X)) = \ 0 + 2X + 9X^2 + 0X^3 = 2X + 9X^2$. On retrouve ainsi bien l'expression du polynôme dérivé .

1.3 Opérations sur les matrices d'applications linéaires

Proposition (Matrice d'une combinaison linéaire)**.**

Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$, de base B_E, et F un espace vectoriel de dimension $n \in \mathbb{N}^*$, de base B_F. Soit f et g deux applications linéaires de E dans F et $\lambda \in \mathbb{K}$. Alors :

$$\operatorname{Mat}_{B_F,B_E}(\lambda f + g) = \lambda \operatorname{Mat}_{B_F,B_E}(f) + \operatorname{Mat}_{B_F,B_E}(g).$$

Démonstration. (démonstration à connaître) On pose $B_E = (e_1, \ldots, e_p)$ et $B_F = (f_1, \ldots, f_n)$. On pose $(a_{ij})_{i \in [\![1,n]\!], j \in [\![1,p]\!]} = \operatorname{Mat}_{B_F,B_E}(f)$ et $(b_{ij})_{i \in [\![1,n]\!], j \in [\![1,p]\!]} = \operatorname{Mat}_{B_F,B_E}(g)$. $\operatorname{Mat}_{B_F,B_E}(\lambda f + g)$ est la matrice dont les vecteurs colonnes sont les coordonnées des vecteurs $(\lambda f + g)(e_j)$ dans la base B_F, on va donc commencer par calculer ces vecteurs. Soit $j \in [\![1, p]\!]$,

$$(\lambda f + g)(e_j) = \lambda f(e_j) + g(e_j) = \lambda \sum_{i=1}^{n} a_{ij} f_i + \sum_{i=1}^{n} b_{ij} f_i = \sum_{i=1}^{n} (\lambda a_{ij} + b_{ij}) f_i.$$

D'où $\operatorname{Mat}_{B_F,B_E}(\lambda f + g) = (\lambda a_{ij} + b_{ij})_{i \in [\![1,n]\!], j \in [\![1,p]\!]} = \lambda \operatorname{Mat}_{B_F,B_E}(f) + \operatorname{Mat}_{B_F,B_E}(g)$. $\square$

Théorème (Matrice d'une composée d'applications linéaires)**.**

Soit E, F et G trois espaces vectoriels de dimension finie, de bases respectives B_E, B_F et B_G. Soit f une application linéaire de E dans F et g une application linéaire de F dans G. Alors :

$$\mathrm{Mat}_{B_G,B_E}(g \circ f) = \mathrm{Mat}_{B_G,B_F}(g)\,\mathrm{Mat}_{B_F,B_E}(f)$$

Démonstration. On pose $B_E = (e_1, \dots, e_p)$, $B_F = (f_1, \dots, f_n)$ et $B_G = (g_1, \dots, g_m)$. On pose $(a_{ij})_{i\in[\![1,n]\!],j\in[\![1,p]\!]} = \mathrm{Mat}_{B_F,B_E}(f)$ et $(b_{ij})_{i\in[\![1,m]\!],j\in[\![1,n]\!]} = \mathrm{Mat}_{B_G,B_F}(g)$. $\mathrm{Mat}_{B_G,B_E}(g \circ f)$ est la matrice dont les vecteurs colonnes sont les coordonnées des vecteurs $g \circ f(e_j)$ dans la base B_G, on va donc commencer par calculer ces vecteurs. Soit $j \in [\![1,p]\!]$,

$$g \circ f(e_j) = g\left(f(e_j)\right) = g\left(\sum_{i=1}^{n} a_{ij} f_i\right) = \sum_{i=1}^{n} a_{ij} g(f_i) = \sum_{i=1}^{n} a_{ij}\left(\sum_{k=1}^{m} b_{ki} g_k\right) = \sum_{k=1}^{m}\left(\sum_{i=1}^{n} b_{ki} a_{ij}\right) g_k.$$

Or $\sum_{i=1}^{n} b_{ki} a_{ij}$ correspond au terme de la k-ième ligne et j-ième colonne de la matrice $\mathrm{Mat}_{B_G,B_F}(g)\,\mathrm{Mat}_{B_F,B_E}(f)$, par formule du produit matriciel. D'où le résultat. $\square$

1.4 Rang d'une matrice

Définition (Rang d'une matrice)**.**

Soit $(n,p) \in (\mathbb{N}^*)^2$ et A une matrice de $M_{n,p}(\mathbb{K})$. On appelle **rang** de A et on note $\mathrm{rg}(A)$ le rang de la famille des vecteurs colonnes de A dans $\mathcal{M}_{n,1}(\mathbb{K})$.

Exemple 6. Quel est le rang de la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 5 \\ 1 & 3 & 4 \end{pmatrix}$?

La troisième colonne de A est la somme des deux précédentes, donc $\mathrm{rg}(A) = \mathrm{rg}\left(\begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 3 \end{pmatrix}\right) = 2$ car ces deux vecteurs forment une famille libre de $\mathcal{M}_{3,1}(\mathbb{R})$.

Proposition (Matrice de rang nul)**.**

Soit $(n,p) \in (\mathbb{N}^*)^2$ et $A \in \mathcal{M}_{n,p}(\mathbb{K})$. On a :

$$\mathrm{rg}(A) = 0 \iff A = 0.$$

Démonstration. Les seules familles de $\mathcal{M}_{n,1}(\mathbb{K})$ de rang 0 sont celles qui ne contiennent que des vecteurs colonnes nuls, d'où le résultat. $\square$

Théorème (Lien entre rang d'une application linéaire et de sa matrice)**.**

Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$, F un espace vectoriel de dimension $n \in \mathbb{N}^*$ et f une application linéaire de E dans F. Soit A la matrice de l'application f dans les bases B_E et B_F. On a :

$$\operatorname{rg}(f) = \operatorname{rg}(A).$$

Démonstration. On pose $B_E = (e_1, \ldots, e_p)$. Les colonnes de A sont formées des coordonnées des vecteurs $f(e_i)$ dans la base B_F. Donc par définition du rang d'une matrice, le rang de A est égal au rang de la famille $(f(e_1), \ldots, f(e_p))$. Par ailleurs, comme B_E est une base de E, on sait que la famille $(f(e_1), \ldots, f(e_p))$ engendre $\operatorname{Im}(f)$. D'où $\operatorname{rg}(A) = \dim(\operatorname{Im}(f)) = \operatorname{rg}(f)$. □

Remarque. Le rang d'une application linéaire est donc le rang de n'importe laquelle de ses matrices associées : le choix des bases n'importe pas.

Proposition (Rang de la transposée)**.**

Soit $(n,p) \in (\mathbb{N}^*)^2$ et $A \in \mathcal{M}_{n,p}(\mathbb{K})$. On a :

$$\operatorname{rg}(A) = \operatorname{rg}({}^tA).$$

Démonstration. Résultat admis. □

2 Cas des endomorphismes et des matrices carrées

2.1 Matrice d'un endomorphisme

Définition (Matrice d'un endomorphisme dans une base)**.**

Soit E un espace vectoriel de dimension $p \in \mathbb{N}^*$, de base $B = (e_1, \ldots, e_p)$ et f un endomorphisme de E. On appelle **matrice de l'application f dans la base B**, notée $\operatorname{Mat}_B(f)$, la matrice carrée de $M_p(\mathbb{K})$ dont la j-ième colonne est composée des coordonnées du vecteur $f(e_j)$ dans la base B.

Remarque. Si E est un espace vectoriel de base $B = (e_1, \ldots, e_p)$, on remarque que pour tout $i \in [\![1,p]\!]$, $Id_E(e_i) = e_i$. Donc la matrice associée à l'endomorphisme identité est I_p et ne dépend pas de la base de E choisie.

Proposition (Formule du binôme de Newton pour deux endomorphismes, rappel)**.**

Soit E un espace vectoriel et f et g deux endomorphismes de E tels que $f \circ g = g \circ f$. Alors pour tout $n \in \mathbb{N}$,

$$(f+g)^n = \sum_{k=0}^{n} \binom{n}{k} f^k \circ g^{n-k}.$$

Proposition (Formule du binôme de Newton pour deux matrices, rappel)**.**

Soit $p \in \mathbb{N}^*$. Pour tous $(A, B) \in (\mathcal{M}_p(\mathbb{K}))^2$ tels que $AB = BA$ et pour tout $n \in \mathbb{N}$,

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k}.$$

2.2 Automorphismes

Définition (Automorphisme)**.**

Soit E un espace vectoriel sur $\mathbb{K}$. On appelle **automorphisme** de E tout endomorphisme bijectif de E. On note $GL(E)$ l'ensemble des automorphismes de E.

Remarque. Les automorphismes de E sont donc les applications qui sont à la fois un endomorphisme de E et un isomorphisme de E dans E.

Définition (Matrice inversible, rappel)**.**

Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{K})$. On dit que A est **inversible** quand il existe une matrice B de $\mathcal{M}_n(\mathbb{K})$ telle que $AB = BA = I_n$. Cette matrice est alors unique et notée A^{-1}. L'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$ est noté $GL_n(\mathbb{K})$.

Théorème (Automorphismes et inverse d'une matrice)**.**

Soit E un espace vectoriel de dimension finie et B_E une base de E. Soit f un endomorphisme de E. Alors f est un automorphisme si et seulement si $\mathrm{Mat}_{B_E}(f)$ est inversible et on a alors $\mathrm{Mat}_{B_E}(f^{-1}) = (\mathrm{Mat}_{B_E}(f))^{-1}$.

Démonstration. (démonstration à connaître) On note $n \in \mathbb{N}^*$ la dimension de E et $B_E = (e_1, \ldots, e_n)$ une base de E.

— Supposons que f est bijective. Alors elle admet une réciproque f^{-1} et $f \circ f^{-1} = Id_E$. En passant aux matrices associées, on trouve :

$$\mathrm{Mat}_{B_E}(f)\,\mathrm{Mat}_{B_E}(f^{-1}) = \mathrm{Mat}_{B_E}(f \circ f^{-1}) = \mathrm{Mat}_{B_E}(Id_E) = I_n.$$

Donc $\mathrm{Mat}_{B_E}(f)$ est inversible et $\mathrm{Mat}_{B_E}(f^{-1}) = (\mathrm{Mat}_{B_E}(f))^{-1}$.

— Réciproquement, supposons que $A = \mathrm{Mat}_{B_E}(f)$ est inversible. Soit g l'endomorphisme de E tel que les coordonnées de $g(e_i)$ dans la base B_E sont les vecteurs colonne de A^{-1}. On a alors, en notant E_i la matrice des coordonnées de e_i dans la base B_E, $\forall i \in [\![1, n]\!]$,

$$g \circ f(e_i) = e_i, \text{ car } \mathrm{Mat}_{B_E}(g \circ f)E_i = A^{-1}AE_i = I_nE_i = E_i.$$

d'où $g \circ f = Id_E$. Puisque f est un endomorphisme, elle est bijective et d'inverse g. Par construction de g, on a de plus $\mathrm{Mat}_{B_E}(f^{-1}) = \mathrm{Mat}_{B_E}(g) = (\mathrm{Mat}_{B_E}(f))^{-1}$.

□

Exemple 7. Soit f l'endomorphisme de $\mathbb{R}^2$ défini pour tout $(x, y) \in \mathbb{R}^2$ par $f((x, y)) = (x + 2y, 2x + 2y)$. Montrer qu'il s'agit d'un automorphisme de $\mathbb{R}^2$ et donner l'expression de sa réciproque.
La matrice de f dans la base canonique est $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$. Comme $2 - 4 = -2 \neq 0$, cette matrice est inversible, d'inverse $\frac{1}{-2}\begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & -\frac{1}{2} \end{pmatrix}$. Donc f est bijective et $\forall (x, y) \in \mathbb{R}^2$, $f^{-1}((x, y)) = (y - x, \frac{2x-y}{2})$.

Proposition (Matrice de rang n)**.**

Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{K})$. On a :

$$\mathrm{rg}(A) = n \iff A \text{ est inversible.}$$

Démonstration. On pose f l'application linéaire canoniquement associée à la matrice A. D'après la proposition précédente, A est inversible si et seulement si f est bijective. Or on a vu dans le chapitre sur les applications linéaire en dimension finie qu'un endomorphisme f de $\mathbb{K}^n$ est bijectif si et seulement si son rang est égal à n. Comme le rang d'une matrice est égal au rang de toute application linéaire qui lui est associée, on en déduit :

$$\mathrm{rg}(A) = n \iff \mathrm{rg}(f) = n \iff f \text{ est bijective } \iff A \text{ est inversible .}$$

□

2.3 Polynômes d'endomorphismes

Définition (Polynôme d'endomorphisme)**.**

Soit E un espace vectoriel de dimension $n \in \mathbb{N}^*$ et f un endomorphisme de E. Soit $r \in \mathbb{N}$ et $P(X) = \sum_{i=0}^{r} a_i X^i$ un polynôme de $\mathbb{K}[X]$. On appelle $P(f)$ l'endomorphisme de E défini par $P(f) = \sum_{i=0}^{r} a_i f^i$.

Exemple 8. Soit $P(X) = 2X^2 + 3X + 3$ et f un endomorphisme de E. Alors $P(f) = 2f \circ f + 3f + 3Id_E$.

Définition (Polynôme de matrice carrée)**.**

Soit $n \in \mathbb{N}^*$, $A \in \mathcal{M}_n(\mathbb{K})$, $r \in \mathbb{N}$ et $P(X) = \sum_{i=0}^{r} a_i X^i$ un polynôme de $\mathbb{K}[X]$. On appelle $P(A)$ la matrice de $\mathcal{M}_n(\mathbb{K})$ définie par $P(A) = \sum_{i=0}^{r} a_i A^i$.

Exemple 9. Soit $P(X) = 2X^2 + 3X + 3$ et A une matrice de $M_n(\mathbb{K})$. Alors $P(A) = 2A^2 + 3A + 3I_n$.

Proposition (Règles de calcul).

Soit P et Q deux polynômes de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Soit f un endomorphisme d'un espace vectoriel E de dimension finie $n \in \mathbb{N}^*$. Alors,

$$(\lambda P + Q)(f) = \lambda P(f) + Q(f) \quad \text{et} \quad (PQ)(f) = P(f) \circ Q(f).$$

De même, soit $A \in M_n(\mathbb{K})$, alors

$$(\lambda P + Q)(A) = \lambda P(A) + Q(A) \quad \text{et} \quad (PQ)(A) = P(A)Q(A).$$

Démonstration. On va montrer le résultat sur les polynômes d'endomorphisme, celui sur les polynômes de matrice s'en déduit ensuite directement. On pose $P(X) = \sum_{i=0}^{r} a_i X^i$ et $Q(X) = \sum_{i=0}^{r} b_i X^i$.

— $(\lambda P + Q)(X) = \sum_{i=0}^{r} (\lambda a_i + b_i) X^i$, d'où :

$$(\lambda P + Q)(f) = \sum_{i=0}^{r} (\lambda a_i + b_i) f^i = \lambda \sum_{i=0}^{r} a_i f^i + \sum_{i=0}^{r} b_i f^i = \lambda P(f) + Q(f).$$

— Soit $k \in \mathbb{N}$. $P(X) \times X^k = \sum_{i=0}^{r} a_i X^{i+k}$ et on a : $\sum_{i=0}^{r} a_i f^{i+k} = \sum_{i=0}^{r} a_i f^i \circ f^k = \left(\sum_{i=0}^{r} a_i f^i\right) \circ f^k = P(f) \circ f^k$.

Or $(PQ)(X) = \sum_{i=0}^{r} b_i (P(X) X^i)$ par linéarité de la somme. On obtient alors :

$$(PQ)(f) = \sum_{i=0}^{r} b_i P(f) \circ f^i = P(f) \circ \sum_{i=0}^{r} b_i f^i = P(f) \circ Q(f).$$

□

Définition (Polynôme annulateur).

Soit E un espace vectoriel de dimension $n \in \mathbb{N}^*$ et f un endomorphisme de E. Soit $P(X) \in \mathbb{K}[X]$. On dit que le polynôme P est **annulateur** de f lorsque $P(f) = 0$.

Remarque. On peut de même parler de polynôme annulateur d'une matrice A si $P(A) = 0$.

Exemple 10. Dans le cas d'un projecteur p, on a $p \circ p = p$, donc $p \circ p - p = 0$ et $X^2 - X$ est un polynôme annulateur de p.

Remarque. Il est possible de déterminer la réciproque d'un endomorphisme en utilisant un polynôme annulateur (qui doit alors avoir un terme constant non nul).

Exemple 11. Soit f un endomorphisme d'un espace vectoriel de dimension finie E et $P(X) = 2X^3 + X + 3$. On suppose que P est un polynôme annulateur de f. Montrer que f est bijective et déterminer une expression de f^{-1}.
Les hypothèses nous donnent $2f^3 + f + 3Id_E = 0$, c'est-à-dire $2f \circ f \circ f + f + 3Id_E = 0$. Donc $f \circ \left(2f^2 + Id_E\right) = -3Id_E$ et par linéarité de f, $f \circ \left(-\frac{2f^2 + Id_E}{3}\right) = Id_E$. Comme f est un endomorphisme, on en déduit que f est bijective et on trouve :

$$f^{-1} = -\frac{2f^2 + Id_E}{3}.$$

Exemple 12. Soit $A \in \mathcal{M}_3(\mathbb{R})$ et $P(X) = X^2 + 5X + 2$. On suppose que P est un polynôme annulateur de A. En déduire que A est inversible et donner une expression de A^{-1}.
Les hypothèses nous donnent $A^2 + 5A + 2I_3 = 0$. On en déduit que $A(A + 5I_3) = -2I_3$ et donc $A\left(-\frac{A+5I_3}{2}\right) = I_3$. Donc A est inversible et

$$A^{-1} = -\frac{A + 5I_3}{2}.$$

Remarque. Les polynômes annulateurs permettent aussi de calculer les puissances d'une matrice.

Exemple 13. Soit $A \in \mathcal{M}_3(\mathbb{R})$ et $P(X) = X^2 - 5X + 6$. On suppose que P est un polynôme annulateur de A. En déduire une expression de A^k, pour $k \in \mathbb{N}$.
Les hypothèses nous donnent :

$$A^2 - 5A + 6I_3 = 0.$$

On en déduit que $A^2 = 5A - 6I_3$. Donc, par multiplication par A, $A^3 = 5A^2 - 6A = 25A - 30I_3 - 6A = 19A - 30I_3$. On pourrait tenter de conjecturer ainsi l'expression cherchée, puis la montrer par récurrence. Mais ce serait long.
On va plutôt se servir de la division euclidienne des polynômes : soit $k \in \mathbb{N}^*$, divisons X^k par $P(X)$: il existe des uniques $Q(X)$ et $R(X) = aX + b \in \mathbb{R}_1[X]$ tels que :

$$X^k = P(X)Q(X) + aX + b.$$

En particulier, $A^k = aA + bI_3$ puisque $P(A) = 0$. Il suffit donc de déterminer a et b pour obtenir les puissances de A. Pour cela on recherche les racines de P : $\Delta = 25 - 24 = 1 > 0$, donc P admet deux racines réelles distinctes : 3 et 2. On en déduit le système :

$$3^k = 3a + b \text{ et } 2^k = 2a + b.$$

Donc $a = 3^k - 2^k$ et $b = 3 \times 2^k - 2 \times 3^k$. D'où $\forall k \in \mathbb{N}^*$,

$$A^k = (3^k - 2^k)A + (3 \times 2^k - 2 \times 3^k)I_3.$$

Ce qu'on peut maintenant simplifier en remplaçant A par sa valeur si on la connaît.