FST Mulhouse. Université de Haute Alsace

Licence 2 Mathématiques

Mathématiques : ALGEBRE LINEAIRE

Elisabeth REMM

Chapitre 13

Polynôme minimal d'un endomorphisme

Table des matières

1. L'anneau des polynômes $\mathbb{K}[X]$

Rappelons que $\mathbb{K}$ désigne soit le corps des complexes $\mathbb{C}$ soit celui des réels $\mathbb{R}$.

1.1. **L'espace vectoriel** $\mathbb{K}[X]$ **sur** $\mathbb{K}$**.** Soit $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ à une indéterminée X. Un élement de $\mathbb{K}[X]$ s'écrit

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_pX^p$$

avec pour tout $i = 1, \cdots, p$, $a_i \in \mathbb{K}$, L'entier p est le degré de $P(X)$. Nous avons vu, en première partie, que $\mathbb{K}[X]$ est muni d'une structure d'espace vectoriel de dimension infinie sur $\mathbb{K}$. Il possède une base dénombrable donnée par la famille

$$\mathcal{B} = \{1, X, X^2, \cdots, X^n, \cdots, \}.$$

Notons, mais nous ne le démontrons pas ici, que tout espace vectoriel de dimension finie ou non, possède une base. Dans un espace de dimension infinie, une base est une famille infinie pour laquelle tout vecteur de l'espace s'écrit de manière unique, comme une combinaison linéaire **finie** d'éléments de cette base. On voit bien que c'est le cas pour l'écriture d'un polynôme, c'est bien une combinaison finie de vecteurs de $\mathcal{B}$.

Nous avons également noté par $\mathbb{K}_p[X]$ le sous-espace vectoriel de $\mathbb{K}[X]$ constitué des polynômes de degré inférieur ou égal à p. Il est de dimension $p+1$ et admet pour base

$$\mathcal{B}_p = \{1, X, X^2, \cdots, X^p\}.$$

1.2. **L'anneau** $\mathbb{K}[X]$**.** On peut définir également dans $\mathbb{K}[X]$ une multiplication commutative : si

$$P(X) = a_0 + a1_X + a_2X^2 + \cdots + a_pX^p$$

et

$$Q(X) = b_0 + b_1X + b_2X^2 + \cdots + b_qX^q$$

sont deux polynômes de $\mathbb{K}[X]$ de degré respectif p et q, alors le polynôme $(PQ)(X) = P(X)Q(X)$ est le polynôme de degré $p+q$ défini par

$$PQ(X) = c_0 + c_1X + \cdots + c_{p+q}X^{p+q}$$

avec

$$\begin{cases} c_0 & = a_0b_0, \\ c_1 & = a_0b_1 + a_1b_0, \\ \cdots & \\ c_k & = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_ib_{k-i} + \cdots + a_{k-1}b_1 + a_kb_0, \\ \cdots & \\ c_{p+q} & = a_pb_q \end{cases}$$

Cette multiplication est

(1) commutative : $(PQ)(X) = P(X)Q(X) = Q(X)P(X)$ pour tout $P(X), Q(X) \in \mathbb{K}[X]$,

(2) distributive par rapport 'a l'addition :

$$P(X)(Q_1(X) + Q_2(X)) = P(X)Q_1(X) + P(X)Q_2(X), \quad P(X), Q_1(X), Q_2(X) \in \mathbb{K}[X],$$

(3) possède un élément unité, à savoir le polynôme

$$1(X) = 1.$$

Muni de l'addition et de cette multiplication, $\mathbb{K}[X]$ est un anneau commutatif. (Voir cours arithmétique et algèbre de première année).

Définition 1. *Un sous-ensemble I de $\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$ si*

(1) I est un sous-groupe de $\mathbb{K}[X]$ pour l'addition des polynômes,

(2)
$$\forall P(X) \in I,\ Q(X) \in \mathbb{K}[X], \quad \text{alors} \quad P(X)Q(X) \in I.$$

Par exemple, si un idéal I contient l'élément unité 1, alors, d'après la deuxième propriété, il contient $1.P(X)$ pour tout $P(X) \in \mathbb{K}[X]$ et donc, dans ce cas, $I = \mathbb{K}[X]$.

1.3. **La division euclidienne dans $\mathbb{K}[X]$.** Il existe enfin une dernière opération fondamentale : la division euclidienne :

Définition 2. *Etant donnés deux polynômes $P_1(X), P_2(X) \in \mathbb{K}[X]$ de degré respectif p_1 et p_2 avec $p_1 \geq p_2$, il existe un unique polynôme $Q(X)$ appelé quotient et un unique polynôme $R(X)$ appelé le reste tels que*

(1) degré $R(X) <$ degré $P_1(X)$,

(2) $P_1(X) = P_2(X)Q(X) + R(X)$.

Dans le cours de première année, des techniques pour calculer cette division ont été enseignées.

2. Le polynôme minimal d'un endomorphisme, $\mathbb{K} = \mathbb{C}$

2.1. **L'idéal $\mathcal{A}nn(f)$.** Soit f un endomorphisme de l'espace vectoriel E. On note par $\mathcal{A}nn(f)$ l'ensemble des polynômes annulateurs de f :
$$\mathcal{A}nn(f) = \{P(X) \in \mathbb{C}[X], \quad P(f) = 0\}.$$
Nous avons vu que cet ensemble n'est jamais réduit à 0, dès que $n > 1$.

Proposition 1. *Soit $f \in \mathcal{E}nd(E)$ un endomorphisme de E. Alors*

(1) $\mathcal{A}nn(f)$ est un sous-espace vectoriel de $\mathbb{C}[X]$,

(2) Si $P(X) \in \mathcal{A}nn(f)$ et $Q(X) \in \mathbb{C}[X]$, alors $PQ(X) = P(X)Q(X) \in \mathcal{A}nn(f)$, autrement dit $\mathcal{A}nn(f)$ est un idéal de $\mathbb{C}[X]$.

Démonstration. Nous avons vu que $\mathcal{A}nn(f)$ est un sous-ensemble non vide de $\mathbb{C}[X]$, ilcontient au moins le polynôme caractéristique de f. Si $P_1(X), P_2(X) \in \mathcal{A}nn(f)$, alors $P_1(f) = P_2(f) = 0$. Soient $\lambda_1, \lambda_2 \in \mathbb{C}$ et considérons le polynôme $\lambda_1 P_1(X) + \lambda_2 P_2(X)$. On a $\lambda_1 P_1(f) + \lambda_2 P_2(f) = 0$ et donc
$$\lambda_1 P_1(X) + \lambda_2 P_2(X) \in \mathcal{A}nn(f).$$
Ainsi $\mathcal{A}nn(f)$ est un sous-espace vectoriel de $\mathbb{C}[X]$. Montrons maintenant que $\mathcal{A}nn(f)$ est un idéal de $\mathbb{C}[X]$. Soient $P(X) \in \mathcal{A}nn(f)$ et $Q(X) \in \mathbb{C}[X]$. Alors $P(f) = 0$. On en déduit
$$(PQ)(f) = P(f)Q(f) = 0$$
et donc le polynôme $(PQ)(X)$ est aussi annulateur de f.

2.2. **Définition du polynôme minimal de f.** Considérons un polynôme $P(X) \in \mathcal{A}nn(f)$ de degré minimum :

$$\forall Q(X) \in \mathcal{A}nn(f),\ deg(P(X)) \leq deg(Q(X)).$$

Nous pouvons donc considérer la division euclidienne de $Q(X)$ par $P(X)$:

$$Q(X) = P(X)Q_1(X) + R(X)$$

avec $deg(R(X)) < deg(P(X))$. D'après la proposition précédente, le polyn^ome $P(X)Q1(X) \in \mathcal{A}nn(f)$ et donc

$$R(X) = Q(X) - P(X)Q1(X) \in \mathcal{A}nn(f).$$

Mais deg(R(X)) < deg(P(X)) et par hypothèse $P(X)$ est de degré minimum dans $\mathcal{A}nn(f)$. On a donc nécessairement $R(X) = 0$ et donc

$$Q(X) = P(X)Q_1(X).$$

En particulier, si $P_1(X)$ et $P_2(X)$ sont deux polynômes de $\mathcal{A}nn(f)$ de même degré et de degré minimum, alors chacun divise l'autre, c'est–à-dire

$$P_1(X) = aP_2(X)$$

avec $a \neq 0 \in \mathbb{C}$. On peut donc énoncer la définition suivante :

Définition 3. *Soit f un endomorphisme de E. On appelle polynôme minimal de f, le polynôme annulateur de degré minimum et unitaire (c'est-à-dire dont le coefficient de plus haut degré est égal à 1). On le note $\mathfrak{m}_f(X)$.*

2.3. **Polynôme minimal d'une matrice carrée complexe.** Si A est la matrice de f dans une base donnée de E, et si $P(X)$ est un polynôme annulateur de f, alors $P(A) = 0$. La réciproque est aussi vraie. On peut donc parler de polynôme minimal d'une matrice de $\mathcal{M}_n(\mathbb{C})$:

Définition 4. *Soit A une matrice carrée complexe. On appelle polynôme minimal de A, le polynôme annulateur de degré minimum et unitaire (c'est-à-dire dont le coefficient de plus haut degré est égal à 1). On le note $\mathfrak{m}_A(X)$.*

Exemples

(1) Soit $A = I_n$ la matrice identité. Alors

$$\mathfrak{m}_{I_n}(X) = X - 1.$$

En effet

$$\mathfrak{m}_{I_n}(Id) = I_n - I_n = 0.$$

Ce polynôme est annulateur et de degré minimum 1.

(2) Soit

$$D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

avec $\lambda_1 \neq \lambda_2$. Alors

$$\mathfrak{m}_D(X) = (X - \lambda_1)(X - \lambda_2) = X^2 - (\lambda_1 + \lambda_2)X + \lambda_1\lambda_2.$$

En effet, tout polynôme annulateur est au moins de degré 2. Calculons $\mathfrak{m}_D(D)$.

$$\mathfrak{m}_D(D) = (D - \lambda_1 I_2)(D - \lambda_2 I_2) = \begin{pmatrix} 0 & 0 \\ 0 & \lambda_2 - \lambda_1 \end{pmatrix} \begin{pmatrix} \lambda_1 - \lambda_2 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

Ainsi $\mathfrak{m}_D(X)$ est annulateur de D et de degré minimum dans $\mathcal{A}nn(D)$. C'est bien le polynôme minimal.

2.4. **Structure du polynôme minimal.** Le théorème suivant nous indique à quoi ressemble le polynôme minimal ce qui va être très utile pour le déterminer.

Théorème 1. *Soient $M \in \mathcal{M}_n(\mathbb{C})$ une matrice (non nulle) et $\mathfrak{m}_M(X)$ son polynôme minimal. Alors*

(1) Toutes les valeurs propres de M sont des racines de $\mathfrak{m}_M(X)$.

(2) Si α est une racine de $m_M(X)$, alors α est une valeur propre de M.

Démonstration. 1. Soit λ une valeur propre de M. Il existe un vecteur propre v non nul associé à λ :

$$M.V = \lambda V$$

. (Ici V est un vecteur colonne correspondant au vecteur v). On a alors, pour tout $k \geq 1$

$$M^k.V = \lambda^k V.$$

et donc λ^k est une valeur propre de M^k et V est toujours un vecteur propre mais pour λ^k. Supposons que

$$\mathfrak{m}_M(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0.$$

Alors

$$0 = \mathfrak{m}_M(M) = M^r + a_{r-1}M^{r-1} + \cdots + a_0 I_n.$$

On en déduit

$$0 = \mathfrak{m}_M(M) \cdot V = M^r V + a_{r-1}M^{r-1} \cdot V + \cdots + a_0 V = \lambda^r V + a_{r-1}\lambda^{r-1}V + \cdots + a_0 V.$$

Comme, par hypothèse $V \neq 0$, on en déduit

$$\lambda^r + a_{r-1}\lambda^{r-1} + \cdots + a_0$$

soit

$$\mathfrak{m}_M(\lambda) = 0$$

et λ est racine du polynôme minimal.

2. Soit α une racine de $\mathfrak{m}_M(X)$. Nous avons alors la factorisation

$$m_M(X) = (X - \alpha)Q(X).$$

En particulier

$$deg(Q(X)) < deg(\mathfrak{m}_M(X)).$$

Comme $\mathfrak{m}_M(X)$ est de degré minimal dans $\mathcal{A}nn(M)$, on en déduit que $Q(X) \notin \mathcal{A}nn(M)$ autrement dit

$$Q(M) \neq 0.$$

Il existe donc un vecteur colonne non nul V tel que

$$Q(M).V \neq 0.$$

Posons $V_1 = Q(M).V$. On a donc

$$\begin{aligned} 0 &= \mathfrak{m}_M(M).V_1 \\ &= (M - \alpha I_n).Q(M).V \\ &= (M - \alpha I_n).V_1. \end{aligned}$$

Ceci signifie, comme $V_1 \neq 0$, que α est une valeur propre de M. D'où le théorème.

Corollaire 1. *Soient $M \in \mathcal{M}_n(\mathbb{C})$ une matrice complexe et $\lambda_1, \cdots, \lambda_p$ l'ensemble des valeurs propres de M deux à deux distinctes ($\lambda_i \neq \lambda_j$ si $i \neq j$). Alors il existe des entiers non nuls $s_1, \cdots, s_p$ tels que*

$$\mathfrak{m}_M(X) = (X - \lambda_1)^{s_1}(X - \lambda_2)^{s_2} \cdots (X - \lambda_p)^{s_p}.$$

Notons, qu'à cette étape, nous n'avons pas de renseignements sur les puissances s_i sauf qu'elles sont non nulles et inférieure à la multiplicité r_i de la valeur propre correspondante :

$$1 \leq s_i \leq r_i.$$

En résumé

Corollaire 2. *Soient $M \in \mathcal{M}_n(\mathbb{C})$ une matrice complexe non nulle . Alors le polynôme minimal divise le polynôme caractéristique de M :*

$$C_M(X) = \mathfrak{m}_M(X) \cdot Q(X).$$

De plus, si on pose

$$C_M(X) = (-1)^n(X - \lambda_1)^{r_1}(X - \lambda_2)^{r_2} \cdots (X - \lambda_p)^{r_p}$$

alors

$$\mathfrak{m}_M(X)(X - \lambda_1)^{s_1}(X - \lambda_2)^{s_2} \cdots (X - \lambda_p)^{s_p}$$

avec

$$1 \leq s_i \leq r_i$$

pour tout $i = 1, \cdots, p$.

2.5. **Méthode de calcul du polynôme minimal.** Les résultats précédents nous fournissent une méthode, (certes parfois un peu longue), de calcul du polynôme minimal d'une matrice $M \in \mathcal{M}_n(\mathbb{C})$ donnée.

(1) Détermination du polynôme caractéristique $C_M(X)$.
(2) Calcul des valeurs propres c'est-à-dire des racines de $C_M(X)$. Notons, toutefois, que ce calcul est loin d'être anodin. Rappelons que les racines d'un polynôme de degré 2

$$P(X) = aX^2 + bX + c$$

sont données par les formules classiques

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \ \alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

que les racines d'un polynôme de degré 3 réduit 'a sa forme canonique

$$P(X) = X^3 + pX + q$$

sont données par les formules de Cardan :

$$j^k \sqrt[3]{\frac{1}{2}(-q+\sqrt{\frac{-\Delta}{27}})} + j^{-k} \sqrt[3]{\frac{1}{2}(-q-\sqrt{\frac{-\Delta}{27}})}$$

avec

$$j = exp(\frac{2i\pi}{3}), \Delta = -(4p^3 + 27q^2)$$

et $k = 1, 2, 3$. Par contre, au delà du degré 5, le célèbre résultat d'Evariste Galois précise qu'il n'existe aucune formule de ce type donnant directement les racines des équations de degré supérieur ou égal à 5 (il y en a peut-être d'une autre nature mais...). Ceci fait l'objet du cours de L3 intitulé "Théorie des corps", disponible également sur ce site. Donc, pour ce type d'équations, on se débrouille en pensant peut–être aux racines évidentes, s'il y en a!!!!

(3) On factorise le polynôme caractéristique :

$$C_M(X) = (-1)^n (X-\lambda_1)^{r_1} (X-\lambda_2)^{r_2} \cdots (X-\lambda_p)^{r_p}$$

(4) On cherche parmi tous les polynômes du type

$$(X-\lambda_1)^{s_1} (X-\lambda_2)^{s_2} \cdots (X-\lambda_p)^{s_p}$$

avec $1 \leq s_i \leq r_i$ celui de plus bas degré qui est annulateur de M. On commence par celui de plus bas degré :

$$(X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_p).$$

S'il est annulateur c'est le bon, sinon on augmente méthodiquement les puissances de chaque facteur.

Exemple. Considérons la matrice

$$M = \begin{pmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{pmatrix}$$

Son polynôme caractéristique est

$$C_M(X) = -(X+1)^2(X-3).$$

Les valeurs propres sont $\lambda_1 = 3$, racine simple et $\lambda_2 = -1$, racine double. On en déduit que le polynôme minimal est l'un des polynômes suivants, rangés par degré croissant :

(1) $P_1(X) = (X+1)(X-3)$

(2) $P_2(X) = (X+1)^2(X-3)$.

En effet ce sont les seuls polynômes ayant -1 et 3 comme racines et n'ayant que ces racines de multiplicité inférieure ou égale à celles du polynôme caractéristique. Pour déterminer lequel des $P_i(X)$ est minimal, on commence par prendre celui de plus bas degré, ici $P_1(X)$. On vérifie s'il est annulateur. S'il est annulateur, il est minimal. Sinon, on prend le suivant dans la liste. Comme ils sont rangés par degré croissant, le premier polynôme annulateur rencontré sera le bon. On a

$$P_1(M) = (M+I_3)(M-3I_3).$$

Soit
$$P_1(M) = \begin{pmatrix} 2 & -3 & 4 \\ 4 & -6 & 8 \\ 6 & -7 & 8 \end{pmatrix} \begin{pmatrix} -2 & -3 & 4 \\ 4 & -10 & 8 \\ 6 & -7 & 4 \end{pmatrix} = \begin{pmatrix} 8 & -4 & 0 \\ 16 & -8 & 0 \\ 8 & -4 & 0 \end{pmatrix}.$$
Ainsi $P_1(X)$ n'est pas annulateur. On en déduit que $P_2(X)$ est annulateur. En fait $P_2(X)$ est, au signe près, le polynôme caractéristique, il est annulateur d'après le théorème de Cayley-Hamilton. Mais les ultra-sceptiques peuvent vérifier :
$$P_2(M) = (M + I_3)^2(M - 3_I 3)$$
soit
$$P_2(M) = \begin{pmatrix} 2 & -3 & 4 \\ 4 & -6 & 8 \\ 6 & -7 & 8 \end{pmatrix} \begin{pmatrix} 2 & -3 & 4 \\ 4 & -6 & 8 \\ 6 & -7 & 8 \end{pmatrix} \begin{pmatrix} -2 & -3 & 4 \\ 4 & -10 & 8 \\ 6 & -7 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

2.6. **Polynôme minimal et diagonalisation.** Dans ce paragraphe, nous allons énoncer un résultat, sans démonstration, mais qui est très utile pour voir si une matrice donnée est ou n'est pas diagonalisable.

Théorème 2. *Une matrice $M \in \mathcal{M}_n(\mathbb{C})$ est diagonalisable si et seulement si les racines du polynôme minimal sont simples.*

Par exemple, dans l'exemple traité ci-dessus, nous avons trouvé comme polynôme minimal
$$\mathfrak{m}_M(X) = (X + 1)^2(X - 3).$$
Ainsi $\mathfrak{m}_M(X)$ possède une racine double et M n'est pas diagonalisable.

3. La décomposition $M = D + N$

3.1. **Matrices et endomorphismes nilpotentes.**

Définition 5. *Une matrice $M \in \mathcal{M}_n(\mathbb{K})$ est dite nilpotente s'il existe un entier $k \geq 0$ tel que*
$$M^k = 0.$$
Le plus petit entier n_M tel que $M^{n_M} = 0$ est appelé l'indice de nilpotence de M.

Soit λ une valeur propre de la matrice nilpotente M. On sait alors que λ^p est une valeur propre de M^p. Or il existe $k \geq 0$ tel que $M^k = 0$. Comme λ^k est une valeur propre de M^k alors $\lambda^k = 0$ et donc $\lambda = 0$.

Proposition 2. *Soit $M \in \mathcal{M}_n(\mathbb{K})$ une matrice nilpotente. Alors les valeurs propres de M sont toutes nulles. En particulier une matrice nilpotente est diagonalisable si et seulement si elle est nulle. Si n_M est son indice de nilpotence, alors le polynôme $m_M(X) = X^{n_M}$ est un polynôme annulateur de M .*

Il est également clair que si M est nilpotente, toute matrice sembleble $M' = P^{-1}MP$ est aussi nilpotente et de même indice de nilpotence.

Définition 6. *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Un endomorphisme f de E est dit nilpotent s'il existe un entier k tel que*
$$f \circ f \circ \cdots \circ f = f^k = 0.$$

Si M est la matrice de f relative à une base de E donnée, alors M est une matrice nilpotente.

3.2. **La décomposition** $M = D + N$**,** $\mathbb{K} = \mathbb{C}$**.** Nous proposons ici, non pas une réduction d'une matrice carrée complexe, mais une écriture de cette matrice sous la forme d'une somme d'une matrice diagonalisable et d'une matrice nilpotente.

Théorème 3. *Soit $M \in \mathcal{M}_n(\mathbb{C})$ une matrice complexe. Il existe un unique couple de matrices (D, N) de $\mathcal{M}_n(\mathbb{C})$ tel que*

(1) D est une matrice diagonalisable,
(2) N est une matrice nilpotente
(3) $M = D + N$
(4) $DN = ND$

Au lieu de démontrer ce résultat, on propose une méthode pratique de détermination directe des matrices D et N.

3.3. **Méthode de calcul des matrices** D **et** N**.** .

(1) On détermine le polynôme minimal $\mathfrak{m}_M(X)$ de la matrice M et on le factorise :
$$\mathfrak{m}_M(X) = (X - \lambda_1)^{s_1}(X - \lambda_2)^{s_2} \cdots (X - \lambda_p)^{s_p}.$$
(2) On décompose en éléments simples la fraction rationnelle $\dfrac{1}{\mathfrak{m}_M(X)}$.
$$\frac{1}{\mathfrak{m}_M(X)} = \frac{R_1(X)}{(X - \lambda_1)^{s_1}} + \frac{R_2(X)}{(X - \lambda_2)^{s_2}} + \cdots + \frac{R_p(X)}{(X - \lambda_p)^{s_p}} \quad (\star)$$
où $R_i(X)$ est un polynôme de degré inférieur ou égal à $s_i - 1$, pour $i = 1, \cdots, p$.

(3) Posons
$$Q_i(X) = (X - \lambda_1)^{s_1} \cdots (X - \lambda_{i-1})^{s_{i-1}}(X - \lambda_{i+1})^{s_{i+1}} \cdots (X - \lambda_p)^{s_p}.$$
(On a enlevé le $i^{\text{ème}}$-facteur) Alors
$$\mathfrak{m}_M(X) = Q_i(X)(X - \lambda_i)^{s_i}$$
pour tout $i = 1, \cdots, p$.

(4) Multiplions les deux membres de l'équation $\star$ par $\mathfrak{m}_M(X)$:
$$1 = \frac{R_1(X)\mathfrak{m}_M(X)}{(X - \lambda_1)^{s_1}} + \frac{R_2(X)\mathfrak{m}_M(X)}{(X - \lambda_2)^{s_2}} + \cdots + \frac{R_p(X)\mathfrak{m}_M(X)}{(X - \lambda_p)^{s_p}}$$
et simplifions
$$1 = R_1(X)Q_1(X) + R_2(X)Q_2(X) + \cdots + Rp(X)Q_p(X).$$

(5) Posons
$$N_i(X) = R_i(X)Q_i(X)$$
pour $i = 1, \cdots, p$ et considérons les matrices
$$\Pi_i = N_i(M).$$

(6) On a alors
$$\begin{cases} D &= \lambda_1\Pi_1(M) + \lambda_2\Pi_2(M) + \cdots + \lambda_p\Pi_p(M). \\ N &= M - D. \end{cases}$$

Exemple. Soit la matrice
$$M = \begin{pmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{pmatrix}$$
Nous avons déterminé précédemment son polynôme minimal :
$$\mathfrak{m}_M(X) = (X+1)^2(X-3).$$
Alors
$$\frac{1}{\mathfrak{m}_M(X)} = \frac{1}{(X+1)^2(X-3)} = \frac{R_1(X)}{(X+1)^2} + \frac{R_2(X)}{(X-3)}$$
les polynômes $R_1(X)$ étant de degré inférieur ou égal à 1 et $R_2(X)$ de degré 0, c'est donc une constante. On détermine directement $R_2(X)$ en multipliant toute l'identité par $X-3$ puis en faisant $X = 3$. On en déduit
$$R_2(X) = \frac{1}{16}.$$
Posons $R_1(X) = aX + b$. On détermine les constantes a et b (comme on veut) : par exemple, on multiplie l'identité par X et on fait tendre X vers l'infini, ceci donne
$$0 = a + \frac{1}{16}$$
soit
$$a = -\frac{1}{16}$$
et si $X = 0$:
$$\frac{-1}{3} = b - \frac{1}{48}$$
soit
$$b = -\frac{15}{48}.$$
On obtient donc
$$\frac{1}{\mathfrak{m}_M(X)} = \frac{1}{(X+1)^2(X-3)} = \frac{-\frac{1}{16}X - \frac{15}{48}}{(X+1)^2} + \frac{\frac{1}{16}}{(X-3)}$$
Multiplions les deux membres par $(X+1)^2(X-3)$. Il vient
$$1 = (-\frac{1}{16}X - \frac{15}{48})(X-3) + \frac{1}{16}(X+1)^2$$

Ainsi

$$\begin{cases} N_1(X) & = (-\dfrac{1}{16}X - \dfrac{15}{48})(X-3) = -\dfrac{1}{16}X^2 - \dfrac{1}{8}X + \dfrac{15}{16} \\ N_2(X) & = \dfrac{1}{16}(X+1)^2 = \dfrac{1}{16}X^2 + \dfrac{1}{8}X + \dfrac{1}{16}. \end{cases}$$

$$\begin{cases} \Pi_1 = N_1(M) = -\frac{1}{16}M^2 - \frac{1}{8}M + \frac{15}{16}I_3 \\ \Pi_2 = N_2(M) = \frac{1}{16} *^2 + \frac{1}{8}M + \frac{1}{16}I_3 \end{cases}$$

et

$$D = \lambda_1\Pi_1 + \lambda_2\Pi_2 = -\Pi_1 + 3\Pi_2.$$

On obtient

$$\Pi_1 = \begin{pmatrix} 0 & 1 & -1 \\ -2 & 3 & -2 \\ -2 & 2 & -1 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -2 & 2 \\ 2 & -2 & 2 \end{pmatrix}$$

et donc

$$D = \begin{pmatrix} 3 & -4 & 4 \\ 8 & -9 & 8 \\ 8 & -8 & 7 \end{pmatrix}, \quad N = \begin{pmatrix} -2 & 1 & 0 \\ -4 & 2 & 0 \\ -2 & 1 & 0 \end{pmatrix}.$$

3.4. **Application : calcul de l'exponentielle.** Soit $M \in \mathcal{M}_n(\mathbb{C})$ et $M = D+N$ sa décomposition. Comme D est diagonalisable, nous savons calculer son exponentielle : Soit $D_0 = P^{-1}DP$ une matrice diagonale semblable à D. Alors

$$\exp D = P\Delta \exp D_0 P^{-1}.$$

Comme N est nilpotente, il existe k tel que $N^k = 0$. Alors

$$\exp N = I + N + \frac{1}{2!}N^2 + \cdots + \frac{1}{(k-1)!}N^{k-1}$$

et cette somme est finie.

Comme les matrices D et N commutent, on en déduit

$$\exp M = \exp D\Delta \exp N.$$