Réduction des Endomorphismes

Chapitre 1

Polynômes annulateurs

Dans tout ce chapitre E est un espace vectoriel sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et f est un endomorphisme de E.

1.1 Polynômes d'endomorphismes, polynômes de matrices carrées

Définition 1.1.1. *Soit* $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{K}[X]$

1. *Pour* $f \in \mathcal{L}(E)$, *on note* $P(f) = a_0 Id_e + a_1 f + a_2 f^2 + \cdots + a_n f^n$, *et* $P(f)$ *est appelé polynôme d'endomorphisme.*
2. *Pour* $A \in \mathcal{M}_n(\mathbb{K})$, *on note* $P(A) = a_0 I_n + a_1 A + a_2 A^2 + \cdots + a_n A^n$, *et* $P(A)$ *est appelé polynôme de matrice.*

Proposition 1.1.1.

1. *Si* $f, g \in \mathcal{L}(E)$ *commutent, alors tout polynôme de* f *commute avec tout polynôme de* g.
2. *Si* $A, B \in \mathcal{M}_n(\mathbb{K})$ *commutent, alors tout polynôme de* A *commute avec tout polynôme de* B.

Démonstration.

1. Soient $f, g \in \mathcal{L}(E)$ tels que $f \circ g = g \circ f$
   • Montrons, par récurrence que : $\forall k \in \mathbb{N}, g^k \circ f = f \circ g^k$.
   La propriété est triviale pour $k = 0$ (car $g^0 = Id_E$), et vraie pour $k = 1$ par hypothèse. Si elle est vraie pour un entier k, alors :
   $$g^{k+1} \circ f = g \circ (g^k \circ f) = g \circ (f \circ g^k) = (g \circ f) \circ g^k = (f \circ g) \circ g^k = f \circ g^{k+1}.$$
   • Il en résulte, par linéarité que : $\forall P \in \mathbb{K}[X], P(g) \circ f = f \circ P(g)$.
   • Le résultat précédent, appliqué à $(P(g), f)$ au lieu de (f, g), montre alors :
   $$\forall P, Q \in \mathbb{K}[X], P(g) \circ Q(f) = Q(f) \circ P(g).$$
2. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ tels que $AB = BA$
   • Montrons, par récurrence : $\forall k \in \mathbb{N}, B^k A = AB^k$.
   La propriété est triviale pour $k = 0$ (car $B^0 = I_n$), et vraie pour $k = 1$ par hypothèse. Si elle est vraie pour un entier k, alors :
   $$B^{k+1} A = B(B^k A) = B(AB^k) = (BA)B^k = (AB)B^k = AB^{k+1}.$$

- Il en résulte, par linéarité que : $\forall P \in \mathbb{K}[X], P(B)A = AP(B)$.
- Le résultat précédent, appliqué à $(P(B), A)$ au lieu de (A, B), montre alors :

$$\forall P, Q \in \mathbb{K}[X], P(B)Q(A) = Q(A)P(B).$$

□

Proposition 1.1.2.
Soient $f \in \mathcal{L}(E), P \in \mathbb{K}[X], A \in \mathcal{M}_n(\mathbb{K})$

1. *Si λ est une valeur propre de f pour le vecteur v, alors $P(\lambda)$ est une valeur propre de $P(f)$ pour le vecteur v, c'est à dire*
$$\forall P \in \mathbb{K}[X] : P(f)(v) = P(\lambda)v.$$
2. *Si λ est une valeur propre de A pour le vecteur v, alors $P(\lambda)$ est une valeur propre de $P(A)$ pour le vecteur v, c'est à dire*
$$\forall P \in \mathbb{K}[X] : P(A)(v) = P(\lambda)v.$$

Démonstration.

1. D'après l'exercice (**??**), on a $\forall k \in \mathbb{N} : f^k(v) = \lambda^k v$.
On a alors, pour tout $P = \sum_{k=0}^{n} a_k X^k$ de $\mathbb{K}[X]$
$$P(f)(v) = \left(\sum_{k=0}^{n} a_0 f^k\right)(v) = \sum_{k=0}^{n} a_0 f^k(v) = \sum_{k=0}^{n} a_0 \lambda^k v = P(\lambda)v.$$
2. Analogue.

□

1.2 Polynômes annulateurs

Définition 1.2.1.

1. *Soient $f \in \mathcal{L}(E), P \in \mathbb{K}[X]$. On dit que P annule f (ou P est un polynôme annulateur de f) si et seulement si : $P(f) = 0$.*
2. *Soient $A \in \mathcal{M}_n(\mathbb{K}), P \in \mathbb{K}[X]$. On dit que P annule A (ou P est un polynôme annulateur de A) si et seulement si : $P(A) = 0$.*

Proposition 1.2.1.

1. *Soient $f \in \mathcal{L}(E)$, P un polynôme annulateur de f. On a alors*
$$Sp(f) \subset P^{-1}(\{0\}).$$
2. *Soient $A \in \mathcal{M}_n(\mathbb{K})$, P un polynôme annulateur de A. On a alors*
$$Sp(A) \subset P^{-1}(\{0\}).$$

Démonstration.

1. Soit $\lambda \in Sp(f)$, c'est à dire
$$\exists v \in E, v \neq 0 : f(v) = \lambda v.$$
Donc,
$$\exists v \in E, v \neq 0 : P(f)(v) = P(\lambda)v = 0.v = 0$$
donc $P(\lambda) = 0$, puisque $v \neq 0$.
2. Même méthode.

□

Notons que la connaissance d'un polynôme annulateur donne immédiatement des renseignements sur le spectre de f. On a

Proposition 1.2.2. *Soit $Q(X)$ un polynôme annulateur de f. Alors les valeurs propres de f figurent parmi les racines de Q, c'est-à-dire :*
$$Sp(f) \subset RacQ.$$
où $RacQ$ est l'ensemble des racines de Q.

Démonstration. Soit λ une valeur propre de f, il existe un vecteur v non nul tel que $f(v) = \lambda v$. On a
$$\begin{array}{rcl} f^2(v) & = & \lambda^2 v \\ f^3(v) & = & \lambda^3 v \\ \vdots & \vdots & \vdots \\ f^k(v) & = & \lambda^k v. \end{array}$$
Soit $Q(X) = a_m X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$ un polynôme tel que $Q(f) = 0$, c'est-à-dire vérifiant :
$$a_m f^m + a_{m-1} f^{m-1} + \ldots + a_1 f + a_0 Id_E = 0.$$
En appliquant cette relation au vecteur v on trouve :
$$(a_m f^m + a_{m-1} f^{m-1} + \ldots + a_1 f + a_0 Id_E)v = 0$$
c'est-à-dire
$$(a_m \lambda^m + a_{m-1} \lambda^{m-1} + \ldots + a_1 \lambda + a_0)v = 0.$$
Or $v \neq 0$, donc $a_m \lambda^m + a_{m-1}\lambda^{m-1} + \ldots + a_1\lambda + a_0 = 0$, c'est-à-dire $Q(\lambda) = 0$.

□

Proposition 1.2.3. *Soit f un endomorphisme et*
$$P_f(X) = (-1)^n (X - \lambda_1)^{\alpha_1} \cdots (X - \lambda_p)^{\alpha_p}$$
son polynôme caractéristique. Alors si f est diagonalisable, le radicale de $P_f(X)$, c'est-à-dire le polynôme $Q(X) = (X - \lambda_1) \cdots (X - \lambda_p)$, annule f.

Démonstration. Puisque f est diagonalisable, il existe une base $B = \{v_1, \ldots, v_n\}$ formée de vecteurs propres. Si $\lambda_1, \ldots, \lambda_p$ sont les valeurs propres, pour tout $v \in B$ il existe au moins une valeur propre λ_j

telle que $(f - \lambda_j Id_E)v = 0$, donc pour tout $v \in B$, on a

$$(f - \lambda_1 Id_E) \circ \cdots \circ (f - \lambda_p Id_E)v = 0,$$

car les endomorphismes $(f - \lambda_k Id_E)$ commutent. Puisque l'endomorphisme $(f - \lambda_1 Id_E) \circ \cdots \circ (f - \lambda_p Id_E)$ s'annule sur une base, il s'annule sur tout vecteur. Donc le polynôme $Q(X) = (X - \lambda_1) \cdots (X - \lambda_p)$ est un annulateur de f.

□

1.2.1 Le Lemme des noyaux

Lemme 1.2.1. *Soit f un endomorphisme sur E et*

$$Q(X) = Q_1(X)Q_2(X) \cdots Q_p(X)$$

un polynôme factorisé en produit de polynômes deux à deux premiers entre eux. Si $Q(f) = 0$, alors

$$E = KerQ_1(f) \oplus KerQ_2(f) \oplus \cdots \oplus KerQ_p(f).$$

Démonstration. Par récurrence sur p.
Pour $p = 1$ le lemme est évident. En effet $Q(X) = Q_1(X)$ et, par hypothèse, $Q_1(X) = 0$, ce qui veut dire que $\forall x \in E :\ Q_1(X) = 0$, c'est-à-dire $E \subset KerQ_1(f)$, donc $E = KerQ_1(f)$.
Cas où $p = 2$. Soit $Q = Q_1Q_2$. Puisque Q_1 et Q_2 sont premiers entre eux, d'après le théorème de Bézout il existe deux polynômes U_1 et U_2 tels que

$$U_1Q_1 + U_2Q_2 = 1$$

d'où :

$$U_1(f) \circ Q_1(f) + U_2(f) \circ Q_2(f) = Id_E.$$

Ainsi

$$\forall x \in E \quad x = U_1(f) \circ Q_1(f)(x) + U_2(f) \circ Q_2(f)(x) \tag{1.1}$$

c'est-à-dire

$$E \subset ImU_1(f) \circ Q_1(f) + ImU_2(f) \circ Q_2(f)$$

et donc

$$E = ImU_1(f) \circ Q_1(f) + ImU_2(f) \circ Q_2(f).$$

Or

$$Q_2(f) \circ U_1(f) \circ Q_1(f) = 0 \quad (car\ Q_2(f) \circ Q_1(f) = 0)$$

donc

$$ImU_1(f) \circ Q_1(f) \subset KerQ_2(f).$$

De même

$$ImU_2(f) \circ Q_2(f) \subset KerQ_1(f)$$

et par conséquence
$$E = KerQ_1(f) + KerQ_2(f).$$
D'autre part, si $x \in KerQ_1(f) \cap KerQ_2(f)$, d'après (1.1) on a $x = 0$ et donc
$$E = KerQ_1(f) \oplus KerQ_2(f).$$

Supposons maintenant le lemme vrai jusqu'à l'ordre $p-1$ et écrivons
$$Q = \underbrace{Q_1Q_2\cdots Q_{p-1}}_{Q_*}Q_p.$$
D'après le cas $p = 2$
$$E = KerQ_*(f) \oplus KerQ_p(f)$$
il reste à monter que
$$KerQ_*(f) = KerQ_1(f) \oplus \cdots \oplus KerQ_{p-1}(f).$$
Soit $F = KerQ_*(f)$. D'après l'hypothèse de récurrence
$$F = \widetilde{Ker}Q_1(f) \oplus \cdots \oplus \widetilde{Ker}Q_{p-1}(f)$$
où $\widetilde{Ker}Q_i(f) = \{x \in E; Q_i(f)(x) = 0\} \subset KerQ_i(f)$.
Or en fait $\widetilde{Ker}Q_i(f) = KerQ_i(f)$. En effet si $x \in KerQ_i(f)$ on a $Q_*(f) = 0$, donc $x \in F$ et donc $x \in \widetilde{Ker}Q_i(f)$. Ainsi donc
$$F = KerQ_1(f) \oplus \cdots \oplus KerQ_{p-1}(f).$$

$\square$

Exemple 1.2.1. *Considérons l'endomorphisme f tel que $f^2 = f$. Le polynôme $Q(X) = X(X-1)$ annule f. Comme X et $X-1$ sont premiers entre eux, on a :*
$$E = Kerf \oplus Ker(f - Id_E).$$
Donc E est somme direct d'espaces propres et, par conséquent, f est diagonalisable.

1.3 Théorème de Cayley-Hamilton

Théorème 1.3.1. *Soient $f \in \mathcal{L}(E)$, $A \in \mathcal{M}_n(\mathbb{K})$.*

1) *Le polynôme caractéristique P_f de f est toujours un polynôme annulateur de f :*
$$P_f(f) = 0.$$

2) *Le polynôme caractéristique P_A de A est toujours un polynôme annulateur de A :*
$$P_A(A) = 0.$$

Démonstration.
Il est clair que 2) est la traduction matricielle de 1).

Supposons d'abord $\mathbb{K} = \mathbb{C}$. Dans ce cas f est trigonalisable. Soit $B = \{e_1, e_2, \ldots, e_n\}$ une base de E telle que :

$$\mathcal{M}at(f)_B^B = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

On a :

$$P_f(X) = (\lambda_1 - X)(\lambda_2 - X) \cdots (\lambda_n - X).$$

Il s'agit de montrer que

$$(\lambda_1 id_E - f) \circ (\lambda_2 id_E - f) \circ \cdots \circ (\lambda_n id_E - f) = 0.$$

Considérons l'application

$$g_i = (\lambda_1 id_E - f) \circ (\lambda_2 id_E - f) \circ \cdots \circ (\lambda_i id_E - f).$$

Nous allons montrer par récurrence que g_i s'annule sur les vecteurs $e_1, e_2, \ldots, e_i$; pour $i = n$ on aura le théorème.
Pour $i = 1$, on a :

$$g_1(e_1) = (\lambda_1 id_E - f)(e_1) = \lambda_1 e_1 - f(e_1) = 0$$

(car $f(e_1)$ est la première colonne de $\mathcal{M}at(f)_B^B$). Supposons que $g_{i-1}(e_1) = 0, \ldots, g_{i-1}(e_{i-1}) = 0$ et montrons que :

$$g_i(e_1) = 0, \ldots, g_i(e_i) = 0.$$

On a : $g_i = g_{i-1} \circ (\lambda_i id_E - f) = (\lambda_i id_E - f) \circ g_{i-1}$, donc :

$$g_i(e_1) = 0, \ldots, g_i(e_{i-1}) = 0.$$

Il reste à montrer que $g_i(e_i) = 0$. On a : $g_i(e_i) = g_{i-1}(\lambda_i(e_i) - f(e_i))$. Or

$$\mathcal{M}at(f)_B^B = \underset{\substack{\uparrow \\ f(e_i)}}{\begin{pmatrix} \lambda_1 & & & a_1 & & & \\ 0 & \ddots & & & & & \\ & & \ddots & a_{i-1} & & * & \\ \vdots & & & \lambda_i & & & \\ & & & 0 & \ddots & & \\ \vdots & & & \vdots & & \ddots & \\ 0 & & & 0 & & & \lambda_n \end{pmatrix}}$$

donc

$$f(e_i) = a_1 e_1 + a_2 e_2 + \cdots + a_{i-1} e_{i-1} + \lambda_i e_i$$

d'où

$$\begin{aligned} g_i(e_i) &= g_{i-1}\left(\lambda_i e_i - (a_1e_1 + a_2e_2 + \cdots + a_{i-1}e_{i-1} + \lambda_i e_i)\right) \\ &= -g_{i-1}(a_1e_1 + a_2e_2 + \cdots + a_{i-1}e_{i-1} + \lambda_i e_i) = 0 \end{aligned}$$

car g_{i-1} s'annule sur $e_1, e_2, \ldots, e_{i-1}$. Ceci montre que si $A \in \mathcal{M}_n(\mathbb{C})$, $P_A(A) = 0$.
Si $A \in \mathcal{M}_n(\mathbb{R})$, on considère A comme une matrice complexe particulière et donc on a : $P_A(A) = 0$.
Le théorème et donc démontré pour $\mathbb{K} = \mathbb{R}$ et $\mathbb{K} = \mathbb{C}$.
Si $\mathbb{K}$ est un corps quelconque, on considère la clôture algébrique $\mathbb{K}'$ de $\mathbb{K}$ (cf. (**??**)). Le théorème se démontre de la même manière en faisant jouer à $\mathbb{K}'$ le rôle de $\mathbb{C}$ et $\mathbb{K}$ le rôle de $\mathbb{R}$. □

Exemple 1.3.1. *Soit f l'endomorphisme de $\mathbb{R}^3$ de matrice $A = \begin{pmatrix} 0 & 2 & -1 \\ 3 & -2 & 0 \\ -2 & 2 & 1 \end{pmatrix}$ sur une base quelconque, et donc on a le polynôme caractéristique de A est :*

$$P(\lambda) = (1-\lambda)(\lambda+4)(\lambda-2) = -\lambda^3 - \lambda^2 + 10\lambda - 8.$$

Alors on a $P(f) = -f^3 - f^2 + 10f - 8 = 0$, et on a aussi $P(A) = -A^3 - A^2 + 10A - 8 = 0$.

1.3.1 Application au calcul de l'inverse

Le théorème de Cayley-Hamilton permet de donner une expression intéressante de l'inverse d'une matrice inversible. Par exemple soit la matrice $A = \begin{pmatrix} 0 & 2 & -1 \\ 3 & -2 & 0 \\ -2 & 2 & 1 \end{pmatrix}$, on a $P(A) = -A^3 - A^2 + 10A - 8 = 0$. On peut écrire cette relation sous la forme :

$$A \times \frac{1}{8}\left(-A^2 - A + 10I_3\right) = I_3$$

ce qui donne $A^{-1} = \frac{1}{8}\left(-A^2 - A + 10I_3\right)$.
Plus généralement, si le polynôme caractéristique de la matrice A est :

$$P(\lambda) = (-1)^n(\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0)$$

expression dans laquelle on sait que $(-1)^n a_0 = detA$, la matrice A est inversible si et seulement si $a_0 \neq 0$, et son inverse est donné par :

$$A^{-1} = -\frac{1}{a_0}(A^{n-1} + a_{n-1}A^{n-2} + \ldots + a_2A + a_1I_n)$$

puisque le théorème de Cayley-Hamilton affirme que :

$$A^n + a_{n-1} + \ldots + a_1A = A \times (A^{n-1} + a_{n-1}A^{n-2} + \ldots + a_2A + a_1I_n) = -a_0I_n.$$

1.3.2 Autre condition nécessaire et suffisante de diagonalisation

Théorème 1.3.2. *Un endomorphisme f est diagonalisable si et seulement si il existe un polynôme annulateur de f, scindé et n'ayant que des racines simples.*

Démonstration. Le lemme des noyaux (1.2.1) s'applique en particulier au polynôme caractéristique qui,d'après le théorème de Cayley-Hamilton, est annulateur de f. La réciproque est une conséquence de la proposition (1.2.3). □

1.4 Polynôme minimal

La théorie du polynôme minimal et le théorème de Cayley-Hamilton donnent une méthode de construction systématique de tous les polynômes annulateurs de f.

Définition 1.4.1. *On appelle polynôme minimal de f -noté $m_f(X)$- le polynôme normalisé annulateur de f de degré le plus petit.*

Il est clair que si un polynôme Q est un multiple de $m_f(X)$ (c'est-à-dire est divisible par $m_f(X)$) alors $Q(f) = 0$. En effet :

$$Q(X) = A(X)m_f(X) \Rightarrow Q(f) = A(f)m_f(f) = 0.$$

On a, en fait, la réciproque :

Proposition 1.4.1. *Les polynômes annulateurs de f sont les polynôme du type*

$$Q(X) = A(X)m_f(X) \quad \textit{avec } A(X) \in \mathbb{K}[X].$$

Démonstration. Supposons en effet que $Q(f) = 0$. En effectuant la division euclidienne de Q par m_f, on a

$$Q(X) = A(X)m_f(X) + R(X)$$

où $dR < dm_f$ (c'est-à-dire : ou $R = 0$ ou, si $R \neq 0$, $dR < dm_f$).
Puisque $Q(f) = 0$ et $m_f(f) = 0$, on a $R(f) = 0$. donc R est un annulateur de f. Mais $m_f(X)$ est l'annulateur de degré le plus petit : ainsi $R \neq 0$ est impossible (car on aurait alors $dR < dm_f$). Donc $R = 0$ et m_f divise Q. □

Corollaire 1.4.1. *$m_f(X)$ devise $P_f(X)$.*

Corollaire 1.4.2. *Le polynôme minimal est unique.*

Démonstration. Soient m_1 et m_2 deux polynômes minimaux. Puisqu'ils sont annulateurs de f, m_1 divise m_2 et m_2 divise m_1. Donc $m_2 = km_1$ ($k \in \mathbb{K}$). Or m_1 et m_2 sont normalisés, donc : $m_1 = m_2$. □

1.4.1 Recherche du polynôme minimal

Le proposition (1.4.1) montre que pour connaître tous les polynômes annulateurs de f, il suffit de connaître le polynôme minimal. Nous allons expliquer maintenant comment on détermine le polynôme minimal.

Proposition 1.4.2. *Les racines de $m_f(X)$ sont exactement les racines de $P_f(X)$, c'est-à-dire les valeurs propres, mais avec une multiplicité en général différente. En d'autre termes, si on considère $P_f(X)$ scindé (éventuellement sur la clôture algébrique $\mathbb{K}'$ de $\mathbb{K}$), c'est-à-dire si*

$$P_f(X) = (-1)^n (X-\lambda_1)^{\alpha_1} \cdots (X-\lambda_p)^{\alpha_p} \quad \textit{avec } \lambda_i \neq \lambda_j,$$

alors :

$$m_f(X) = (-1)^n (X-\lambda_1)^{\beta_1} \cdots (X-\lambda_p)^{\beta_p} \quad \textit{avec } 1 \leq \beta_i \leq \alpha_i.$$

Démonstration. On sait que $P_f(X) = A(X)m_f(X)$, donc si λ est racine de m_f, alors elle est racine de P_f. Réciproquement, soit λ racine de P_f, c'est-à-dire valeur propre de f, alors λ est racine de m_f, parce que m_f annule f. □

Exemple 1.4.1.

1. $A = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ \frac{3}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix}$. *On a :* $P_A(X) = (1-X)(2-X)(\frac{1}{2}-X)$.
   donc :
   $$m_A(X) = (1-X)(2-X)(\frac{1}{2}-X).$$

2. $B = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$. *On a :* $P_B(X) = -(X-1)(X+2)^2$.
   On a donc deux possibilités :
   $$\textit{soit} \quad m_B(X) = -(X-1)(X+2)$$
   $$\textit{soit} \quad m_B(X) = -(X-1)(X+2)^2.$$
   Calculons $(B-I_3)(B+2I_3)$, si l'on trouve la matrice nulle alors le polynôme minimal sera le premier, sinon ce sera le second.
   $$(B-I_3)(B+2I_3) = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$
   Donc :
   $$m_B(X) = -(X-1)(X+2).$$

Théorème 1.4.1. *Un endomorphisme f est diagonalisable si et seulement si son polynôme minimal est scindé et il a toutes ses racines simples.*

Démonstration. Découle du Théorème (1.3.2). □

Proposition 1.4.3. *Soit f un endomorphisme de E, $\mathbb{K}$-espace vectoriel de dimension finie. Alors les valeurs propres de f sont exactement les racines du polynôme minimal de f.*

Démonstration. D'abord, d'après le théorème de Cayley-Hamilton, le polynôme caractéristique est annulateur et c'est donc un multiple du polynôme minimal. Alors les racines du polynôme minimal sont racines du polynôme caractéristique, c'est-à-dire valeurs propres de f. Réciproquement, soit λ une valeur propre de f et v un vecteur propre associé (non nul). Alors pour tout polynôme P, on a $P(f)(v) = P(\lambda)v$. Puisque $m_f(f) = 0$, on doit avoir $m_f(\lambda) = 0$ et donc λ est racine du polynôme minimal de f. $\square$