

Recasages possibles : 122, 150, 151.

Référence : Algèbre, GOURDON (p. 194-195, 224-225)

Développement Soit $f \in \mathcal{L}(E)$, avec E un \mathbb{K} -espace vectoriel de dimension finie.

Lemme 1 Soit $\mu_f = M_1^{\alpha_1} \cdots M_r^{\alpha_r}$ la décomposition en facteurs irréductibles de μ_f dans $\mathbb{K}[X]$. Pour $i \in \llbracket 1, r \rrbracket$, notons $N_i = \text{Ker}(M_i^{\alpha_i}(f))$. Alors, $E = N_1 \oplus \cdots \oplus N_r$ et la projection p_i sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en f .

Lemme 2 Soit $F \leq E$ stable par f . On a $F = \bigoplus_{i=1}^r (N_i \cap F)$.

Proposition 3 Si μ_f est irréductible dans $\mathbb{K}[X]$, alors f est semi-simple.

Théorème 4 f est semi-simple si et seulement si μ_f est sans facteur carré.

- *Preuve du Lemme 1* : La décomposition $E = N_1 \oplus \cdots \oplus N_r$ provient directement du lemme des noyaux appliqué à l'endomorphisme nul $\mu_u(f)$. Montrons que les projections données dans l'énoncé sont bien des polynômes en f . Pour cela, posons pour $i \in \llbracket 1, r \rrbracket$, $Q_i = \prod_{j \neq i} M_j^{\alpha_j} = \mu_u M_i^{-\alpha_i} \in \mathbb{K}[X]$. Comme les M_i sont irréductibles et deux à deux premiers entre eux, les Q_i sont premiers entre eux dans leur ensemble. D'après le théorème de Bézout, il existe $U_1, \dots, U_r \in \mathbb{K}[X]$ tels que $U_1 Q_1 + \cdots + U_r Q_r = 1$. Alors, $\text{id}_E = (U_1 Q_1)(f) + \cdots + (U_r Q_r)(f)$. En particulier, pour tout $x \in E$, on a

$$x \stackrel{(*)}{=} (U_1 Q_1)(f)(x) + \cdots + (U_r Q_r)(f)(x).$$

Soit $i \in \llbracket 1, r \rrbracket$. Montrons que $(U_i Q_i)(f)(x) \in N_i = \text{Ker}(M_i^{\alpha_i}(f))$. Comme les polynômes en f commutent, on a

$$\begin{aligned} M_i^{\alpha_i}(f)((U_i Q_i)(f)(x)) &= U_i(f)((M_i^{\alpha_i} Q_i)(f)(x)) \\ &= U_i(f)(\mu_f(f)(x)) \\ &= U_i(f)(0) = 0 \end{aligned}$$

Par conséquent, $(U_i Q_i)(f)(x) \in N_i$ donc $(*)$ est exactement l'écriture de x associée à la décomposition $E = N_1 \oplus \cdots \oplus N_r$, et ainsi $p_i(x) = (U_i Q_i)(f)(x)$ puis $p_i = (U_i Q_i)(f)$ est bien un polynôme en f .

- *Preuve du Lemme 2* : Soit $F \leq E$ stable par f . Comme p_i est un polynôme en f , F est stable par p_i . On a par ailleurs $p_i(F) \subset p_i(E) = N_i$ donc $p_i(F) \subset N_i \cap F$. En utilisant la relation $(*)$, on obtient

$$F \subset \sum_{i=1}^r p_i(F) \subset \sum_{i=1}^r (N_i \cap F) = \bigoplus_{i=1}^r (N_i \cap F).$$

L'inclusion réciproque est triviale, d'où $F = \bigoplus_{i=1}^r (N_i \cap F)$.

- *Preuve du Lemme 3* : On suppose que μ_f est irréductible dans $\mathbb{K}[X]$. On pose alors $\mathbb{L} = \mathbb{K}[X]/(\mu_f)$, qui est un corps contenant \mathbb{K} , et donc une extension de \mathbb{K} de degré $\deg(\mu_f)$. On va construire une structure de \mathbb{L} -espace vectoriel naturelle sur E pour laquelle les sous-espaces vectoriels de E sont exactement ses sous- \mathbb{K} -espaces stables par f . Plus précisément, pour $P \in \mathbb{K}[X]$, et pour $x \in E$, en notant \bar{P} la classe de P dans \mathbb{L} , on pose

$$\bar{P} \cdot x = P(f)(x).$$

Cette définition est licite, *i.e.* $P(f)(x)$ ne dépend de la classe de P dans \mathbb{L} , et non de P lui-même. En effet, si $R \in \mathbb{K}[X]$ est tel que $\bar{P} = \bar{R}$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = Q\mu + R$ et alors

$$P(f)(x) = Q(f)(\mu(f)(x)) + R(f)(x) = Q(f)(0) + R(f)(x) = R(f)(x).$$

En fait c'est simplement la structure naturelle de $\mathbb{K}[X]$ -module sur E induite par f qui passe au quotient, et comme \mathbb{L} est un corps, on obtient une structure d'espace vectoriel. Si F est un sous-groupe additif de E , on notera dans la suite $F \leq_{\mathbb{K}} E$ (resp. $F \leq_{\mathbb{L}} E$) si F est un sous- \mathbb{K} -espace (resp. sous- \mathbb{L} -espace) de E , *i.e.* si F est stable par la multiplication externe par les éléments de \mathbb{K} (resp. \mathbb{L}). Montrons alors pour tout sous-groupe additif F de E l'équivalence

$$F \leq_{\mathbb{L}} E \iff F \leq_{\mathbb{K}} E \quad \text{et} \quad f(F) \subseteq F.$$

(\Rightarrow) : Soit $F \leq_{\mathbb{L}} E$. Alors, comme $\mathbb{K} \subseteq \mathbb{L}$, on a évidemment $F \leq_{\mathbb{K}} E$. De plus, si $x \in F$, on a $f(x) = \bar{X} \cdot x \in F$ ce qui montre bien $f(F) \subseteq F$.

(\Leftarrow) : Soit $F \leq_{\mathbb{K}} E$ stable par f et soient $P \in \mathbb{K}[X]$ et $x \in F$. Comme F est stable par f , F est stable par tout polynôme en f donc $P(f)(x) \in F$. Ainsi, $\bar{P} \cdot x = P(f)(x) \in F$, ce qui montre bien que F est un sous- \mathbb{L} -espace vectoriel de E et conclut l'équivalence.

Soit F un sous- \mathbb{K} -espace vectoriel de E stable par f . D'après ce qui précède, F est un sous- \mathbb{L} -espace de E , donc il existe $G \leq_{\mathbb{L}} E$, *i.e.* $G \leq_{\mathbb{K}} E$ stable par f , tel que $F \oplus G = E$. Ainsi, f est bien un endomorphisme semi-simple.

- *Preuve du Théorème 4* : Montrons l'équivalence par double implication :

(\Leftarrow) : Supposons que μ_f est sans facteurs carrés. Écrivons $\mu_f = M_1 \cdots M_r$ la décomposition en produit d'irréductibles de $\mathbb{K}[X]$ de μ_f . Par hypothèse, les M_i sont deux à deux distincts. Soit $F \leq E$ stable par f . Notons $N_i = \text{Ker}(M_i(f))$ pour $i \in \llbracket 1, r \rrbracket$. D'après le **Lemme 2**, on a

$$F = \bigoplus_{i=1}^r (F \cap N_i).$$

Soit $i \in \llbracket 1, r \rrbracket$. L'espace N_i est stable par f donc on peut considérer l'endomorphisme f_i de N_i induit par f par restriction et corestriction. On a clairement $M_i(f_i) = 0$: si $x \in N_i = \text{Ker}(M_i(f))$, alors $M_i(f_i)(x) = M_i(f)(x) = 0$ (la restriction et la corestriction commutent avec l'évaluation d'un polynôme en f). Or, M_i est irréductible dans $\mathbb{K}[X]$ donc c'est exactement le polynôme minimal de f_i . Ainsi, d'après le **Lemme 3**, f_i est semi-simple. L'espace $F \cap N_i$ est clairement f_i -stable, donc admet un supplémentaire S_i dans N_i qui est f_i -stable. Posons $S = S_1 \oplus \cdots \oplus S_r$. Alors d'une part

$$((F \cap N_1) \oplus S_1) \oplus \cdots \oplus ((F \cap N_r) \oplus S_r) = N_1 \oplus \cdots \oplus N_r = E$$

et d'autre part

$$\begin{aligned} ((F \cap N_1) \oplus S_1) \oplus \cdots \oplus ((F \cap N_r) \oplus S_r) &= (F \cap N_1) \oplus \cdots \oplus (F \cap N_r) \oplus S \\ &= F \oplus S \end{aligned}$$

Ainsi, S est un supplémentaire f -stable de F dans E , ce qui montre que f est semi-simple.

- (\Rightarrow) : Supposons que f est semi-simple et que μ_f s'écrit $\mu_f = M^2N$ avec M, N dans $\mathbb{K}[X]$. Soit $F = \text{Ker}(M(f))$. C'est un sous-espace vectoriel f -stable de E , donc il admet un supplémentaire f -stable S dans E . Notons que $MN(f)|_F = 0$. En effet, si $x \in F$, alors

$$MN(f)(x) = N(f)(M(f)(x)) = N(f)(0) = 0.$$

Montrons alors que $MN(f)$ est aussi nul sur S . Soit donc $x \in S$. On a $MN(f)(x) \in F$ car $M(f)(MN(f)(x)) = M^2N(f)(x) = \mu_f(f)(x) = 0$. Or S est f -stable, donc $MN(f)$ -stable et ainsi $MN(f)(x) \in S$. Finalement, $MN(f)(x) \in F \cap S = \{0\}$ donc $MN(f)$ s'annule sur S . Comme $E = F \oplus S$ et que $MN(f)$ est nul sur F et sur S , on a $MN(f) = 0$ en tant qu'endomorphisme de E , ce qui contredit la minimalité de μ_f . Ainsi, μ_f est nécessairement sans facteurs carrés, ce qui termine la preuve du **Théorème 4**.