1) Le théorème de Cayley-Hamilton.

<u>Thm</u> Soit A une matrice $(n\times n)$ et $P(X)=\sum_{i=0}^{n} a_i X^i$ son polynome caractéristique. Alors

$$P(A):=\sum_{i=0}^{n} a_i A^i = 0$$

Avant de démontrer ce théorème remarquons que l'on peut supposer que k est algébriquement clos (ex $k=\mathbb{C}$).

D'autre part $P(Q^{-1}AQ)=Q^{-1}P(A)Q$

$[\text{car } (Q^{-1}AQ)^n = Q^{-1}A^nQ]$

On peut donc supposons que A est triangulaire

$$A=\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Soit $E_i=\langle e_1,\dots,e_i\rangle$. On a donc $A(e_i)=\lambda_i e_i+\sum_{j=1}^{i-1} a_{ji}e_j$

donc $(A-\lambda_i)E_i \subset E_{i-1}$. En effet $(A-\lambda_i\cdot \mathrm{Id})\,e_i \subset E_{i-1}$

et si $j<i$, $(A-\lambda_i)e_j \in E_j \subset E_{i-1}$

En particulier

$$(A-\lambda_n)E\subset E_{n-1}$$

$$(A-\lambda_{n-1})(A-\lambda_n)E\subset E_{n-2}$$

$$\dots$$

$$\prod_{i=1}^{n}(A-\lambda_i)E\subset\{0\}.$$

Or $P(A)=\prod_{i=1}^{n}(A-\lambda_i)$ ▶

On a bien sûr le même résultat pour les endomorphismes

2.) Rappels sur les polynomes

On note $k[X]$ l'anneau des polynomes d'une variable à coefficients dans k

Un sous-ensemble $I \subset k[X]$ est un idéal si

$$(i)\ \forall P, Q \in I\ ;\ P+Q \in I$$

$$(ii)\ \forall P \in I,\ \forall Q \in k[X]\ ;\ Q \cdot P \in I$$

Exemple. Si P_0 est un polynome,

$$I := P_0 \cdot k[X] = \{P \mid Q \in k[X],\ P = P_0 \cdot Q\}$$

est un ideal dit principal de $k[X]$

On rappelle le theoreme

Theorème : tout idéal I de $k[X]$ est principal

si P_0 est un polynome (non nul) de plus petit degré dans I, Alors $I = P_0 \cdot k[X]$.

◀ Idee de preuve. si $Q \in I$, on peut ecrire $Q = P \cdot P_0 + R$ avec $d^\circ R < d^\circ P_0$

mais $-P.P_0 \in I$, donc $R = Q - P.P_0 \in I$ et donc $R = 0$. ▶

Rq On peut choisir $P_0 = X^{d^\circ P_0} + \ldots$

Soit P et Q deux polynomes, $I := P \cdot k[X]$ et $J := Q \cdot k[X]$ les deux idéaux principaux associé. Alors $I + J$ est un ideal. P et Q sont dit premiers entre eux si $I + J = k[X]$. Autrement dit si il existe deux polynomes A et B tel que $A \cdot P + BQ = 1$.

proposition : si P et $Q \in \mathbb{C}[X]$ ils sont premiers entre eux si et seulement si ils n'ont au aucune racine commune (sur $\mathbb{C}$)

◀ Idée de la preuve : on fait une récurrence sur $n = d^\circ P + d^\circ Q$

C'est vrai pour $n = 1$. Si $d^\circ P \geq d^\circ Q$; on ecrit

$P = A \cdot Q + R$; alors $R \neq 0$ et R et P n'ont aucune racine commune [pourquoi ?]. Alors $d^oP + d^oR < d^oP + d^oQ$.

Il existe alors B, C tel que $B \cdot P + C \cdot R = 1$

Donc $B \cdot P + C(P - AQ) = 1$

Ainsi $(B+C) \cdot P - (CA)Q = 1$ et donc P et Q sont premiers entre eux

La reciproque est facile et laissée en exercice ▶

3.) le polynome minimal et ses racines

Soit A un endomorphisme d'un espace vectoriel sur un corps k

prop $I = \{P \in k[X] \mid P(A) = 0\}$ est un ideal

le polynome minimal de A est le polynome P_0 (de terme de plus haut degre λ^m) tel que $I = P_0 \cdot k[X]$.

Par le theorème de Cayley-Hamilton, le polynome minimal divise le polynome caractéristique.

prop Si λ est valeur propre de g, si P est un polynome $P(g) = 0 \Rightarrow P(\lambda) = 0$

En particulier si P_0 est le polynome minimal de g alors $P_0(\lambda) = 0$.

◀ En effet pour tout polynome, si u est vecteur propre associé à λ

$$Q(g) \cdot u = Q(\lambda) \cdot u$$

Donc $0 = P(g)(u) = P(\lambda) \cdot u = 0$ comme $u \neq 0$; $P_0(\lambda) = 0$ ▶

Nous en déduisons :

<u>Proposition</u> Les racines du polynome minimal sont les valeurs propres

◀ Nous venons de voir que les valeurs propres sont racines du polynome minimal.

Reciproquement, toute racine du polynome minimal est racine du polynome caractéristique (car il le divise) et donc valeur propre ▶

<u>Corollaire</u> $\underset{(A)}{\text{polynome minimal } P_0 \text{ scindé}} \Leftrightarrow \underset{(B)}{\text{polynome caractéristique } P \text{ scindé}}$.

◀ (B)⇒(A) car P_0 divise P ; (A)⇒(B) : notons $\bar{k}$ la cloture algébrique de k

[Example : $k = \mathbb{R}$, $\bar{k} = \mathbb{C}$]. Soit M une matrice à coefficients dans k. Si son polynome minimal est scindé sur k, alors touts les valeurs propres de M (vue comme matrice à coefficients dans $\bar{k}$) appartiennent à k (en tant que racine de P_0). En particulier, touts les racines de P (qui est scindé sur $\bar{k}$) appartiennent à k.

Ainsi P est scindé sur k. ▶

4. Polynome minimal et diagonalisation.

Commençons par un lemme

<u>proposition</u> Soit P et Q deux polynomes premiers entre eux

si $(P \cdot Q)(g) = 0$

Alors $E = \ker(P(g)) \oplus \ker(Q(g))$

◀ Comme P et Q premiers entre eux, par Bezout il existe A et B $\in k[X]$ tels que $A \cdot P + B \cdot Q = 1$

$$u = A(g) \cdot P(g) \cdot u + B(g) \cdot Q(g) \cdot u \quad (*)$$

mais $P(g)[Q(g)\, W] = 0$.

Donc $A(g)P(g)(u) \in \ker(Q(g))$

$B(g)\,Q(g)\cdot u \in \ker(P(g))$

En particulier $u \in \ker(P(Q)) + \ker(Q(g))$

De même, si $u \in \ker(P(Q)) \cap \ker(Q(g))$

(*) donne $u=0$. Donc $E = \ker(Q(g)) \oplus \ker(P(g))$ ▶

Corollaire Si $P = \prod_{i=1}^{q} Q_i$ avec les Q_i deux à deux premiers entre eux et $P(g)=0$. Alors $E = \bigoplus_{i=1}^{q} \ker(Q_i(g))$

◀ Indication : on procède par récurrence en utilisant

Q premier avec Q_1 et $Q_2 \Rightarrow Q$ premier avec $Q_1 \cdot Q_2$.

[En effet $A_1Q_1 + B_1Q = 1$, $A_2Q_2 + B_2Q = 1 \Rightarrow$

$A_1A_2 \cdot Q_1Q_2 + Q(A_1B_2Q_1 + A_2B_1Q_2 + B_1B_2Q) = 1$] ▶

Théorème Un endomorphisme est diagonalisable si et seulement si son polynome minimal n'a que des racines simples et est scindé.

Corollaire si Q est un polynome scindé n'admettant que des racines simples tel que $Q(g)=0$. Alors g est diagonalisable

◀ Si Q est scindé sans racines multiples si P divise Q alors P est scindé et ses racines sont simples ▶

Preuve du theoreme

Soit P le polynome minimal.

① Montrons tout d'abord. A diagonalisable $\Rightarrow P$ scindé sans racines multiples

Si A est diagonalisable de valeurs propres distinctes $\lambda_1, \dots, \lambda_q$ et espaces propres $E_1, \dots, E_q$.

Alors $(A-\lambda_i)(E_i)=\{0\}$

Donc $(A-\lambda_i)[E_1 \oplus \cdots \oplus E_i] \subset [E_1 \oplus \cdots \oplus E_{i-1}]$

On en deduit $\prod_{i=1}^{q}(A-\lambda_i)=0$

Comme $\prod_{i=1}^{q}(A-\lambda_i)$ divise le polynome minimal. On en deduit

que $P_{min}(\lambda)=\prod_{i=1}^{q}(\lambda-\lambda_q)$ ●

② Pour la réciproque montrons

Pscindé sans racines multiples $\Rightarrow$ A diagonalisable

• Comme tous les λ_i sont distincts

si $P[X]=\prod_{i=1}^{n}[X-\lambda_i]$

En utilisant le lemme $E=\bigoplus_{i-1}^{p}\ker[g-\lambda_i]=\bigoplus_{i=1}^{p}E_{\lambda_i}$

Retour sur les exercices - Montrez que si $A^2=A$, ou $A^2=1$ alors A est diagonalisable.