Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

151

Cadre : E est un ev. sur un corps (commutatif) $\mathbb{K}$.

I - THEORIE DE LA DIMENSION

1. Familles libres, génératrices, bases.

Déf 1. Une famille de vecteurs $(v_1, .. v_p)$ de E est
- génératrice si $E = \text{vect}\{v_1, .. v_p\}$
- libre si $\forall (\lambda_1, .. \lambda_p) \in \mathbb{K}^p \quad \sum_{i=1}^{p} \lambda_i v_i = 0 \Rightarrow \forall i \in [\![1, p]\!], \lambda_i = 0$.

Déf 2. Une base est une famille libre et génératrice.

Prop 3.
- Toute famille contenant une famille génératrice est génératrice.
- Toute sous-famille d'une famille libre est libre.

2. Existence de bases d'un ev. de dimension finie

Déf 4. E est de dimension finie s'il admet une famille génératrice finie. Sinon, E est de dimension infinie.

Cadre. Dans la suite, on considère des ev. de dimension finie.

TR 5. Supposons $E \neq \{0\}$. Soient G une famille génératrice et L une famille libre telle que $L \subset G$. Alors il existe une base $\mathcal{B}$ telle que $L \subset \mathcal{B} \subset G$.

Cor 6. Supposons $E \neq \{0\}$.
- E admet une base.
- De toute famille génératrice, on peut extraire une base.
- TRéorème de la base incomplète : Toute famille libre peut être complétée en une base.

Prop 7. Soit $\mathcal{B} = (v_1, .. v_n)$ une base de E. Il existe un isomorphisme $\varphi_{\mathcal{B}} : E \to \mathbb{K}^n$; $x = \sum_{i=1}^{n} x_i e_i \longmapsto (x_1, .. x_n)$ de $\mathbb{K}$-ev

3. Dimension d'un ev.

Lem 8. Si E est engendré par n éléments, toute famille contenant plus de $n+1$ éléments n'est pas libre.

TR 9. Toutes les bases de E ont le même cardinal, appelé dimension de E sur $\mathbb{K}$ et notée $\dim_{\mathbb{K}} E$ ou $\dim E$

App 10. Soit A une $\mathbb{K}$-algèbre de dimension n.
Soit $a \in A$. Il existe un polynôme annulateur non nul de a.

Ex 11.
- $\dim_{\mathbb{K}} \mathbb{K}^n = n$,
- $\dim_{\mathbb{K}} \mathbb{K}_n[X] = n+1$,
- $\dim_{\mathbb{K}} \mathcal{M}_{n,m}(\mathbb{K}) = nm$,
- Si $u \in \mathcal{L}(E)$, $\dim_{\mathbb{K}} \mathbb{K}[u] = \deg(\pi_u)$ où π_u est le polynôme minimal de u.

Ex 12. $E_{\alpha,\beta} = \{(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}, u_{n+2} = \alpha u_{n+1} + \beta u_n\}$ est de dimension 2 où $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$.

App 13. Soient $E_1, .. E_p$ des $\mathbb{K}$-ev de dimension finie. Alors $\dim_{\mathbb{K}}(E_1 \times .. \times E_p) = \sum_{i=1}^{p} \dim_{\mathbb{K}}(E_i)$.

Cor 14. Si $\dim_{\mathbb{K}} E = n$, toute famille ayant moins de $n-1$ éléments n'est pas génératrice.

TR 15. Soit $n = \dim_{\mathbb{K}} E$. Toute famille libre ou génératrice ayant n éléments est une base.

4. Sous-espaces vectoriels (sev) d'un ev de dimension finie.

Prop 16. Soit F un sev de E. Alors F est de dimension finie et $\dim_{\mathbb{K}} F \leq \dim_{\mathbb{K}} E$. De plus, $\dim_{\mathbb{K}} F = \dim_{\mathbb{K}} E$ ssi $E = F$.

App 17. Une forme linéaire $f \in \mathcal{L}(E, \mathbb{K})$ est soit nulle, soit surjective.

Ex 18. Soit $\mathbb{K} \subset \mathbb{L}$ deux corps. $\mathbb{L}$ est muni d'une structure de $\mathbb{K}$-ev et le degré de $\mathbb{L}$ sur $\mathbb{K}$, noté $[\mathbb{L}:\mathbb{K}]$ est $\dim_{\mathbb{K}} \mathbb{L}$. De plus, si Π est un corps tel que $\mathbb{K} \subset \mathbb{L} \subset \Pi$ alors $[\Pi:\mathbb{K}] = [\Pi:\mathbb{L}][\mathbb{L}:\mathbb{K}]$.

Prop 19. Soient $E_1, .. E_p$ des sev de E. Alors $E = E_1 \oplus .. \oplus E_p$ ssi $E = E_1 + .. + E_p$ et $\dim_{\mathbb{K}} E = \sum_{i=1}^{p} \dim_{\mathbb{K}} E_i$.

App 20. Soit $f \in \text{End}(E)$. f est diagonalisable ssi la somme des dimensions de ses sous-espaces propres vaut $\dim_{\mathbb{K}} E$.

Prop 21. Tout sev de E admet un supplémentaire dans E.

App 22. Si $\mathbb{K}$ est algébriquement clos, tout endomorphisme de E est trigonalisable.

Prop 23 - Formule de Grassman.
Soient F et G des sev de E. Alors :
$\dim(F+G) = \dim F + \dim G - \dim(F \cap G)$.

Cor 23 - Soient F, G des sev de E. Alors $E = F \oplus G$ ssi $\dim E = \dim F + \dim G$ et $F \cap G = \{0\}$.

App 24 - Soit F un sev de E. Alors :
$\operatorname{codim}(F) := \dim(E/F) = \dim E - \dim F$.

Ex 25 - $\mathcal{GL}_n(\mathbb{K}) = S_n(\mathbb{K}) \oplus A_n(\mathbb{K})$.

II - APPLICATIONS LINEAIRES, DIMENSION, RANG

L' est un $\mathbb{K}$-ev →

1 - Dimension d'ev et applications linéaires

Prop 25 - Soit $f \in \mathcal{L}(E,E')$. Si
- Si f est injective (resp. surjective) alors l'image par f d'une famille libre (resp. génératrice) de E est une famille libre (resp. génératrice) de E'.
- f est bijective ssi l'image par f d'une base est une base.

TR 26 - E est isomorphe à E' ssi $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} E'$.

App 27 - L'ensemble des solutions de $Y'(t) = A(t)Y(t)$, où $t \in \mathbb{R}$ et $t \mapsto A(t) \in \mathcal{M}_n(\mathbb{C})$ est continue, est un ev de dimension n.

Prop 28 - Soient $n = \dim_{\mathbb{K}} E$ et $p = \dim_{\mathbb{K}} E'$. Alors $\mathcal{L}_{\mathbb{K}}(E,E')$ est isomorphe à $\mathcal{M}_{p,n}(\mathbb{K})$.

App 29 - $\dim_{\mathbb{K}} \mathcal{L}_{\mathbb{K}}(E,E') = np$.

2 - Théorème du rang.

Déf 30 - Soit $f \in \mathcal{L}(E,E')$. L'entier $\dim_{\mathbb{K}}(\operatorname{Im}(f))$ est appelé rang de f et noté $\operatorname{rg}(f)$.

Prop 31 - Soient $f \in \mathcal{L}(E,F)$, $g \in \mathcal{L}(G,E)$ et $h \in \mathcal{L}(F,G)$.
- Si g est surjective alors $\operatorname{rg}(f \circ g) = \operatorname{rg}(f)$.
- Si h est injective alors $\operatorname{rg}(h \circ f) = \operatorname{rg}(f)$.

Donc en composant f à gauche ou à droite par une application bijective, le rang de f ne change pas.

TR 32 - Théorème du rang.
Soit $f \in \mathcal{L}(E,E')$. $\dim_{\mathbb{K}} E = \operatorname{rg}(f) + \dim_{\mathbb{K}} \ker f$.

App 33 - Soit $f \in \mathcal{L}(E,E')$ où E et E' sont de même dimension finie. Alors f est injective ssi f est surjective ssi f est bijective.

Cex 34 - $\mathbb{R}[X] \to \mathbb{R}[X]$, $P \mapsto P'$ est surjective et non injective.

App 35 - Soit A une $\mathbb{K}$-algèbre de dimension finie. Alors A est intègre ssi A est un corps.

App 36 - Si p est un projecteur de E alors $E = \ker p \oplus \operatorname{Im} p$.

3 - Formes linéaires et dimension

Prop 37 - $\dim E = \dim E^*$ où E^* est le dual de E.

Prop 38 - Le noyau d'une forme linéaire non nulle est un hyperplan.

Ex 39 - $\dim\{A \in \mathcal{M}_n(\mathbb{K}), \operatorname{Tr}(A) = 0\} = n^2 - 1$.

Prop 40 - E est canoniquement isomorphe à E^{**}.

Déf 41 -
- Soit $A \subset E$. L'orthogonal de A est le sev de E^* $A^\perp := \{\varphi \in E^*, \forall x \in A, \varphi(x) = 0\}$.
- Soit $B \subset E^*$. L'orthogonal de B est le sev de E $B^\circ := \{x \in E, \forall x \in B, \varphi(x) = 0\}$.

Prop 42 -
- Soit F un sev de E. Alors $\dim F + \dim F^\perp = \dim E$.
- Soit G un sev de E^*. Alors $\dim G + \dim G^\circ = \dim E$.

App 43 - Soit $n = \dim E$.
- Soient $\varphi_1, .. \varphi_p \in E^*$ telles que $\dim(\operatorname{vect}\{\varphi_1, .. \varphi_p\}) = r$. Alors le sev $F = \{x \in E, \forall i \in \{1..p\}, \varphi_i(x) = 0\}$ est de dimension $n-r$.
- Réciproquement, si F est un sev de E de dimension q alors il existe $n-q$ formes linéaires indépendantes telles que $F = \bigcap_{i=1}^{n-q} \ker(\varphi_i)$.

DEVELOPPEMENT N°1

App 44 - Invariants de similitude.
Soit $f \in \mathcal{L}(E)$. Il existe une unique famille de polynômes unitaires $P_1, .. P_r$ et une famille $E_1, .. E_r$ de sev de E vérifiant :
i) $P_r | .. | P_1$
ii) $E = E_1 \oplus .. \oplus E_r$
iii) $\forall i \in \{1..r\}$, E_i est stable par u et $u_{|E_i}$ est cyclique de polynôme minimal P_i.

III - MATRICES ET CALCUL EFFECTIF DU RANG.

1 - Matrices et rang

Déf 45 - • Le rang d'une famille $(v_1 .. v_p)$ de vecteurs de E est la dimension de $\text{vect}\{v_1 .. v_p\}$.
• Le rang d'une matrice est le rang de ses vecteurs colonnes.

Prop 46 - Soient $f \in \mathcal{L}(E,E')$, $\mathcal{B}$ une base de E et $\mathcal{B}'$ une base de E'. Alors $\text{rg}(f) = \text{rg}(\text{mat}_{\mathcal{B},\mathcal{B}'}(f))$.

App 47 - Soit $M \in \mathcal{M}_n(\mathbb{K})$. Alors $\text{rg}\, M = n$ ssi M est inversible.

2 - Calcul du rang.

Prop 48 - Les opérations élémentaires sur les lignes et les colonnes ainsi que les permutations de lignes et colonnes ne changent pas le rang de M.
Utilisation du pivot de Gauss : le rang d'une matrice échelonnée est égal au nombre d'échelons non nuls.

Prop 49 - Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$. $\text{rg}(A) = r$ ssi A est équivalente à $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

App 50 - Deux matrices de $\mathcal{M}_{n,p}(\mathbb{K})$ sont équivalentes ssi elles ont le même rang.

App 51 - $\text{rg}(A) = \text{rg}({}^tA)$.

Th 52 - Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$. Le rang de A est le plus grand des ordres des sous-matrices carrées inversibles de A.

App 53 - Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et $A \in \mathcal{M}_{n,p}(\mathbb{K})$ est de rang r, alors il existe un voisinage V de A tel que $\forall M \in V$, $\text{rg}\, M \geq r$.

App 54 - Le rang est une notion invariante par extension de corps.

IV - APPLICATIONS

1 - Algorithme de Berlekamp — DEVELOPPEMENT N°2

Th 55 - Soient p premier, $q = p^s$ et $P \in \mathbb{F}_q[X]$, polynôme sans facteurs carrés. Soient $d = \deg(P)$, $x = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$ et $\mathcal{B} = (1, x, .. x^{d-1})$, base de $\mathbb{F}_q[X]/(P)$.
On considère l'application $S_p : \mathbb{F}_q[X]/(P) \to \mathbb{F}_q[X]/(P)$, $\overline{Q} \mapsto \overline{Q^q}$.

Cette application est linéaire et l'algorithme suivant termine et renvoie la décomposition de P en facteurs irréductibles :

1. Calculer la matrice de $S_p - Id$ dans $\mathcal{B}$ et calculer $r = \dim(\ker(S_p - Id))$. Si $r = 1$, P est irréductible et on retourne P. Sinon, on passe à 2.
2. Calculer $V \in \mathbb{F}_q[X]$ tel que $V \bmod P$ ne soit pas représenté par un polynôme constant et tel que $V \bmod P \in \ker(S_p - Id)$. Calculer, pour $\alpha \in \mathbb{F}_q$, $\text{pgcd}(P, V - \alpha)$ avec l'algorithme d'Euclide. Alors $P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V - \alpha)$. Retourner en 4 avec chacun des facteurs non triviaux de ce produit.

2 - Codes correcteurs

Déf 56 - Un code linéaire de longueur n sur $\mathbb{K}$ et de dimension k (noté $[n,k]$) est un sev de $\mathbb{K}^n$ de dimension k.

Déf 57 - Le poids de $x = (x_1, .. x_n)$, noté $\omega(x)$, est le nombre de ses composantes non nulles.

Déf 58 - La distance minimale d'un code linéaire $\mathcal{C}$ est $d := \min\{\omega(x),\ x \in \mathcal{C} \setminus \{0\}\}$. Un code linéaire est t-correcteur si $d = 2t+1$ ou $d = 2t+2$.

Th 59 - Borne de singleton
Soit $\mathcal{C}$ un code linéaire $[n,k]$ de distance minimale d. Alors $d \leq n - k + 1$.

Déf 60 - Une matrice génératrice d'un code linéaire $\mathcal{C}$ $[n,k]$ sur $\mathbb{K}$ est une matrice sur $\mathbb{K}$ dont les lignes forment une base de $\mathcal{C}$. On a $\mathcal{C} = \{uG,\ u \in \mathbb{K}^k\}$.

Prop 61 - Soit $\mathcal{C}$ un code linéaire sur un corps $\mathbb{K}$.
• Si G est une matrice génératrice alors $G \in \mathcal{M}_{k,n}(\mathbb{K})$ avec $k \leq n$ et $\text{rg}\, G = k$.
• Si $G \in \mathcal{M}_{k,n}(\mathbb{K})$ est de rang k, alors G est une matrice génératrice d'un code $[n,k]$ sur $\mathbb{K}$.

Ex 62 -
Soit $G = \begin{pmatrix} 1&0&0&1&1&0 \\ 0&1&0&1&1&1 \\ 0&0&1&0&1&1 \end{pmatrix}$. $\text{rg}\, G = 3$ donc G est la matrice génératrice d'un code linéaire $[5,3]$ sur $\mathbb{F}_2$, dont les mots sont : $(1\,0\,0\,1\,1\,0)$, $(0\,1\,0\,1\,1\,1)$, $(0\,0\,1\,0\,1\,1)$, $(1\,1\,0\,0\,1\,1)$, $(1\,0\,1\,1\,1\,0)$, $(0\,1\,1\,1\,0\,0)$, $(1\,1\,1\,0\,0\,0)$, $(0\,0\,0\,0\,0\,0)$. Donc $d = 2$.

Références :

- Grifone, Algèbre linéaire.
- Gourdon, Algèbre
- Papini, Wolfmann, Algèbre discrète des codes correcteurs
- Beck, Malick, Peyré, objectif agrégation.

Algorithme de Berlekamp

But : Décomposer un polynôme en produit des polynômes irréductibles sur un corps fini.

Algorithme 1. *Soit p un nombre premier et $q = p^s$. Soit $P \in F_q[X]$ un polynôme sans facteurs carrés. On note $x = XmodP$ dans l'anneau $F_q[X]/(P)$ dont une base est alors $\mathcal{B} = \{1, x, .., x^{\deg(P)-1}\}$.*

Alors l'algorithme suivant se termine en un nombre fini d'étapes et donne la décomposition de P en facteurs irréductibles.

1. *$S_P : F_q[X]/(P) \to F_q[X]/(P); Q \mapsto Q^q$ est linéaire.*
   On calcule la matrice de $S_P - Id$ dans la base $\mathcal{B}$.
2. *Le nombre r de facteurs irréductibles de P est égal à $\dim(\ker(S_P - Id))$. On calcule r avec le pivot de Gauss.*
   Si $r = 1$, P est irréductible et l'algorithme renvoie P.
   Sinon, on passe à 3.
3. *On choisit V non constant dans $F_q[X]/(P)$ tel que $V \in \ker(S_P - id)$.*
   On calcule avec l'algorithme d'Euclide les $pgcd(P, V - \alpha)$ pour $\alpha \in F_q$. Alors $P = \prod_{\alpha \in F_q} pgcd(P, V - \alpha)$.
   On réapplique l'algorithme aux facteurs non triviaux de ce produit.

Démonstration. Soit $P = P_1...P_r$ la décomposition en produit de polynômes irréductibles différents deux à deux et r le nombre de polynômes irréductibles dans la décomposition de P.

1. $F_q[X]/(P)$ est un anneau de caractéristique p et par propriété du morphisme de Frobenius, S_P est F_q linéaire.
2. Montrons que $r = \dim(\ker(S_P - \mathrm{Id}))$.
   Soit $\phi : F_q[X]/(P) \to K_1 \times .. \times K_r; Q \mod P \mapsto (Q \mod P_1, .., Q \mod P_r)$, où $K_i = F_q[X]/(P_i)$ pour tout $i \in \{1, .., r\}$, l'isomorphisme obtenu par le théorème chinois, les P_i étant premiers entre eux deux à deux.
   Pour tout $i \in \{1, .., r\}$, K_i est un corps car P_i est irréductible.
   Soit $Q \in F_q[X]/(P)$. Posons $\phi(Q) = (Q_1, .., Q_r)$.
   Alors $Q \in \ker(S_P - \mathrm{Id})$ si et seulement si $Q^q = Q$ dans $F_q[X]/(P)$ si et seulement si $\phi(Q)^q = \phi(Q)$ dans $K_1 \times .. \times K_r$ si et seulement si pour tout $i \in \{1, .., r\}$, $Q_i^q = Q_i$ dans K_i soit encore si et seulement si pour tout $i \in \{1, .., r\}$, $Q_i \in F_q$.
   En effet, les éléments de F_q sont les q racines du polynôme $X^q - X$ sur K_i. Comme K_i est un corps et que $\deg(X^q - X) = q$, ce sont donc ses seules racines.
   Donc $\ker(S_P - \mathrm{Id}) = \phi^{-1}(F_q^r)$.
   Comme ϕ est un isomorphisme, $r = \dim(\ker(S_P - \mathrm{Id}))$.
3. Déterminons une factorisation de P.
   Si $r = 1$, alors P est irréductible.
   Supposons $r > 1$. La droite vectorielle $F_q.1$ de $F_q[X]/(P)$ étant de dimension 1 et $\ker(S_P - \mathrm{Id})$ étant de dimension $r > 1$, on peut trouver $V \in F_q[X]$ tel que $V \mod P \in \ker(S_P - \mathrm{Id})$ et $V \mod P$ n'est pas constant.
   Or $V \mod P \in \ker(S_P - \mathrm{Id})$ si et seulement si pour tout $i \in \{1, .., r\}$, $V \mod P_i \in F_q$. Notons alors $\alpha_i = V \mod P_i \in F_q$ pour tout $i \in \{1, .., r\}$.
   Montrons que $P = \prod_{\alpha \in F_q} \mathrm{pgcd}(P, V - \alpha)$.
   Soit $\alpha \in F_q$. Comme $\mathrm{pgcd}(P, V - \alpha)$ divise P, on peut écrire $\mathrm{pgcd}(P, V - \alpha) = P_{i_1}...P_{i_k}$ avec $i_1, ..i_k \in \{1, .., r\}$.
   Or les polynômes $P_{i_1}, .., P_{i_k}$ sont premiers entre eux deux à deux donc par le théorème de Gauss, ils divisent tous $V - \alpha$.
   Or pour tout $i \in \{1, .., r\}$, $P_i | V - \alpha$ si et seulement si $V - \alpha = 0 \mod P_i$ soit encore si et seulement si $\alpha = \alpha_i$.
   Donc $\mathrm{pgcd}(P, V - \alpha) = \prod_{\alpha_i = \alpha} P_i$.
   Alors, $P = \prod_{i=1}^r P_i = \prod_{\alpha \in F_q} (\prod_{\alpha_i = \alpha} P_i) = \prod_{\alpha \in F_q} \mathrm{pgcd}(P, V - \alpha)$.
4. Montrons que l'algorithme s'arrête, et plus précisément, montrons que r diminue strictement à chaque itération.
   C'est le cas car au moins l'un des $\mathrm{pgcd}(P, V - \alpha)$ est un diviseur strict de P.

En effet, $V \mod P$ n'est pas constant donc il existe $i \neq j$ tels que $\alpha_i \neq \alpha_j$. (Sinon, pour tout $i \in \{1, ..., r\}$, $\alpha_i = \alpha \in F_q$ et $P_i | V - \alpha$ donc $\prod_{i=1}^{r} P_i = P | V - \alpha$ car les P_i sont premiers entre eux, ie $V = \alpha \mod P$. Contradiction.)
Donc $P_i | \text{pgcd}(P, V - \alpha_i)$ donc $\deg(\text{pgcd}(V - \alpha_i, P)) > 0$ et P_j ne divise pas $\text{pgcd}(P, V - \alpha_i)$ donc $\deg(\text{pgcd}(V - \alpha_i, P)) < deg(P)$ et $\text{pgcd}(V - \alpha_i, P)$ est un facteur strict.
Par ailleurs, tous les facteurs divisent P donc sont sans facteurs carrés et on peut leur appliquer l'algorithme.

□

Invariants de similitude

Références. H2G2 p148 A VERIFIER, Gourdon p290.

On se place dans E, un espace vectoriel de dimension finie sur un corps $\mathbb{K}$. On considère u un endomorphisme dans $\mathcal{L}(E)$, on note π_u sont polynôme minimal et χ_u son polynôme caractéristique.

"Rappels" - Pré-requis

Propositon - Définition. Pour tout $x \in E$, il existe un unique polynôme unitaire $\pi_{u,x}$ tel que pour tout polynôme P de $\mathbb{K}[X]$,

$$P(u)(x) = 0 \Leftrightarrow \pi_{u,x} | P.$$

En particulier, $\pi_{u,x}$ divise π_u. Le degré de $\pi_{u,x}$ est égal à la dimension de $\mathbb{K}[u]x$, le sous-espace vectoriel de E engendré par la famille $(x, u(x), u^2(x), ...)$.

Démonstration. Soit $x \in E$. L'ensemble $\{P \in \mathbb{K}[X],\ P(u)(x) = 0\}$ est un idéal de $\mathbb{K}[X]$. Comme K est un corps, cet idéal est principal. D'où l'existence et l'unicité d'un tel polynôme unitaire $\pi_{u,x}$.
Si on note $k = \deg \pi_{u,x}$, alors $\pi_{u,x}$ s'écrit $\pi_{u,x} = X^k + \lambda_{k-1}X^{k-1} + ... + \lambda_1 X + \lambda_0$ et comme $\pi_{u,x}(u)(x) = 0$, on a $u^k(x) + \lambda_{k-1}u^{k-1}(x) + ... + \lambda_0 x = 0$, donc la famille $(x, u(x), ...u^k(x))$ est liée. La réciproque est claire. Ainsi, $\deg \pi_{u,x}$ est le plus petit k tel que la famille $(x, u(x), ...u^k(x))$ est liée. Ainsi $(x, u(x), ...u^{k-1}(x))$ est une famille libre dans $\mathbb{K}[u]x$, et par récurrence, pour tout m supérieur ou égal à k, $u^m(x)$ est combinaison linéaire de ces vecteurs. La famille $(x, u(x), ...u^{k-1}(x))$ est donc une base de $\mathbb{K}[u]x$ et $\mathbb{K}[u]x$ est de dimension $k = \deg \pi_{u,x}$. □

Proposition. *Il existe $x \in E$ tel que $\pi_u = \pi_{u,x}$.*

Démonstration. Soit $\pi_u = P_1^{m_1}...P_r^{m_r}$ la décomposition en irréductibles de π_u dans $\mathbb{K}[X]$. On note $K_i = \ker P_i^{m_i}(u)$ et $u_i = u_{|K_i}$. On remarque que $\pi_{u_i} = P_i^{m_i}$. Par le lemme des noyaux,

$$E = K_1 \oplus ... \oplus K_r.$$

On montre d'abord la proposition sur chaque sous-espaces K_i pour l'endomorphisme u_i. Soit $i \in \{1, ...r\}$. On suppose par l'absurde que pour tout $x_i \in K_i$, π_{u_i,x_i} est différent de π_{u_i}. Alors pour tout x_i, π_{u_i,x_i} divise strictement $\pi_{u_i} = P_i^{m_i}$. Comme P_i est irréductible, π_{u_i,x_i} divise $P_i^{m_i-1}$. Ainsi $P_i^{m_i-1}(u_i)(x_i) = 0$, pour tout $x_i \in K$, et donc $P_i^{m_i-1}(u_i)$ est nul sur K_i. C'est absurde par minimalité du polynôme $\pi_{u_i} = P_i^{m_i}$. On dispose donc d'éléments x_i comme dans l'énoncé sur chaque sous-espaces K_i.
Soit $x = x_1 + ... + x_r$. Vérifions que x convient, c'est à dire que $\pi_u = \pi_{u,x}$. On a déjà que $\pi_{u,x}$ divise π_u, montrons la réciproque. D'une part, $\pi_{u,x}(u)(x) = 0$, par définition de $\pi_{u,x}$. D'autre part, $\pi_{u,x}(u)(x) = \pi_{u,x}(u)(x_1) + ... + \pi_{u,x}(u)(x_r)$, par linéarité. Comme $E = K_1 \oplus ... \oplus K_r$, et les sous-espaces K_i sont stables par $\pi_{u,x}(u)$, on déduit que pour tout i, $\pi_{u,x}(u)(x_i) = 0$ donc

$\pi_{u,x}(u_i)(x_i) = 0$. Ainsi, pour tout i, $\pi_{u_i,x_i} = \pi_{u_i} = P_i^{m_i}$ divise $\pi_{u,x}$. Comme les P_i sont premiers entre eux, $\pi_u = P_1^{m_1}...P_r^{m_r}$ divise $\pi_{u,x}$. □

Définition. On dit qu'un endomorphisme u est cyclique s'il existe $x \in E$ tel que $E = \mathbb{K}[u]x$.

Remarque. Cela équivaut à dire que le degré de π_u est la dimension de E, et donc que $\pi_u = \chi_u$. En effet, soit $x \in E$ tel que $E = \mathbb{K}[u]x$. Alors d'après la première proposition, $\dim E = \dim \mathbb{K}[u]x = \deg\pi_{u,x}$. Or $\pi_{u,x}$ divise π_u donc $\dim E = \deg\pi_{u,x} \leq \deg\pi_u$, mais on a toujours $\deg\pi_u \leq \dim E$, d'où ici $\deg\pi_u = \dim E$
Réciproquement, soit $x \in E$ tel que $\pi_u = \pi_{u,x}$. Comme $\deg\pi_u = \dim E$, alors $\deg\pi_{u,x} = \dim E$. Or par la première proposition, $\mathbb{K}[u]x$ est de dimension le degré de $\pi_{u,x}$, donc $E = \mathbb{K}[u]x$ et l'endomorphisme u est cyclique.

Développement

Théorème. *Il existe une suite $E_1, ...E_r$ de sous-espaces vectoriels de E et une unique suite $P_1, ...P_r$ de polynômes unitaires de $\mathbb{K}[X]$ telles que :*

1. *les E_i sont stables par u et $E = E_1 \oplus ... \oplus E_r$,*
2. *pour $i \in \{1, ...r\}$, l'endomorphisme $u_{|E_i}$ est cyclique et son polynôme minimal est P_i,*
3. *$P_r \mid ... \mid P_1$.*

Les polynômes $P_1, ...P_r$ sont appelés invariants de similitude de l'endomorphisme u.

Remarque. $P_1 = \pi_u$ et $\chi_u = P_1...P_r$.

Démonstration.
Existence [H2G2] :

On note d le degré de π_u. Soit $x \in E$ tel que $\pi_u = \pi_{u,x}$. Soit $E_1 = \text{Vect}\{x, ...u^{d-1}(x)\}$. Cet espace est stable par u et $u_{|E_1}$ est cyclique. Les polynôme minimaux de $u_{|E_1}$ et u sont tous les deux de degré d et sont donc les mêmes, on pose $P_1 = \pi_u = \pi_{u_{|E_1}}$. On va montrer que E_1 admet un supplémentaire stable par u. car $\pi_{u|E_1} \mid \pi_u$

Soit $\phi \in E^*$ une forme linéaire telle que $\phi(x) = ... = \phi(u^{d-2}(x)) = 0$ et $\phi(u^{d-1}(x)) = 1$. La famille $(\phi, \phi \circ u, ...\phi \circ u^{d-1})$ est une famille libre de E^* (se montre classiquement). On note Φ le sous-espace engendré par cette famille. On pose

$$F = \Phi^\circ = \{y \in E,\ \forall \psi \in \Phi,\ \psi(y) = 0\}.$$

Montrons que G est un supplémentaire de E_1 stable par u.

F est stable par u : Soit $y \in F$. On veut montrer que $u(y) \in F$, c'est à dire que $\phi(u(y)) = ... = \phi \circ u^{d-1}(u(y)) = 0$
Comme $y \in F$, on a que $\phi(y) = \phi(u(y)) = ... = \phi \circ u^{d-2}(u_y) = 0$ et il reste à montrer que $\phi(u^d(y)) = 0$. Comme π_u est de degré d, $u^d(y) \in \text{Vect}(y, ...u^{d-1}(y))$. On vient de voir que ϕ s'annule sur chacun de ces vecteurs, donc $\phi(u^d(y)) = 0$.

$E_1 \cap F = \{0\}$: Soit $y \in E_1 \cap F$. Comme $y \in E_1$, y s'écrit $y = a_0x + ... + a_{d-1}u^{d-1}(x)$. Et comme $y \in F$, en appliquant $\phi \circ u^i$ pour i allant de 0 à $d-1$ à l'écriture de y précédente et en utilisant le définition de ϕ, on obtient successivement $a_{d-1} = 0, ...a_0 = 0$ donc $y = 0$.

$\dim E_1 + \dim F = n$: Cela vient du fait que $\dim \Phi + \dim \Phi^\circ = n$ et $\dim \Phi = d = \dim E_1$, $\dim \phi^\circ = \dim F$.

F est donc bien un supplémentaire de E_1 stable par u.

On conclut la preuve en raisonnant par récurrence sur $\dim E$. L'initialisation pour $\dim E = 1$ est claire. Ensuite, on suppose que le théorème est vrai pour les endomorphismes d'espaces vectoriels de dimension inférieure ou égale à $n-1$. On peut donc l'appliquer à $u_{|F}$, et on obtient des polynômes unitaires $P_2, ...P_r$ et des sous espaces vectoriels $E_2, ...E_r$ vérifiant :

1. les espaces $E_2, ...E_r$ sont stables par $u_{|F}$ donc par u, et $F = E_2 \oplus ... \oplus E_r$ donc $E = E_1 \oplus ... \oplus E_r$.
2. pour $i \in \{2, ...r\}$, l'endomorphisme $\left(u_{|F}\right)_{|E_i} = u_{|E_i}$ est cyclique et son polynôme minimal est P_i. (On a vu au début de la preuve que c'était aussi bon pour $i = 1$).
3. $P_r \mid ... \mid P_2$. On a posé $P_1 = \pi_u$. Comme le polynôme minimal de $u_{|F}$ est P_2 , et que $\pi_u(u_{|F}) = 0$, on déduit que P_2 divise P_1.

Unicité [Gourdon] :

On suppose l'existence d'une autre famille $Q_1, ...Q_s$ et d'une autre décomposition $E = F_1 \oplus ... \oplus F_s$ comme dans le théorème. On a déjà que $P_1 = Q_1 = \pi_u$.

Soit j_0 le premier indice tel que $P_{j_0} \neq Q_{j_0}$. Un tel indice existe toujours même si $r \neq s$ car $\sum_i \deg P_i = n = \sum_j \deg Q_j$.

Comme pour $k \geq j_0$, $P_{j_0}(u)(E_k) = 0$ (du fait du troisième point du théorème), et par la décomposition $E = E_1 \oplus ... \oplus E_r$ avec les E_i stables par u, on déduit que pour $k \geq j_0$,

$$P_{j_0}(u)(E) = P_{j_0}(u)(E_1) \oplus ... \oplus P_{j_0}(u)(E_{j_0-1}). \quad (1)$$

Ensuite, de la décomposition $E = F_1 \oplus ... \oplus F_s$ avec les F_i stables par u, on déduit que

$$P_{j_0}(u)(E) = P_{j_0}(u)(F_1) \oplus ... \oplus P_{j_0}(u)(F_{j_0-1}) \oplus P_{j_0}(u)(F_{j_0}) \oplus ... \oplus P_{j_0}(u)(F_s). \quad (2)$$

Mais pour $i < j_0$, $P_i = Q_i$ donc il existe une base $\mathcal{B}_i$ de E_i et une base $\mathcal{B}'_i$ de F_i dans lesquelles les matrices de $u_{|E_i}$ et de $u_{|F_i}$ sont les mêmes ($C_{P_i} = C_{Q_i}$).

Ainsi, pour $i < j_0$, $\dim P_{j_0}(u)(E_i) = \dim P_{j_0}(u)(F_i)$.

Puis, en prenant les dimensions dans (1) et (2), on obtient que

$$\dim P_{j_0}(u)(F_{j_0}) = ... = \dim P_{j_0}(u)(F_s) = 0,$$

donc

$$P_{j_0}(u)(F_{j_0}) = ... = P_{j_0}(u)(F_s) = \{0\}.$$

Ainsi, Q_{j_0} divise P_{j_0}, et par symétrie, P_{j_0} divise Q_{j_0}, donc $P_{j_0} = Q_{j_0}$, ce qui est absurde. Finalement, $r = s$ et $P_i = Q_i$ pour tout i. □