

Décomposition de Frobenius

CloudSea

Cadre

Soit f un endomorphisme de E , il existe une décomposition $E = F_1 \oplus \cdots \oplus F_r$ en sous espaces stables telle que

1. pour tout i , l'induit f_{F_i} sur F_i est cyclique
2. pour tout i , le polynôme minimal μ_i de f_{F_i} vérifie $\mu_{i+1} | \mu_i$

A mettre dans le plan

il existe x tel que $\mu_f = \mu_{f,x}$ (voir plus loin pour la preuve)

Recasages :

- [[150 Réduction d'endomorphismes]]
- [[151 Sous espaces stables]]
- [[154 Décompositions de matrices]]
- [[159 Dualité]]

Référence : Goudron algèbre

Déroulé du développement

Montrer l'existence

Soit $d = \deg(\mu_f)$ et x tel que $\mu_f = \mu_x$

$F = \text{Vect}(f^k(x))_{k \in \mathbb{N}}$ est alors un sous espace de dimension d stable par f , et $(x, f(x), \dots, f^{d-1}(x))$ en est une base. Notons la $(e_1, \dots, e_{d-1})$ et complétons la en $\mathcal{B} = (e_1, \dots, e_n)$ une base de E

On introduit $G = \Gamma^\circ$ où $\Gamma = \{e_d^* \circ f^k, k \in \mathbb{N}\}$

Dit autrement G est l'ensemble des x dont la d -e coordonnée de $f^k(x)$ dans $\mathcal{B}$ est nulle pour tout k

C'est un sev de E stable par f , montrons que $E = F \oplus G$

Soit $y \in F \cap G$

$y \in F$, donc y s'écrit $y = \sum_{k=1}^d \lambda_k e_k$

Si $y \neq 0$, on a un k maximal tel que $\lambda_k \neq 0$

On a alors

$$0 = e_d^*(f^{d-k}(y)) = e_d^*\left(\sum_{i=1}^k \lambda_i f^{d-k}(e_i)\right) = e_d^*\left(\sum_{i=1}^k \lambda_i e_{i+d-k}\right) = \lambda_k$$

Absurde, donc on a $F \cap G = \{0\}$

Soit $\varphi : \mathbb{K}[f] \rightarrow \text{Vect}(\Gamma)$ $g \mapsto e_d^* \circ g$, on va montrer que c'est un iso

Déjà φ est surjective par définition de Γ

Soit $v \in \ker(\varphi)$, g s'écrit $g = \sum_{k=1}^d \lambda_k f^{k-1}$

Si $g \neq 0$, on a un k maximal tel que $\lambda_k \neq 0$, on a alors

$$0 = e_d^*(g(f^{d-k}(x))) = e_d^*\left(\sum_{i=1}^d \lambda_i f^{d-k+i-1}(x)\right) = e_d^*\left(\sum_{i=1}^d \lambda_i e_{d-k+i}\right) = \lambda_k$$

Absurde, donc φ est injective, donc c'est un iso

Donc $\dim(\text{Vect}(\Gamma)) = \dim(\mathbb{K}[f]) = d$, donc $\dim(G) = \dim(\Gamma^\circ) = n - d$

Donc on a bien $E = F \oplus G$

Soit μ_2 le polynôme minimal de f_G , on a $\mu_2 | \mu_u = \mu_1$

En itérant la construction jusqu'à obtenir $G = \{0\}$, on obtient bien la décomposition voulue

Montrer l'unicité

Soient $E = F_1 \oplus \dots \oplus F_r = G_1 \oplus \dots \oplus G_s$ deux décompositions, avec $r \leq s$

Notons $P_1, \dots, P_r$ les polynômes minimaux des induits sur les F_i et $Q_1, \dots, Q_s$ ceux des G_i

On va montrer par récurrence que $P_k = Q_j$ pour tout $j \leq r$

$j = 1$

Par construction, P_1 est un polynôme annulateurs de f , donc multiple de μ_f , et pour P de degré inférieur strict à P_1 , P n'annule pas f_{F_1} , donc n'annule pas f . Donc $P_1 = \mu_f$, et de même $Q_1 = \mu_f$, donc on a bien $P_1 = Q_1$

$j - 1 \rightarrow j$

On a pour tout $k \geq j$, $P_j(f)(F_k) = \{0\}$

Et les F_i sont stables par par f donc on a

$$P_j(f)(E) = P_j(f)(F_1) \oplus \cdots \oplus P_j(f)(F_{j-1})$$

De même, on a

$$P_j(f)(E) = P_j(f)(G_1) \oplus \cdots \oplus P_j(f)(G_s)$$

Or par HR, pour tout $i < j$, les induits sur F_i et G_i sont semblables (ils s'écrivent avec la même matrice compagnon dans des bases adaptées) donc en passant aux dimensions dans la 2e égalité on obtient

$$0 = \dim(P_j(f)(G_j)) = \cdots = \dim(P_j(f)(G_s))$$

donc P_j est un polynôme annulateur de f_{G_j} , donc est multiple de Q_j

Et on montre de la même manière que Q_j est multiple de P_j , et que donc $P_j = Q_j$

En déduire la décomposition de Frobenius

f est cyclique sur chaque F_i , donc on a $x_1, \dots, x_r$ tels que pour tout i , $\mathcal{B}_i = (x_i, f(x_i), \dots, f^{d_i-1}(x_i))$ est une base de F_i où d_i est la dimension de F_i

Par construction, on a vu que d_i est le degré du polynôme minimal de f_{F_i} , donc ce polynôme s'écrit $\mu_i = X^{d_i} + \sum_{k=0}^{d_i-1} \lambda_k X^k$, donc la matrice de f_{F_i} dans la base $\mathcal{B}_i$ correspond à la matrice compagnon de μ_i

Donc en concaténant ces bases, on obtient une base dans laquelle la matrice de f s'écrit $C(\mu_1) \oplus \cdots \oplus C(\mu_r)$

Détail de certains points

Montrer qu'il existe x tel que $\mu_f = \mu_x$

Soit $x \in E$, on note μ_x le générateur unitaire de l'idéal des polynômes P tels que $P(f)(x) = 0$

Soit d son degré, $(x, f(x), \dots, f^{d-1}(x))$ est alors une base de $E_x = \{P(f)(x); P \in \mathbb{K}[X]\}$

lemme 1 : Soient x, y tels que $E_x \cap E_y = \{0\}$, montrons que μ_{x+y} est le ppcm de μ_x et μ_y

Soit P le ppcm de μ_x et μ_y

On a P est multiple de μ_x et μ_y donc $P(f)(x) = P(f)(y) = 0$, donc $P(f)(x+y) = 0$, donc μ_{x+y} divise P

Et on a $\mu_{x+y}(x+y) = 0$, donc $\mu_{x+y}(x) = -\mu_{x+y}(y)$, donc comme $E_x \cap E_y = \{0\}$, les deux sont nuls, et donc μ_{x+y} est multiple de μ_x et μ_y donc de leur ppcm

Donc on a bien $\mu_{x+y} = P$

Soit maintenant $x_1, \dots, x_p$ et x leur somme. Si les E_{x_i} sont en somme directe, on obtient par récurrence immédiate en utilisant l'associativité du ppcm que μ_x est le ppcm des μ_{x_i}

lemme 2 : Si μ_x et μ_y sont premiers entre eux, montrons que $E_{x+y} = E_x \oplus E_y$

Soit $z \in E_x \cap E_y$, on a $P, Q \in \mathbb{K}[X]$ tels que $z = P(f)(x) = Q(f)(y)$

On a alors

$$0 = (P\mu_x)(f)(x) = \mu_x(f)(z) = (\mu_x Q)(f)(y)$$

Donc μ_y divise $\mu_x Q$, donc divise Q , donc $Q(y) = 0$, donc $z = 0$

Et par le lemme précédent, on a que μ_{x+y} est le ppcm de μ_x et μ_y , donc leur produit car ils sont premiers entre eux, donc

$$\dim(E_{x+y}) = \deg(\mu_{x+y}) = \deg(\mu_x \mu_y) = \deg(\mu_x) + \deg(\mu_y) = \dim(E_x) + \dim(E_y)$$

Le même raisonnement donne la généralisation pour p vecteurs

lemme 3 : Soit M un facteur irréductible de μ et α tel que $\mu = M^\alpha N$ avec M qui divise pas N , montrons qu'il existe $x \in \ker(M^\alpha(f))$ tel que $\mu_x = M^\alpha$

Si par l'absurde il n'existe pas de tel x , alors pour tout $x \in \ker(M^\alpha(f))$, on a $\mu_x | M^{\alpha-1}$, donc $\ker(M^\alpha(f)) \subseteq \ker(M^{\alpha-1}(f))$

Donc le lemme des noyaux donne

$$E = \ker(M^\alpha(f)) \oplus \ker(N(f)) = \ker(M^{\alpha-1}(f)) \oplus \ker(N(f))$$

Et donc $M^{\alpha-1}N$ est un polynôme annulateur de f , absurde

Plus qu'à assembler toutes les pièces :

Soit $\mu = M_1^{\alpha_1} \cdots M_p^{\alpha_p}$ la décomposition en irréductibles de μ

Par lemme 3 il existe $x_1, \dots, x_p$ tels que $\mu_{x_i} = M_i^{\alpha_i}$ pour tout i

Soit x leur somme, on a donc par lemme 2 $E_x = E_{x_1} \oplus \cdots \oplus E_{x_p}$

Donc par lemme 1, μ_x est le ppcm des μ_{x_i} , donc vaut leur produit, donc $\mu_x = \mu$

Version révisions

Soit f un endomorphisme de E , on se propose de montrer qu'il existe une décomposition de E en sous espaces stables $E = F_1 \oplus \cdots \oplus F_r$ tels que les induits f_i sur les F_i sont cycliques, et pour tout i le polynôme minimal μ_i de u_i vérifie $\mu_{i+1} | \mu_i$

On va faire une récurrence forte sur n la dimension de E

Soit $d = \deg(\mu_f)$, on admet qu'il existe x tel que $\mu_f = \mu_{f,x}$

$F = \text{Vect}(f^k(x))_{k \in \mathbb{N}}$ est alors un sous espace de dimension d stable par f , et $(x, f(x), \dots, f^{d-1}(x))$ en est une base. Notons la $(e_1, \dots, e_{d-1})$ et complétons la en $\mathcal{B} = (e_1, \dots, e_n)$ une base de E

On introduit $G = \Gamma^\circ$ où $\Gamma = \{e_d^* \circ f^k, k \in \mathbb{N}\}$

1. Montrer par l'absurde que $F \cap G = \{0\}$
2. Montrer que $\varphi : \mathbb{K}[f] \rightarrow \text{Vect}(\Gamma) \ v \mapsto e_d^* \circ v$ est un isomorphisme en reprenant le même principe
3. En déduire que $E = F \oplus G$ par un argument de dimension
4. En déduire l'existence de $E = F_1 \oplus \cdots \oplus F_r$ en appliquant l'hypothèse de récurrence
5. En déduire une version matricielle de la décomposition de Frobénius