Concours Agrégation, Mathématiques générales

Leçon 54- Sous-espaces stables d'un endomorphisme ou une famille d'endomorphismes en dimension finie. Applications.

Commentaires du jury 2015 : Les candidats doivent s'être interrogés sur les propriétés de l'ensemble des sous-espaces stables par un endomorphisme. Des études détaillées de cas sont les bienvenues, par exemple le cas d'une matrice diagonalisable, le cas d'une matrice nilpotente d'indice maximum. La décomposition de Frobenius trouve tout à fait sa place dans la leçon. Notons qu'il a été ajouté à l'intitulé la notion de familles d'endomorphismes. Ceci peut déboucher par exemple sur des endomor- phismes commutant entre eux ou sur la théorie des représentations.
Commentaires du jury 2016 : Dans cette leçon, il faut présenter des propriétés de l'ensemble des sous-espaces stables par un endomorphisme. Des études détaillées sont les bienvenues, par exemple le cas d'une matrice diagonalisable ou le cas d'une matrice nilpotente d'indice maximum. La décomposition de Frobenius trouve tout à fait sa place dans cette leçon. Il ne faut pas oublier d'examiner le cas des sous-espaces stables par des familles d'endomorphismes. Ceci peut déboucher par exemple sur des endomorphismes commutant entre eux ou sur la théorie des représentations.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
Errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
Compléments et errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. B-C-D] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)

Développements conseillés :

(1) Diagonalisation et trigonalisation simultanée, [Fr. A] p. 235-236.
(2) Décomposition de Frobenius, [F. M. 2] p. 11.
(3) Soit $G \to GL_n(k)$ une représentation linéaire d'un groupe fini G avec $(\operatorname{car} k, |G|) = 1$ si $\operatorname{car} k > 0$ et W un sous espace stable par G alors W admet un supplémentaire stable par G. Application à la décomposition en somme directe de représentations irréductibles, [F. M. 1] par. 4.1 et 4.2 p. 202 et 211. Application : le groupe fini G est abélien si et seulement si ses caractères irréductibles sont de degré 1. Enfin si A est un sous-groupe commutatif de G alors toute représentation irréductible de G est de degré $\leq \frac{|G|}{|A|}$, [F. M. 2] p. 171-172.

Exercice 1 Soit $E \neq \{0\}$ un k-espace vectoriel de dimension finie et $u \in End_k(E)$. On suppose qu'il existe $x \in E$ avec $E = k[u](x)$. Soit $F \subset E$ un sous-espace stable par u. On note v resp. w l'endomorphisme de F resp. $\frac{E}{F}$ induit par u. On rappelle que $ppcm(m_v, m_w) | m_u | m_v m_w$ où m_u, m_v, m_w désignent les polynômes minimaux de u, v, w.

(1) Rappeler pourquoi on a $\chi_u = \chi_v \chi_w$ où χ_u est le polynôme caractéristique de u.
Preuve. Soit B une base de F que l'on complète en une base de E en relevant une base B' de E/F. Il suit que la matrice de u dans cette base est triangulaire supérieure par blocs avec sur la diagonale un bloc constitué de la matrice de v dans B et un bloc qui est la matrice w dans la base B'. Il suit que $\chi_u = \chi_v \chi_w$ (développement du déterminent d'une matrice triangulaire par blocs). ///
(2) Montrer que $\chi_v = m_v$ et en déduire que F est un sous-espace monogène de (E, u).
Preuve. On a $\chi_u = m_u | m_v m_w | \chi_v \chi_w = \chi_u$ ainsi $m_u | m_v m_w$ et donc $1 = \frac{\chi_u}{m_u} = \frac{\chi_v}{m_v} \frac{\chi_w}{m_w}$ ce qui avec Cayley-Hamilton est une identité polynomiale et montre que $\chi_v = m_v$ mais aussi $\chi_w = m_w$ et donc

que (F,v) et $(\frac{E}{F},w)$ sont monogènes. Ainsi il existe $y\in F$ avec $F=k[v](y)$ et donc $F=k[u](y)$ est un sous-espace monogène de (E,u).///

(3) Montrer qu'il existe $P\in k[X]$ avec $F=P(u)k[u](x)$ et en déduire que $F=P_F(u)k[u](x)$ avec $P_F\in k[X]$ unitaire et $P_F|m_u$ (considérer le PGCD de P et de m_u).

Preuve. On a $F=k[u](y)$. Puisque $E=k[u](x)$ il suit que $y=P(u)(x)$ où $P\in k[X]$. Ainsi $F=P(u)k[u](x)$. Soit $\delta=PGCD(P,m_u)$, alors $\delta(u)k[u]=P(u)k[u]+m_u(u)k[u]=P(u)k[u]$. Ainsi $P_F:=\delta$ convient. ///

(4) En considérant $I_F:=\{Q\in k[X]\mid Q(u)(F)=0\}$, montrer que $P_F=\frac{m_u}{m_v}$. Ainsi $F=k[u](\frac{m_u}{m_v})(u)(x)$.

Preuve. Puisque $Q(u)(F)=0$ équivaut à $Q(u)P_F(u)(x)=0$, c'est à dire à $m_u|QP_F$, il suit que $I_F=\frac{m_u}{P_F}k[X]$, ainsi $m_v=\frac{m_u}{P_F}$. ///

(5) Soit $D\in k[X]$ un diviseur unitaire de m_u et $F:=k[u](y)$ avec $y=P(u)(x)$ et $P:=\frac{m_u}{D}$. Montrer que $m_v=D$ où v est l'endomorphisme de F induit par u.

Preuve. On applique ce qui précède à F et $P_F:=P$. ///

(6) Exprimer le cardinal de l'ensemble des sous-espaces de E stables par u en fonction de la décomposition en irréductibles de m_u

Preuve. Puisque les sous-espaces stables de E sont en bijection avec les diviseurs unitaires de m_u, il suffit de remarquer que m_u n'a qu'un nombre fini de diviseurs unitaires. Notez que si $m_u=\prod_{1\le i\le s}P_i^{\alpha_i}$ est la décomposition en irréductibles de m_u alors ce nombre est $\prod_{1\le i\le s}(\alpha_i+1)$. ///

(7) Caractériser les espaces monogènes (E,u) qui admettent seulement deux sous-espaces stables.

Preuve. D'abord $E\neq 0$, ainsi $m_u\neq 1$. Par la question précédente ce sont les espaces monogènes tels que m_u est irréductible. ///

(8) *S*upplémentaire stable. Pour une généralisation voir [F. M. 2] par. 1.3.2. p. 18.

(a) Soit $F\subset E$ un sous-espace stable par u et v l'endomorphisme de F induit par u. Montrer que si F admet un supplémentaire G qui est stable par u alors $(m_v,\frac{m_u}{m_v})=1$.
Preuve. Si $E=F\bigoplus G$ avec G stable par u et si w est la restriction de u à G alors $\chi_u=\chi_v\chi_w$ et $m_u=ppcm(m_v,m_w)$. Puisque (E,u), (F,v) et (G,w) sont des espaces monogènes par les questions précédentes, il suit que $m_u=m_vm_w$ et que $(m_v,m_w)=1$. ///

(b) Réciproquement soit $F\subset E$ un sous-espace stable par u et v l'endomorphisme de F induit par u. On suppose que $(m_v,\frac{m_u}{m_v})=1$, montrer que F admet un et un seul supplémentaire G qui est stable par u.
Preuve. Par (4) $F=k[u](\frac{m_u}{m_v})(u)(x)$. Soit $G:=k[u](m_v)(u)(x)$ alors si w désigne l'endomorphisme de G induit par u, avec (4) on a $m_w=\frac{m_u}{m_v}$. Soit $x\in F\cap G$ alors $m_v(u)(x)=0$ et $m_w(u)(x)=0$ et puisque $1=Am_v+Bm_w$ pour $A,B\in k[X]$ il suit que $x=0$. Puisque $\deg m_v+\deg m_w=\deg m_u=\dim E$, il suit que $E=F\bigoplus G$. L'unicité du supplémentaire stable suit de la caractérisation d'un sous-espace stable G de E par le polynôme minimal de l'endomorphisme de G induit par u. ///

(c) Dénombrer les sous-espaces stable de E qui admettent un supplémentaire stable.
Preuve. Cela revient à compter le cardinal de $\mathcal{P}:=\{P\in k[X],P|m_u,\ pgcd(P,\frac{m_u}{P})=1$ et unitaires. Si $m_u=\prod_{1\le i\le s}P_i^{\alpha_i}$ est la décomposition en irréductibles de m_u, on note pour P unitaire qui divise m_u, $I_P:=\{i,\ \mid 1\le i\le s,\ P_i|P\}$. Si $P\in\mathcal{P}$ alors $P_i|P$ si et seulement si $P_i^{\alpha_i}|P$; ainsi $P=\prod_{i\in I_P}P_i^{\alpha_i}$. Il suit que l'application qui à $P\mathcal{P}$ associe I_P définit une bijection de $\mathcal{P}$ sur l'ensemble des parties de $\{1\le i\le s\}$; ainsi $|\mathcal{P}|=2^{s+1}$. ///
Remarque. *Ce calcul rappelle le dénombrement des idempotents de l'algèbre $k[u]$. De fait si $e\in k[u]$ est un idempotent de $k[u]$, alors $E=F\bigoplus G$ avec $F=eE$ et $G=(1-e)E$. Réciproquement si $E=F\bigoplus G$ avec F,G des sous-espaces stables alors $F=k[u](\frac{m_u}{m_v})(u)(x)$ et $G:=k[u](m_v)(u)(x)$ avec $m_v|m_u$ et $(m_v,\frac{m_u}{m_v})=1$. Soit $1=Am_v+B\frac{m_u}{m_v})$ avec $A,B\in k[X]$ alors si $1-e:=(Am_v)(u)$ alors $e=(B\frac{m_u}{m_v})(u)$ est un idempotent et $(1-e)E=A(u)G\subset G$ et $eE=B(u)F\subset F$. Puisque $E=F\bigoplus G$, il suit que l'on a les égalités $F=eE$ et $G=(1-e)E$.*

On aurait pu aussi remarquer que $1 = Am_v \mod \frac{m_u}{m_v}$ *et ainsi* $A(u)$ *induit un automorphisme de* G.

(d) Montrer que (E, u) n'est pas somme directe de 2 sous-espaces stables non triviaux (on dit alors que E est indécomposable) si et seulement si m_u est puissance d'un irréductible.

Preuve. L'espace monogène (E, u) *est indécomposable ssi les seules décompositions en somme directe de sous-espaces stable sont* $E = E \bigoplus \{0\}$ *et* $E = \{0\} \bigoplus E$ *i.e.* $s = 1$. ///

Exercice 2 Sur les endomorphismes u du K-espace vectoriel de dimension finie E tels que pour tout sous-espace $F \subset$ stable par u il existe $P \in K[X]$ avec $F = \operatorname{Ker} P(u)$, resp. $F = \operatorname{Im} P(u)$.

Soit E un k-espace vectoriel de dimension finie et $u \in \operatorname{End}_k(E)$. On note $m_u \in k[X]$ le polynôme minimal de u. On rappelle qu'il existe $x \in E$ tel que m_u est aussi le polynôme minimal m_x de la restriction de u à $k[u](x)$ (c'est le lemme fondamental).

(1) On suppose que pour tout sous-espace F stable par u il existe $P_F \in k[X]$ avec $F = \operatorname{Ker} P_F(u)$. Montrer que E est un espace monogène.

Preuve. Soit donc $x \in E$ *tel que* m_u *est aussi le polynôme minimal de la restriction de* u *à* $k[u](x)$ *et montrons que* $E = k[u](x)$. *Par hypothèse il existe* $P \in k[X]$ *avec* $k[u](x) = \operatorname{Ker} P(u)$. *Ainsi* $P(u)(x) = 0$ *et donc par définition de* m_x *on a* $P = Qm_x = Qm_u$ *et donc* $P(u)$ *est l'endomorphisme nul.///*

(2) On suppose que pour tout sous-espace F stable par u il existe $Q \in k[X]$ avec $F = \operatorname{Im} Q(u)$.

(a) Soit $Q \in k[x]$ et $\delta := PGCD(Q, m_u)$. Montrer que $Q(u)(E) = \delta(u)(E)$.

Preuve. Immédiat puisque $Id \in k[u]$ *il suit que* $k[u](E) = E$ *et donc* $\delta(u)(E) = (\delta(u)k[u])(E) = (Q(u)k[u] + m(u)k[u])(E) = Q(u)(E)$. *Ainsi si* $Q \neq 0$ *on peut supposer que* Q *divise* m_u. ///

(b) Montrer que E est un espace monogène.

Preuve. Soit donc $x \in E$ *tel que* m_u *est aussi le polynôme minimal de la restriction de* u *à* $k[u](x)$ *et montrons que* $E = k[u](x)$. *Si* $E = \{0\}$ *c'est bon. On suppose donc que* $E \neq \{0\}$. *Par hypothèse il existe* $Q \in k[X] - \{0\}$ *avec* $k[u](x) = \operatorname{Im} Q(u)$ *et par la question précédente on peut supposer que* $Q(X)$ *est unitaire et divise* m_u. *Ainsi* $x = Q(u)(y)$ *et donc* $\frac{m_u}{Q}(u)(x) = m_u(u)(y) = 0$. *Ainsi* m_x *divise* $\frac{m_u}{Q}$ *et puisque* $m_x = m_u$, *il suit que* $Q = 1$ *et donc* $\operatorname{Im} Q(u) = E$.///

Remarque. En utilisant l'exercice précédent on vérifie que si (E, u) est monogène alors si F est un sous-espace stable par u c'est le noyau et l'image de polynômes d'endomorphismes de u.

Exercice 3 Sur les sous-espaces d'un espace monogène qui admettent un supplémentaire stable. Pour une généralisation voir [F. M. 2] par. 1.3.2. p. 18.

Soit $E := K[u](x)$, un espace monogène de dimension finie. Soit $F \subset E$ un sous-espace stable et v la restriction de u à F. Montrer que F admet un supplémentaire stable ssi $(m_v, \frac{m_u}{m_v}) = 1$.

Preuve. Si $E = F \bigoplus G$ *avec* G *stable par* u *et si* w *est la restriction de* u *à* G *alors ([Fr. A] p. 143)* $\chi_u = \chi_v \chi_w$ *et* $m_u = ppcm(m_v, m_w)$. *Puisque* (E, u), (F, v) *et* (G, w) *sont des espaces monogènes (exercice précédent) il suit que* $m_u = m_v m_w$ *et que* $(m_v, m_w) = 1$.

La réciproque. Avec les notations de l'exercice précédent, soit $G := F_{\frac{m_u}{m_v}}$ *et* w *la restriction de* u *à* G. *Alors* $m_w = \frac{m_u}{m_v}$. *Soit* $x \in F \cap G$ *alors* $m_v(u)(x) = 0$ *et* $m_w(u)(x) = 0$ *et puisque* $1 = Am_v + Bm_w$ *pour* $A, B \in K[X]$ *il suit que* $x = 0$. *Puisque* $\deg m_v + \deg m_w = \deg m_u = \dim E$ *le résultat suit.* ///

Exercice 4 Le lemme fondamental, [F. M. 2] p. 12-14.

Soit E un k-espace vectoriel de dimension finie > 0. Soit $u \in End_k(E)$ un endomorphisme, $m_u = \prod P_i^{\alpha_i}$ pour $i = 1, ..., s$, la décomposition en irréductibles du polynôme minimal de u et E_i, le sous-espace caractéristique $\ker P_i(u)_i^{\alpha}$. On note u_i la restriction de u à E_i.

(1) Montrer que $P_i^{\alpha_i}$ est le polynôme minimal de u_i.
Preuve. Si $x_i \in E_i$, on a $P_i(u_i)_i^{\alpha}(x_i) = P_i(u)_i^{\alpha}(x_i) = 0$, ainsi $m_{u_i}|P_i^{\alpha_i}$. Soit $z := \sum_{1\leq i\leq s} x_i$ où $x_i \in E_i$, alors $[\prod_{1\leq i\leq s} m_{u_i}](u)(z) = \sum_{1\leq i\leq s}[\prod_{1\leq i\leq s} m_{u_i}](u)(z_i) = 0$, ainsi $m_u|\prod_{1\leq i\leq s} m_{u_i}|\prod_{1\leq i\leq s} P_i^{\alpha_i}$. Puisque $m_u = \prod P_i^{\alpha_i}$, il suit que $m_u = \prod_{1\leq i\leq s} m_{u_i} = \prod P_i^{\alpha_i}$ et puisque $m_{u_i}|P_i^{\alpha_i}$ on a l'égalité par l'unicité de la décomposition en irréductibles.

(2) En déduire l'existence de $x_i \in E_i$ tel que $P_i(u)^{\alpha_i - 1}(x_i) \neq 0$.
Preuve. Puisque $m_{u_i} = P_i^{\alpha_i}$ alors $P_i^{\alpha_i-1}\|m_{u_i}$ et donc $P_i^{\alpha_i-1}(u_i) =\neq 0$.

(3) Montrer que $F_i := k[u_i](x_i)$ est un sous-espace monogène de E et que le polynôme minimal de u restreint à F_i est $m_{x_i} := P_i^{\alpha_i}$
Preuve. On a $P_i(u)^{\alpha_i}(x_i) = 0$, ainsi $m_{x_i}|P_i^{\alpha_i}$ et donc $m_{x_i} = P_i^{\beta_i}$ avec $\beta_i \leq \alpha_i$ (P_i est irréductible!). Puisque $P_i(u)^{\alpha_i-1}(x_i) \neq 0$, il suit que $\beta_i > \alpha_i - 1$ et donc $\beta_i = \alpha_i$.

(4) Montrer que si $z = x_1 + ... + x_s$ et si $P \in k[x] - \{0\}$ vérifie $0 = P(u)(z)$ alors m_u divise P.
Preuve. On a $0 = P(u)(z) = \sum_{1\leq i\leq s} P(u)(x_i)$, comme $E = \bigoplus_{1\leq i\leq s} E_i$, il suit que $P(u)(x_i) = 0$ ainsi $\forall i,\ m_{x_i}|P$ et donc m_u divise P.

(5) En déduire que $m_z = m_u$.
Preuve. On applique la question précédente à $P = m_z$ ainsi $m_u|m_z$. Enfin $m_u(z) = 0$ et donc $m_z|m_u$. D'où l'égalité $m_z = m_u$.

Exercice 5 Supplémentaire stable et dualité, [F. M. 2] p. 14.

Exercice 6 Espaces caractéristiques.

Montrer que si $E = \bigoplus_{1\leq i\leq s} E_i$ est la décomposition en sous-espaces caractéristiques de (E, u) et si $F \subset E$ un sous-espace stable alors $F = \bigoplus_{1\leq i\leq s}(F \cap E_i)$

Exercice 7

Soient $E \neq \{0\}$ un $\mathbb{R}$-espace vectoriel de dimension finie et u un endomorphisme de E. Montrer qu'il existe un sous-espace de E stable par u avec $1 \leq \dim V \leq 2$, [Fr. B-C-D] lemme 5.1.2 p.11.

Exercice 8 Une application du théorème de la base incomplète, [F. M. 2] p. 1.

Soit E un k-espace vectoriel de dimension finie et $u \in End_k E$. Montrer les équivalences :
i) u est diagonalisable
ii) tout sous-espace F de E admet un supplémentaire stable par u.
Preuve. Pour i) implique ii) considérer une base $B := (e_i)_{1\leq i\leq n}$ qui diagonalise u et compléter une base de F par des vecteurs de B. Pour ii) implique i) construire une base de vecteurs propres en considérant des supplémentaires d'hyperplans.

Exercice 9 Endomorphismes semi-simples, [Fr. A.] p. 221.

Notez qu'il y a une caractérisation des matrices semisimples sur les corps finis : précisément, si $A \in M_n(F_q)$ alors ses valeurs propres sont dans F_{q^m} où $m = ppcm(2, \ldots, n)$, et il existe $P \in GL_n(F_q)$ tel que $P^{-1}AP$ estun tableau diagonal de blocs de Jordan $\lambda_i Id + N_i$ avec $1 \leq i \leq s$. Puisque $(\lambda_i Id + N_i)^{q^m} = \lambda_i Id$ (notez que $q^m > n$), ainsi A est semisimple ssi $A^{q^m} = A$.

Exercice 10 Espaces indécomposables sous un endomorphisme,[Fr. A.] exercice 4.7.6 p 189.

Exercice 11 Quelques calculs d'invariants de similitude, [F. M. 1] $n°12$ p. 19.

Exercice 12 La décomposition de Frobenius. Variante algorithmique pour le calcul des invariants de similitude.

On montre l'équivalence: $XId - A$ et $XId - B$ équivalentes modulo $GL_n(k[X])$ est équivalent à A et B semblables dans $M_n(k)$, [Fr. A.] exercice 4.7.7 p. 190.

Puis on utilise le pivot de Gauss dans $M_n(k[X])$ pour en déduire que $XId-A$ est équivalente à un tableau diagonal avec $P_1 = ... = P_{s-1} = 1|P_s(X)|P_{s+1}(X)|, ...|P_n(X)$ sur la diagonale avec $0 < degP_s$. Conclure en remarquant que la matrice caractéristique de la matrice compagne du polynôme P est équivalente à la matrice diagonale avec des 1 et P, [Fr. A.] p. 143.