

Développement : Réduction de Frobenius d'un endomorphisme

Thomas W.

21 juillet 2023

Leçons concernées :

- 122 : Anneaux principaux. Exemples et applications.***
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.****
- 148 : Exemples de décompositions de matrices. Applications.*****
- 151 : Dimension d'un espace vectoriel. Rang. Exemples et applications.*****
- 153 : Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.*****
- 154 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.*****
- 159 : Formes linéaires et dualité en dimension finie. Exemples et applications.*****

Références :

- Algèbre/Probabilités, X.Gourdon
- Nouvelles Histoires Hédonistes de Groupes et de Géométries (NH2G2), P.Caldero et J.Germoni

Excellent recasage pour ce très beau développement qui va j'en suis sûr vous réconcilier avec la dualité (et pourtant c'est pas gagné!). Seulement 3 étoiles pour la 122 car la primalité n'intervient que pour l'existence du polynôme minimal local, et éventuellement le fait que $\mathbb{K}[X]$ est factoriel... Pour la 141, 4 étoiles et pas 5 car on utilise l'irréductibilité de certains polynômes seulement au début de la preuve, pour prouver que le polynôme minimal s'accomplit en un polynôme minimal local. Cela me paraît peu par rapport à d'autres développements où l'irréductibilité est au centre du problème, comme par exemple l'irréductibilité des polynômes cyclotomiques, ou le dénombrement des polynômes irréductibles unitaire de degré fixé sur un corps fini. Mais 4 étoiles c'est pas mal quand même et vous pouvez ne pas être d'accord avec moi. Pour les autres recasages c'est assez clair qu'ils méritent

5 étoiles. Le recasage dans la 159 est vraiment très intéressant car c'est une belle application de la dualité. Je vais essayer de rédiger ce développement en motivant les démarches et les constructions que nous allons faire. Cela permet de prendre du recul sur la preuve et de retenir le développement plus facilement. J'aime beaucoup les Gourdon par leur exhaustivité sur les programmes, mais les preuves et corrections d'exercices manquent cruellement d'intuition. Je trouve les preuves vraiment dénaturées, et un étudiant n'ayant pas réussi qui doit se contenter de la correction (ce qui a souvent été mon cas) ne progresse en général pas. Cela se voit bien justement dans le Tome Algèbre sur la réduction de Frobenius où l'intervention de la dualité semble vraiment sortir de nulle part. L'exemple le plus flagrant reste l'exercice sur la suite $u_{n+1} = \sin(u_n)$ où il faut donner un équivalent dans le Tome Analyse, et où l'auteur félicite les étudiants ayant trouvé l'astuce mais n'explique aucunement comment on aurait pu y penser. Mais bon, si on devait expliquer à chaque fois les démarches les Gourdon feraient chacun plus de 1000 pages... Faites bien attention à prendre la version du Tome Algèbre avec la partie probabilités. J'ai adoré cette partie probabilité qui est vraiment très bien faite et qui donne du bon contenu pour les leçons de probabilités et la leçon de dénombrement.

Je commence ce document dans un style un peu de discussion, de présentation du problème, de quelques idées, etc... et je rédigerai une démonstration qui va à l'essentiel ensuite. Je précise que ce n'est peut-être pas la raison qui a poussé Frobenius à chercher une telle décomposition, j'ai juste essayé de motiver le problème. Ce sera peut-être très critiquable, je ne suis qu'un amateur.

Introduction :

Soit $\mathbb{K}$ un corps quelconque. On veut trouver une forme normale simple dans les orbites de $\mathcal{M}_n(\mathbb{K})$ sous l'action de $GL_n(\mathbb{K})$ par conjugaison, c'est-à-dire une matrice qui soit de forme assez simple, par exemple diagonale par blocs (ce sont souvent de telles formes qu'on cherche). Par exemple, si $\mathbb{K}=\mathbb{C}$, le polynôme caractéristique de toute matrice est scindé donc on peut appliquer la réduction de Jordan, et une forme normale simple est donc la réduite de Jordan. Sur $D_n(\mathbb{K})$ l'espace des matrices diagonalisables, une forme normale simple est la matrice diagonale formée des valeurs propres, (qui coïncide ici avec la réduite de Jordan). Une première idée serait de se ramener à la réduite de Jordan en plongeant $\mathbb{K}$ dans sa clôture algébrique $\overline{\mathbb{K}}$. On aurait alors que deux matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont $GL_n(\overline{\mathbb{K}})$ -semblables ssi elles ont la même réduite de Jordan. Comment se ramener dans $GL_n(\mathbb{K})$? Un exercice classique est de montrer que c'est vrai : pour toute extension $\mathbb{L}$ de $\mathbb{K}$, on a " $GL_n(\mathbb{K})$ semblables" $\iff$ " $GL_n(\mathbb{L})$ semblables". Je connais une preuve dans le cas où $\mathbb{K}$ est infini (C'est fait dans Gourdon). Mais dans le cas des corps finis, je n'en connais pas sans passer justement par les invariants

de similitudes. On démontrera tout ça après le développement. Donc pour l'instant, cette démarche n'est pas concluante. Cherchons en une autre. On va raisonner en termes d'endomorphismes et de bases.

Prenant E un $\mathbb{K}$ -espace vectoriel de dimension n et u un endomorphisme de E quelconque (aucune hypothèse supplémentaire), on cherche une décomposition de E en somme directe de sous-espaces stables par u . Les premiers sous-espaces stables par u qui nous viennent en tête sont les sous-espaces caractéristiques, mais on doit avoir que le polynôme caractéristique de u est scindé. Or, on ne veut faire aucune hypothèse sur u . D'autres sous-espaces stables sont les sous-espaces cycliques. Etant donné $x \in E$, le sous-espace cyclique de E associé à u et à x est $E_{u,x} = \text{Vect}(u^k(x), k \in \mathbb{N})$. Il est évidemment stable par u . Quelle est sa dimension ? Il existe un $d \in \mathbb{N}^*$ minimal tel que $(x, u(x), \dots, u^{d-1}(x))$ soit libre. On vérifie alors facilement que $E_{u,x} = \text{Vect}(u^k(x), k \in \{0, \dots, d-1\})$, et donc $\dim(E_{u,x}) = d$. Ce n'est pas sans rappeler la caractérisation du degré du polynôme minimal de u : $\deg(\mu_u) = \min \{d \in \mathbb{N}^*, (Id, u, \dots, u^{d-1}) \text{ est libre} \}$. De même ici, on définit le polynôme minimal local de u en x : l'ensemble $\{P(u)(x), P \in \mathbb{K}[X]\}$ est un idéal de $\mathbb{K}[X]$, qui est principal, donc il possède un unique polynôme unitaire de degré minimal qui l'engendre. On note ce polynôme $\mu_{u,x}$, qui est le polynôme minimal local de u en x . Si $d = \deg(\mu_{u,x})$, on a $\dim(E_{u,x}) = d$. Pour obtenir une décomposition de E en somme directe de sous-espaces stables par u , il suffit de trouver un supplémentaire stable par u de $E_{u,x}$ pour un certains $x \in E$, puis de raisonner par récurrence. La recherche de supplémentaire stable n'est pas du tout évidente. Pour l'instant, en prenant un supplémentaire, on peut écrire $E = E_{u,x} \oplus H$. On note $\mu_{u,x} = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0$. Une base de $E_{u,x}$ (qu'on peut qualifier de canonique à ce point) est $(x, u(x), \dots, u^{d-1}(x))$. On note

$$C_{\mu_{u,x}} = \begin{pmatrix} 0 & 0 & \cdots & \cdots & -a_0 \\ 1 & 0 & \cdots & \cdots & -a_1 \\ 0 & 1 & \ddots & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$$

la matrice compagnon associée au polynôme $\mu_{u,x}$. On vérifie alors que la matrice de u dans une base $\mathcal{B}$ de E , obtenue en concaténant $(x, u(x), \dots, u^{d-1}(x))$

à une base de H , est de la forme $\left(\begin{array}{c|c} C_{\mu_{u,x}} & B \\ \hline 0 & C \end{array} \right)$. Notons qu'à ce niveau

là, il n'y a plus qu'à se baisser pour démontrer le théorème de Cayley-Hamilton (passer au polynôme caractéristique et évaluer en x). Ce qu'on voudrait c'est trouver H tel que $B = 0$. Si on passe à la transposée, on aura que la matrice de ${}^t u$ dans la base duale $\mathcal{B}^*$ de $\mathcal{B}$ est de la forme $\left(\begin{array}{c|c} {}^t C_{\mu_{u,x}} & 0 \\ \hline {}^t B & {}^t C \end{array} \right)$. Si on arrive à avoir ${}^t B = 0$, alors c'est bon. On veut

donc que $Vect(x^*, u(x)^*, \dots, u^{d-1}(x)^*)$ soit stable par ${}^t u$. Malheureusement je n'arrive pas à pousser l'intuition dans ce sens plus loin, car je ne vois pas en quoi la recherche d'un tel x conduit à la preuve qu'on retrouve dans le Gourdon ou dans NH2G2. J'en suis assez déçu car jusque là je trouvais les démarches assez naturelles. Si vous arrivez à continuer la construction de la preuve avec l'interprétation matricielle à l'appui je suis preneur. On peut se consoler en se disant qu'au moins cette démarche nous fait penser au passage au dual. Poursuivons quand même. On cherche un sev H de dimension $n - d$ qui soit stable par u . Mais on a l'équivalence, pour un sev F de E , F est stable par $u \iff F^\perp$ est stable par ${}^t u$. Et ça va aussi dans le sens de l'orthogonal dans le sens du dual. Ainsi, on peut être tenté de réaliser H comme l'orthogonal d'un sev G de E^* de dimension d , qui soit stable par ${}^t u$. Un tel G va forcément dépendre de x car il dépend de d , qui dépend de x . Mais on peut refaire exactement ce qu'on a déjà fait au début car on connaît des sev de E^* stable par ${}^t u$: les sous-espaces cycliques. On cherche alors $\phi \in E^*$ telle que $G = Vect(\phi, {}^t u(\phi), \dots, ({}^t u)^{d-1}(\phi))$ soit stable par ${}^t u$, et tel que $E = E_{u,x} \oplus G^\circ$. Tout d'abord, il faut que $(\phi, {}^t u(\phi), \dots, ({}^t u)^{d-1}(\phi))$ soit libre dans E^* pour avoir un sev de E^* de dimension d . Soient alors $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{K}$ tels que $\lambda_0 \phi + \dots + \lambda_{d-1} ({}^t u)^{d-1}(\phi) = 0 \iff \lambda_0 \phi + \dots + \lambda_{d-1} \phi \circ u^{d-1} = 0$. Comme souvent, on évalue de telles égalités dans des espaces de fonctions en des éléments pour prouver que les scalaires sont nuls. Rappelons nous que G doit dépendre de x , donc que ϕ va dépendre de x . Nous sommes tentés d'évaluer en x . Ceci donne : $\lambda_0 \phi(x) + \dots + \lambda_{d-1} \phi(u^{d-1}(x)) = 0$. Quelle forme linéaire ϕ , qui dépends de x , considérer alors pour obtenir que tous les λ_i sont nuls? Une idée qui vient naturellement est $\phi = x^*$ (on considère la base duale de E constituée des vecteurs de $(x, u(x), \dots, u^{d-1}(x))$ complétée en une base quelconque. x^* est alors la projection sur la coordonnée en x dans cette base). On obtient alors $\lambda_0 = 0$ et c'est un bon début. Ceci donne $\lambda_1 \phi \circ u + \dots + \lambda_{d-1} \phi \circ u^{d-1} = 0$. Le seul moyen de refaire apparaître x est d'évaluer en $u(x)$ pour avoir $u^{d-1}(u(x)) = u^d(x) = -a_{d-1}u^{d-1}(x) - \dots - a_1 u(x) - a_0 x = 0$. L'évaluation en $u(x)$ va alors donner $a_0 \lambda_{d-1} = 0$. Il nous faudrait avoir a_0 non nul, mais rien ne le garantit. $\phi = x^*$ est à priori non concluant. Essayons en un autre : le deuxième dans la base duale, c'est-à-dire $\phi = u(x)^*$. L'évaluation en x va donner cette fois $\lambda_1 = 0$. Puis l'évaluation en $u(x)$ va donner $\lambda_0 - \lambda_{d-1} a_1 = 0$. Nous sommes de nouveaux coincés. Mais c'est encore à cause de ce λ_{d-1} . On peut commencer par montrer que $\lambda_{d-1} = 0$ en prenant $\phi = u^{d-1}(x)^*$. Et c'est ce ϕ là qui va fonctionner : en évaluant successivement en $x, u(x), \dots, u^{d-1}(x)$, on montre que les λ_i sont tous nuls et donc que la famille $(\phi, {}^t u(\phi), \dots, ({}^t u)^{d-1}(\phi))$ est libre dans E^* .

Le sev G de E^* engendré par cette famille est-il stable par ${}^t u$? Il suffit d'avoir $({}^t u)^d(\phi) \in G$. Cela arrive ssi le degré du polynôme minimal local de ${}^t u$ en ϕ est de degré inférieur ou égal à d . On cherche donc $P \in \mathbb{K}[X]$ de degré inférieur ou égal à d tel que $P({}^t u)(\phi) = 0$. On pense bien sûr tout de

suite à $\mu_{u,x}$ qui est de degré d . Mais cela ne donne rien, car cela revient à regarder $\mu_{u,x}(\phi)$, dont on ne sait rien dire. Cependant, on sait que pour tout $P \in \mathbb{K}[X]$, $P({}^t u) = {}^t P(u)$ donc u et ${}^t u$ admettent le même idéal annulateur, en particulier ils ont le même polynôme minimal. Donc $\mu_u({}^t u) = 0$. Ainsi, un cas qui va permettre de conclure est celui dans lequel le polynôme minimal de u est de degré inférieur ou égal à d . Or, $\mu_{u,x}$ est de degré d et divise μ_u . Ainsi, si μ_u est de degré $\leq d$, on aura $\mu_{u,x} = \mu_u$. Cela nous conduit à nous demander s'il existe x tel que $\mu_{u,x} = \mu_u$. La réponse est oui, on le démontrera plus tard. En attendant, en admettant l'existence de $x \in E$ tel que $\mu_u = \mu_{u,x}$, on peut conclure à la stabilité par ${}^t u$ de G qui est alors un sev de E^* de dimension d .

On pose alors $H = G^\circ$ l'orthogonal de G au sens du dual. H est stable par u et est de dimension $n - d$. Il ne nous reste plus qu'à montrer que $E_{u,x} \cap H = \{0\}$ pour conclure. Soit alors $z \in E_{u,x} \cap H$. Il existe donc $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{K}$ tels que $z = \lambda_0 x + \dots + \lambda_{d-1} u^{d-1}(x)$. Mais comme $z \in H = G^\circ$, on a $\phi(z) = \phi(u(z)) = \dots = \phi(u^{d-1}(z)) = 0$. Ceci donne successivement $\lambda_{d-1} = \lambda_{d-2} = \dots = \lambda_0 = 0$, d'où le résultat. Il ne reste plus qu'à raisonner par récurrence pour obtenir la décomposition de E en sous-espaces u -cycliques qui va mener aux invariants de similitudes, ce qu'on verra juste après dans la démonstration "qui va à l'essentiel".

Comme je l'ai déjà dit, l'intérêt de cette partie était de motiver les démarches prises dans la preuve, i.e. de ne pas parachuter le supplémentaire stable par u . Je pense qu'on peut améliorer ce que j'ai fait en poussant le raisonnement sur l'interprétation matricielle (si c'est possible), mais c'est déjà mieux que rien. Voici une autre remarque qui met encore plus à la lumière l'importance de la dualité dans cette preuve :

Imaginons que l'on ait $E = E_{u,x} \oplus F$ où F est stable par u . On a $F = F^{\perp^\circ}$, ce qui est vrai de manière générale dans un ev de dimension finie. On va montrer qu'on a $F^\perp = \text{Vect}(\phi, \phi \circ u, \dots, \phi \circ u^{d-1})$, où $\phi = u^{d-1}(x)^*$. En fait, on peut vérifier que l'inclusion $\text{Vect}(\phi, \phi \circ u, \dots, \phi \circ u^{d-1}) \subseteq F^\perp$ est vraie pour $\phi = x^*, u(x)^*, \dots, u^{d-1}(x)^*$. En effet, soit $\phi = u^k(x)^*$ avec $k \in \{0, \dots, d-1\}$. Soit $z \in F$. On a $\phi(u^i(z)) = 0$ pour tout i car F étant stable par u , on a $u^i(z) \in F$ pour tout i . Ainsi, la composante en $u^k(x)$ de $u^i(z)$ est nulle pour tout i et donc $\phi(u^i(z)) = 0$. D'où $\text{Vect}(\phi, \phi \circ u, \dots, \phi \circ u^{d-1}) \subseteq F^\perp$. Comme $F^\perp$ est de dimension d , on aura égalité ssi la famille $(\phi, \phi \circ u, \dots, \phi \circ u^{d-1})$ est libre, ce qui arrive lorsque $\phi = u^{d-1}(x)^*$ comme on a vu précédemment.

Fin de l'introduction

Passons maintenant à l'énoncé qui nous intéresse pour le développement et à sa preuve.

Théorème

Soit $\mathbb{K}$ un corps quelconque et E un $\mathbb{K}$ -espace vectoriel de dimension finie

$n \in \mathbb{N}^*$. Soit u un endomorphisme de E . Il existe $s > 0$ et une famille de polynômes $F_1, \dots, F_s \in \mathbb{K}[X]$ tels que

1. $F_s | F_{s-1} | \dots | F_1$
2. $E = \bigoplus_{k=1}^s E_{u, x_k}$ avec $F_k = \mu_{u, x_k}$

Les polynômes $F_1, \dots, F_s$ sont appelés invariants de similitudes de u .

On commence comme bien souvent par le lemme suivant :

Lemme

Il existe $x \in E$, $\mu_u = \mu_{u, x}$.

Démonstration (Preuve du lemme)

On voit facilement qu'on a déjà $\mu_{u, x} | \mu_u$ pour tout $x \in E$. Le lemme dit que l'égalité est atteinte. On va raisonner sur les facteurs irréductibles de μ_u et revenir au cas général par le lemme des noyaux. Tout d'abord, il existe des polynômes $P_1, \dots, P_k \in \mathbb{K}[X]$ irréductibles et des entiers $\alpha_1, \dots, \alpha_k$ tels que $\mu_u = P_1^{\alpha_1} \dots P_k^{\alpha_k}$. Pour tout $i \in \{1, \dots, k\}$, on note $K_i = \text{Ker}(P_i^{\alpha_i}(u))$ et $u_i = u|_{K_i}$ (K_i est bien stable par u). Tout d'abord, par le lemme des noyaux, on a $E = \bigoplus_{i=1}^k K_i$. Ensuite, montrons que $\mu_{u_i} = P_i^{\alpha_i}$. En effet, on a déjà $P_i^{\alpha_i}(u_i) = 0$ car u_i est un endomorphisme de $K_i = \text{Ker}(P_i^{\alpha_i}(u))$, donc μ_{u_i} divise $P_i^{\alpha_i}$. Ainsi, μ_{u_i} est de la forme $P_i^{\beta_i}$ avec $\beta_i \leq \alpha_i$. Supposons par l'absurde qu'il existe i tel que $\beta_i < \alpha_i$. Alors le polynôme $P = P_1^{\alpha_1} \dots P_i^{\beta_i} \dots P_k^{\alpha_k}$ est annulateur de u : en effet, si $x \in K_j$ avec $j \in \{1, \dots, k\}$, $P(u)(x) = P_1^{\alpha_1}(u) \circ \dots \circ P_i^{\beta_i}(u) \circ \dots \circ P_k^{\alpha_k}(u)(x) = Q(u) \circ P_j^{\alpha_j}(x) = 0$ car $x \in K_j$ et car les $P_l^{\alpha_l}(u)$ commutent. La rédaction n'est pas totalement rigoureuse mais vous avez compris l'idée. Mais le polynôme P ne peut pas être annulateur de u car il est de degré strictement inférieur au degré de μ_u , ce qui donne une contradiction.

Montrons ensuite que pour tout $i \in \{1, \dots, k\}$ il existe $x_i \in K_i$ tel que $\mu_{u_i} = \mu_{x_i, u_i}$. Tout d'abord, on a toujours $\mu_{x, u_i} | \mu_{u_i}$ pour tout i et tout $x \in K_i$. Ainsi, μ_{x, u_i} est de la forme $P_i^{\beta_i(x)}$ où $\beta_i(x) \leq \alpha_i$ pour tout $x \in K_i$. Supposons par l'absurde qu'il existe un i tel que l'égalité ne soit jamais atteinte. C'est-à-dire qu'il existe i tel que $\beta_i(x) < \alpha_i$ pour tout $x \in K_i$. Alors on aurait $\mu_{x, u_i} | P_i^{\alpha_i-1}$ pour tout $x \in K_i$ et donc $P_i^{\alpha_i-1}(u_i)(x) = 0$, pour tout $x \in K_i$. Ainsi, $P_i^{\alpha_i-1}$ serait annulateur de u_i , ce qui est absurde car μ_{u_i} est de degré α_i .

Soit $x = x_1 + \dots + x_k$. On vérifie que $\mu_u = \mu_{x, u}$. Il suffit de montrer que $\mu | \mu_{x, u}$. Par définition de $\mu_{x, u}$, on a $\mu_{x, u}(u)(x) = 0$ donc $\mu_{x, u}(u)(x_1) + \dots + \mu_{x, u}(u)(x_k) = 0$. Mais comme les K_i sont stables par u , cette égalité est dans la somme directe $E = \bigoplus_{i=1}^k K_i$, donc chaque terme de la somme est nul. On a alors $\mu_{x, u}(u)(x_i) = \mu_{x, u}(u_i)(x_i) = 0$ pour tout i , donc $\mu_{x_i, u_i} = \mu_{u_i} = P_i^{\alpha_i}$ divise $\mu_{x, u}$ pour tout i . Comme les P_i sont irréductibles deux à deux distincts, cela implique que le produit des $P_i^{\alpha_i}$ divise $\mu_{x, u}$, mais ce produit est μ_u . D'où le résultat.

Démonstration (Preuve du théorème)

Soit $x \in E$ tel que $\mu_u = \mu_{x,u}$. On note d le degré de μ_u . Ainsi, la famille $(x, u(x), \dots, u^{d-1}(x))$ est une base de $E_{x,u}$. On complète la famille $(x, u(x), \dots, u^{d-1}(x))$ en une base quelconque de E de sorte à pouvoir considérer la forme linéaire $\phi = u^{d-1}(x)^*$ de la base duale. On pose $G = \text{Vect}(\phi, {}^t u(\phi), \dots, {}^t u^{d-1}(\phi))$ qui est un sev de E^* . Soit $H = G^\circ$ (Tout ce que j'ai écrit jusque là servait juste à ne pas parachuter tout ceci !! On comprends bien pourquoi les auteurs de livres ne le font pas en général, et pourquoi il est très utile d'avoir un professeur pour nous aider à travailler). Montrons que $E = E_{x,u} \oplus H$ et que H est stable par u . On montre que G est stable par ${}^t u$ comme précédemment mais faisons le directement pour changer. Soit $x \in H$. On a donc $\phi(x) = \phi(u(x)) = \dots = \phi(u^{d-1}(x)) = 0$. Pour montrer que $u(x) \in H$, on doit montrer que $\phi(u(x)) = \dots = \phi(u^{d-1}(x)) = \phi(u^d(x)) = 0$. La question ne se pose que pour le dernier. Si on note $\mu_u(x) = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0$, alors $u^d = -a_{d-1}u^{d-1} - \dots - a_1u - a_0\text{Id}$, et on a bien $\phi(u^d(x)) = 0$ par linéarité.

Ensuite, H est de dimension $n - d$, ce qui équivaut à montrer que G est de dimension d , qui équivaut à montrer que $(\phi, {}^t u(\phi), \dots, {}^t u^{d-1}(\phi))$ est libre. Bon, rien ne change par rapport à ce qu'on a fait dans l'introduction donc je ne le rédige pas. De même pour $E_{x,u} \cap H = \{0\}$.

Finalement, $E = E_{x,u} \oplus H$, où H est stable par u .

On établit alors le résultat du théorème.

On note x_1 le vecteur tel que $\mu_u = \mu_{x_1,u}$. D'après ce qui précède, il existe un sev H_1 de E stable par u tel que $E = E_{x_1,u} \oplus H_1$. Si $H_1 = \{0\}$, c'est bon (c'est le cas lorsque u est un endomorphisme cyclique). Supposons $\dim(H_1) \geq 1$. En appliquant ce qu'on a fait avant à la restriction de u à H_1 , qu'on note u_1 , on trouve qu'il existe $x_2 \in H_1$ tel que $\mu_{u_1} = \mu_{x_2,u_1}$ et un sev H_2 de H_1 stable par u_1 tels que $E = E_{x_1,u} \oplus E_{x_2,u_1} \oplus H_2$. Mais il est évident que $E_{x_2,u_1} = E_{x_2,u}$ (en tant que sev de E). Mais on sait que le polynôme minimal de la restriction d'un endomorphisme à un sev stable divise le polynôme minimal de cet endomorphisme. Ceci donne que $\mu_{x_2,u} | \mu_{x_1,u}$. Si $H_2 = \{0\}$ alors c'est bon. Si $\dim(H_2) \geq 1$, on refait exactement le même raisonnement appliqué à la restriction de u à H_2 . Le processus va forcément s'arrêter car E est un espace vectoriel de dimension finie. On obtient donc la décomposition

$$E = \bigoplus_{i=1}^s E_{x_i,u}$$

et les polynômes minimaux locaux qui se divisent successivement, ce qui termine la preuve.

Les invariants de similitude $F_1, \dots, F_s$ ne dépendent pas de la décomposition de E choisie, dans le sens où si on écrit $E = G_1 \oplus \dots \oplus G_l$ où les G_i sont des sev de E stables par u qui vérifient :

— Pour tout i , la restriction de u à G_i est cyclique

— Si on note P_i le polynôme minimal de $u|_{G_i}$, on a $P_{i+1}|P_i$ pour tout i . Alors $l = s$ et $P_i = F_i$ pour tout i . C'est fait dans le Gourdon pour ceux qui veulent.

On en déduit enfin qu'une forme normale dans la classe de similitude d'une matrice A est la matrice diagonale par blocs, dont les blocs sont les matrices compagnons associées aux polynômes de la suite d'invariants de similitude de A , et ce quel que soit le corps, et sans aucune hypothèse supplémentaire sur A . Précisons que les invariants de similitude de A sont les invariants de similitude de l'endomorphisme de $\mathbb{K}^n$ qui admet A pour matrice dans la base canonique. Ceci est à comparer avec la décomposition des groupes abéliens finis en produit direct de groupes cycliques, qui peut se prouver à l'aide des caractères de G (intervention du dual encore!). Mais ces deux résultats font parti d'un résultat plus général issu de la théorie des modules, notamment des modules sur un anneau principale : $\mathbb{Z}$ -module pour les groupes abéliens, et structure de $\mathbb{K}[X]$ -module sur E .

Quelques résultats supplémentaires

C'est un développement dans lequel il est très important de connaître des applications, et de savoir si ce théorème est indispensable dans la démonstration de ses corollaires. Je voulais rédiger tout ça mais j'en ai un peu marre, donc je vais plutôt vous renvoyer à ce [document](#). Voir aussi le Gourdon Algèbre, et le NH2G2 qui explique comment trouver les invariants de similitudes à partir de la réduite de Jordan. Peut-être que je rédigerai ça un jour...

Bon courage pour vos révisions.