ALGÈBRE LINÉAIRE : COMPLÉMENTS DE COURS POUR L'AGRÉGATION EXTERNE

OLIVIER SERMAN

Le but de ces notes est de présenter le théorème des invariants de similitude, ainsi que divers compléments (concernant notamment les notions d'endomorphismes cycliques et d'endomorphismes semi-simples) qui se présentent naturellement au cours de cette étude.

Rappelons dès à présent que le problème central auquel répond ce théorème est celui de décrire les orbites de l'action par conjugaison du groupe linéaire $\mathbf{GL}(E)$ d'un espace vectoriel de dimension finie E sur l'espace $\mathrm{L}(E)$ des endomorphismes de E, ou, de manière équivalente, les orbites de l'action par conjugaison de $\mathbf{GL}_n(k)$ sur l'espace des matrices [1] $\mathbf{M}_n(k)$. Ces orbites sont appelées *classes de similitude*.

On commence par introduire et étudier les sous-espaces cycliques, qui sont les briques élémentaires mises en œuvre pour décrire les classes de similitude. On présente ensuite le théorème des invariants de similitude, et quelques unes de ses conséquences [2].

J'ai essayé de donner une présentation linéaire du sujet, avec pour seuls prérequis la notion de sous-espaces stables et le lemme des noyaux (et ses conséquences essentiellement immédiates concernant la réduction des endomorphismes : trigonalisation, diagonalisation, décomposition de « Dunford » [3]). J'ai inclus au fil du texte divers commentaires concernant l'approche en termes de $k[X]$-modules.

Dans toute la suite, k désigne un corps commutatif (et $k[X]$ l'anneau des polynômes en une indéterminée X).

On note $\mathrm{L}(E)$ l'algèbre des endomorphismes d'un espace vectoriel de dimension finie E. On désigne par χ_u et π_u les polynômes caractéristique et minimal d'un endomorphisme $u \in \mathrm{L}(E)$.

Rappel. Rappelons le point de départ de l'approche en termes de $k[X]$-modules :

Tout endomorphisme u d'un espace vectoriel E munit E d'une structure de $k[X]$-module.

Cette structure est définie de la seule façon possible :

$$\begin{array}{rcl} k[X] \times E & \longrightarrow & E \\ (P, x) & \longmapsto & P(u)(x). \end{array}$$

On notera E_u le $k[X]$-module ainsi défini. Cette structure dépend de l'endomorphisme u. La remarque suivante est essentielle :

Les sous-$k[X]$-modules de E_u sont exactement les sous-espaces de E stables par u.

Rappelons également qu'on désigne par $k[u]$ l'algèbre des polynômes en u. C'est une sous-algèbre (commutative !) de $\mathrm{L}(E)$, qui est isomorphe à $k[X]/(\pi_u)$. En particulier, c'est un k-espace vectoriel de dimension $\deg(\pi_u)$:

$$\dim_k k[u] = \deg(\pi_u).$$

Date: 22 novembre 2018.

1. En d'autres termes, le théorème donne une description du quotient (ensembliste) $\mathbf{M}_n(k)/\mathbf{GL}_n(k)$.

2. On donne en particulier quelques résultats de nature topologique, qui montrent que la topologie quotient dont hérite $\mathbf{M}_n(k)/\mathbf{GL}_n(k)$ n'est pas séparée.

3. Profitons-en pour signaler la possibilité de déterminer la décomposition de Dunford d'un endomorphisme sans connaître ses valeurs propres, via une méthode effective directement inspirée de la méthode de Newton (voir par exemple [2], Problème 3.1).

1. Endomorphismes cycliques

Soit E un k-espace vectoriel de dimension n.

Définition 1.1 (Endomorphisme cyclique)**.** Un endomorphisme $u \in \mathrm{L}(E)$ est *cyclique* s'il existe $x \in E$ tel que

$$E = \langle x \rangle_u = \mathrm{Vect}(u^k(x), k \in \mathbf{N}).$$

Remarque 1.2. Pourquoi une telle définition ? Il faut absolument remarquer que, pour tout endomorphisme u, $\langle x \rangle_u$ est le plus petit sous-espace *stable* par u contenant x. On peut ainsi appeler $\langle x \rangle_u$ le « sous-espace engendré par x ». Dire que u est cyclique revient donc à dire que E est *monogène*.

Remarquons que cela revient encore à dire qu'il est monogène pour sa structure de $k[X]$-module associée à u : en effet,

$$\langle x \rangle_u = \{P(u)(x), P \in k[X]\} = k[X] \cdot x$$

est bien le $k[X]$-sous-module [4] de E_u engendré par x.

Remarque 1.3. Notons que pour tout endomorphisme u et tout vecteur non nul x il existe un unique entier p tel que $x, u(x), \ldots, u^{p-1}(x)$ forme une base de $\langle x \rangle_u = \mathrm{Vect}(u^k(x), k \in \mathbf{N})$: c'est le plus petit entier p tel que la famille $(x, u(x), \ldots, u^p(x))$ est liée. Cet entier est inférieur ou égal à $n = \dim E$, de sorte qu'on aurait pu définir $\langle x \rangle_u$ comme $\mathrm{Vect}(x, u(x), \ldots, u^{n-1}(x))$.

On a les équivalences [5] :

$$\begin{aligned} u \text{ cyclique} &\Leftrightarrow \exists x, k[X] \xrightarrow{\varphi_x} E, P \mapsto P(u)(x) \text{ est surjective,} \\ &\Leftrightarrow \exists x, k[u] \xrightarrow{\varphi_x} E, f \mapsto f(x) \text{ est surjective,} \\ &\Leftrightarrow \exists x, k[u] \xrightarrow{\varphi_x} E \text{ est un isomorphisme.} \end{aligned}$$

En particulier [6], u cyclique $\Rightarrow \deg(\pi_u) = \dim_k E$.

Remarquons que, dans les équivalences précédentes, on peut remplacer les mentions « $\exists x$ tel que $k[X] \xrightarrow{\varphi_x} E, P \mapsto P(u)(x)$ vérifie ... » par « il existe un morphisme de $k[X]$-modules $k[X] \to E_u$ tel que ... ». En effet, un morphisme de $k[X]$-modules $\varphi\colon k[X] \to E_u$ (ou $k[u] \to E_u$) est caractérisé par l'image de 1 : en notant x cette image, on a $\varphi = \varphi_x$.

1.4. **Interprétation matricielle.** Soit u un endomorphisme cyclique, et x un « générateur » de E. La famille $(x, u(x), \ldots, u^{n-1}(x))$ forme alors une base de E, et $u^n(x)$ s'écrit donc $u^n(x) = -a_0 x - a_1 u(x) - \cdots - a_{n-1} u^{n-1}(x)$. Dans la base $(x, u(x), \ldots, u^{n-1}(x))$, u admet donc la matrice suivante (souvent appelée *matrice compagnon*)

$$\mathcal{C}(P) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

où P désigne le polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$.

On vérifie alors que le polynôme caractéristique de u est égal à P. On a par définition $P(u)(x) = 0$, ce qui entraîne (puisque x engendre E) $P(u) = 0$, i.e. $\pi_u | P = \chi_u$. Comme $\deg \pi_u = n$, on en déduit

$$\pi_u = \chi_u = P.$$

4. Cette remarque montre combien est naturelle l'utilisation du langage des $k[X]$-modules dans cette situation.

5. Seule la dernière équivalence mérite un mot : elle est immédiate dès que l'on sait que $\dim_k k[u] \leqslant \dim_k E$, ce qui résulte de Cayley-Hamilton. Mais, pour ne pas avoir à se priver d'une énième démonstration de ce théorème, notons comment s'en passer : puisque u est cyclique, une relation $\sum_{i=0}^n a_i u^i(x) = 0$ de dépendance linéaire non triviale entre les $n+1$ vecteurs $x, u(x), \ldots, u^n(x)$ fournit un polynôme $P = \sum a_i X^i$ annulant u. On a alors $\pi_u | P$, d'où $\deg \pi_u \leqslant \deg P \leqslant n$.

6. On verra plus loin (Corollaire 2.6) qu'on a en fait équivalence.

En particulier, deux endomorphismes cycliques sont conjugués si et seulement si ils ont le même polynôme minimal.

Exemple 1.5 (**Endomorphismes simples**)**.** Rappelons qu'un endomorphisme est *simple* si ses seuls sous-espaces stables sont $\{0\}$ et E. Un tel endomorphisme est bien sûr cyclique : le sous-espace $\langle x\rangle_u$ engendré par un élément $x \in E, x \neq 0$ est stable et non nul, donc égal à E tout entier.

Rappelons au passage l'importante proposition suivante :

Proposition 1.6 (Caractérisation des endomorphismes simples)**.** *Un endomorphisme u d'un espace vectoriel de dimension finie est simple si et seulement si son polynôme caractéristique χ_u est irréductible.*

Démonstration. Si u est simple, il est cyclique, de polynôme minimal $\pi_u = \chi_u$. Si $\chi_u = PQ$, alors $P(u)Q(u) = \chi_u(u) = 0$, de sorte que $P(u)$ ou $Q(u)$ n'est pas injectif. Si $P(u)$ n'est pas injectif, alors $\ker P(u)$ est un sous-espace stable non nul, et la simplicité de u assure que $\ker P(u) = E$, i.e. $P(u) = 0$. Le polynôme P est donc un multiple de $\pi_u = \chi_u$, et Q est donc inversible. Cela montre que χ_u est irréductible.

La réciproque est évidente : soit $F \subset E$ un sous-espace stable par u ; alors $\chi_{u_{|F}}$ divise χ_u, et l'irréductibilité de χ_u entraîne $F = \{0\}$ ou E. □

Exemple 1.7 (**Blocs de Jordan**)**.** Un endomorphisme u dont une matrice est un « bloc de Jordan » de taille n et de valeur propre λ est un endomorphisme cyclique, automatiquement associé au polynôme $\chi_u(X) = (X-\lambda)^n$:

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \sim \mathcal{C}((X-\lambda)^n).$$

Les générateurs de E sont les éléments de $E \setminus \ker((u-\lambda\mathrm{id})^{n-1})$.

En particulier, si $\lambda = 0$, on obtient que les endomorphismes nilpotents d'indice maximal sont cycliques (et associés au polynôme X^n).

Exemple 1.8 (**Récurrences linéaires**)**.** Un exemple à mentionner survient lors de l'étude des *suites récurrentes linéaires* : on cherche à décrire l'ensemble des suites $(u_n)_{n\geqslant 0} \in \mathbf{C}^{\mathbf{N}}$ à valeurs complexes satisfaisant la relation de récurrence (« linéaire d'ordre r »)

$$u_{n+r} = \alpha_{r-1}u_{n+r-1} + \alpha_{r-2}u_{n+r-2} + \cdots + \alpha_1 u_{n+1} + \alpha_0 u_n,\ \forall n \geqslant 0 \tag{1}$$

avec $\alpha_0, \ldots, \alpha_{r-1} \in \mathbf{C}$, $\alpha_0 \neq 0$.

L'ensemble des solutions forme un sous-espace vectoriel E de l'espace $\mathbf{C}^{\mathbf{N}}$ des suites à valeurs complexes, et on vérifie sans mal que l'application

$$\begin{array}{rccc} \varphi\colon & E & \longrightarrow & \mathbf{C}^r \\ & (u_n)_{n\geqslant 0} & \longmapsto & (u_0, \ldots, u_{r-1}) \end{array}$$

est un isomorphisme : E est donc de dimension r, et les suites $\delta^{(0)}, \ldots, \delta^{(r-1)}$ déterminées par les conditions « initiales » $\delta_j^{(i)} = \delta_{ij}$, $0 \leqslant j \leqslant r-1$ en forment une base.

L'espace E possède un endomorphisme naturel, à savoir le morphisme de « décalage » $T \in \mathrm{L}(E)$ envoyant la suite u sur la suite Tu définie par $(Tu)_n = u_{n+1}, n \geqslant 0$. Son intérêt ici réside en l'observation

« pour toute suite u vérifiant (1), on a $u_n = (T^n u)_0, \forall n \in \mathbf{N}$ »

qui motive l'étude des itérées T^n du morphisme T.

La matrice de ce morphisme dans la base formée par les suites $\delta^{(i)}$ est [7]

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{r-2} & \alpha_{r-1} \end{pmatrix},$$

d'où l'on déduit aussitôt que T est cyclique : en effet, E est engendré (par exemple) par $\delta^{(r-1)}$ (voir que $\mathrm{Vect}(\delta^{(r-1)}, \dots, T^k(\delta^{(r-1)})) = \mathrm{Vect}(\delta^{(r-1)}, \dots, \delta^{(r-1-k)})$ pour tout $k = 0, \dots, r-1$). En particulier, la matrice précédente est semblable à la matrice compagnon $\mathcal{C}(P)$ associée au polynôme $P(X) = \chi_T(X) = X^r - \alpha_{r-1}X^{r-1} - \cdots - \alpha_1 X - \alpha_0$.

Saisissons cette occasion pour rappeler comment la considération de ce morphisme permet de résoudre la récurrence linéaire (1). Le lemme des noyaux permet de décomposer l'espace des solutions E en somme directe des sous-espaces caractéristiques de T

$$E = \bigoplus \ker(T - \lambda_i \mathrm{id})^{r_i}$$

où les λ_i sont les racines de P, toutes non nulles, et les r_i leurs multiplicités. On se ramène ainsi au cas des suites appartenant à $\ker(T - \lambda\mathrm{id})^{r_\lambda}$, c'est-à-dire vérifiant la relation

$$u_{n+r_\lambda} = r_\lambda \lambda u_{n+r_\lambda - 1} + \cdots + (-1)^{r_\lambda - k}\binom{r_\lambda}{k}\lambda^{r_\lambda - k}u_{n+k} + \cdots + (-1)^{r_\lambda}\lambda^{r_\lambda}u_n, \ \forall n \geqslant 0, \tag{2}$$

soit encore au cas où P admet une seule racine, non nulle : autrement dit, $T_\lambda = T_{|\ker(T-\lambda\mathrm{id})^{r_\lambda}}$ « a un seul bloc de Jordan ».

On peut dans ce cas écrire T_λ sous la forme $T_\lambda = \lambda\mathrm{id} + N_\lambda$, avec N_λ nilpotent d'indice r_λ, et les puissances T_λ^n de T_λ sont alors égales à $T_\lambda^n = \sum_{k=0}^{r_\lambda - 1}\binom{n}{k}\lambda^{n-k}N_\lambda^k$, et on a donc, pour toute suite $(u_n)_{n\geqslant 0}$ vérifiant (2),

$$u_n = (T_\lambda^n(u))_0 = \sum_{k=0}^{r_\lambda - 1}\binom{n}{k}\lambda^{n-k}(N_\lambda^k(u))_0, \quad \forall n \geqslant 0.$$

On obtient ainsi directement que toute suite satisfaisant la relation de récurrence (2) est combinaison linéaire des suites $(n^k\lambda^n)_{n\geqslant 0}$, $k = 0, \dots, r-1$. Puisque l'on sait par ailleurs que l'espace des solutions est de dimension r_λ, on en déduit que toute combinaison linéaire de ces suites est solution de (2), et que ces suites forment une base de l'espace de ces solutions.

Revenant au problème initial, on a finalement montré [8] :

Proposition 1.9. *Soit $P(X) = X^r - \alpha_{r-1}X^{r-1} - \cdots - \alpha_1 X - \alpha_0 = \prod_{i=1}^m (X - \lambda_i)^{r_i}$ le polynôme associé à la relation de récurrence (1). Les solutions de (1) sont alors les combinaisons linéaires des suites*

$$(n^k\lambda_i^n)_{n\geqslant 0}, \ i = 1, \dots, m, \ k = 0, \dots, r_i - 1.$$

Qui plus est, ces suites sont linéairement indépendantes.

---

7. Une autre façon de voir apparaître cette même matrice est la variante suivante : soit $(u_n)_n \in E$ une suite satisfaisant la relation de récurrence considérée. La suite vectorielle définie par $U_n = \begin{pmatrix} u_n \\ \vdots \\ u_{n+r-1} \end{pmatrix}$ vérifie une relation de récurrence $U_{n+1} = AU_n$ où $A \in \mathbf{M}_r(\mathbf{C})$ est justement la matrice obtenue ici.

8. On peut bien évidemment suivre la variante vectorielle pour obtenir ce résultat : la suite vectorielle $U_n = \begin{pmatrix} u_n \\ \vdots \\ u_{n+r-1} \end{pmatrix}$ vérifie la relation $U_{n+1} = AU_n$, de sorte que $U_n = A^nU_0$ pour tout n. Si A est à valeurs propres $\lambda_1, \dots, \lambda_r$ deux à deux distinctes, on obtient immédiatement, en décomposant $U_0 = \sum c_i X_i$ dans une base de vecteurs propres $X_1, \dots, X_r \in \mathbf{C}^r$, que u_n, qui est la première coordonnée de U_n, est égal à $c_1\lambda_1^n + \cdots + c_r\lambda_r^n$ pour tout $n \geqslant 0$. Dans le cas général, il suffit de savoir qu'il existe $P \in \mathbf{GL}_n(\mathbf{C})$ telle que $P^{-1}AP = \mathrm{diag}(T_1, \cdots, T_m)$ soit diagonale par blocs T_i triangulaires supérieurs de la forme $T_i = \lambda_i I_{r_i} + N_i \in \mathbf{M}_{r_i}(\mathbf{C})$ avec N_i triangulaire supérieure stricte (ce qui résulte du lemme des noyaux et de la trigonalisabilité des matrices nilpotentes), avec en particulier $N_i^{r_i} = 0$. Alors u_n est la première coordonnée de $U_n = P\,\mathrm{diag}(T_i^n)P^{-1}U_0$. On en déduit qu'il existe des polynômes $R_1, \dots, R_m$ de degrés $\deg R_i \leqslant r_i - 1$ et des scalaires $c_1, \dots, c_m$ tels que $u_n = \sum_i c_i R_i(n)\lambda_i^n$ pour tout $n \geqslant 0$. Puisque l'espace des solutions est de dimension $r = \sum r_i$, toute suite de cette forme est solution.

Exercice 1.10 (**Endomorphismes cycliques et sous-espaces stables**)**.** Si u est cyclique, alors E n'admet qu'un nombre fini de sous-espaces stables. La réciproque est vraie lorsque le corps k est infini [9].

Cet excellent exercice montre une nouvelle fois que le point de vue $k[X]$-module est incontournable. Soit u un endomorphisme cyclique. Il existe donc $x \in E$ tel que $\varphi_x \colon k[u] \to E_u, f \mapsto f(x)$ est un isomorphisme de $k[X]$-modules. On a alors les « correspondances » suivantes

$$\begin{array}{rcll} F \subset E \text{ stable} & \longleftrightarrow & \varphi_x^{-1}(F) \subset k[u] \text{ idéal de } k[u] & \\ & \longleftrightarrow & I \text{ idéal de } k[X] \text{ contenant } (\pi_u) & (\text{car } k[u] \simeq k[X]/(\pi_u)) \\ & \longleftrightarrow & D \in k[X] \text{ diviseur (unitaire) de } \pi_u & (\text{car } k[X] \text{ est principal}). \end{array}$$

Les sous-espaces de E stables par u correspondent donc bijectivement aux diviseurs unitaires de π_u (dans $k[X]$), qui sont en nombre fini [10].

Soit maintenant u un endomorphisme d'un espace vectoriel E défini sur un corps infini k n'admettant qu'un nombre fini de sous-espaces stables. Comme k est infini, E ne peut être réunion de ses sous-espaces stables propres. Il existe donc $x \in E$ n'appartenant à aucun sous-espace stable $F \neq E$. Le sous-espace $\langle x \rangle_u$ engendré par u est alors un sous-espace stable qui n'est contenu dans aucun sous-espace stable propre. C'est donc E lui-même, et u est bien cyclique.

2. Sous-espaces cycliques

On introduit ici la notion de sous-espace cyclique pour un endomorphisme $u \in \mathrm{L}(E)$, essentielle à la suite : l'objet du théorème des invariants de similitude est de fournir une décomposition de E en somme directe de tels sous-espaces, qui caractérise la classe de similitude de u.

On désigne toujours par E un k-espace vectoriel de dimension n, et u un endomorphisme de E.

Définition 2.1 (Sous-espace cyclique)**.** Un sous-espace $F \subset E$ stable par u est dit *cyclique* (ou cyclique sous u) si la restriction $u_{|F}$ de u à F est cyclique.

Remarque 2.2.

- Cela signifie qu'il existe $x \in E$ tel que $F = \langle x \rangle_u$ est le sous-espace engendré par u. Ou encore que F est un sous-$k[X]$-module monogène : en effet, dire que x engendre F signifie que $(x, u(x), \ldots, u^{\dim F - 1}(x))$ est une base de F, autrement dit que le morphisme de $k[X]$-modules $k[X] \to F$ envoyant 1 sur x est surjectif.
- L'endomorphisme u est cyclique si et seulement si E est un espace cyclique.
- Si F est cyclique, alors $\pi_{u_{|F}} = \chi_{u_{|F}}$.

Proposition 2.3 (Cayley–Hamilton)**.** *Soit $u \in \mathrm{L}(E)$. Alors $\pi_u | \chi_u$.*

Démonstration [11]. Montrons que $\chi_u(u) = 0$. Soit $x \in E$, et $F = \langle x \rangle_u$. Comme F est stable, $\chi_{u_{|F}} | \chi_u$. Mais, comme F est cyclique, $\chi_{u_{|F}}(u)(x) = \pi_{u_{|F}}(u)(x) = 0$, d'où $\chi_u(u)(x) = 0$. $\square$

---

9. Si k est fini, le nombre de sous-espaces stables est toujours fini !

10. On peut bien sûr préférer paraphraser ainsi ce qui précède : soit F un sous-espace-stable de E. Alors $I = \{P \in k[X] | P(u)(x) \in F\}$ est un idéal de $k[X]$ contenant π_u. Cet idéal est donc de la forme $I = (D)$ pour un diviseur unitaire D de π_u, et $F = \langle D(u)(x) \rangle_u$. Tout sous-espace stable de E est donc défini par un diviseur de π_u.

11. Ce théorème fondamental admet de nombreuses preuves. L'une des plus basiques repose sur la formule $\det M \cdot I_n = M {}^t\mathrm{Com}\, M$ où $\mathrm{Com}\, M$ désigne la comatrice d'une matrice $M \in \mathbf{M}_n(A)$ à coefficients dans un anneau commutatif A : en effet, si $M \in \mathbf{M}_n(k)$, on a dans $M_n(k[X])$

$$\chi_M(X) I_n = \det(X I_n - M) I_n = (X I_n - M) {}^t\mathrm{Com}(X I_n - M).$$

En écrivant $\chi_M(X) = \sum_{i=0}^n c_i X^i$ et ${}^t\mathrm{Com}(X I_n - M) = \sum_{i=0}^{n-1} X^i A_i$ avec $A_i \in \mathbf{M}_n(k)$, on obtient

$$\begin{array}{rcl} c_0 I_n & = & -M A_0 \\ c_1 I_n & = & A_0 - M A_1 \\ & \vdots & \\ c_{n-1} I_n & = & A_{n-1} - M A_n \\ c_n I_n & = & A_{n-1}. \end{array}$$

En multipliant la i-ème ligne par M^i et en sommant, on obtient $\chi_M(M) = \sum_i c_i M^i = 0$.

Venons-en maintenant au principal résultat de cette section, qui est le point de départ de la démonstration du théorème des invariants de similitude [12].

Théorème 2.4. *Il existe un sous-espace cyclique $F \subset E$ tel que $\pi_{u_{|F}} = \pi_u$.*

Remarque 2.5. Cet énoncé est naturel : en effet, si F est un sous-espace cyclique (ou même simplement stable), alors $\pi_{u_{|F}}$ divise automatiquement π_u, et il est légitime de se demander si l'égalité peut avoir lieu pour certains sous-espaces de E. Le théorème apporte une réponse positive à cette question.

Avant de donner la démonstration du théorème 2.4, énonçons en un corollaire à retenir :

Corollaire 2.6 (Caractérisation des endomorphismes cycliques)**.**

$$\begin{aligned} u \text{ cyclique} \quad &\Leftrightarrow \quad \pi_u = \chi_u \\ &\Leftrightarrow \quad \deg \pi_u = \dim_k E. \end{aligned}$$

Démonstration. On a déjà vu que u cyclique implique $\pi_u = \chi_u$. Soit donc u tel que $\pi_u = \chi_u$. D'après 2.4, E contient un sous-espace cyclique F de polynôme minimal $\pi_u = \chi_u$. On a donc $\dim F = \deg \chi_u = \dim E$, i.e. $E = F$ est cyclique. □

En particulier, un endomorphisme (ou une matrice) à valeurs propres deux à deux distinctes est cyclique.

Exercice 2.7. Soit $k = \mathbf{R}$ ou $\mathbf{C}$, et E un k-espace vectoriel de dimension n. Montrer que le lieu $\{u \in \mathrm{L}(E) | \chi_u = \pi_u\}$ est un ouvert connexe dense dans $\mathrm{L}(E)$. [13]

Le théorème 2.4 est un résultat d'existence : on doit trouver un vecteur $x \in E$ tel que

$$\pi_{u_{|\langle x \rangle_u}} = \pi_u.$$

Soit $\pi_u = \prod P_i^{\alpha_i}$ la décomposition de π_u en produits d'irréductibles deux à deux non associés. On a alors une décomposition $E = \oplus \ker P_i^{\alpha_i}(u)$ en somme de sous-espaces stables. L'idée est de démontrer d'abord le théorème pour chacun de ces sous-espaces, puis de « recoller » les morceaux. On s'appuie sur les deux lemmes suivants :

Lemme 2.8. *Si $\pi_u = P^\alpha$, avec P irréductible, alors il existe un sous-espace cyclique $F \subset E$ tel que $\pi_{u_{|F}} = P^\alpha$.*

Démonstration [14]. Par hypothèse, il existe $x \in E$ tel que $P^{\alpha-1}(u)(x) \neq 0$. Le sous-espace cyclique $F = \langle x \rangle_u$ engendré par x convient : en effet, le polynôme minimal de la restriction $u_{|F}$ de u à F divise $\pi_u = P^\alpha$, et $P^{\alpha-1}(u_{|F})$ est non nul, de sorte que $\pi_{u_{|F}} = P^\alpha$. □

Lemme 2.9. *Soient $x, y \in E$ tels que $\pi_{u_{|\langle x \rangle_u}} = P$ et $\pi_{u_{|\langle y \rangle_u}} = Q$ sont premiers entre eux. Alors le polynôme minimal de la restriction de u au sous-espace cyclique $\langle x + y \rangle_u$ engendré par $x + y$ est $\pi_{u_{|\langle x+y \rangle_u}} = PQ$.*

12. Il faut remarquer ici que cet énoncé est contenu dans le théorème des invariants de similitude.

13. Pour l'ouverture, noter que $\chi_u = \pi_u \Leftrightarrow \exists x \in E | \det(x, u(x), \ldots, u^{n-1}(x)) \neq 0$ (ou, mieux, que $\chi_u = \pi_u$ équivaut à $\mathrm{rg}(\mathrm{id}, u, \ldots, u^{n-1}) = n$). Pour la connexité, le plus rapide est de relier u à un endomorphisme à valeurs propres deux à deux distinctes (donc cyclique), et de noter que la classe de similitude d'un tel endomorphisme est connexe (si $k = \mathbf{C}$, cela résulte de la connexité de $\mathbf{GL}(E)$; si $k = \mathbf{R}$, cela vient de ce que le stabilisateur d'un tel endomorphisme contient un automorphisme de déterminant négatif). Enfin la densité s'obtient pour $k = \mathbf{C}$ en remarquant à nouveau qu'un endomorphisme à valeurs propres deux à deux distinctes est cyclique. Si $k = \mathbf{R}$, on peut adapter l'argument utilisé pour $\mathbf{C}$ pour montrer que les matrices dont le polynôme caractéristique est sans carré sont denses dans $\mathbf{M}_n(\mathbf{R})$ (commencer par trigonaliser sur $\mathbf{C}$, pour ensuite bouger pertinemment les paires de valeurs propres conjuguées, et enfin conclure en se rappelant que deux matrices réelles semblables dans $\mathbf{M}_n(\mathbf{C})$ sont déjà semblables dans $\mathbf{M}_n(\mathbf{R})$ (pourquoi ?)). On peut aussi utiliser le théorème 3.1. Ou encore remarquer que le lieu considéré contient, pour tout x, l'ensemble $\{u \in \mathrm{L}(E) | \det(x, u(x), \ldots, u^{n-1}(x)) \neq 0\}$ qui, pour x non nul, est un ouvert dense (son complémentaire est le lieu des zéros dans $\mathbf{M}_n(k)$ d'un polynôme non nul, donc est d'intérieur vide).

14. Notons qu'on retrouve ici le début de l'argument mené pour réduire un endomorphisme nilpotent. Cela n'est pas surprenant (au contraire) : un endomorphisme nilpotent est justement un endomorphisme u tel que $\pi_u = X^\alpha$.

Démonstration. L'égalité $(PQ)(u)(x+y)=0$ montre que $\pi_{u_{|\langle x+y\rangle_u}}$ divise PQ.

En notant $R=\pi_{u_{|\langle x+y\rangle_u}}$, on a

$$0=R(u)(x+y)=\underbrace{R(u)(x)}_{\in\langle x\rangle_u\subset\ker P(u)}+\underbrace{R(u)(y)}_{\in\langle y\rangle_u\subset\ker Q(u)}$$

et, la somme $\ker P(u)\oplus\ker Q(u)$ étant directe, on en déduit que $R(u)(x)=0$ et $R(u)(y)=0$, i.e. $P|R$ et $Q|R$, d'où finalement $PQ|R$. □

Démonstration du théorème 2.4. La décomposition $\pi_u=\prod_{i=1}^r P_i^{\alpha_i}$ du polynôme minimal de u en produit d'irréductibles deux à deux non associés définit une décomposition de E en somme directe de sous-espaces stables

$$E=\bigoplus_{i=1}^r \ker P_i^{\alpha_i}(u).$$

Le polynôme minimal π_i de la restriction de u à $\ker P_i^{\alpha_i}(u)$ est $P_i^{\alpha_i}$ (car π_i divise $P_i^{\alpha_i}$ pour tout i, et $\prod\pi_i$ annule u) [15]. Le lemme 2.8 assure alors l'existence d'éléments $x_1,\dots,x_r$ tels que le polynôme minimal de la restriction de u à $\langle x_i\rangle_u$ est $P_i^{\alpha_i}$. D'après le lemme 2.9, le polynôme minimal de la restriction de u au sous-espace cyclique F engendré par $x=x_1+\cdots+x_r$ est le produit $\prod_{i=1}^r P_i^{\alpha_i}=\pi_u$, et F vérifie donc les conditions souhaitées. □

3. Invariants de similitude

On peut maintenant énoncer le théorème des invariants de similitude.

Théorème 3.1 (Invariants de similitude)**.** *Soit $u\in\mathrm{L}(E)$ un endomorphisme d'un espace vectoriel E de dimension finie. Il existe une* unique *famille de polynômes unitaires non constants $P_1,\dots,P_r$ tels que*

$$P_r\mid P_{r-1}\mid\cdots\mid P_1$$

et E admette une décomposition

$$E=\bigoplus_{i=1}^r F_i$$

en somme directe de sous-espaces cycliques *$F_1,\dots,F_r$ associés aux polynômes $\pi_{u|F_i}=P_i$.*

Remarque 3.2. Plusieurs remarques s'imposent.

- Les sous-espaces cycliques $F_1,\dots,F_r$ ne sont certainement *pas* uniques [16].
- Matriciellement, cet énoncé devient : soit $M\in\mathbf{M}_n(k)$. Il existe une unique famille $P_r|\cdots|P_1$ de polynômes unitaires non constants tels que M est semblable à la matrice diagonale par blocs $\begin{pmatrix}\mathcal{C}(P_1)&&\\&\ddots&\\&&\mathcal{C}(P_r)\end{pmatrix}$.
- On a $\pi_u=P_1$ et $\chi_u=\prod_{i=1}^r P_i$.

15. On peut aussi établir le lemme général suivant :

Lemme. *Soient $u\in\mathrm{L}(E)$ et $P\in k[X]$. Le polynôme minimal de la restriction de u à $\ker P(u)$ est*

$$\pi_{u_{|\ker P(u)}}=\mathrm{pgcd}(\pi_u,P).$$

Démonstration. Notons $Q=\mathrm{pgcd}(\pi_u,P)$. Comme $\pi_u(u)$ et $P(u)$ sont nuls sur $\ker P(u)$, on a immédiatement $\pi_{u_{|\ker P(u)}}|Q$. D'autre part, $Q|P$ implique $\ker Q(u)\subset\ker P(u)$ (et on a même égalité, vu que $\pi_{u_{|\ker P(u)}}|Q$ signifie exactement que $Q(u)=0$ sur $\ker P(u)$, i.e. $\ker P(u)\subset\ker Q(u)$). Enfin, puisque $Q|\pi_u$, on peut écrire $\pi_u=QR$, et on a alors

$$\begin{aligned}Q(u)R(u)=\pi_u(u)=0\quad&\Leftrightarrow\quad \mathrm{im}\,R(u)\subset\ker Q(u)=\ker P(u)\Rightarrow(\pi_{u_{|\ker P(u)}}R)(u)=0\\&\Rightarrow\quad \pi_u\mid\pi_{u_{|\ker P(u)}}R\mid QR=\pi_u,\end{aligned}$$

ce qui implique $\pi_{u_{|\ker P(u)}}=Q$. □

16. Exercice : donner une condition nécessaire et suffisante à leur unicité.

Corollaire 3.3 ([17]). *Tout diviseur irréductible de χ_u divise π_u.*

La famille de polynômes unitaires non constants $P_1, \ldots, P_r$ donnée par le théorème précédent caractérise donc la classe de similitude de u (ou de M). Cela motive la définition suivante :

Définition 3.4 (Facteurs invariants)**.** Les polynômes $P_1, P_2, \ldots, P_r$ associés à $u \in \mathrm{L}(E)$ (ou $M \in \mathbf{M}_n(k)$) par le théorème 3.1 sont appelés *facteurs invariants* de u (ou de M).

Remarque 3.5. On peut se débarasser des « non constants » en fixant la longueur de la suite des invariants de similitude (le but étant de garder l'unicité de la suite). On passe ainsi de la suite $P_r|\cdots|P_1$ à la suite $P_n|\cdots|P_1$ en ajoutant les polynômes $P_n = \cdots = P_{r+1} = 1$. Cette distinction n'a aucune importance, et le seul but de cette remarque est de signaler que les deux définitions coexistent.

On a ainsi

Corollaire 3.6. *Deux endomorphismes de E (ou matrices) sont conjugués si et seulement si ils ont les mêmes facteurs invariants.*

Démonstration du théorème 3.1. Démontrons l'existence de cette décomposition par récurrence sur la dimension de E.

Soit donc $u \in \mathrm{L}(E)$ un endomorphisme d'un espace vectoriel de dimension n. D'après le théorème 2.4, il existe un sous-espace cyclique $F_1 \subset E$ tel que $\pi_{u_{|F_1}} = \pi_u$. Posons $d_1 = \dim F_1 = \deg \pi_u$.

Le point clé de la démonstration est alors de *trouver un supplémentaire stable de F_1 stable par u.*

Soit $x \in E$ tel que $F_1 = \langle x \rangle_u$. Considérons une forme linéaire $\lambda \in E^*$ telle que $\lambda(x) = \cdots = \lambda(u^{d_1-2}(x)) = 0$ et $\lambda(u^{d_1-1}(x)) = 1$. Si ${}^t u\colon E^* \to E^*, \varphi \mapsto \varphi \circ u$ est la transposée de u, notons $\tilde{G} = \langle \lambda \rangle_{{}^t u}$ le sous-espace de E^* engendré par λ, et

$$G = \tilde{G}^\perp = \{y \in E | \varphi(y) = 0, \forall \varphi \in \tilde{G}\}$$

son orthogonal. Montrons alors que [18]

$$G \text{ est un supplémentaire de } F_1 \text{ stable par } u.$$

17. En voici deux démonstrations directes et élémentaires. Soit P un diviseur irréductible de χ_u. Alors $P(u)$ ne peut être inversible (en effet, $\det P(u)$ est nul, comme on le voit en considérant, sur un corps de décomposition de P, un vecteur propre associé à une racine de P), de sorte que P doit diviser π_u (si un polynôme irréductible Q ne divise pas π_u, alors $Q(u)$ est inversible).

La seconde démonstration est encore plus simple. Soit $M \in \mathbf{M}_n(k)$. Montrons que $\chi_M | \pi_M^n$. Dans toute algèbre A, deux éléments a et b qui commutent vérifient $a^i - b^i = (a-b)Q_i(a,b)$ où Q_i est le polynôme en deux indéterminées $Q_i(X,Y) = \sum_{j=0}^{i-1} X^{i-1-j}Y^j$. En particulier, dans $\mathbf{M}_n(k)$ on a, pour tout i, $X^i I_n - M^i = (XI_n - M)A_i$ où $A_i = Q_i(XI_n, M) \in \mathbf{M}_n(k[X])$. En écrivant $\pi_M(X) = \sum_{i=0}^d a_i X^i$, on en déduit $\pi_M(X)I_n = \pi_M(X)I_n - \pi_M(M) = (XI_n - M)\sum_i a_i A_i$ dans $\mathbf{M}_n(k[X])$, d'où, en prenant le déterminant, $\pi_M(X)^n = \det(XI_n - M)\det(\sum a_i A_i)$. On a donc $\chi_M | \pi_M^n$. Il s'ensuit que tout diviseur irréductible de χ_M divise π_M.

18. Mais d'où vient une telle idée ? Il faut avoir en tête les liens naturels d'« orthogonalité » entre E et son dual E^*, notamment ceux impliquant u et sa transposée ${}^t u$: ainsi $F_1^\perp = \{\varphi \in E^* | \varphi(y) = 0, \forall y \in \langle x \rangle_u\}$ est un sous-espace stable par ${}^t u$ de codimension d_1, et l'orthogonal d'un supplémentaire $\tilde{G}$ de $F_1^\perp$ stable par ${}^t u$ est automatiquement un supplémentaire G de F_1 stable par u. Ces remarques n'ont d'intérêt que s'il est plus simple de trouver $\tilde{G} \subset E^*$ (de dimension d_1) que $G \subset E$ (de codimension d_1). Mais on a dans E^* des sous-espaces stables de dimension d_1 tout trouvés, à savoir les sous-espaces cycliques de polynôme π_u donnés par 2.4. Il ne reste qu'à en choisir un qui soit un supplémentaire de $F_1^\perp$. Pour ce faire, remarquons que si la matrice de u dans une base $\mathcal{B}$ de E adaptée à F_1 est (comme on l'espère) $\mathrm{diag}(\mathcal{C}(P_i))$, alors la matrice de ${}^t u$ dans la base duale $\mathcal{B}^*$ est $\mathrm{diag}({}^t\mathcal{C}(P_i))$: cela indique qu'il suffit de choisir pour $\tilde{G}$ le sous-espace engendré par les d_1 premiers vecteurs de la base duale. En écrivant la matrice ${}^t\mathcal{C}(P_1)$, il apparaît clairement qu'il s'agit du sous-espace engendré sous ${}^t u$ par le d_1-ième vecteur de la base duale de la base $\mathcal{B} = (x, u(x), \ldots, u^{d_1-1}(x), \ldots)$, d'où le choix de cette forme linéaire $\lambda \in E^*$ vérifiant $\lambda(u^i(x)) = \delta_{n-1,i}$.

Voici d'ailleurs une présentation plus efficace de la construction de G : $F_1 \subset E$ induit une surjection $E^* \twoheadrightarrow F_1^*$ (dont le noyau est l'orthogonal $F_1^\perp$), et le dual F_1^* est cyclique sous ${}^t u$, de polynôme $\pi_{{}^t u} = \pi_u$. Soit $\lambda \in E^*$ un relèvement d'un générateur (sous ${}^t u$) de F_1^*. Le sous-espace cyclique $\tilde{G}$ engendré par λ est stable, et de dimension $\geqslant \dim F_1$ (car $\tilde{G} \twoheadrightarrow F_1^*$) et $\leqslant \dim F_1$ (car $\tilde{G}$ est cyclique, d'où $\dim \tilde{G} \leqslant \deg \pi_{{}^t u} = \deg \pi_u = \dim F_1$). On a ainsi $E^* = F_1^\perp \oplus \tilde{G}$ avec $\tilde{G}$ stable par ${}^t u$, d'où $E = F_1 \oplus \tilde{G}^\perp$ avec $\tilde{G}^\perp$ stable par u.

— G est stable par u : clair,
— $F_1 \cap G = \{0\}$: dire que $y = \sum a_i u^i(x) \in F_1$ appartient à G implique successivement $a_{d_1-1} = \lambda(y) = 0$, $a_{d_1-2} = \lambda(u(y)) = 0$, ..., et enfin $a_0 = \lambda(u^{d_1-1}(y)) = 0$,
— $\dim F_1 + \dim G = \dim E$: puisque $\pi_u({}^t u)$ est nul [19], la dimension du sous-espace cyclique $\tilde{G}$ est $\leqslant \deg \pi_u = \dim F_1$, d'où l'on tire $\dim G = \dim E - \dim \tilde{G} \geqslant \dim E - \dim F_1$.

Par récurrence, on peut décomposer G en une somme directe $G = \oplus_{i=2}^r F_i$ de sous-espaces cycliques $F_2, \ldots, F_r$ dont les polynômes $P_2, \ldots, P_r$ vérifient $P_r | \cdots | P_2$. Puisque $P_1 = \pi_u$ annule u, le polynôme minimal P_2 de $u_{|G}$ divise P_1. On a donc établi l'existence de la décomposition annoncée.

Établissons à présent l'unicité : soient $E = F_1 \oplus \cdots \oplus F_r$ et $E = G_1 \oplus \cdots \oplus G_s$ deux décompositions de E en somme des sous-espaces cycliques respectivement associés aux polynômes $P_r | \cdots | P_1$ et $Q_s | \cdots | Q_1$. Montrons que les suites $P_1, \ldots, P_r$ et $Q_1, \ldots, Q_s$ sont égales. Il suffit de montrer que, si les égalités $P_j = Q_j, j < i$ ont lieu pour un entier $i \geqslant 1$, alors $P_i = Q_i$.

Soit donc $i \geqslant 1$ tel que $P_j = Q_j$ pour tout $j < i$. Appliquons le morphisme $P_i(u)$ aux deux décompositions en somme directe de sous-espaces stables pour u précédentes :

$$P_i(u)(E) = P_i(u)(F_1) \oplus \cdots \oplus P_i(u)(F_{i-1}) = P_i(u)(G_1) \oplus \cdots \oplus P_i(u)(G_s). \tag{3}$$

Remarquons alors que $\dim P_i(u)(F_j) = \dim P_i(u)(G_j)$ si $j < i$: en effet, P_j est alors égal à Q_j, et les deux sous-espaces cycliques $F_j \simeq k[u_{|F_j}]$ et $G_j \simeq k[u_{|G_j}]$ sont donc isomorphes à $k[X]/(P_j)$. On en déduit $P_i(u)(F_j) \simeq P_i k[X]/(P_j) \simeq P_i(u)(G_j)$. Alors (3) montre que $P_i(u)$ est nul sur G_i, d'où $Q_i = \pi_{u_{|G_i}} | P_i$. On obtient de même $P_i | Q_i$, d'où $P_i = Q_i$, ce qui achève la démonstration du théorème. □

Donnons-en les conséquences habituelles.

Corollaire 3.7. *Soit K un corps contenant k. Alors deux matrices dans $\mathbf{M}_n(k)$ sont semblables (dans $\mathbf{M}_n(k)$) si et seulement si elles sont semblables dans $\mathbf{M}_n(K)$.*

Démonstration. L'unicité des facteurs invariants fait que les facteurs invariants $P_1, \ldots, P_r \in k[X]$ de M sur k sont encore les facteurs invariants de M sur K. □

Exercice 3.8. Donner une démonstration directe du corollaire précédent dans le cas où k est infini [20].

Corollaire 3.9. *Une matrice $M \in \mathbf{M}_n(k)$ est semblable à sa transposée ${}^t M$.*

Démonstration. Il suffit de voir que M et ${}^t M$ ont les mêmes facteurs invariants, ce qui résulte de ce que la transposée ${}^t\mathcal{C}(P)$ d'une matrice compagnon $\mathcal{C}(P)$ est la matrice d'un endomorphisme cyclique de même polynôme minimal (car $\pi_{{}^t\mathcal{C}(P)} = \pi_{\mathcal{C}(P)} = \chi_{\mathcal{C}(P)} = \chi_{{}^t\mathcal{C}(P)}$), et lui est donc semblable. □

Remarque 3.10. Ce théorème résulte également du théorème de structure des modules de type fini sur un anneau principal. Rappelons que ce théorème assure qu'un module M de type fini sur un anneau principal est isomorphe à une somme directe

$$M \simeq A^s \oplus \bigoplus_{i=1}^r A/(a_i)$$

de modules monogènes, où les a_i vérifient $a_r | \cdots | a_1$ (et $a_i \notin A^*$, $a_i \neq 0$). Les entiers r et s et les a_i sont uniquement déterminés.

En particulier, le $k[X]$-module E_u, qui est de type fini et de torsion (car de dimension finie en tant qu'espace vectoriel sur k), est isomorphe à une somme directe

$$E_u \simeq \bigoplus k[X]/(P_i)$$

19. En fait on a facilement $\pi_{{}^t u} = \pi_u$, par exemple via l'isomorphisme $k[u] \xrightarrow{\sim} k[{}^t u]$ donné par $f \mapsto {}^t f$.

20. Si $M, N \in \mathbf{M}_n(k)$ sont semblables dans $\mathbf{M}_n(K)$, il existe $P \in \mathbf{GL}_n(K)$ telle que $M = PNP^{-1}$, i.e. telle que $MP = PN$. En déduire que le déterminant définit un polynôme non nul sur le sous-espace vectoriel $\{A \in \mathbf{M}_n(k) | MA = AN\}$ et conclure.

avec $P_r|\cdots|P_1$. On conclut en se rappelant que l'image F_i de $k[X]/(P_i)$ est un sous-espace cyclique, de polynôme minimal P_i (F_i étant engendré par l'image de $1 \in k[X]/(P_i)$).

4. Liens avec la réduction de Jordan

Lorsque le polynôme minimal de l'endomorphisme (ou la matrice) considéré est scindé, on dispose donc de deux réductions différentes : la réduction de Jordan, et la réduction précédente (parfois appelée réduction de Frobenius). Il est utile de savoir passer de l'une à l'autre.

Notons déjà qu'un bloc de Jordan d'ordre q et de valeur propre λ est semblable à la matrice compagnon $\mathcal{C}((X-\lambda)^q)$. On aura également besoin de la conséquence suivante du lemme chinois (à rapprocher du lemme 2.9) :

Lemme 4.1. *Soit $P = \prod \pi_i^{q_i}$ la décomposition d'un polynôme $P \in k[X]$ en produit d'irréductibles deux à deux non associés. La matrice compagnon $\mathcal{C}(P)$ est alors semblable à la matrice diagonale par blocs* $\operatorname{diag}(\mathcal{C}(\pi_i^{q_i}))$.

Démonstration. Soit u l'endomorphisme associé à la matrice $\mathcal{C}(P)$. Alors $\pi_u = \chi_u = P$ et on a les isomorphismes de $k[X]$-modules suivants :

$$E_u \simeq k[u] \simeq k[X]/(\pi_u) \simeq \prod k[X]/(\pi_i^{q_i})$$

(le dernier étant donné par le lemme chinois). Le sous-espace stable F_i image du sous-module $k[X]/(\pi_i^{q_i})$ est cyclique sous u (il est engendré par l'image de 1), de polynôme minimal $\pi_i^{q_i}$. Il existe donc une base de E adaptée à la décomposition $E = \oplus F_i$ dans laquelle la matrice de u est constituée des blocs $\mathcal{C}(\pi_i^{q_i})$. □

4.2. **De Frobenius à Jordan.** Le plus simple est d'aller de la réduction de Frobenius à celle de Jordan.

Soit donc $M \in \mathbf{M}_n(k)$ une matrice dont le polynôme minimal est scindé. Soient $P_r|\cdots|P_1 = \pi_M$ ses facteurs invariants. Si $\lambda_1, \ldots, \lambda_s$ désignent les valeurs propres de π_M (avec $\lambda_i \neq \lambda_j$ pour $i \neq j$), on peut écrire $P_i = \prod_j (X-\lambda_j)^{q_{ji}}$ (et, pour tout j, $q_{j1} \geqslant q_{j2} \geqslant \cdots$). Chacun des blocs $\mathcal{C}(P_i)$ apparaissant dans la réduction de Frobenius de M est donc semblable à la matrice constituée des blocs $\mathcal{C}((X-\lambda_j)^{q_{ji}})$, $j = 1, \ldots, s$, et chacun de ces blocs est à son tour semblable au bloc de Jordan d'ordre q_{ji} et de valeur propre λ_j.

La réduction de Jordan de M est donc la matrice consituée des blocs d'ordre q_{ji} et de valeur propre λ_j ainsi obtenus (et il y a autant de blocs que de coefficients non nuls parmi les q_{ji}).

Remarquons qu'on a en fait redémontré l'existence de cette réduction de Jordan [21].

4.3. **De Jordan à Frobenius.** Inversement, supposons connue la réduction de Jordan d'une matrice M annulant un polynôme scindé, dont on note encore $\lambda_1, \ldots, \lambda_s$ les valeurs propres (avec $\lambda_i \neq \lambda_j, i \neq j$). Chacun des blocs de Jordan apparaissant dans cette réduction est associé à un polynôme de la forme $(X-\lambda_i)^q$. On écrit sur une même ligne les polynômes $(X-\lambda_i)^{q_{ij}}$ provenant des blocs de Jordan de même valeur propre λ_i, classés par ordre décroissant des multiplicités q_{ij}. On a donc

$$\begin{matrix} (X-\lambda_1)^{q_{11}} & (X-\lambda_1)^{q_{12}} & \ldots \\ (X-\lambda_2)^{q_{21}} & (X-\lambda_2)^{q_{22}} & \ldots \\ \vdots & \vdots & \end{matrix}$$

avec $q_{i1} \geqslant q_{i2} \geqslant \cdots$ pour tout i.

21. L'argument direct repose sur l'étude du cas nilpotent. Voici un argument assez efficace, par récurrence sur $\dim E$: un endomorphisme $u \in \mathrm{L}(E)$ nilpotent (d'indice k) induit un endomorphisme $\bar{u}\colon E/\ker u \to E/\ker u$ nilpotent (d'indice $k-1$). Par récurrence, l'espace quotient $\bar{E} = E/\ker u$ est somme de sous-espaces cycliques $\bar{F}_i = \langle \bar{x}_i \rangle_{\bar{u}}$, $i = 1, \ldots, s$. Soient $x_1, \ldots, x_s$ des relèvements dans E de ces $\bar{x}_i$. On vérifie alors que la somme $F = \bigoplus_i \langle x_i \rangle_u$ est directe, et admet un supplémentaire N contenu dans $\ker u$. Dans une base adaptée à la décomposition $E = N \oplus \bigoplus_i \langle x_i \rangle_u$, la matrice de u est formée de blocs de Jordan de valeur propre nulle, comme attendu.

On obtient alors les invariants de similitude de M en formant les produits des éléments d'une même colonne.

Exercice 4.4. Justifier la méthode précédente.

Exemple 4.5. Si une matrice M admet une réduction de Jordan dont les blocs sont de polynômes minimaux

$$X^3, X, (X-1)^2, (X-1)^2, (X-2)^3, (X-2)^2, X-2, X-3,$$

on écrit alors

$$\begin{array}{ccc} X^3 & X & \\ (X-1)^2 & (X-1)^2 & \\ (X-2)^3 & (X-2)^2 & X-2 \\ X-3 & & \end{array}$$

d'où l'on déduit que les invariants de similitude de M sont

$$X-2, \quad X(X-1)^2(X-2)^2, \quad X^3(X-1)^2(X-2)^3(X-3).$$

Remarque 4.6. Je n'ai trouvé qu'une seule référence où cette présentation pratique est bien expliquée : [1], §5 no 4 p. 35, remarque 2. Signalons d'ailleurs que l'ensemble de ce paragraphe §5, consacré justement à la réduction des endomorphismes, est remarquablement détaillé. Il s'ouvre notamment par un très clair exposé du dictionnaire $k[X]$-modules / endomorphismes.

5. Endomorphismes semi-simples

Définition 5.1. Un endomorphisme $u \in \mathrm{L}(E)$ est dit *semi-simple* si tout sous-espace vectoriel $F \subset E$ stable par u admet un supplémentaire stable.

Remarque 5.2 (Exemples)**.**

(1) Un endomorphisme simple est semi-simple : puisque les seuls sous-espaces stables d'un endomorphisme simple sont $\{0\}$ et E, c'est automatique.

(2) Un endomorphisme diagonalisable est semi-simple : remarquons d'abord que, si $E = \oplus_i E_i$ où les $E_i = \ker(u - \lambda_i \mathrm{id}_E)$ sont les sous-espaces propres, alors tout sous-espace F stable par u est la somme directe $F = \bigoplus_i (F \cap E_i)$ (en effet, le polynôme minimal de la restriction u_F de u à F divise π_u, donc est scindé à racines simples, et ces racines sont parmi les λ_i ; la restriction u_F est donc diagonalisable, autrement dit F est somme directe $F = \bigoplus \ker(u_F - \lambda_i \mathrm{id}_F)$, et on conclut en observant que $\ker(u_F - \lambda_i \mathrm{id}_F)$ est exactement $\ker(u - \lambda_i \mathrm{id}_E) \cap F = E_i \cap F$). Puisque la restriction de u à E_i est une homothétie, tout sous-espace de E_i est stable par u. Soit donc F un sous-espace stable par u. Choisissons pour tout i un supplémentaire G_i de $F \cap E_i$ dans E_i. Alors $G = \bigoplus G_i$ est un supplémentaire de $F = \bigoplus (F \cap E_i)$ et est stable par u.

(3) Soit E un espace euclidien (ou hermitien). Un endomorphisme autoadjoint est semi-simple : en effet, l'orthogonal $F^\perp$ d'un sous-espace stable F est encore stable par F (c'est d'ailleurs ce qui permet de montrer qu'un endomorphisme auto-adjoint est diagonalisable).

Plus généralement, tout endomorphisme *normal* est semi-simple. Rappelons qu'un endomorphisme u d'un espace euclidien ou hermitien E est dit normal si $u^*u = uu^*$. Dans le cas hermitien [22], un tel endomorphisme est diagonalisable (car l'orthogonal d'un sous-espace propre d'un endomorphisme normal u est automatiquement stable par u, et que la restriction de u à un tel orthogonal est encore normale, puisque l'adjoint de la restriction est la restriction de l'adjoint) donc semi-simple. On peut alors diagonaliser u et u^* dans une même base, et en déduire que $u^* \in \mathbf{C}[u]$. Cela montre, a posteriori, que l'orthogonal de tout sous-espace stable est stable [23]. Ce résultat peut s'obtenir

22. Dans le cas euclidien, u n'est pas diagonalisable, mais admet une réduction sympathique (que l'on peut déduire du cas hermitien) qui permet de montrer la semi-simplicité.

23. Dans le cas euclidien, si $M \in \mathbf{M}_n(\mathbf{R})$ est la matrice d'un endomorphisme normal u, on a ${}^tM = Q(M)$ avec $Q \in \mathbf{R}[X]$, soit $u^* = Q(u)$, de sorte que l'orthogonal d'un sous-espace stable est encore stable.

directement (dans les cas euclidien ou hermitien) ainsi : soit F un sous-espace de E stable par u, et soit $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ la matrice de u dans une base orthonormée adaptée à la décomposition $E = F \oplus F^\perp$ de E. L'hypothèse $M^*M = MM^*$ équivaut à $A^*A = AA^* + BB^*$, $A^*B = BC^*$ et $B^*B + C^*C = CC^*$. En prenant la trace de la première égalité, on obtient $\mathrm{Tr}(BB^*) = 0$, ce qui entraîne $B = 0$ (si $B = (b_{ij})$, alors $\mathrm{Tr}(BB^*) = \sum_{i,j} |b_{ij}|^2$). Cela signifie que $F^\perp$ est stable par u, et les égalités $A^*A = AA^*$ et $C^*C = CC^*$ montrent également que les restrictions de u à F et à $F^\perp$ sont encore normales.

(4) Un endomorphisme nilpotent est semi-simple si et seulement si il est nul. En effet, supposons u nilpotent et semi-simple. Son noyau $\ker u$ est stable donc admet un supplémentaire stable G. La restriction u_G de u à G est alors injective. Comme u_G est aussi nilpotent, G est nul, et $\ker u$ est donc égal à E.

Proposition 5.3. *La restriction d'un endomorphisme semi-simple à un sous-espace stable est encore semi-simple.*

Démonstration. C'est une conséquence immédiate du théorème 5.5, mais il est intéressant d'en donner une preuve directe. Soit F un sous-espace stable par u. Soit $F' \subset F$ un sous-espace de F stable par u. Puisque u est semi-simple, F admet un supplémentaire stable G dans E. Le sous-espace $F' \oplus G$ est encore stable, donc admet un supplémentaire F'' stable par u. Ainsi $E = F' \oplus F'' \oplus G$. Vérifions que le sous-espace stable $G' = F \cap (F'' \oplus G)$ est un supplémentaire de F' dans F. L'intersection $F' \cap G'$ est évidemment nulle. Si $x = x' + y'$ est la décomposition de $x \in F$ avec $x' \in F'$ et $y' \in F'' \oplus G$, on constate que $y' = x - x'$ appartient à $(F'' \oplus G) \cap F = G'$. □

Remarque 5.4. Si u est semi-simple, on peut décomposer E en somme de sous-espaces stables par u tels que u induise un endomorphisme simple sur chacun de ces sous-espaces. En effet, il suffit de considérer un sous-espace stable non nul où u est simple (en prenant par exemple un sous-espace stable non nul de dimension minimale), puis de considérer la restriction de u à un supplémentaire stable, encore semi-simple d'après la proposition précédente, pour conclure par récurrence [24].

Théorème 5.5. *Un endomorphisme u est semi-simple si et seulement si son polynôme minimal π_u est sans-facteur carré (i.e. n'est divisible par aucun carré non constant dans $k[X]$).*

Démonstration. Si π_u s'écrit $\pi_u = P^2Q$ avec P non constant, montrons que $\ker(PQ)(u)$ n'admet pas de supplémentaire stable [25]. Soit F' un tel supplémentaire. Alors $P(u)(F') \subset F' \cap \ker(PQ)(u) = \{0\}$. On a donc $(PQ)(u) = 0$, ce qui contredit l'égalité $\pi_u = P^2Q$.

Réciproquement, supposons que $\pi_u = \prod \pi_i$ est produit d'irréductibles $\pi_1, \ldots, \pi_r$ deux à deux non associés. Soit $F \subset E$ un sous-espace stable. On a alors

$$F = \bigoplus_i F \cap \ker \pi_i(u)$$

car les projections sur chaque $E_i = \ker \pi_i(u)$ sont des polynômes en u. Il suffit de trouver pour tout i un supplémentaire de $F \cap E_i$ stable par $u_{|E_i}$ dans E_i et de former la somme de

24. Voici un autre argument : supposons qu'il existe F_1, F_2, …, F_r sous-espaces stables en somme directe tels que $u_{|F_i}$ est simple. Si $F_1 \oplus \cdots \oplus F_r = E$ le résultat est démontré. Sinon, puisque u est semi-simple, $F = F_1 \oplus \cdots \oplus F_r$ admet un supplémentaire stable. Il existe donc un sous-espace stable F_{r+1} non nul en somme directe avec F de dimension minimale. La restriction de u à F_{r+1} est alors simple. On conclut par récurrence.

25. On peut aussi montrer directement que, si u est semi-simple, alors π_u est sans carré : soit P un diviseur irréductible de π_u. Il existe alors un sous-espace $F \subset E$ stable tel que le polynôme minimal de la restriction de u à F soit $\pi_{u_{|F}} = P$ (en effet, il existe un sous-espace cyclique $\langle x \rangle_u$ de polynôme minimal π_u, et, si $\pi_u = PQ$, alors $F = \langle Q(u)(x) \rangle_u$ convient). Mais F admet un supplémentaire F' stable par u, et la restriction $u_{|F'}$ de u à F' est encore semi-simple. On conclut par récurrence sur la dimension, grâce à l'égalité $\pi_u = \mathrm{ppcm}(\pi_{u_F}, \pi_{u_{F'}}) = \mathrm{ppcm}(P, \pi_{u_{F'}})$.

ces sous-espaces. Mais [26] un sous-espace vectoriel $F' \subset E_i$ stable par $u_{|E_i}$ est exactement un sous-$k[u_{|E_i}]$-module de E_i (pour la structure de module définie par $u_{|E_i}$). Comme $\pi_{u_{|E_i}} = \pi_i$ est irréductible, l'anneau $k[u_{|E_i}] \simeq k[X]/(\pi_i)$ est un corps (c'est une extension de k de degré $\deg \pi_i$) : un k-sous-espace vectoriel de E_i stable par u est donc exactement un $k[X]/(\pi_i)$-sous-espace vectoriel de E_i. En particulier, tout sous-espace de E_i stable par u admet un supplémentaire stable. □

Remarque 5.6. On peut reformuler ainsi ce théorème : u est semi-simple si et seulement si l'algèbre $k[u]$ est un produit de corps, ou encore si et seulement si $k[u]$ est réduite (i.e. ne contient pas d'élément nilpotent non nul).

Corollaire 5.7. *Un endomorphisme u est semi-simple si et seulement si E admet une décomposition $E = \bigoplus E_i$ en somme directe de sous-espaces stables par u tels que les restrictions $u_{|E_i}$ à chacun de ces espaces soient simples.*

Démonstration. On a déjà remarqué (cf. remarque 5.4) qu'un endomorphisme semi-simple induit une décomposition de E en somme de sous-espaces stables où u définit un endomorphisme simple [27].

Inversement, si on dispose d'une telle décomposition, le polynôme minimal π_u de u est le ppcm des polynômes minimaux des restrictions $u_{|E_i}$ de u à chacun de ces E_i. Mais d'après la proposition 1.6, la simplicité de $u_{|E_i}$ implique que son polynôme minimal est irréductible, Ainsi π_u est sans facteur carré, et u est donc semi-simple [28]. □

Remarque 5.8. On obtient ainsi que la semi-simplicité généralise la notion de diagonalisabilité : si le polynôme minimal π_u d'un endomorphisme u de E est scindé, alors u est semi-simple si et seulement si u est diagonalisable. En particulier :

Corollaire 5.9. *Si k est algébriquement clos, $u \in \mathrm{L}(E)$ est semi-simple si et seulement si il est diagonalisable.*

5.10. **Semi-simplicité et géométrie des classes de similitude.** La notion de semi-simplicité joue un rôle crucial dans l'étude des classes de similitude. Plaçons nous sur $k = \mathbf{R}$ ou $\mathbf{C}$. Les classes de similitude forment une partition de $\mathbf{M}_n(k)$, et l'on peut étudier les aspects topologiques associés à cette partition. On a en particulier le résultat frappant suivant :

Théorème 5.11. *Soit $M \in \mathbf{M}_n(\mathbf{C})$ (resp. $\mathbf{M}_n(\mathbf{R})$). Alors la classe de conjugaison de M est fermée si et seulement si M est diagonalisable (resp. semi-simple).*

Démonstration. Si M est diagonalisable, sa classe de conjugaison est formée des matrices N diagonalisables ayant les mêmes valeurs propres avec les mêmes multiplicités. Notons de plus que N est semblable à M si et seulement si $\chi_N = \chi_M$ et $\pi_N = \pi_M$ (en effet, N est alors diagonalisable, et ses valeurs propres et leurs multiplicités sont celles de M). Autrement dit, la classe de conjugaison de M est exactement :

$$\mathbf{GL}_n(\mathbf{C}) \cdot M = \{N \in \mathbf{M}_n(\mathbf{C}) \mid \chi_N = \chi_M \ \text{ et } \ \pi_M(N) = 0\}.$$

26. Voici une présentation sans langage des modules de ce même argument : soit G_i un sous-espace de E_i maximal parmi les sous-espaces de E_i stables par u et en somme directe avec $F_i = F \cap E_i$. Montrons par l'absurde que c'est un supplémentaire de F_i dans E_i. Sinon, il existe $x \in E_i \setminus (F_i \oplus G_i)$. Alors $\langle x \rangle_u$ est un sous-espace de E_i sur lequel la restriction de u est simple (car cyclique de polynôme minimal π_i irréductible). Mais alors $\langle x \rangle_u \cap (F_i \oplus G_i) = \{0\}$ et $G_i \oplus \langle x \rangle_u$ est un sous-espace stable en somme directe avec F_i, ce qui contredit la maximalité de G_i.

27. On peut aussi le voir comme conséquence du théorème précédent et du théorème 3.1 : les facteurs invariants d'un endomorphisme semi-simple étant sans carré, on a (avec le lemme 4.1) une décomposition de E en somme de sous-espaces cycliques de polynômes minimaux irréductibles. D'après la proposition 1.6, u induit sur chacun de ces espaces un endomorphisme simple.

28. En voici une démonstration directe : si $F \subset E$ est un sous-espace stable, on montre par récurrence sur sa codimension que F admet un supplémentaire stable. En effet, E s'écrit $E = \bigoplus E_i$ comme somme de sous-espaces stables tels que $u_{|E_i}$ soit simple. Chacun des sous-espaces $F \cap E_i$ est stable par u, donc est égal $\{0\}$ ou E_i. Si $F \neq E$, il existe i tel que $F \cap E_i = \{0\}$. On obtient alors un supplémentaire stable de F en formant la somme de E_i et d'un supplémentaire stable de $F \oplus E_i$.

L'application $N \in \mathbf{M}_n(\mathbf{C}) \mapsto \chi_N \in \mathbf{C}[X]$ étant continue, cette classe de conjugaison est fermée[29].

Remarquons maintenant que l'adhérence de la classe de similitude de toute matrice $M \in \mathbf{M}_n(\mathbf{C})$ contient une matrice diagonalisable. Pour cela il suffit de trigonaliser M (utiliser la décomposition de Dunford est plus satisfaisant) : soit $P \in \mathbf{GL}_n(\mathbf{C})$ telle que $T = P^{-1}MP$ soit une matrice triangulaire supérieure. En notant Q_t la matrice $P_t = \mathrm{diag}(1, t, t^2, \ldots, t^{n-1})$ pour $t \in \mathbf{C}^*$, $Q_t^{-1}TQ_t$ tend vers la matrice diagonale $D = \mathrm{diag}(t_{11}, \ldots, t_{nn})$ quand t tend vers 0. En particulier, la matrice diagonale D appartient à l'adhérence de la classe de conjugaison de M. Si cette classe est fermée, M est nécessairement diagonalisable.

Le résultat sur $\mathbf{R}$ s'obtient en rappelant que deux matrices réelles sont conjuguées dans $\mathbf{M}_n(\mathbf{C})$ si et seulement si elles le sont dans $\mathbf{M}_n(\mathbf{R})$. □

La démonstration précédente montre en particulier que l'adhérence de la classe de similitude d'une matrice nilpotente contient 0. On a en fait :

Théorème 5.12. *Soit $M \in \mathbf{M}_n(k)$, $k = \mathbf{R}$ ou $\mathbf{C}$. Alors M est nilpotente si et seulement si 0 est contenu dans l'adhérence de la classe de conjugaison de M.*

Démonstration. Il reste à montrer que si 0 est contenu dans l'adhérence de l'orbite de M, alors M est nilpotente. Cela résulte immédiatement de la continuité de $N \mapsto \chi_N$. En effet, cette application est constante sur la classe de similitude de M, et envoie 0 sur X^n. On a donc $\chi_M = X^n$, i.e. M nilpotente. □

Remarque 5.13. La démonstration montre plus : la classe de similitude d'une matrice nilpotente N est un cône (épointé). En effet, on a vu que pour tout $t \neq 0$, tN est semblable à N.

Remarque 5.14. On est alors en mesure de comprendre la topologie quotient sur l'espace quotient

$$\mathbf{M}_n(\mathbf{C})/\mathbf{GL}_n(\mathbf{C}).$$

Il apparaît en particulier que certains points ne sont pas fermés : en fait le théorème précédent signifie que la classe de 0 est adhérente à celle de toute matrice nilpotente. Autrement dit le point $0 \in \mathbf{M}_n(\mathbf{C})/\mathbf{GL}_n(\mathbf{C})$ appartient à l'adhérence du point représentant la classe d'une matrice nilpotente. Pour éviter les désagréments liés à une telle situation, on peut considérer plutôt le quotient de l'ensemble des endomorphismes semi-simples par l'action par conjugaison de $\mathbf{GL}_n(\mathbf{C})$. Le quotient obtenu est alors séparé. En fait il est tout simplement homéomorphe à $\mathbf{C}^n$. On se contentera de montrer ici le théorème suivant :

Théorème 5.15. *Soit $\Delta_n(\mathbf{C})$ l'ensemble des matrices diagonalisables dans $\mathbf{M}_n(\mathbf{C})$. Alors l'ensemble quotient $\Delta_n(\mathbf{C})/\mathbf{GL}_n(\mathbf{C})$ pour l'action par conjugaison est en bijection avec $\mathbf{C}^n$.*

Démonstration. Deux matrices diagonalisables sont équivalentes si et seulement si elles ont le même polynôme caractéristique. Autrement dit, l'application

$$\begin{array}{rcl} \Delta_n(\mathbf{C}) & \xrightarrow{\varphi} & \{P \text{ unitaires } \in \mathbf{C}[X], \deg P \leqslant n\} \simeq \mathbf{C}^n \\ M & \longmapsto & \chi_M \end{array}$$

induit une bijection $\Delta_n(\mathbf{C})/\mathbf{GL}_n(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}^n$. □

Remarque 5.16. Cet énoncé est bien sûr valable sur tout corps algébriquement clos[30]. Il est instructif d'expliciter le comportement de la restriction de cette application à l'ensemble $D_n(\mathbf{C})$ des matrices diagonales. Cet ensemble s'identifie à $\mathbf{C}^n$, et φ envoie alors $(\lambda_1, \ldots, \lambda_n)$ sur les coefficients du polynôme $\prod_i (X - \lambda_i)$, autrement dit sur les fonctions symétriques

29. Voici une intéressante variante de l'argument : soient $\lambda_1, \ldots, \lambda_s$ les valeurs propres de M, et $d_i = \dim_{\mathbf{C}} \ker(M - \lambda_i I_n)$, $i = 1, \ldots, s$ leurs multiplicités. Alors N est semblable à M si et seulement si $\dim_{\mathbf{C}} \ker(N - \lambda_i I_n) \geqslant d_i$ pour tout $i = 1, \ldots, s$, autrement dit si et seulement si $\mathrm{rg}(N - \lambda_i I_n) \leqslant n - d_i$ pour tout $i = 1, \ldots, s$. Comme ces conditions équivalent à l'annulation de mineurs (de taille $n - d_i$), on a une autre description de la classe de M comme intersection de fermés.

30. Sur un corps quelconque il faut bien sûr remplacer diagonalisable par semi-simple.

élémentaires en les λ_i. On peut noter que deux matrices dans $D_n(\mathbf{C})$ sont semblables si et seulement si elles correspondent à des n-uplets déduits l'un de l'autre par une permutation $\sigma \in \mathfrak{S}_n$. On retrouve donc ici l'isomorphisme $\mathbf{C}^n/\mathfrak{S}_n \simeq \mathbf{C}^n$.

6. Polynômes sur $\mathbf{M}_n(\mathbf{C})$ invariants par conjugaison

On donne dans cette courte section [31] une description des fonctions polynomiales $\mathbf{M}_n(\mathbf{C}) \to \mathbf{C}$ invariantes sous l'action de $\mathbf{GL}_n(\mathbf{C})$ par conjugaison, autrement dit des fonctions polynômiales $f\colon \mathbf{M}_n(\mathbf{C}) \to \mathbf{C}$ telles que $f \circ g = f$ pour tout $g \in \mathbf{GL}_n(\mathbf{C})$. Rappelons une fois encore que l'on considère ici l'action de $\mathbf{GL}_n(\mathbf{C})$ sur $\mathbf{M}_n(\mathbf{C})$ par conjugaison, et que la condition précédente signifie donc

$$f(gMg^{-1}) = f(M) \quad \text{pour tout } M \in \mathbf{M}_n(\mathbf{C}) \text{ et tout } g \in \mathbf{GL}_n(\mathbf{C}).$$

Considérons à nouveau l'application $\varphi\colon \mathbf{M}_n(\mathbf{C}) \to \mathbf{C}^n$ associant à une matrice M quelconque les coefficients de son polynôme caractéristique χ_M. Cette application est continue, surjective, et admet une *section* [32]

$$\sigma\colon (a_0, \ldots, a_{n-1}) \in \mathbf{C}^n \mapsto \mathcal{C}(X^n + a_{n-1}X^{n-1} + \cdots + a_0) \in \mathbf{M}_n(\mathbf{C})$$

également continue. Noter que la matrice $\mathcal{C}(X^n + a_{n-1}X^{n-1} + \cdots + a_0)$ n'est pas toujours semi-simple, au contraire : la section σ sélectionne des matrices cycliques, dont les orbites sont très loin d'être fermées. On obtient alors le remarquable résultat suivant :

Proposition 6.1. *Pour toute application continue $f\colon \mathbf{M}_n(\mathbf{C}) \to Y$ de $\mathbf{M}_n(\mathbf{C})$ vers un espace topologique Y telle que $f \circ g = f$ pour tout $g \in \mathbf{GL}_n(\mathbf{C})$ (on dit que f est* invariante*), il existe une unique application continue $\bar{f}\colon \mathbf{C}^n \to Y$ telle que $f = \bar{f} \circ \varphi$, i.e. telle que $\bar{f}$ fasse commuter le diagramme*

$$\begin{tikzcd} \mathbf{M}_n(\mathbf{C}) \arrow[r, "f"] \arrow[d, "\varphi"'] & Y. \\ \mathbf{C}^n \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Démonstration. L'unicité est immédiate : en effet, l'égalité $f = \bar{f} \circ \varphi$ impose $\bar{f} = f \circ \sigma$.

Il reste à vérifier que $\bar{f} = f \circ \sigma$, qui est évidemment continue, satisfait la condition voulue, autrement dit que

$$f \circ \sigma \circ \varphi = f,$$

ce qui équivaut à $f(M) = f(\mathcal{C}(\chi_M))$ pour toute matrice $M \in \mathbf{M}_n(\mathbf{C})$. Les deux fonctions f et $f \circ \sigma \circ \varphi$ étant continues, il suffit de vérifier cette égalité sur l'ouvert dense constitué des matrices diagonalisables à valeurs propres deux à deux distinctes, où c'est évident (en effet, $\mathcal{C}(\chi_M)$ est alors semblable à M, et l'invariance de f assure que $f(M) = f(\mathcal{C}(\chi_M))$) [33]. □

L'application continue $\varphi\colon \mathbf{M}_n(\mathbf{C}) \to \mathbf{C}^n$ jouit donc d'une certaine propriété universelle relative aux applications continues invariantes sous l'action de $\mathbf{GL}_n(\mathbf{C})$: c'est en un certain sens « le quotient de $\mathbf{M}_n(\mathbf{C})$ par $\mathbf{GL}_n(\mathbf{C})$ » (bien que φ n'induit absolument pas une bijection entre $\mathbf{M}_n(\mathbf{C})/\mathbf{GL}_n(\mathbf{C})$ et $\mathbf{C}^n$).

On peut en déduire le théorème suivant :

---

31. Signalons que cette section est indépendante de ce qui précède : on utilise seulement la densité de l'ensemble des matrices à valeurs propres deux à deux distinctes, et le fait qu'une telle matrice est semblable à la matrice compagnon associée à son polynôme caractéristique (autrement dit qu'une matrice à valeurs propres deux à deux distinctes est diagonalisable). On aurait donc pu faire figurer le contenu de cette section dans la section 1. Il est cependant souhaitable d'avoir en tête les résultats concernant la géométrie des classes de conjugaison présentés dans la section précédente.

32. Rappelons que dire que σ est une section de φ signifie simplement que $\varphi \circ \sigma = \mathrm{id}_{\mathbf{C}^n}$.

33. On peut aussi remarquer (en considérant les réduites de Jordan) que toute matrice M appartient à l'adhérence de l'orbite de $\mathcal{C}(\chi_M)$ (en fait l'ensemble des matrices de polynôme caractéristique P est précisement l'adhérence de l'orbite de la matrice compagnon $\mathcal{C}(P)$ associée à P). Comme f est à la fois continue et constante sur chaque orbite, la valeur $f(M)$ de f en M coïncide donc avec $f(\mathcal{C}(\chi_M))$.

Théorème 6.2 (Polynômes invariants sur $\mathbf{M}_n(\mathbf{C})$)**.** *Soit $f \in \mathbf{C}[X_{ij}, 1 \leqslant i,j \leqslant n]$ une fonction polynomiale $f\colon \mathbf{M}_n(\mathbf{C}) \to \mathbf{C}$ définie sur l'espace des matrices. Si f est invariante par conjugaison (i.e. vérifie $f \circ g = f$ pour tout $g \in \mathbf{GL}_n(\mathbf{C})$), alors il existe un unique polynôme $P \in \mathbf{C}[T_1, \dots, T_n]$ tel que*

$$f(M) = P(\sigma_1(M), \dots, \sigma_n(M))$$

où $\sigma_1, \dots, \sigma_n$ désignent les coefficients du polynôme caractéristique (de sorte que $\chi_M(X) = X^n - \sigma_1(M)X + \cdots + (-1)^n\sigma_n(M)$).

Démonstration. La fonction $f\colon \mathbf{M}_n(\mathbf{C}) \to \mathbf{C}$ est continue et invariante. D'après la proposition 6.1, il existe alors $\bar{f}\colon \mathbf{C}^n \to C$ telle que $f = \bar{f} \circ \varphi$. De plus, l'égalité $\bar{f} = f \circ \sigma$ montre que $\bar{f}$ est une fonction polynomiale sur $\mathbf{C}^n$, et la conclusion suit. □

7. Matrices à coefficients dans un anneau principal

Soit A un anneau principal.

Théorème 7.1. *Soit $M \in \mathbf{M}_n(A)$. Il existe deux matrices inversibles $P, Q \in \mathbf{GL}_n(A)$ et des éléments $a_1, a_2, \dots, a_r \in A$ tels que*

$$M = P \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & 0 & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix} Q \qquad \text{et} \qquad a_1 \mid a_2 \mid \cdots \mid a_r.$$

De plus, les éléments $a_1, \dots, a_r$ sont uniquement déterminés (à multiplication par des inversibles près).

Démonstration. Voir [3], 6.2.1. □

Remarque 7.2.

— Puisque les éléments $a_1, \dots, a_r$ caractérisent la classe d'équivalence de $M \in \mathbf{M}_n(A)$, il est tentant de les appeler également « facteurs invariants » de M. On aurait cependant pour $A = k$ une incompatibilité avec la définition donnée plus haut [34].

— Lorsque A est euclidien, on peut donner une démonstration effective de ce résultat, qui montre également qu'on peut choisir pour P et Q des produits de matrices de la forme $I + aE_{ij}$ avec $i \neq j$ et $a \in A$ (où E_{ij} désigne la matrice que l'on imagine).

Théorème 7.3. *Soient $M, N \in \mathbf{M}_n(k)$. Les matrices M et N sont conjuguées (dans $\mathbf{M}_n(k)$) si et seulement si $XI_n - M$ et $XI_n - N$ sont équivalentes dans $\mathbf{M}_n(k[X])$.*

Démonstration. Il suffit de montrer que la classe d'équivalence de $XI_n - M$ est caractérisée par la classe de similitude de M, i.e. par ses facteurs invariants. Et il suffit pour cela de montrer que la classe d'équivalence de $XI_n - \mathcal{C}(P)$ est caractérisée par $P \in k[X]$. Mais on voit facilement que, si $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, la matrice $XI_n - \mathcal{C}(P)$ est équivalente (dans $\mathbf{M}_n(A)$) à $\begin{pmatrix} 0 & 0 & \cdots & 0 & P(X) \\ -1 & 0 & \ddots & \vdots & a_1 \\ 0 & -1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & -1 & a_{n-1} \end{pmatrix}$, qui est clairement équivalente à la matrice diagonale $\mathrm{diag}(1, \dots, 1, P(X))$.

Cela montre que les polynômes caractérisant la classe d'équivalence de $XI_n - M$ (dans $\mathbf{M}_n(A)$) sont les facteurs invariants de $M \in \mathbf{M}_n(k)$ (et des 1). □

34. On peut aussi, comme dans [3], décider d'appeler facteurs invariants ces éléments, et nommer alors « invariants de similitudes » ou « polynômes invariants » les polynômes appelés ici facteurs invariants...

Remarque 7.4. Les polynômes caractérisant la classe d'équivalence dans $\mathbf{M}_n(k[X])$ d'une matrice de la forme $XI_n - M$ avec $M \in \mathbf{M}_n(k)$ sont ainsi (à l'ordre et aux 1 près) les facteurs invariants de M. En particulier, ils sont tous non nuls.

Remarque 7.5. On peut également retrouver le théorème 3.1 à partir du théorème 7.1 (en donnant en fait une démonstration directe du théorème 7.3) : voir [3], Théorème 6.3.1.

8. Exercices

Dans ces exercices, E désigne un espace vectoriel de dimension finie sur un corps k, et $u \in \mathrm{L}(E)$ un endomorphisme de cet espace.

Exercice 8.1. Si $E = E_1 \oplus E_2$ est somme de deux sous-espaces stables par u, et si u_i désigne la restriction de u à E_i, montrer que $\pi_u = \mathrm{ppcm}(\pi_{u_1}, \pi_{u_2})$.

Exercice 8.2. Soit $P \in k[X]$. Montrer que le polynôme minimal de la restriction de u à $\ker P(u)$ est égal à $\pi_{u_{|\ker P(u)}} = \mathrm{pgcd}(\pi_u, P)$.

Exercice 8.3. Soit $r \geqslant 1$. Montrer que, si $M \in \mathbf{M}_n(\mathbf{C})$ est une matrice inversible dont une puissance M^r est diagonalisable, alors M est diagonalisable. Qu'en est-il si M n'est plus inversible ? si $M \in \mathbf{M}_n(\mathbf{R})$?

Exercice 8.4. Quand un endomorphisme cyclique est-il diagonalisable ?

Exercice 8.5. Soient $M \in \mathbf{M}_n(k)$, et $t \in k \setminus \{0\}$. Montrer que si M est nilpotente, alors M et tM sont semblables. Réciproquement, montrer que si t n'est pas une racine de l'unité dans k et que M et tM sont semblables, alors M est nilpotente.

Exercice 8.6. Quels sont les facteurs invariants
- d'une homothétie ?
- d'un endomorphisme diagonalisable à valeurs propres deux à deux distinctes ?
- d'une projection ?

Plus généralement, comment exprimer les facteurs invariants d'un endomorphisme diagonalisable en fonction des valeurs propres et de leurs multiplicités ?

Exercice 8.7 (Sous-espaces stables)**.** Soient E un k-espace vectoriel, et $u \in \mathrm{L}(E)$.

(1) Si $k = \mathbf{C}$, montrer que, pour tout $m = 0, \ldots, n = \dim E$, il existe un sous-espace de E stable par u de dimension m.

(2) Si $k = \mathbf{R}$ (et $\dim E \geqslant 2$), montrer que E admet une droite ou un plan stable[35] par u. Quelles sont les dimensions des sous-espaces de E stables par u ? (On pourra distinguer les cas selon que E est de dimension paire ou impaire.)

(3) Si $k = \mathbf{Q}$, montrer qu'il existe toujours un endomorphisme simple $u \in \mathrm{L}(E)$.

Exercice 8.8. Combien y a-t-il de classes de conjugaison de matrices nilpotentes dans $\mathbf{M}_n(k)$?

Exercice 8.9. Donner la réduction de Jordan de la matrice $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Exercice 8.10. Soient $P, Q \in k[X]$. Montrer que les facteurs invariants de la matrice

$$\begin{pmatrix} \mathcal{C}(P) & 0 \\ 0 & \mathcal{C}(Q) \end{pmatrix}$$

sont $\mathrm{pgcd}(P, Q)$ et $\mathrm{ppcm}(P, Q)$.

Plus généralement, comment exprimer les facteurs invariants de la matrice diagonale par blocs $\mathrm{diag}(\mathcal{C}(P_1), \ldots, \mathcal{C}(P_s))$?

35. Pour un argument élémentaire, voir que pour tout diviseur D non constant de π_u, $D(u)$ est non injectif, et considérer un élément non nul du noyau de $D(u)$ pour D irréductible...

Exercice 8.11. Le but de cet exercice est d'établir que toute matrice $M \in \mathbf{M}_n(\mathbf{C})$ est semblable à une matrice symétrique.

(1) Soit $P(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_0 =\in k[X]$ un polynôme unitaire. Montrer qu'il existe $b_1, \ldots, b_n \in k^n$ tels que $b_1 = 1$ et $S_b\mathcal{C}(P)$ est une matrice symétrique, où S_b désigne la matrice $S_b = \begin{pmatrix} 0 & 0 & \cdots & 0 & b_1 \\ 0 & & & b_1 & b_2 \\ \vdots & & & \vdots & \vdots \\ 0 & b_1 & \cdots & b_{n-2} & b_{n-1} \\ b_1 & b_2 & \cdots & b_{n-1} & b_n \end{pmatrix}$.

(2) Soit $M \in \mathbf{M}_n(k)$. Montrer qu'il existe une matrice symétrique inversible S telle que SM est symétrique. En déduire qu'il existe P symétrique inversible telle que $M = P^t M P^{-1}$.

(3) Si $k = \mathbf{C}$, montrer que toute matrice symétrique inversible P s'écrit $P = {}^tQQ$ avec Q inversible. (Indication : utiliser la réduction des formes quadratiques.)

(4) Conclure : toute matrice $M \in \mathbf{M}_n(\mathbf{C})$ est semblable à une matrice symétrique. (En fait il suffit de se placer sur un corps de caractéristique différente de 2 dans lequel tout élément admet une racine carrée.)

(5) Donner un exemple de matrice $M \in \mathbf{M}_n(\mathbf{C})$ symétrique non diagonalisable.

Références

[1] Nicolas Bourbaki, Algèbre, Chapitre 7.

[2] Jean-Jacques Risler et Pascal Boyer, Algèbre pour la Licence 3.

[3] Denis Serre, Les Matrices.