Invariants de similitude

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

Références : [BMP, Gou].

1 Introduction

Soit k un corps et soit E un k-espace vectoriel de dimension finie. On dit que $u, v \in \mathrm{L}(E)$ sont *conjugués* s'il existe $\phi \in \mathrm{GL}(E)$ tel que $u = \phi v \phi^{-1}$. Les classes de conjugaisons sont aussi appelées *classes de similitudes*.

Définition 1.1. — Un *invariant partiel de similitude* sur E est la donnée d'un ensemble $\mathcal{X}$ et d'une application $I : \mathrm{L}(E) \to \mathcal{X}$ tel que pour tout $u, v \in \mathrm{L}(E)$ on a :

$$u \text{ et } v \text{ sont semblables } \implies I(u) = I(v).$$

— Un *invariant (complet) de similitude* sur E est la donnée d'un ensemble $\mathcal{X}$ et d'une application $I : \mathrm{L}(E) \to \mathcal{X}$ tel que pour tout $u, v \in \mathrm{L}(E)$ on a :

$$u \text{ et } v \text{ sont semblables } \iff I(u) = I(v).$$

Proposition 1.2. *Soit $\mathcal{X}$ un ensemble et $I : \mathrm{L}(E) \to \mathcal{X}$ une application. Alors I est un invariant partiel de similitude si et seulement si I est invariant par conjugaison.*

Exemple 1.3. La trace, le déterminant ($\mathcal{X} = k$), le rang ($\mathcal{X} = \mathbb{N}$), le polynôme caractéristique ($\mathcal{X} = k[X]$), etc. sont des invariants partiels de similitude.

Exemple 1.4. Si $\mathcal{X}$ est l'ensemble des classes de conjugaison de $\mathrm{L}(E)$ alors l'application qui à u associe sa classe de conjugaison est un invariant de similitude.

On aimerait avoir un invariant avec un $\mathcal{X}$ assez simple. L'un des buts de ce complément est d'énoncer le théorème suivant, où $\mathcal{X}$ est l'ensemble des suites à au plus $\dim k$ termes d'éléments de $k[X]$.

Définition 1.5. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in k[X]$. La *matrice compagnon* associée à P est

$$\mathrm{C}_P \coloneqq \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{Mat}_n(k)$$

Remarque 1.6. Si $P = X + a_0$ alors $\mathrm{C}_P = \begin{pmatrix} -a_0 \end{pmatrix} \in \mathrm{Mat}_1(k)$.

Théorème 1.7 (Réduction de Frobenius[1])**.** *Soit $M \in \mathrm{Mat}_n(k)$. Il existe unique famille $(P_1, \dots, P_s)$ de polynômes unitaires non constants de $k[X]$ avec $1 \leq s \leq n$ et $P_s \mid \cdots \mid P_1$ telle que M soit semblable à la matrice*

$$\begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_s} \end{pmatrix}.$$

De plus, on a $\pi_M = P_1$ et $\chi_M = P_1 \cdots P_s$.

Définition 1.8. Soit $u \in \mathrm{L}(E)$ et soit $\mathcal{B}$ une base de E. Les polynômes $P_1, \dots, P_s$ précédents associés à la matrice $\mathrm{mat}_{\mathcal{B}}(u)$ (ne dépendent pas de $\mathcal{B}$ et) sont appelés les *invariants de similitude* de u.

Corollaire 1.9. *Deux endomorphismes $u, v \in \mathrm{L}(E)$ sont conjugués si et seulement si u et v ont les mêmes invariants de similitude.*

2 Échauffement : matrice compagnon

Soit $P \in k[X]$ unitaire non constant. La proposition suivante est classique.

Proposition 2.1. *Le polynôme caractéristique de la matrice compagnon C_P est P.*

La proposition suivante est encore classique, mais nous allons en donner deux démonstrations.

Proposition 2.2. *Le polynôme minimal de la matrice compagnon C_P est P.*

Première démonstration. Soit n le degré de P et soit $i \in \{0, \dots, n-1\}$. On remarque que la première colonne de C_P^i est le vecteur e_{i+1} de la base canonique de k^n. Ainsi, la famille $\{I_n, \mathrm{C}_P, \dots, C_P^{n-1}\}$ est libre donc $\deg \pi_{\mathrm{C}_P} \geq n$. D'après le théorème de Cayley–Hamilton et la proposition précédente, on a $\pi_{\mathrm{C}_P} \mid P$ d'où $\pi_{\mathrm{C}_P} = P$ puisque P est unitaire. □

Deuxième démonstration. Écrivons $P = X^n + \sum_{i=0}^{n-1} a_i X^i$, soit $(e_1, \dots, e_n)$ la base canonique de k^n et soit u l'endomorphisme associé. Pour chaque $i \in \{1, \dots, n-1\}$ on a

$$u(e_i) = e_{i+1} = u^i(e_1),$$

et

$$u(e_n) = \sum_{i=0}^{n-1} -a_i e_{i+1},$$

d'où

$$u^n(e_1) = -\sum_{i=0}^{n-1} a_i u^i(e_1) \text{ i.e. } P(u)(e_1) = 0.$$

En particulier, la famille $\big(e_1, u(e_1), \dots, u^{n-1}(e_1)\big) = (e_1, \dots, e_n)$ est une base de k^n. L'application $\Phi : k^n \to k[X]/(P)$ définie sur cette base par

$$\Phi\big(u^i(e_1)\big) \coloneqq X^i,$$

pour tout $i \in \{0, \dots, n-1\}$, est donc un isomorphisme d'espace vectoriels. De plus, la propriété suivante est vérifiée :

$$\Phi \circ u = \mu_X \circ \Phi,$$

1. Georg Ferdinand Frobenius, 1849–1917

où μ_X est l'endomorphisme de multiplication par X dans $k[X]/(P)$. En effet, pour $i \in \{0, \dots, n-2\}$ on a

$$\begin{aligned}\Phi(u(u^i(e_1))) &= \Phi(u^{i+1}(e_1)) \\ &= X^{i+1} \\ &= X \cdot \Phi(u^i(e_1)),\end{aligned}$$

et

$$\begin{aligned}\Phi(u(u^{n-1}(e_1))) &= \Phi(u^n(e_1)) \\ &= -\sum_{i=0}^{n-1} a_i \Phi(u^i(e_1)) \\ &= -\sum_{i=0}^{n-1} a_i X^i \\ &= X^n \\ &= X \cdot \Phi(u^{n-1}(e_1)).\end{aligned}$$

Ainsi, on a $u = \Phi^{-1} \circ \mu_X \circ \Phi$ donc u et μ_X ont le même polynôme minimal. On conclut par le lemme suivant.

Lemme 2.3. *Le polynôme minimal de μ_X dans $k[X]/(P)$ est P.*

Démonstration. Soit Π le polynôme minimal de μ_X dans $k[X]/(P)$. On a $\Pi \mid P$ puisque $P(\mu_X)$ est la multiplication par $P(X)$ dans $k[X]/(P)$, or P y est nul. Réciproquement, puisque $0 = \Pi(\mu_X)$ est la multiplication par $\Pi(X)$ dans $k[X]/(P)$ on a $0 = \Pi(\mu_X)(1) = \Pi(X) \cdot 1 = \Pi(X)$ dans $k[X]/(P)$ donc $P \mid \Pi$ par définition du quotient. On conclut puisque P est unitaire. □

□

3 Structures de $k[X]$-module sur E

Soit E un k-espace vectoriel de dimension finie et soit $u \in \mathrm{L}(E)$. On munit E d'une structure de $k[X]$-module où :

— l'action de k est celle de la structure de k-espace vectoriel sur E ;

— l'action de X est donnée par celle de u, autrement dit, on a $X \cdot x \coloneqq u(x)$ pour tout $x \in E$.

Ainsi, pour tout $P \in k[X]$ et $x \in E$ on a $P \cdot x = P(u)(x)$. On note E_u l'espace vectoriel E vu comme $k[X]$-module.

Voici deux propositions qui permettent de jouer un peu avec cette vision.

Proposition 3.1. *Soit $u \in \mathrm{L}(E)$. On a une correspondance bijective entre les sous-k-espaces vectoriels de E stables par u et les sous-$k[X]$-modules de E_u.*

Démonstration. Soit F un sous-k-espace vectoriel de E. Le sous-k-espace vectoriel $F \subseteq E$ est stable par u si et seulement si $F \subseteq E_u$ est stable par μ_X. □

On rappelle que si M et N sont des A-modules, on désigne par $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-module de M vers N. C'est l'ensemble des applications additives $f : M \to N$

qui commutent avec la structure de A-module, c'est-à-dire, qui vérifient

$$\begin{aligned} \forall m, m' \in M, && f(m+m') = f(m) + f(m'), \\ \forall a \in A, \forall m \in M, && f(a \cdot m) = a \cdot f(m), \end{aligned}$$

On note $\mathrm{End}_A(M) \coloneqq \mathrm{Hom}_A(M, M)$.

Proposition 3.2. *Soient E, F deux k-espaces vectoriels et $u \in \mathrm{L}(E)$ et $v \in \mathrm{L}(F)$. Un élément $\phi \in \mathrm{Hom}_{k[X]}(E_u, F_v)$ est une application linéaire $\phi : E \to F$ qui vérifie $\phi \circ u = v \circ \phi$. En particulier, on a*

$$\mathrm{End}_{k[X]}(E_u) = \mathrm{Comm}(u),$$

où

$$\mathrm{Comm}(u) \coloneqq \{w \in \mathrm{L}(E) : w \circ u = u \circ w\},$$

est le commutant de u.

Démonstration. Soit $\phi \in \mathrm{L}(E, F)$. On a

$$\begin{aligned} \phi \in \mathrm{Hom}_{k[X]}(E_u, F_v) &\iff \forall x \in E, \phi(X \cdot x) = X \cdot \phi(x) \\ &\iff \forall x \in E, \phi(u(x)) = v(\phi(x)) \\ &\iff \phi \circ u = v \circ \phi. \end{aligned}$$

□

Corollaire 3.3. *Deux endomorphismes $u, v \in \mathrm{L}(E)$ sont semblables si et seulement si les $k[X]$-modules E_u et E_v sont isomorphes.*

On peut déjà faire des choses avec cette observation.

Lemme 3.4. *Soit $u \in \mathrm{L}(E)$ et soient $P_1, \dots, P_r \in k[X]$ unitaires non constants. La matrice de u dans une base est $\mathrm{diag}(\mathrm{C}_{P_1}, \dots, C_{P_r})$ si et seulement si $E_u \simeq \oplus_{i=1}^r k[X]/(P_i)$ en tant que $k[X]$-modules.*

Démonstration. Il suffit de montrer le cas $r = 1$, le cas général découlant de la Proposition 3.1. Mais le cas $r = 1$ est exactement la deuxième démonstration donnée pour la Proposition 2.2. □

Remarque 3.5. Dans le lemme on n'a pas nécessairement de relation de divisibilité (comparer avec le Théorème 1.7) !

Exemple 3.6. Les matrices

$$A \coloneqq \begin{pmatrix} 0 & 2 & & & \\ 1 & 1 & & & \\ & & 0 & 0 & 0 \\ & & 1 & 0 & 0 \\ & & 0 & 1 & -1 \end{pmatrix}$$

et

$$B \coloneqq \begin{pmatrix} 0 & 0 & 0 & 0 & \\ 1 & 0 & 0 & 0 & \\ 0 & 1 & 0 & 2 & \\ 0 & 0 & 1 & 1 & \\ & & & & -1 \end{pmatrix}$$

sont semblables si k est de caractéristique différente de 2. Tout d'abord, un bon réflexe est de regarder si les traces (et ici, les déterminants, car faciles à calculer) coïncident, ce qui est le cas. Maintenant, par le Lemme 3.4 on trouve pour A

$$\begin{aligned} E_A &\simeq k[X]/\langle X^2 - X - 2\rangle \oplus k[X]/\langle X^3 + X^2\rangle \\ &\simeq k[X]/\langle (X+1)(X-2)\rangle \oplus k[X]/\langle X^2(X+1)\rangle, \end{aligned}$$

et pour B

$$\begin{aligned} E_B &\simeq k[X]/\langle X^4 - X^3 - 2X^2\rangle \oplus k[X]/\langle X+1\rangle \\ &\simeq k[X]/\langle X^2(X+1)(X-2)\rangle \oplus k[X]/\langle X+1\rangle \\ &\simeq E_A, \end{aligned}$$

le dernier isomorphisme découlant du lemme chinois [2] (on a $0 \neq 2$ par hypothèse sur la caractéristique de k). Ainsi, par le Corollaire 3.3 les matrices A et B sont semblables.

On suppose maintenant que k est de caractéristique 2. On remarqu'alors A et B n'ont pas le même rang donc ne sont pas semblables. On va quand même montrer comment se passe le calcul : on a

$$\begin{aligned} E_A &\simeq k[X]/\langle (X+1)X\rangle \oplus k[X]/\langle X^2(X+1)\rangle, \\ E_B &\simeq k[X]/\langle X^3(X+1)\rangle \oplus k[X]/\langle X+1\rangle, \end{aligned}$$

donc puisque $(X+1)X \mid X^2(X+1)$ (resp. $X+1 \mid X^3(X+1)$), par le Théorème 1.7 on sait que les invariants de similitude de A (resp. B) sont $X^2(X+1)$ et $(X+1)X$ (resp. $X^3(X+1)$ et $X+1$), donc on retrouve bien le fait que A et B ne sont pas semblables. On peut aussi remarquer que, en pensant secrètement à la mention du polynôme minimal dans le Théorème 1.7, le polynôme $X^2(X+1)$ va annuler A mais pas B (on a $\pi_A = X^2(X+1)$ et $\pi_B = X^3(X+1)$).

Illustrons l'exemple précédent avec Sage. On définit d'abord les deux matrices (sur $\mathbb{Q}$) :

```
A = block_diagonal_matrix(matrix([[0,2],
                                  [1,1]]),
                          matrix([[0,0,0],
                                  [1,0,0],
                                  [0,1,-1]]));

B = block_diagonal_matrix(matrix([[0,0,0,0],
                                  [1,0,0,0],
                                  [0,1,0,2],
                                  [0,0,1,1]]),
                          matrix([-1]));
```

puis on teste si elles sont conjuguées (sur $\mathbb{Q}$) avec `A.is_similar(B)`. L'option `transformation=true` renvoie une matrice de passage.

La forme des matrices de l'exemple précédent fait penser à des réduites de Frobenius, comme dans le Théorème 1.7. On va maintenant donner une idée de comment obtenir une telle réduite, via la théorie des $k[X]$-modules de type fini.

2. On a bien le droit car les structures de $k[X]$-modules sur les quotients de $k[X]$ sont compatibles avec la structure d'anneau.

Théorème 3.7 (Théorème de structure)**.** *Soit E un k-espace vectoriel de dimension finie et $u \in \mathrm{L}(E)$. Il existe un unique entier $s \in \{1, \dots, \dim E\}$ et une unique famille $(P_1, \dots, P_s)$ de polynômes unitaires non constants de $k[X]$ vérifiant $P_s \mid \cdots \mid P_1$ tels que l'on ait un isomorphisme de $k[X]$-modules*

$$E_u \simeq \bigoplus_{i=1}^{s} k[X]/(P_i).$$

Remarque 3.8. L'énoncé se généralise aux modules de type fini sur un anneau principal.

Étant donné le Théorème 3.7 de structure, par le Lemme 3.4 on obtient bien la matrice réduite de Frobenius du Théorème 1.7. En particulier, les polynômes $P_1, \dots, P_s$ sont les invariants de similitude de u.

Exemple 3.9. D'après le Lemme 3.4, si $P \in k[X]$ est unitaire non constant alors P est l'unique invariant de similitude de C_P.

Exemple 3.10. Les invariants de similitude des matrices A et B de l'Exemple 3.6, dans le cas où k est de caractéristique impaire, sont $X^2(X-2)(X+1)$ et $X+1$, et non pas $(X-2)(X+1)$ et $X^2(X+1)$.

4 Calcul des invariants de similitude

Le Théorème 3.7 de structure est bien joli, mais comment calculer les P_i ? La *forme normale de Smith* donne la réponse à cette question.

Théorème 4.1 (Forme normale de Smith)**.** *Soit $M \in \mathrm{Mat}_n(k[X])$. Il existe un unique $r \in \{0, \dots, n\}$ et une unique famille $(Q_1, \dots, Q_r)$ de polynômes unitaires (non nuls) de $k[X]$ vérifiant $Q_1 \mid \cdots \mid Q_r$ tels que M soit équivalente dans $\mathrm{Mat}_n(k[X])$ à*

$$\mathrm{diag}(Q_1, \dots, Q_r, 0, \dots, 0),$$

autrement dit, tels qu'il existe des matrices inversibles $U, V \in \mathrm{GL}_n(k[X])$ de sorte que

$$M = U\,\mathrm{diag}(Q_1, \dots, Q_r, 0, \dots, 0)V.$$

La famille $(Q_1, \dots, Q_r)$ est la famille des *facteurs invariants* de M. L'idée de la preuve repose sur la démarche suivante :

- on permute des lignes et colonnes de M afin de mettre un élément Q de degré minimal de M en haut à gauche ;
- on fait la division euclidenne de chaque élément de la première ligne de M par Q, en remplaçant Q par le reste (via des opérations sur les colonnes) si ce dernier est non nul ;
- pareil pour la première colonne.

Notons que lors de la dernière étape, les coefficients de la sous-matrice $\widetilde{M}$ inférieure droite $(n-1) \times (n-1)$ de M ne changent pas puisque la première ligne (excepté le premier coefficient) ne comporte que des 0. Après cette dernière étape, tous les coefficients de la première ligne et colonne de M sont donc nuls, excepté l'élément $\widetilde{Q}$ en haut à gauche. Si un élément non nul de $\widetilde{M}$ de divise pas $\widetilde{Q}$, on rajoute sa colonne à la première de M et on retourne à l'étape précédente, sinon on recommence l'algorithme dans $\widetilde{M}$.

Remarque 4.2. C'est une généralisation de la décomposition donnant le rang d'une matrice. De façon analogue au Théorème 3.7 de structure, l'énoncé se généralise aux cas des matrices de taille $m \times n$ sur un anneau principal (euclidien pour l'algorithme).

Remarque 4.3. Avec Sage, la forme normale de Smith s'obtient avec l'instruction `smith_form`. Attention, cette instruction renvoie un triplet avec les matrices de passage : la matrice diagonale est la première composante. Par exemple, si l'on veut trouver la forme normale de Smith de la matrice A de l'Exemple 3.6 sur les rationnels, on peut utiliser les instructions suivantes :

```
_.<X> = QQ[]

(A - X).smith_form()[0]
```

ou bien simplement `(A-X).elementary_divisors()`.

Le théorème suivant donne une façon de calculer les invariants de similitude d'une matrice.

Théorème 4.4. *Soit $M \in \mathrm{Mat}_n(k)$. Les invariants de similitude de M sont les facteurs invariants non inversibles de $M - XI_n$. Autrement dit, deux matrices $M, N \in \mathrm{Mat}_n(k)$ sont semblables si et seulement si $M - XI_n$ et $N - XI_n$ sont équivalentes dans $\mathrm{Mat}_n(k[X])$.*

Démonstration. D'après notre Théorème 1.7, il suffit de traiter le cas où $M = \mathrm{C}_P$ où $P \in k[X]$ est unitaire non constant. On veut montrer que le seul invariant de similitude non inversible de $\mathrm{C}_P - XI_n$ est P. On s'inspire de la technique de preuve de la Proposition 2.1. On écrit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ et on note $\equiv$ la relation d'équivalence dans $\mathrm{Mat}_n(k[X])$.

$$\mathrm{C}_P - XI_n = \begin{pmatrix} -X & 0 & \cdots & 0 & -a_0 \\ 1 & -X & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & -X & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -X - a_{n-1} \end{pmatrix}$$

$$\equiv \begin{pmatrix} 0 & 0 & \cdots & 0 & -P \\ 1 & -X & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & -X & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -X - a_{n-1} \end{pmatrix} \qquad (L_1 \leftarrow L_1 + \sum_{i=2}^{n} X^{i-1} L_i),$$

$$\equiv \begin{pmatrix} 0 & \cdots & \cdots & 0 & -P \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix} \qquad (C_i \leftarrow C_i + XC_{i-1}, \quad \text{pour } i \text{ allant de 2 à } n)$$

$$\equiv \begin{pmatrix} 0 & \cdots & \cdots & 0 & -P \\ 1 & \ddots & & \vdots & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \qquad (C_n \leftarrow C_n + \sum_{i=1}^{n-1} a_i C_i)$$

$$\equiv \mathrm{diag}(1, \ldots, 1, P).$$

□

Exercice 4.5. Montrer que la matrice

$$\begin{pmatrix} 0 & 2 & -1 & 1 & -2 \\ 1 & 1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 1 & 2 & -7 \\ 0 & 0 & 0 & 1 & -3 \end{pmatrix}$$

est semblable à la matrice A de l'Exemple 3.6. (Voir Section 6 pour un calcul possible.)

5 Corollaires

Théorème 5.1. *Soit k'/k une extension du corps k. Si $A, B \in \mathrm{Mat}_n(k)$ sont semblables sur k' alors elles sont semblables sur k.*

Démonstration. D'après l'unicité dans le Théorème 1.7, les invariants de similitude de A sur k et k' coincident. On conclut. □

Remarque 5.2. Cet énoncé généralise le traditionnel « si $A, B \in \mathrm{Mat}_n(\mathbb{R})$ sont semblables sur $\mathbb{C}$ alors elles sont semblables sur $\mathbb{R}$ ».

Théorème 5.3. *On rappelle que k est un corps. Toute matrice $A \in \mathrm{Mat}_n(k)$ est semblable à sa transposée.*

Démonstration. Il suffit de remarquer que facteurs invariants de $A - XI_n$ sont également ceux de sa transposée. C'est bien le cas :

$$\begin{aligned} A^T &= (U\mathrm{diag}(Q_1, \dots, Q_r, 0, \dots, 0)V)^T \\ &= V^T \mathrm{diag}(Q_1, \dots, Q_r, 0, \dots, 0)U^T. \end{aligned}$$

□

Remarque 5.4. Attention, les deux énoncés précédents sont faux sur des anneaux ! Pour le premier cf. [BMP, Contre-exemple 6.98] et le deuxième (qui fonctionne donc aussi pour le premier) prendre par exemple $\left(\begin{smallmatrix} 1 & 3 \\ -5 & -1 \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathbb{Z})$ (cf. [Co, page 11]). En particulier, ce deuxième contre-exemple montre que si deux matrices $A, B \in \mathrm{Mat}_n(\mathbb{Z})$ sont semblables sur tous les $\mathbb{F}_p$ alors elles ne sont pas nécessairement semblables sur $\mathbb{Z}$.

Pour $\lambda \in k$ et $n \in \mathbb{N}^*$, on définit la matrice

$$\mathrm{J}_n^\lambda := \begin{pmatrix} \lambda & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix} \in \mathrm{Mat}_n(k).$$

Théorème 5.5 (Réduction de Jordan[3])**.** *Soit $M \in \mathrm{Mat}_n(k)$. Si $\chi_M \in k[X]$ est scindé sur k (en particulier, si k est algébriquement clos), il existe une famille $(\lambda_1, \dots, \lambda_r) \in k^r$ d'éléments de k deux à deux distincts, des entiers $N_1, \dots, N_r \in \mathbb{N}^*$ et des entiers $n_{i,1} \geq \cdots \geq n_{i,N_i} > 0$ pour chaque $i \in \{1, \dots, r\}$ tels que M soit semblable à la matrice*

$$\mathrm{diag}\Big(\mathrm{diag}(\mathrm{J}_{n_{1,1}}^{\lambda_1}, \dots, \mathrm{J}_{n_{1,N_1}}^{\lambda_1}), \dots, \mathrm{diag}(\mathrm{J}_{n_{r,1}}^{\lambda_r}, \dots, \mathrm{J}_{n_{r,N_r}}^{\lambda_r})\Big).$$

De plus, il y a unicité à permutation des λ_i près.

3. Marie Ennemond Camille Jordan, 1838–1922.

Démonstration. On applique le lemme chinois dans notre Théorème 3.7 de structure, en remarquant que la matrice de μ_X dans $k[X]/\langle (X-\lambda)^n \rangle$ pour la base $\{1, X-\lambda, \dots, (X-\lambda)^{n-1}\}$ est justement J_n^λ. □

Théorème 5.6. *Soient $M, N \in \mathrm{Mat}_n(k)$ avec $n \in \{2,3\}$. Alors M et N sont semblables si et seulement si $\pi_M = \pi_N$ et $\chi_M = \chi_N$.*

Démonstration. Découle du fait que si $P_s \mid \cdots \mid P_1$ sont les invariants de similitude de M alors $P_1 = \pi_M$ et $P_1 \cdots P_s = \chi_M$ (cf. réduction de Frobenius Théorème 1.7). □

Remarque 5.7. L'énoncé devient faux dès que $n \geq 4$. Par exemple, les matrices :

$$A \coloneqq \begin{pmatrix} 0 & 0 & & \\ 1 & 0 & & \\ & & 0 & 0 \\ & & 1 & 0 \end{pmatrix}$$

et

$$B \coloneqq \begin{pmatrix} 0 & 0 & & \\ 1 & 0 & & \\ & & 0 & 0 \\ & & 0 & 0 \end{pmatrix}$$

ont même polynôme caractéristique (X^4) et même polynôme minimal (X^2) mais ne sont pas semblables. En effet, on peut soit dire qu'elles sont sous forme de Frobenius ou de Jordan, ou plus simplement car $\dim \ker A = 2 \neq \dim \ker B = 3$.

Finalement, ce dernier théorème est la réciproque de l'Exemple 3.9.

Théorème 5.8. *Soit $u \in \mathrm{L}(E)$. Alors $\mathrm{Comm}(u) = k[u]$ si et seulement si u ne possède qu'un invariant de similitude (i.e. $s = 1$), en d'autres termes u possède une matrice dans une base de la forme C_{χ_u}.*

Démonstration. Si u ne possède qu'un invariant de similitude P alors $\mathrm{Comm}(u) = \mathrm{End}_{k[X]}(k[X]/\langle P \rangle) = k[X]/\langle P \rangle$ (il suffit de regarder l'image de 1) $\simeq k[u]$ puisque $P = \pi_u$. Réciproquement, si $\mathrm{Comm}(u) = k[u]$, supposons que u possède $s \geq 2$ invariants de similitude et considérons une décomposition de $E = \oplus_{i=1}^s E_i$ adaptée à la réduite de Frobenius de u. Le sous-k-espace vectoriel E_i est stable par u, et la matrice de u dans une bonne base est C_{P_i} avec $P_s \mid \cdots \mid P_1$. La projection p sur $\oplus_{i>1} E_i$ parallèlement à E_1 commute avec u donc est un polynôme en u par hypothèse. Soit $Q \in k[X]$ tel que $p = Q(u)$. On a $p|_{E_1} = 0$ donc $Q(u)|_{E_1} = Q(\widetilde{u}|_{E_1}) = 0$ donc $\pi_{\widetilde{u}|_{E_1}} \mid Q$. Puisque $\pi_{\widetilde{u}|_{E_1}} = P_1 = \pi_u$, on en déduit que $\pi_u \mid Q$ et donc $p = Q(u) = 0$, ce qui est absurde. □

6 Correction de l'Exercice 4.5

Comme dans la preuve du Théorème 4.4, on utilise $\equiv$ pour la relation d'équivalence dans $\mathrm{Mat}_n(k[X])$. On utilise ce théorème pour calculer les invariants de similitude de M (la matrice de l'exercice), en calculant les facteurs invariants de $M - XI_5$ comme décrit après le Théorème 4.1.

$$
\begin{aligned}
M - XI_5 &= \begin{pmatrix} -X & 2 & -1 & 1 & -2 \\ 1 & 1-X & 0 & -1 & 1 \\ 0 & 0 & -X & 1 & -3 \\ 0 & 0 & 1 & 2-X & -7 \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} \\
&\equiv \begin{pmatrix} 1 & 1-X & 0 & -1 & 1 \\ -X & 2 & -1 & 1 & -2 \\ 0 & 0 & -X & 1 & -3 \\ 0 & 0 & 1 & 2-X & -7 \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} && (L_1 \leftrightarrow L_2) \\
&\equiv \begin{pmatrix} 1 & 1-X & 0 & -1 & 1 \\ 0 & 2+X-X^2 & -1 & 1-X & -2+X \\ 0 & 0 & -X & 1 & -3 \\ 0 & 0 & 1 & 2-X & -7 \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} && (L_2 \leftarrow L_2 + XL_1) \\
&\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2+X-X^2 & -1 & 1-X & -2+X \\ 0 & 0 & -X & 1 & -3 \\ 0 & 0 & 1 & 2-X & -7 \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} && (C_i \leftarrow C_i + *C_1, \forall i \in \{2, \ldots, 5\}) \\
&\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2+X-X^2 & 1-X & -2+X \\ 0 & X & 0 & 1 & -3 \\ 0 & -1 & 0 & 2-X & -7 \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} && \begin{pmatrix} C_3 \leftarrow -C_3, \\ C_2 \leftrightarrow C_3 \end{pmatrix} \\
&\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2+X-X^2 & 1-X & -2+X \\ 0 & 0 & -2X-X^2+X^3 & 1-X+X^2 & -3+2X-X^2 \\ 0 & 0 & 2+X-X^2 & 3-2X & -9+X \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} && \begin{pmatrix} L_3 \leftarrow L_3 - XL_2, \\ L_4 \leftarrow L_4 + L_2 \end{pmatrix} \\
&\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -2X-X^2+X^3 & 1-X+X^2 & -3+2X-X^2 \\ 0 & 0 & 2+X-X^2 & 3-2X & -9+X \\ 0 & 0 & 0 & 1 & -3-X \end{pmatrix} && (C_i \leftarrow C_i + *C_2, \forall i \in \{3, \ldots, 5\}) \\
&\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1-X+X^2 & -2X-X^2+X^3 & -3+2X-X^2 \\ 0 & 0 & 3-2X & 2+X-X^2 & -9+X \\ 0 & 0 & 1 & 0 & -3-X \end{pmatrix} && (C_3 \leftrightarrow C_4) \\
&\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -3-X \\ 0 & 0 & 3-2X & 2+X-X^2 & -9+X \\ 0 & 0 & 1-X+X^2 & -2X-X^2+X^3 & -3+2X-X^2 \end{pmatrix} && (L_3 \leftrightarrow L_5)
\end{aligned}
$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3-2X & 2+X-X^2 & -2X-2X^2 \\ 0 & 0 & 1-X+X^2 & -2X-X^2+X^3 & X^2+X^3 \end{pmatrix} \qquad (C_5 \leftarrow C_5 + (3+X)C_3)$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2+X-X^2 & -2X-2X^2 \\ 0 & 0 & 0 & -2X-X^2+X^3 & X^2+X^3 \end{pmatrix} \qquad (L_i \leftarrow L_i + *L_3, \forall i \in \{4,5\})$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & X^2-X-2 & 2X^2+2X \\ 0 & 0 & 0 & X^3-X^2-2X & X^3+X^2 \end{pmatrix} \qquad (L_3 \leftarrow -L_3)$$

On doit maintenant faire des « vraies » divisions euclidiennes dans $k[X]$. On a $2X^2+2X = 2(X^2-X-X)+4X+4$ donc on obtient

$$M - XI_5 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & X^2-X-2 & 4X+4X \\ 0 & 0 & 0 & X^3-X^2-2X & -X^3+3X^2+4X \end{pmatrix} \qquad (C_5 \leftarrow C_5 - 2C_4) \qquad (6.1)$$

Cas où k est de caractéristique différente de 2. On a

$$M - XI_5 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4X+4X & X^2-X-2 \\ 0 & 0 & 0 & -X^3+3X^2+4X & X^3-X^2-2X \end{pmatrix} \qquad (C_4 \leftrightarrow C_5)$$

Puisque $X^2-X-2 = (\frac{1}{4}X - \frac{1}{2})(4X+4)$, on obtient

$$M - XI_5 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4X+4X & 0 \\ 0 & 0 & 0 & -X^3+3X^2+4X & \frac{1}{4}X^2(X+1)(X-2) \end{pmatrix} \qquad (C_5 \leftarrow C_5 - (\tfrac{1}{4}X - \tfrac{1}{2})C_4)$$

On conclut que $M - XI_5$ est équivalente à $\mathrm{diag}(1,1,1,X+1,X^2(X+1)(X-2))$ donc, puisque $X+1 \mid X^2(X+1)(X-2)$, les invariants de similitude de M sont $X^2(X+1)(X-2)$ et $X+1$ donc M est bien semblable à la matrice A de l'Exemple 3.6.

Cas où k est de caractéristique 2. De (6.1) on a

$$M - XI_5 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & X^2+X & 0 \\ 0 & 0 & 0 & X^3+X^2 & X^3+X^2 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & X^2+X & 0 \\ 0 & 0 & 0 & 0 & X^3+X^2 \end{pmatrix} \qquad (L_5 \leftarrow L_5 + XL_4)$$

donc puisque $X^2 + X \mid X^3 + X^2$ on en déduit que les invariants de similitude de M sont $X^3 + X^2$ et $X^2 + X$, donc M est semblable à A.

Références

[BMP] V. Beck, J. Malick et G. Peyré, *Objectif Agrégation*. H& K (2e édition).

[Co] K. Conrad, *Ideal classes and matrix conjugation over* **Z**. http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/matrixconj.pdf

[Gou] X. Gourdon, *Algèbre*. Ellipses, les maths en tête (2e édition).