

Sous-espaces caractéristiques et Jordan vs. Sous-espaces cycliques et facteurs invariants

1 Introduction

Un but de la réduction des endomorphismes est de trouver un représentant privilégié dans chaque classe de similitude de $M_n(k)$. Il faut également être capable étant donnée une matrice A de calculer le représentant dans la classe de A . Enfin, les représentants choisis doivent être aussi simple que possible, on doit pouvoir répondre à « toute » question naïve à leur sujet. L'idée étant que pour étudier finement un endomorphisme, on calcule son représentant et on montre la propriété cherchée sur ce représentant.

Ces buts peuvent être atteints de deux manières différentes ; chacune d'entre elles présente des avantages et des inconvénients. Ici, nous présentons ces deux approches. Nous expliquons ensuite comment passer de l'une à l'autre et essayons de dégager les avantages de l'une et de l'autre des méthodes.

2 Théorème de Jordan

2.1

Soit E un k -espace vectoriel de dimension finie. Le théorème de Jordan est le suivant :

Théorème 1 (Jordan) *Soit u un endomorphisme de E dont le polynôme caractéristique est scindé.*

Alors, il existe une base de E dans laquelle la matrice de u est diagonale par blocs carrés du type

$$J_{\lambda,l} = \left(\begin{array}{cccc} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{array} \right) \Bigg\} l,$$

où $\lambda \in k$.

De plus, l'ensemble (avec multiplicités) des couples (λ, l) tels que $J_{\lambda, l}$ apparaît ainsi ne dépend que de u et pas de la base.

Une matrice diagonale par blocs du type $J_{\lambda, l}$ est appelé *matrice de Jordan*.

2.2 Existence

Nous donnons ici les grandes lignes de la démonstration de l'existence :

Étape 1 : Réduction au cas nilpotent

Grâce au **théorème de décomposition des noyaux** et à celui de **Cayley-Hamilton** on montre que E est la somme directe des sous-espaces caractéristiques de u . Cette décomposition est stable par u , il suffit donc de montrer l'existence dans le cas où u a un seul sous-espace caractéristique c'est-à-dire $u = \lambda Id + n$, avec n nilpotente. Il suffit alors, de traiter le cas où u est nilpotente.

Étape 2 : Le cas nilpotent

La démonstration se fait par récurrence sur la dimension de E .

Supposons que $u^s = 0$ et $u^{s-1} \neq 0$. Soit x dans E tel que $u^{s-1}(x) \neq 0$. Alors, la famille $\mathcal{F} = (u^{s-1}(x), \dots, u(x), x)$ est libre, et le sous-espace F engendré par \mathcal{F} est stable par u . De plus, la matrice de la restriction de u à F dans la base \mathcal{F} est $J_{0, s}$.

Pour pouvoir appliquer l'hypothèse de récurrence, il suffit maintenant de trouver un supplémentaire à F stable par u .

Comme $u^{s-1} \neq 0$, il existe $\varphi \in E^*$ tel que

$$\varphi(u^{s-1}(x)) \neq 0. \tag{1}$$

Soit G' le sous-espace de E^* engendré par les ${}^t u^i(\varphi)$. D'après (1), ${}^t u^{s-1}(\varphi) \neq 0$. De plus, $({}^t u)^s = {}^t(u^s) = 0$. On en déduit $({}^t u^{s-1}(\varphi), \dots, \varphi)$ est une base de G' et que G' est stable par ${}^t u$.

Mais alors, l'orthogonal de G' est stable par u et a la dimension d'un supplémentaire de F . Il nous reste donc à montrer que cet orthogonal est en somme directe avec F .

Soit $y = \sum_{i=0}^{s-1} a_i u^i(x) \in F$. Supposons que y est dans l'orthogonal de G' et montrons que y est nul. Si ce n'est pas le cas notons i l'indice minimal tel que $a_i \neq 0$. On a : $0 = {}^t u^{s-1-i}(\varphi)(y) = a_i \varphi(u^{s-1}(x))$. Mais alors, la condition (1) montre que $a_i = 0$. Contradiction.

2.3 Unicité

La démonstration de l'unicité que nous esquissons ci-dessous est aussi un moyen de calculer une matrice de Jordan à laquelle est semblable une matrice donnée.

Supposons que u a une matrice de Jordan M dans une certaine base de E . On va expliquer que l'on peut décrire les blocs de M en ne parlant que de u : cela montrera bien l'unicité !

On remarque tout d'abord que l'ensemble des λ qui apparaissent est le spectre de u . Fixons λ dans le spectre de u et considérons la suite : $d_0 = 0$, $d_i = \dim(\text{Ker}(u - \lambda \text{Id})^i)$. On vérifie que si u est un $J_{\lambda, l}$ (dans une base) cette suite augmente de 1 en 1 jusqu'à atteindre la valeur l puis stationne. On en déduit alors que $d_i - d_{i-1}$ est le nombre de blocs $J_{\lambda, l}$ de M vérifiant $l \geq i$. Posons $\delta_i = d_i - d_{i-1}$. Notons $l_1 \geq l_2 \geq \dots \geq l_r$, la suite ordonnée des tailles des blocs $J_{\lambda, l}$ de M . On remarque alors que l_i est le nombre de δ_j supérieurs à i . Nous avons bien exprimé les l tels que $J_{\lambda, l}$ apparaît dans M en fonction des $\dim(\text{Ker}(u - \lambda \text{Id})^i)$.

2.4 Calcul de la matrice de Jordan d'un endomorphisme

Une question naturelle est maintenant : Étant donnée une matrice A explicite, comment calculer une matrice de Jordan J à laquelle elle est semblable et comment calculer une matrice de passage P ?

Ces deux questions qui se ressemblent sont en fait très différentes. Pour le comprendre, on peut regarder le cas d'une matrice A diagonalisable à valeurs propres distinctes. Dès que l'on a scindé le polynôme caractéristique de A , on sait à quelle matrice diagonale A est semblable. Trouver une matrice de passage revient à trouver une base constituée de vecteurs propres et revient donc à résoudre autant de systèmes linéaires qu'il y a de valeurs propres.

Dans les deux cas, il faut commencer par calculer puis scinder le polynôme caractéristique de A . Pour chaque valeur propre λ , on calcule alors la suite des sous-espaces $\text{Ker}(A - \lambda I_n)^i$.

Pour répondre à la première question, on a presque terminé puisque l'on peut alors facilement calculer les δ_i de la section précédente, puis les l_i as-

sociés. Autrement dit, on refait de manière explicite la démonstration de l'unicité pour calculer J .

En revanche, pour trouver une matrice de passage, on refait explicitement la démonstration de l'existence.

Exemple. Calculer la réduite de Jordan et une base de Jordan pour

$$A := \begin{bmatrix} 0 & -1 & 2 & -2 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \end{bmatrix}.$$

On vérifie que

$$A^2 = \begin{bmatrix} 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$A^3 = 0$ et que le rang de A vaut 3. Donc, la suite des dimensions des noyaux des puissances de A vaut $0 < 2 < 4 < 5$. Les différences de telles dimensions successives valent $2 \geq 2 \geq 1$. On en déduit que A est semblable à la matrice :

$$B := \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Cherchons maintenant une base dans laquelle l'endomorphisme associé à A a B pour matrice. On commence par choisir un vecteur qui n'est pas dans le noyau de A^2 . **On prend un vecteur de la base canonique pour simplifier les calculs !** Posons

$$V_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad V_2 = A(V_1) = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ -1 \end{pmatrix} \quad V_3 = A^2(V_1) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

On cherche maintenant un sous-espace stable par A et supplémentaire à $\text{Vect}(V_1, V_2, V_3)$. Soit $\varphi = e_1^*$ une forme linéaire simple (base canonique) telle que $\varphi(V_3) \neq 0$. On calcule les itérés de φ par tA :

$$\varphi = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad {}^tA(\varphi) = \begin{pmatrix} 0 \\ -1 \\ 2 \\ -2 \\ -1 \end{pmatrix} \quad {}^t(A^2)(\varphi) = \begin{pmatrix} 0 \\ -1 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

Soit G' le sous-espace engendré par ces trois formes linéaires. On cherche maintenant V_4 orthogonal à ces trois formes linéaires tel que $A^1(V_4) \neq 0$ (car on cherche maintenant un bloc de Jordan 2×2). L'orthogonal de G' est

$$\left\{ \begin{pmatrix} 0 \\ x \\ y \\ y-x \\ x \end{pmatrix} : \text{tels que } x, y \in \mathbb{R} \right\}.$$

Autrement dit,

$$\left(\left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right) \right)$$

est une base de l'orthogonal de G' . On vérifie qu'en prenant pour V_4 le premier vecteur de la base ci-dessus, on a bien $A(V_4) \neq 0$. On calcule :

$$A(V_4) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} =: V_5.$$

La matrice de A dans la base $(V_3, V_2, V_1, V_5, V_4)$ est B . Autrement dit, la matrice

$$P := \begin{bmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$

est une matrice de passage de A à B , c'est-à-dire $P^{-1}AP = B$.

Exercice 1. Calculer la réduite de Jordan puis une base de Jordan des matrices :

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{bmatrix} \quad \text{et} \quad N := \begin{bmatrix} 6 & 1 & -2 & 1 \\ 8 & 5 & -2 & 3 \\ 11 & 0 & -4 & 1 \\ -22 & -11 & 6 & -7 \end{bmatrix}.$$

Afin de limiter vos calculs, on vous indique que $N^2 = 0$.

2.5 Applications

Les propriétés suivantes se montrent grâce au théorème de Jordan et sont difficiles sans celui-ci :

1. Toute matrice de $M_n(\mathbb{C})$ est semblable à sa transposée. Le résultat est vrai sur \mathbb{R} car deux matrices réelles semblables sur \mathbb{C} sont semblables sur \mathbb{R} .
2. Toute matrice de $M_n(\mathbb{C})$ est semblable à une matrice symétrique. Sur \mathbb{R} , les matrices semblables à des matrices symétriques sont les matrices diagonalisables.
3. Soit $A \in M_n(\mathbb{C})$. Posons $\text{Com}(A) := \{B \in M_n(\mathbb{C}) : AB = BA\}$. Posons $\text{Com}(\text{Com}(A)) := \{C \in M_n(\mathbb{C}) : BC = CB \ \forall B \in \text{Com}(A)\}$. Alors, $\text{Com}(\text{Com}(A))$ est l'ensemble des polynômes en A .

Remarque. Il va de soit que cette liste n'est pas exhaustive et ne demande qu'à être complétée.

3 Facteurs cycliques

Dans cette section, le corps de base est quelconque et on ne fait aucune hypothèse sur $u \in \mathcal{L}(E)$.

3.1 Le lemme fondamental

Si $x \in E$, on note I_x l'idéal de $k[X]$ constitué des polynômes P tels que $P(u)(x) = 0$. On note $\mu_{u,x}$ le générateur unitaire de cet idéal. On voit facilement que $\mu_{u,x}$ divise μ_u . On a de plus le :

Lemme 1 *Il existe x dans E tel que $\mu_{u,x} = \mu_u$.*

Preuve. On écrit $\mu_u = P_1^{\alpha_1} \cdots P_s^{\alpha_s}$, avec P_i des polynômes irréductibles 2 à 2 distincts et α_i des entiers strictement positifs. D'après le **théorème de décomposition des noyaux**, on a :

$$E = \text{Ker}(\mu_u(u)) = \text{Ker}(P_1^{\alpha_1}(u)) \oplus \cdots \oplus \text{Ker}(P_s^{\alpha_s}(u)).$$

On vérifie que pour tout i , $\text{Ker}(P_i^{\alpha_i}(u))$ est stable par u et $\mu_{u|_{\text{Ker}(P_i^{\alpha_i}(u))}} = P_i^{\alpha_i}$. En effet, sinon μ_u serait plus petit ! Soit $x_i \in \text{Ker}(P_i^{\alpha_i}(u)) - \text{Ker}(P_i^{\alpha_i-1}(u))$. Posons $x = x_1 + \cdots + x_s$.

On vérifie alors, que $P(u)(x) = 0$ si et seulement si pour tout i , $P(u)(x_i) = 0$, c'est-à-dire si et seulement si pour tout i , $P_i^{\alpha_i} = \mu_{u|_{\text{Ker}(P_i^{\alpha_i}(u))}}$ divise P ; si et seulement si μ_u divise P . On en déduit que μ_u divise $\mu_{u,x}$. CQFD. \square

3.2 Théorème de Frobenius

Commençons par quelques définitions :

Définition.

1. Un endomorphisme $u \in \mathcal{L}(E)$ est dit *cyclique* s'il existe x dans E tel que $(u^i(x))_{i \in \mathbb{N}}$ engendre E .
2. Un vecteur $x \in E$ est dit *cyclique* si $(u^i(x))_{i \in \mathbb{N}}$ engendre E .
3. Un sous-espace F de E est dit *cyclique* s'il est stable par u et si la restriction de u à F est cyclique.

Le théorème fondamental de la réduction des endomorphismes par les sous-espaces cycliques est le suivant :

Théorème 2 Soit $u \in \mathcal{L}(E)$. Il existe une décomposition (non unique) de E en somme directe de sous-espaces cycliques : $E = F_1 \oplus \cdots \oplus F_s$ telle que

$$\mu_{u|_{F_s}} | \mu_{u|_{F_{s-1}}} | \cdots | \mu_{u|_{F_1}}.$$

De plus, les polynômes $\mu_{u|_{F_i}}$ ne dépendent pas de la décomposition : on les appelle les facteurs invariants de u .

Démonstration. Existence. La démonstration de l'existence ressemble à celle de l'existence dans le théorème de Jordan pour les endomorphismes nilpotents. Ceci n'est pas surprenant car si u est nilpotent l'énoncé ci-dessus n'est autre que celui de Jordan. La démonstration est cependant plus délicate ici et utilise le lemme 1 et certaines propriétés des matrices compagnons.

On fait une récurrence sur la dimension de E . Soit x dans E tel que $\mu_{u,x} = \mu_u$. Notons F_1 le sous-espace engendré par les itérés $u^i(x)$ de x . Posons

$$l := \max\{i \text{ tels que } (x, u(x), \dots, u^i(x)) \text{ est libre}\}.$$

Alors, $(x, u(x), \dots, u^l(x))$ est une base de F_1 . Mais alors, $\mu_u = \mu_{u,x} = \mu_{u|_{F_1}}$.

Pour pouvoir appliquer l'hypothèse de récurrence, il suffit de trouver un supplémentaire à F_1 stable par u .

La restriction de u à F_1 est cyclique, donc sa transposée aussi. Soit φ un vecteur de F_1^* cyclique pour ${}^t(u|_{F_1})$. Alors, $(\varphi, {}^t(u|_{F_1})(\varphi), \dots, {}^t(u|_{F_1})^l(\varphi))$ est une base de F_1^* .

Soit $\tilde{\varphi}$ une forme linéaire sur E dont la restriction à F_1 est φ . En remarquant que ${}^t(u|_{F_1})(\varphi) = ({}^t u)(\tilde{\varphi})|_{F_1}$, la liberté de $(\varphi, {}^t(u|_{F_1})(\varphi), \dots, {}^t(u|_{F_1})^l(\varphi))$ entraîne celle de $(\tilde{\varphi}, \dots, {}^t u^l(\tilde{\varphi}))$. Soit G' le sous-espace de E^* engendré par cette famille.

Montrons que l'orthogonal G de G' est un supplémentaire de F_1 stable par u .

On a $\dim(G') = l + 1$.

Par ailleurs, la famille $(\tilde{\varphi}, \dots, {}^t u^{l+1}(\tilde{\varphi}))$ est liée car le degré de $\mu_{{}^t u} = \mu_u$ vaut $l + 1$. On en déduit que G' est stable par ${}^t u$.

Il reste donc à montrer que $G \cap F_1 = \{0\}$. Soit y dans cette intersection. Comme $(\varphi, {}^t(u|_{F_1})(\varphi), \dots, {}^t(u|_{F_1})^l(\varphi))$ engendre F_1^* , on a pour tout $\psi \in F_1^*$, $\psi(y) = 0$. Mais alors, $y = 0$.

L'hypothèse de récurrence appliquée à G montre qu'il existe F_2, \dots, F_s des sous-espaces de E u -cycliques tels que :

1. $E = F_1 \oplus F_2 \oplus \dots \oplus F_s$, et
2. $\mu_{u|_{F_s}} \mid \dots \mid \mu_{u|_{F_2}}$.

Il nous reste à montrer que $\mu_{u|_{F_2}}$ divise $\mu_{u|_{F_1}}$. Or, μ_u est le ppcm des $\mu_{u|_{F_i}}$, c'est-à-dire compte tenu de 2, le ppcm de $\mu_{u|_{F_1}}$ et de $\mu_{u|_{F_2}}$. Par ailleurs, $\mu_{u|_{F_1}} = \mu_u$ par construction. Ainsi, $\mu_u = \text{ppcm}(\mu_u, \mu_{u|_{F_2}})$; donc $\mu_{u|_{F_2}} \mid \mu_{u|_{F_1}}$.

Unicité :

Supposons que $E = F_1 \oplus \dots \oplus F_s = G_1 \oplus \dots \oplus G_r$, avec les F_i et G_j vérifiant le théorème. Posons $P_i := \mu_{u|_{F_i}}$ et $Q_j := \mu_{u|_{G_j}}$. On a déjà remarqué que, $P_1 = Q_1 = \mu_u$. Supposons par l'absurde que les P_i n'égalent pas les Q_j . Soit i l'indice minimal tel que $P_i \neq Q_i$. On a :

$$\begin{aligned} P_i(u)(E) &= P_i(u)(F_1) \oplus \dots \oplus P_i(u)(F_{i-1}) \\ &= P_i(u)(G_1) \oplus \dots \oplus P_i(u)(G_i). \end{aligned}$$

Or, pour $j = 1, \dots, i-1$, $u|_{F_j}$ est semblable à $u|_{G_j}$ (deux endomorphismes cycliques ayant même polynôme minimal sont semblables). Donc, $P_i(u)(F_j)$ et $P_i(u)(G_j)$ ont même dimension, pour $j = 1, \dots, i-1$. Mais alors, $P_i(u)(G_i) = 0$; c'est-à-dire Q_i divise P_i . Comme les P_j et les Q_j jouent le même rôle, on en déduit que $P_i = Q_i$. Ceci est une contradiction. \square

Soit u un endomorphisme cyclique dont le polynôme minimal est $X^d - a_1X^{d-1} - \dots - a_d$. Alors, la matrice de u dans une base cyclique est :

$$\begin{pmatrix} 0 & & & a_d \\ 1 & 0 & & a_{d-1} \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \\ & & & 1 & a_1 \end{pmatrix}.$$

En déduire un théorème du type : toute matrice carrée est semblable à une unique matrice de la forme suivante...

2. La seconde méthode consiste à appliquer les théorèmes de Cayley-Hamilton et de décomposition des noyaux, puis d'appliquer le théorème de Frobenius sur chaque sous-espace caractéristique.

3.4.2 Changement de corps de base

Soit $k \subset K$ une extension de corps et $A \in M_n(k)$. Alors, les facteurs invariants de $A \in M_n(k)$ sont visiblement des (donc les) facteurs invariants de $A \in M_n(K)$. Cette remarque montre la

Proposition 2 *Deux matrices de $M_n(k)$ qui sont semblables dans $M_n(K)$ sont semblables dans $M_n(k)$.*

3.4.3 Petite dimension

Proposition 3 *Dans $M_2(k)$ et $M_3(k)$, deux matrices sont semblables si et seulement si elles ont même polynômes caractéristiques et minimaux.*

3.4.4 Commutant

Proposition 4 *Soit u un endomorphisme de E . Alors, u est cyclique si et seulement si $\text{Com}(u) = k[u]$.*

3.4.5 Transposé

Proposition 5 *Toute matrice carrée est semblable à sa transposée.*

3.5 Le point de vue $k[X]$ -module

3.5.1 A -modules

Soit A un anneau euclidien. Très vite A sera égal à $k[X]$. Un autre exemple intéressant pour l'agrégation est $A = \mathbb{Z}$.

Les notions supposées connues ici sont celles de A -module, de A -module de type fini, de A -module libre de type fini, de morphisme de A -module etc...

Il convient également de savoir montrer le lemme suivant :

Lemme 2 *1. Les A -modules A^n et A^m sont isomorphes si et seulement si $n = m$.*

Cet entier est appelé le rang de A^n . Cette notion est l'équivalent de la

dimension pour les espaces vectoriels. Son comportement est cependant *ASSEZ DIFFÉRENT*.

Par exemple, un sous \mathbb{Z} -module de \mathbb{Z}^n de rang n peut être strict.

2. Soit M un A -module. Une famille (v_1, \dots, v_n) de M est une A -base si et seulement si le morphisme $\phi : A^n \rightarrow M, (\lambda_i) \mapsto \sum_i \lambda_i v_i$ est un isomorphisme.

ATTENTION : on peut définir libre et générateur. Cependant on a pas : libre+bon cardinal implique générateur !!

3. Soit $u : M \rightarrow N$ un morphisme de A -module libres de même rang n . Munissons M et N de deux bases. Alors, u est représenté par une matrice carrée M de taille $n \times n$ à coefficients dans A . De plus, u est injectif si et seulement si $\det(M) \neq 0$ et u est inversible si et seulement si $\det(M)$ est inversible dans A .

Posons, $\mathrm{GL}_n(A) := \{M \in M_n(A) : \det(M) \text{ est inversible dans } A\}$.

Un théorème important pour l'algèbre linéaire est le

Théorème 3 (Théorème de la base adaptée) *Rappelons que A est euclidien. Soit M une matrice carrée de taille $n \times n$ à coefficients dans A . Alors, il existe P et Q dans $\mathrm{GL}_n(A)$, d_1, \dots, d_s dans A tels que :*

1. $d_1 | d_2 | \dots | d_s$,

2. et

$$PMQ = \begin{pmatrix} d_1 & & & & & & & & \\ & \dots & & & & & & & \\ & & d_s & & & & & & \\ & & & 0 & & & & & \\ & & & & \dots & & & & \\ & & & & & & & 0 & \end{pmatrix}$$

De plus, les d_i ne dépendent que de (l'image de) M .

Une démonstration algorithmique mélangeant pivot de Gauss et algorithme d'Euclide pour le calcul du pgcd se trouve dans le livre intitulé *Algebra* de Jacobson.

Remarque. Dans le théorème ci-dessus, l'hypothèse A euclidien peut être remplacée par A principal. Cependant, cette amélioration complique la démonstration alors que son utilité n'est pas flagrante pour l'agrégation.

Le corollaire suivant explique le nom donnée à ce théorème :

Corollaire 1 *Soit M un sous-module de A^n . Alors, il existe une base (e_1, \dots, e_n) de A^n et des éléments d_1, \dots, d_s dans A tels que*

1. $d_1 | d_2 | \dots | d_s$,
2. $(d_1 e_1, \dots, d_s e_s)$ est une base de M .

De plus, les d_i ne dépendent que de M .

Ce corollaire a un corollaire très connu :

Corollaire 2 *Tout groupe abélien G est isomorphe à un unique produit $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$ avec $d_1 | d_2 | \dots | d_s$.*

3.5.2 Application à l'algèbre linéaire

On se donne un endomorphisme u d'un k -espace vectoriel de dimension finie E . Alors, E est muni d'une structure de $k[X]$ -module par la formule :

$$P.x = P(u)(x) \quad \forall x \in E \quad \forall P \in k[X].$$

On fixe une base $\mathcal{B} = (e_1, \dots, e_n)$ de E . Considérons alors l'application

$$\begin{aligned} \varphi : \quad k[X]^n &\longrightarrow E \\ (P_1, \dots, P_n) &\longmapsto \sum_i P_i \cdot e_i. \end{aligned}$$

D'après le théorème 3, il existe une base (E_1, \dots, E_n) de $k[X]^n$ et des polynômes non nuls P_1, \dots, P_s tels que $(P_1.E_1, \dots, P_s.E_s)$ est une base de $\text{Ker}\varphi$. De plus, $k[X]^n/\text{Ker}\varphi$ est isomorphe à E , qui est l'image de φ . En particulier, ce k -espace vectoriel est de dimension finie. On en déduit que $s = n$.

Plus précisément,

$$k[X]^n/\text{Ker}\varphi \simeq k[X]/(P_1) \times \dots \times k[X]/(P_n).$$

Notons d_i le degré de P_i . Posons

$$\mathcal{B}_1 = (E_1, XE_1, \dots, X^{d_1-1}E_1, E_2, XE_2, \dots, X^{d_n-1}E_n).$$

Alors, $\varphi(\mathcal{B}_1)$ est une base du k -espace vectoriel E . On vérifie alors aisément que la matrice de u dans cette base est la juxtaposition diagonale des matrices compagnons des polynômes P_1, \dots, P_n . On retrouve donc le résultat d'existence du théorème 2.

Remarque. Dans la discussion ci-dessus, il se peut que certains polynômes soient égaux à 1. Il n'intervient alors nulle part. On pourra en guise d'exercice caractériser les endomorphismes pour lesquels aucun de ces polynômes n'est égal à 1.

Soit M la matrice de u dans la base de départ \mathcal{B} . Considérons la matrice $\tilde{M} = M - XI_n$ à coefficients dans $k[X]$. Cette matrice induit un morphisme de $k[X]$ -module de $k[X]^n$ dans lui-même. On a alors le

Théorème 4 *L'image de \tilde{M} est égale au noyau de φ .*

Preuve. Notons \mathcal{I} l'image de \tilde{M} et \mathcal{N} le noyau de φ . Pour montrer que \mathcal{I} est inclus \mathcal{N} , il suffit de montrer que chaque vecteur colonne de \tilde{M} appartient à \mathcal{N} . Par exemple, le premier vecteur colonne de \tilde{M} est

$$\begin{pmatrix} e_1^*(Me_1) - X \\ e_2^*(Me_1) \\ \vdots \\ e_n^*(Me_1) \end{pmatrix}.$$

Son image par φ est donc : $(e_1^*(Me_1)e_1 - Me_1 + \sum_{j \geq 2} e_j^*(Me_1)e_j = Me_1 - Me_1 = 0$.

Ensuite, on raisonne par un argument de dimension, en considérant $k[X]^n/\mathcal{I}$ et $k[X]^n/\mathcal{N}$ comme des k -espaces vectoriels (et non plus comme des $k[X]$ -modules). Nous savons déjà que $k[X]^n/\mathcal{N}$ est un k -espace vectoriel de dimension n . Le lecteur vérifiera qu'il suffit donc de montrer la même propriété pour $k[X]^n/\mathcal{I}$.

D'après le théorème 3, il existe P et Q dans $\text{GL}_n(k[X])$ et Q_1, \dots, Q_n tels que

$$P\tilde{M}Q^{-1} = \begin{pmatrix} Q_1 & & \\ & \ddots & \\ & & Q_n \end{pmatrix}.$$

Mais alors, $k[X]^n/\mathcal{I}$ est isomorphe comme k -espace vectoriel à $k[X]/(Q_1) \times \dots \times k[X]/(Q_n)$. En particulier, sa dimension est la somme des degrés des Q_i , c'est-à-dire le degré de $\prod_{i=1}^n Q_i = \det(P\tilde{M}Q^{-1}) = \det(P) \cdot \det(Q)^{-1} \det(\tilde{M})$. Or, $\det(P)$ et $\det(Q)$ sont des éléments inversibles de $k[X]$, c'est-à-dire des éléments de k . Finalement, la dimension du k -espace vectoriel $k[X]^n/\mathcal{I}$ est égal au degré de $\det(\tilde{M})$ c'est-à-dire à n . \square

Le théorème 4 est un moyen très pratique de calculer les facteurs invariants d'une matrice donnée. En effet, on considère la matrice $M - XI_n$, on lui applique l'algorithme qui permet de montrer le théorème 3. On calcule ainsi des polynômes unitaires P_1, \dots, P_n se divisant les uns les autres tels qu'il existe P et Q dans $\text{GL}_n(k[X])$ tels que

$$P\tilde{M}Q^{-1} = \begin{pmatrix} P_1 & & \\ & \ddots & \\ & & P_n \end{pmatrix}.$$

Les polynômes P_i non égaux à un ainsi obtenus sont les facteurs invariants de M .

Exercice 2. Déterminer les facteurs invariants de la matrice :

$$A = \begin{bmatrix} -17 & 8 & 12 & -14 \\ -46 & 22 & 35 & -41 \\ 2 & -1 & -4 & 4 \\ -4 & 2 & 2 & -3 \end{bmatrix}$$

4 Comparaison de Jordan et de Frobenius

4.1 La théorie

D'un point de vue théorique, le théorème de Frobenius ne présente pas d'inconvénient majeur par rapport à celui de Jordan puisqu'il est plus général (on ne suppose pas que le polynôme caractéristique est scindé) et qu'il entraîne facilement ce dernier.

Se passer de l'hypothèse « polynôme caractéristique scindé » est indispensable pour montrer la proposition 3.4.2. Ceci montre la supériorité de Frobenius par rapport à Jordan. Une fois la proposition 3.4.2 démontrée, on peut souvent dans des problèmes de similarité de matrices supposer les polynômes caractéristiques scindés en prenant une extension du corps de base.

Un énorme avantage de Frobenius sur Jordan est qu'il ne nécessite pas de scinder le polynôme caractéristique. Même sur \mathbb{C} cela est très intéressant car on ne sait pas trouver les racines d'un polynôme complexe. Ainsi, le théorème de Frobenius permet un algorithme exact pour décider si deux matrices sont semblables ou pas.

4.2 Passages de Frobenius à Jordan

Soit \mathcal{C} une classe de similitude de $M_n(k)$. On suppose que le polynôme caractéristique des éléments de \mathcal{C} est scindé. On a choisi (essentiellement, car il y a plusieurs matrices de Jordan) deux matrices particulières dans \mathcal{C} . Une question naturelle est étant donnée une de ces deux matrices comment retrouver l'autre. Autrement dit, comment calculer la réduite de Jordan d'une matrice de Frobenius et vice versa ?

De Frobenius à Jordan. En raisonnant bloc par bloc, il suffit de savoir calculer la matrice de Jordan d'une matrice compagnon. Ceci est facile, une matrice compagnon dont le polynôme caractéristique est $\prod_i (X - \lambda_i)^{\alpha_i}$ est semblable à la matrice de Jordan dont les blocs diagonaux sont les J_{λ_i, α_i} .

De Jordan à Frobenius. Il s'agit cette fois de reconnaître les endomorphismes cycliques parmi les matrices de Jordan. Ceci est fait par le

Lemme 3 *Une matrice de Jordan dont les blocs diagonaux sont les J_{λ_i, α_i} est cyclique si et seulement si les λ_i sont deux à deux distincts.*

La preuve de ce lemme est facile sachant trois choses :

1. le polynôme caractéristique d'une matrice triangulaire par blocs est le produit des polynômes caractéristiques des blocs diagonaux.
2. le polynôme minimal d'une matrice diagonale par blocs est le ppcm des polynômes minimaux des blocs diagonaux.
3. un endomorphisme est cyclique si et seulement si son polynôme minimal est égal à son caractéristique.

Soit M une matrice de Jordan. On ordonne les blocs de Jordan de la manière suivante :

1. Pour chaque valeur propre, on choisit un bloc de taille maximale. On met les blocs ainsi repéré au début.
2. Parmi les blocs restants, on refait la même opération.
3. etc...

les matrices construites à chaque étape ne font intervenir qu'au plus une fois chaque valeur propre. D'après le lemme précédent, elles sont cycliques. De plus, à valeur propre fixée la taille des blocs triés par la méthode sus-citée est décroissante. Donc les polynômes minimaux des blocs cycliques ainsi construit se divisent les uns les autres. On obtient ainsi la décomposition de Frobenius.

4.3 Avantages de Jordan

Comme nous l'avons déjà expliqué, il ne faut pas chercher les avantages de Jordan dans la théorie. En effet, les avantages de Jordan sur Frobénius sont à chercher dans la pratique et la pédagogie.

La démarche de Jordan est naturelle.

En effet, la démarche menant à Jordan est finalement assez naturelle. On commence par comparer un endomorphisme aux endomorphismes les plus simples c'est-à-dire les homothéties. Ceci conduit à définir les éléments propres. Pour les endomorphismes diagonalisables, la théorie est terminée.

A l'inverse, les endomorphismes n'ayant qu'une valeur propre ne sont que peut réduit par la théorie des éléments propres. On remarque alors que tout endomorphisme est une juxtaposition de tels endomorphismes (décomposition de Dunford). Ainsi, on est ramené à ce cas des endomorphismes n'ayant qu'une valeur propre, puis par soustraction d'une homothétie à des endomorphismes nilpotents.

J'espère que ces quelques lignes vous convainquent que la démarche adoptée pour la réduction de Jordan est à la fois naturelle et graduelle dans la difficulté. Ces deux aspects constituent un avantage indéniable pour un cours.

Il est raisonnable de penser que la réduction optimale d'un endomorphisme diagonalisable est sous forme diagonale. Ceci n'est pourtant pas le point de vue de la réduction de Frobenius. A ce sujet, on peut se poser les questions suivantes : à quelle condition un endomorphisme diagonalisable est cyclique ? S'il l'est quels sont ces vecteurs cycliques ?

Pour des questions pratiques, la réduction de Jordan est plus simple que celle en blocs compagnons.

Voici quelques questions de base que l'on peut se poser sur un endomorphisme :

- Quel est son noyau ?
- Quelle est son image ?
- Quelles sont ses valeurs propres ?
- Calculer l'exponentielle de la matrice.

Il est plus facile de répondre à ces questions (et à d'autres) sur une matrice de Jordan que sur une matrice de Frobenius.

Il est plus facile de trouver une matrice de passage pour Jordan.

4.4 La décomposition de Frobénius dans une leçon d'Oral

Présenter le théorème de Frobenius le jour de l'oral est délicat. En effet, ce théorème est assez difficile et trivialisé à peu près tous les autres. Il nécessite plusieurs compétences :

1. Savoir le démontrer et en proposer une partie en développement.

2. Bien connaître l'anneau $k[X]$. Il faut savoir montrer qu'il est euclidien, savoir faire une division euclidienne, avoir des méthodes pour montrer qu'un polynôme est irréductible etc...
3. Connaître les résultats et pièges de base sur les modules sur un anneau principal. En effet, même s'il n'est pas stricto sensu nécessaire de parler de $k[X]$ -module pour montrer le théorème de Frobenius, ce point de vue est derrière tout ce que l'on fait. Le jury ne manquera donc pas de poser quelques questions de base sur cette notion. Il faut donc savoir montrer qu'un sous-module d'un module libre est libre, connaître le théorème de la base adaptée, connaître les éléments de $GL_n(k[X])$, savoir à quelle condition un élément de $k[X]^n$ se complète en une base de $k[X]^n$ etc... Le mieux pour éviter des questions trop pointues est de ne pas parler de $k[X]$ -module car sinon vous allez épuiser les questions faciles et le jury en posera des plus difficiles.
4. Il faut bien connaître les endomorphismes cycliques puisque ce sont les briques à partir desquelles tout endomorphisme est construit.

Une fois les points ci-dessus maîtrisés, il faut organiser la leçon. Pour cela il faut voir de quels préliminaires on a besoin pour montrer le théorème de Frobenius. On a besoin du théorème de décomposition des noyaux, du lemme 1 et de résultats sur les endomorphismes cycliques.

Une autre possibilité (moins risquée) consiste à donner le théorème de Frobenius à la fin en disant bien quel est son statut : difficile, n'utilisant presque rien et pouvant donc servir de base. IL FAUT ALORS expliquer pourquoi vous n'avez pas fait ce choix : pas naturel, trop abrupt si ceci était un vrai cours etc...

Dans tous les cas, pour présenter le théorème de Frobenius il faut être solide sur les endomorphismes cycliques. Voici un exercice difficile sans indication :

Exercice 3. Est-ce que la restriction d'un endomorphisme cyclique est cyclique ?

Indication : La réponse est oui. On peut le montrer rapidement en considérant $I := \{P \in k[X] : P(u)(x) \in F\}$ où u est l'endomorphisme, x un vecteur cyclique pour u et F le sous-espace stable. On vérifie alors que I est

un idéal de $k[X]$ et que si Q est un générateur de I , alors $y = Q(u)(x)$ est cyclique pour $u|_F$.