LA RÉDUCTION PAR LA THÉORIE DES MODULES

À recaser dans les leçons 150, 151 et peut-être dans les leçons 122 et 148

HOSTEIN Matthias
3A Maths
ENS Rennes
Année 2023 - 2024

Table des matières

Introduction

La théorie des modules sort clairement du programme de l'agrégation de mathématiques en algèbre. Pourtant, les problèmes linéaires posés sur des anneaux apparaissent naturellement dans certains pans du programme : équations diophantiennes linéaires sur $\mathbb{Z}$, espaces vectoriels munis d'un endomorphisme, sous-espaces stables, groupes abéliens de type fini, matrices à coefficients dans un anneau... Les gros théorèmes de structure sont, eux, au programme et le point de vue des modules permet d'avoir un éclairage plus global sur ces notions, qu'il peut être utile de connaître pour avoir du recul ! Je propose dans ce document de compléments d'étudier le lien entre la réduction d'un endomorphisme sur un K-espace vectoirle et les sous-espaces stables par cet endomorphisme et la théorie des modules (plus précisément des $K[X]$-modules). J'espère que cela vous sera utile !

1 Liens entre $K[X]$-modules et K-espaces vectoriels munis d'un endomorphisme [BMP05], [DTLQ14]

1.1 Les bases sur les modules

La notion de module sur un anneau commutatif unitaire est l'équivalent, en quelque sorte, de la notion d'espace vectoriel sur un corps, comme vous pouvez le constater par cette définition :

Définition 1.1 (Module sur un anneau commutatif unitaire)**.** Soit $(A, +_A, \times_A)$ un anneau commutatif unitaire. On appelle A-module la donnée d'un triplet $(M, +, \cdot)$ où M est un ensemble muni de deux lois :
- Une loi d'addition $+ : M \times M \longrightarrow M$ faisant de $(M, +)$ un groupe abélien de neutre noté 0_M,
- Une loi externe de multiplication par un scalaire $\cdot : A \times M \longrightarrow M$ vérifiant les axiomes suivants :
  1. $0_A \cdot m = 0_M$ pour tout $m \in M$,
  2. $1_A \cdot m = m$ pour tout $m \in M$,
  3. $(a +_A b) \cdot m = a \cdot m + b \cdot m$ pour tout $(a, b, m) \in A^2 \times M$,
  4. $a \cdot (m + m') = a \cdot m + a \cdot m'$ pour tout $(a, m, m') \in A \times M^2$,
  5. $a \cdot (b \cdot m) = (a \times_A b) \cdot m$ pour tout $(a, b, m) \in A^2 \times M$.

Remarque 1.1.1. *De manière équivalente, un A-module correspond à la donnée d'un groupe abélien $(M, +)$ et d'un morphisme d'anneaux unitaires $A \longrightarrow \mathrm{End}_{\mathrm{gr}}(M)$ (endomorphismes de groupe de M).*

Vous connaissez sans doutes des exemples de A-module : A^n, $\mathscr{M}_{n,m}(A)$ (matrices de taille $n \times m$ à coefficients dans A), mais mon propos est surtout de vous faire comprendre qu'un K-espace vectoriel E muni d'un endomorphisme u est en fait un $K[X]$-module !

Proposition 1.2. Soit K un corps. Alors tout $K[X]$-module $(E, +, \cdot)$ est muni d'une structure de K-espace vectoriel en restreignant la multiplication scalaire aux éléments de K, et d'un endomorphisme

$$\begin{array}{rccc} u & : & E & \longrightarrow & E \\ & & x & \longmapsto & X \cdot x. \end{array}$$

Réciproquement, si (E, u) désigne la donnée d'un K-espace vectoriel $(E, +_{\mathrm{ev}}, \cdot_{\mathrm{ev}})$ et d'un endomorphisme $u \in \mathscr{L}(E)$, alors E peut être muni d'une structure de $K[X]$-module compatible avec la structure de K-espace vectoriel (comprendre que la loi $+_{\mathrm{mod}}$ de $K[X]$-module reste la loi $+_{\mathrm{ev}}$ de K-espace vectoriel et que pour tout *polynôme constant* $\lambda \in K$, on a $\lambda \cdot_{\mathrm{mod}} x = \lambda \cdot_{\mathrm{ev}} x$) telle que :

$$\forall x \in E, \quad X \cdot_{\mathrm{mod}} x = u(x).$$

Plus explicitement, on a :

$$\forall P \in K[X],\ \forall x \in E, \quad P \cdot_{\mathrm{mod}} x = P(u)(x).$$

On notera alors souvent les $K[X]$-modules (E, u) avec E un K-espace vectoriel et u un endomorphisme de E.

Remarque 1.1.2. *Dans un $K[X]$-module (E,u), l'action de $K[X]$ sur E passe au quotient en une structure de $K[u]$-module sur (E,u). Cela vient de l'isomorphisme entre $K[u]$ et $\dfrac{K[X]}{(\pi_u)}$.*

1.2 Sous-$K[X]$-modules et sous-espaces stables

On va voir déjà apparaître l'intérêt du formalisme des $K[X]$-modules pour étudier un endomorphisme sur un espace vectoriel grâce au lien qu'il existe entre les sous-modules de (E,u) et les sous-espaces vectoriels de E stables par u :

Définition 1.3 (Sous-A-module)**.** Soit A un anneau commutatif unitaire et soit $(M,+,\cdot)$ un A-module. On dit que $N \subset M$ est un *sous-A-module* de M si $(N,+)$ est un sous-groupe de $(M,+)$ et si les restrictions de $+$ et $\cdot$ à N le munissent d'une structure de A-module.

Exemple 1.2.1. *Si A est un anneau commutatif unitaire, alors les sous-A-modules de A sont les idéaux de A. Ainsi, contrairement aux espaces vectoriels, il y a "de la place" entre $\{0\}$ et A pour des sous-modules.*

On voit alors apparaître la propriété centrale que j'évoquais plus haut :

Proposition 1.4 (Sous-modules vs sous-espaces stables)**.** Soit (E,u) un $K[X]$-module. Alors $F \subset E$ est un sous-$K[X]$-module de (E,u) si et seulement si F est un sous-espace vectoriel de E stable par l'endomorphisme u.

Démonstration. $\Rightarrow$: Si $F \subset E$ est un sous-$K[X]$-module de (E,u), alors on a que $(F,+)$ est un sous-groupe de $(E,+)$ et :

$$\forall \lambda \in K,\ \forall x \in F \quad \lambda \cdot x \in F$$

étant donné que F est un sous-$K[X]$-module de (E,u), et que λ est vu comme un polynôme constant. Ainsi, F est un sous-espace vectoriel de E et :

$$\forall x \in F, \quad u(x) = X \cdot x \in F$$

et donc F est stable par u.
$\Leftarrow$: Si $F \subset E$ est un sous-espace vectoriel stable par u, alors $(F,+)$ est bien un sous-groupe de $(E,+)$ et :

$$\forall P \in K[X],\ \forall x \in F, \quad P \cdot x = P(u)(x) \in F$$

étant donné que F est stable par u. Ainsi, F est un sous-$K[X]$-module de (E,u). □

Afin de poursuivre l'étude du lien entre $K[X]$-modules et espaces vectoriels munis d'un endomorphisme, intéressons-nous aux applications $K[X]$-linéaires et aux isomorphismes de $K[X]$-modules.

1.3 Applications $K[X]$-linéaires et isomorphismes de $K[X]$-modules

Les applications linéaires correspondent aux transformations naturelles entre modules et il est donc nécessaire de les étudier. Les applications $K[X]$-linéaires permettent d'ailleurs de faire émerger naturellement un objet que vous connaissez sans doutes et que vous avez pu étudier : le commutant d'un endomorphisme.

Définition 1.5 (Applications A-linéaires)**.** Soit A un anneau commutatif unitaire et M, N deux A-modules. On dit qu'une application $f : M \longrightarrow N$ est un *morphisme* de A-modules ou une application *A-linéaire* si f vérifie les propriétés suivantes :

1. $\forall m, m' \in M, \quad f(m +_M m') = f(m) +_N f(m')$,
2. $\forall (a,m) \in A \times M, \quad f(a \cdot_M m) = a \cdot_N f(m)$.

Si de plus f est bijective, on dit que f est un *isomorphisme* A-linéaire. On notera souvent l'ensemble des applications A-linéaires entre M et N $\mathrm{Hom}_A(M,N)$ ou $\mathscr{L}_A(M,N)$ par analogie avec les espaces vectoriels. Lorsque $M = N$, on notera plutôt $\mathrm{End}_A(M)$.

Que se passe-t-il alors quand $A = K[X]$ et quel est le lien entre les applications linéaires entre espaces vectoriels ?

Proposition 1.6. Soient (E,u) et (F,v) deux $K[X]$-modules. Alors $\varphi : E \longrightarrow F$ est une application $K[X]$-linéaire si et seulement si :

1. $\varphi \in \mathscr{L}(E,F)$ (au sens des K-espaces vectoriels),
2. $\varphi \circ u = v \circ \varphi$.

En particulier, $\mathrm{End}_{K[X]}((E,u)) = \mathscr{C}(u) := \{v \in \mathscr{L}(E) \mid u \circ v = v \circ u\}$: c'est le commutant de u !

Le point 2 de la proposition précédente traduit la linéarité par rapport à l'action de l'indéterminée X sur les espaces E et F et est en fait suffisante pour avoir la linéarité par rapport à tous les polynômes grâce à la K-linéarité de φ. Cette proposition nous éclaire quant à la classification des endomorphismes à similitude près :

Corollaire 1.7. Deux $K[X]$-modules (E,u) et (F,v) sont isomorphes si et seulement si les K-espaces vectoriels E et F sont isomorphes et les endomorphismes u et v sont semblables.

Classifier les endomorphismes de E à similitude près revient donc à déterminer les structures possibles de $K[X]$-modules sur E !

Remarque 1.3.1 (Interprétation matricielle)**.** *Si (E,u) et (F,v) sont deux $K[X]$-modules tels que E et F sont de K-dimension finie, alors ils sont isomorphes en tant que $K[X]$-modules si et seulement s'il existe $\mathscr{B}$ une base de E et $\mathscr{B}'$ une base de F telles que :*

$$\mathrm{Mat}_{\mathscr{B}}(u) = \mathrm{Mat}_{\mathscr{B}'}(v).$$

On peut également avoir un éclairage nouveau sur les espaces vectoriels quotients grâce aux modules quotients.

1.4 Modules quotients

Rappelons la définition d'un module quotient.

Définition 1.8 (Module quotient)**.** Soient A un anneau commutatif unitaire et soit M un A-module. Si N est un sous-A-module de M, alors le quotient de M par la relation d'équivalence $\sim_N$ suivante :

$$x \sim_N y \iff x - y \in N$$

noté $\dfrac{M}{N}$ est muni d'une unique structure de A-module rendant la projection canonique $\pi : M \longrightarrow \dfrac{M}{N}$ A-linéaire.

Corollaire 1.9. Soit $F \subset E$ un sous-espace vectoriel stable par un endomorphisme $u \in \mathscr{L}(E)$. Alors il existe une unique application linéaire $\tilde{u} \in \mathscr{L}\left(\dfrac{E}{F}\right)$ (l'espace $\dfrac{E}{F}$ étant l'espace vectoriel quotient de E par F) telle que, si π désigne la projection canonique $\pi : E \longrightarrow \dfrac{E}{F}$, on ait :

$$\pi \circ u = \tilde{u} \circ \pi$$

Démonstration. Si $F \subset E$ est un sous-espace stable par u, alors il s'agit d'un sous $K[X]$-module de (E,u). On peut alors munir $\dfrac{E}{F}$ d'une structure de $K[X]$-module quotient, et donc d'un endomorphisme $\tilde{u}$. Par $K[X]$-linéarité de la projection $\pi : E \longrightarrow \dfrac{E}{F}$, on a donc :

$$\forall x \in E, \quad \tilde{u}(\pi(x)) = X \cdot \pi(x) = \pi(X \cdot x) = \pi(u(x)).$$

□

Remarque 1.4.1 (Interprétation matricielle)**.** *Si E est un K-espace vectoriel de dimension finie, que $u \in \mathscr{L}(E)$ et que F est un sous-espace vectoriel de E stable par u, alors, si G désigne un supplémentaire de F et $\mathscr{B}$ une base adaptée*

à cette somme directe, alors :

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} \mathrm{Mat}_{\mathscr{B}\cap F}\left(u_{|F}\right) & * \\ \boldsymbol{O} & \mathrm{Mat}_{\pi(\mathscr{B})}(\tilde{u}) \end{pmatrix}$$

1.5 Supplémentaires dans un module et endomorphismes semi-simples

Nous avons vu que classifier les endomorphismes de E à similitude près revient à classifier les structures de $K[X]$-modules sur E. Un outil pour le faire est de découper le $K[X]$-module (E,u) en *somme directe* de sous-modules jusqu'à obtenir une décomposition la plus simple possible.

Définition 1.10. Si M est un A-module, alors deux sous-A-modules N et N' sont dits *en somme directe* si l'application :

$$\begin{array}{ccc} N \times N' & \longrightarrow & M \\ (n,n') & \longmapsto & n+n' \end{array}$$

est injective. Si de plus cette application est surjective, alors N et N' sont dits supplémentaires et on note alors :

$$M = N \oplus N'.$$

Cela permet alors de comprendre le module M en restreignant notre étude aux deux sous-modules N et N', ce qui est souvent plus simple ! Si on peut réitérer ce procédé ce serait fantastique mais malheureusement on ne peut pas toujours. D'ailleurs, si N est un sous-module de M, alors, contrairement aux espaces vectoriels, il n'existe pas toujours de sous-module supplémentaire à N ! Par exemple, $2\mathbb{Z}$ est un sous-$\mathbb{Z}$-module de $\mathbb{Z}$ qui ne possède pas de supplémentaire. Dans le cas des $K[X]$-modules, on peut faire le lien entre sous-modules supplémentaires et sous-espaces stables :

Proposition 1.11. Soient (E,u) un $K[X]$-module et F un sous-espace vectoriel de E stable par u. Alors F' est un supplémentaire de F en tant que $K[X]$-module si et seulement si $F \oplus F' = E$ en tant que K-espaces vectoriels et si F' est stable par u.

Dans ce contexte, il est intéressant d'étudier les endomorphismes u de E tels que tout sous-module de (E,u) possède un supplémentaire : ce sont les endomorphismes semi-simples.

Définition 1.12 (Endomorphisme semi-simple)**.** Soient E un K-espace vectoriel et $u \in \mathscr{L}(E)$. On dit que u est *semi-simple* si tout sous-espace vectoriel de E stable par u possède un supplémentaire stable par u. De manière équivalente, u est semi-simple si tout sous-$K[X]$-module de (E,u) possède un supplémentaire.

Remarque 1.5.1. *Les endomorphismes normaux sur un espace euclidien sont les archétypes d'endomorphismes semi-simples. En effet, si F est un sous-espace stable par un endomorphisme u normal, alors son supplémentaire "naturel" $F^{\perp}$ est aussi stable par u !*

Ainsi, si on a trouvé un sous-espace F stable par un endomorphisme u semi-simple, on a une décomposition de l'espace :

$$E = F \oplus F'$$

avec F' également stable par u. En réitérant ce processus, on peut arriver à découper l'action de l'endomorphisme u sur des sous-espaces de plus en plus petits. Nous reparlerons de tout cela dans la section suivante faisant lien entre la théorie des $K[X]$-modules et la réduction.

2 Réduction de l'endomorphisme u [BMP05], [DTLQ14], [Rom], [CG15]

Pour rappel, la théorie de la réduction trouve sa justification dans le fait de vouloir comprendre un endomorphisme sur un gros espace en découpant cet espace en somme directe de sous-espaces plus petits, compatibles avec l'action de u, c'est-à-dire stables par u. On va donc chercher à découper notre $K[X]$-module (E,u) en somme directe de sous-modules quand c'est possible de le faire. Dans cette section, les espaces vectoriels considérés seront tous de dimension finie.

2.1 Un premier outil : le lemme des noyaux

Théorème 2.1 (Lemme des noyaux)**.** Soient E un K-espace vectoriel, $u \in \mathscr{L}(E)$ et $P_1, \dots, P_r \in K[X]$ r polynômes deux à deux premiers entre eux. Notons P le produit $P_1 \dots P_r$. Alors on a la décomposition suivante :

$$\ker\left(P(u)\right) = \bigoplus_{i=1}^{r} \ker\left(P_i(u)\right).$$

De plus, les projecteurs $p_i : \ker\left(P(u)\right) \longrightarrow \ker(P_i(u))$ sont des polynômes en u.

On peut avoir une interprétation de ce résultat en terme de module et faire un lien avec le théorème chinois, mais cela nécessite la notion de module de torsion (et un magnifique complément de Matthieu Romagny [Rom]) :

Définition 2.2. Soient A un anneau commutatif unitaire, M un A-module et $a \in A$. On dit que M est de a-torsion si pour tout $m \in M$, on a $a \cdot m = 0$.

Exemple 2.1.1.
— *Si A est un anneau commutatif unitaire, alors les quotients $\dfrac{A}{(a)}$ sont des A-modules de a-torsion.*
— *Si (E, u) est un $K[X]$-module avec E de dimension finie, alors (E, u) est un module de π_u-torsion.*

On a alors naturellement que tout A-module possède un plus grand sous-module de a-torsion :

Proposition 2.3. Soient M un A-module et $a \in A \setminus \{0\}$. Notons $M(a)$ le plus grand sous-A-module de M qui soit de a-torsion. Alors on a :

$$M(a) = \ker(\mu_a)$$

où μ_a désigne le morphisme A-linéaire de multiplication par a :

$$\begin{array}{rccc} \mu_a & : & M & \longrightarrow & M \\ & & m & \longmapsto & a \cdot m \end{array}$$

Si $M(a) = \{0\}$ pour tout $a \in A \setminus \{0\}$, on dit alors que M est *sans torsion.*

Remarque 2.1.1. *Si (E, u) est un $K[X]$-module, alors pour $P \in K[X]$, le plus grand sous-module de P-torsion correspond au sous-espace* $\ker(P(u))$ *!*

On a alors une version générale du lemme des noyau, ainsi qu'une version module du lemme chinois :

Théorème 2.4. Soient A un anneau principal, M un A-module et $a_1 \dots a_r \in A$ r éléments deux à deux premiers entre eux. Notons $a = a_1 \dots a_r$. Alors :

1. (Lemme des noyaux) On a la décomposition en somme directe suivante :

$$M(a) = \bigoplus_{i=1}^{r} M\left(a_i\right)$$

2. (Théorème chinois) On a l'isomorphisme A-linéaire suivant :

$$\begin{array}{ccc} \dfrac{M}{aM} & \xrightarrow{\simeq} & \displaystyle\prod_{i=1}^{r} \frac{M}{a_i M} \\ \overline{m}^{aM} & \longmapsto & \left(\overline{m}^{a_1 M}, \dots, \overline{m}^{a_r M}\right) \end{array}$$

où on a noté aM l'image du morphisme μ_a défini avant.

On peut en fait "identifier" le théorème chinois et le lemme des noyaux grâce au résultat suivant :

Théorème 2.5. Soient A un anneau principal et $a = a_1 \dots a_r$ comme dans l'énoncé précédent. Alors :

1. Le morphisme composé $\varphi_i : M(a_i) \hookrightarrow M(a) \to \dfrac{M(a)}{a_i M(a)}$ est un isomorphisme.
2. Le morphisme suivant :

$$\begin{array}{rccc} \varphi & : & \displaystyle\prod_{i=1}^{r} M(a_i) & \longrightarrow & \displaystyle\prod_{i=1}^{r} \frac{M(a)}{a_i M(a)} \\ & & (x_1, \dots, x_r) & \longmapsto & (\varphi_1(x_1), \dots, \varphi_r(x_r)) \end{array}$$

est un isomorphisme permettant d'identifier les décompositions :

$$M(a) = \bigoplus_{i=1}^{r} M(a_i)$$

et :

$$M(a) = \frac{M(a)}{aM(a)} \simeq \prod_{i=1}^{r} \frac{M(a)}{a_i M(a)}.$$

C'est-à-dire que si s désigne l'isomorphisme entre $\displaystyle\prod_{i=1}^{r} M(a_i)$ et $M(a)$ donné par la somme directe et si Ψ désigne l'isomorphisme du théorème chinois, alors on a :

$$\varphi = \Psi \circ s$$

Remarque 2.1.2. *Avec plus de travail, j'aurais pu dessiner un magnifique diagramme commutatif mais bon...*

Le lemme des noyaux permet d'obtenir un critère de diagonalisabilité bien connu :

Corollaire 2.6. Si E est un K-espace vectoriel et $u \in \mathscr{L}(E)$, alors l'endomorphisme u est diagonalisable si et seulement si son polynôme minimal π_u est scindé à racines simples. Il est trigonalisable si et seulement si son polynôme caractéristique χ_u est scindé.

2.2 La réduction de Frobenius en lien avec le théorème de structure des modules de type fini (et ses applications) [BMP05] [CG15]

On avait discuté, grâce au corollaire 1.7, que classifier les endomorphismes à similitude près revenait à classifier les structures de $K[X]$-modules sur E. Ça tombe bien, $K[X]$ étant principal, on a un résultat de classification des modules de type fini sur cet anneau.

2.2.1 Le théorème de structure des modules de type fini

On se place, dans cette section, dans un anneau A *principal*. D'abord, commençons par définir ce que sont des modules de type fini, et également des modules libres :

Définition 2.7 (Modules libres, modules de type fini)**.** Un A-module M est dit *de type fini* si M possède une famille génératrice finie, c'est-à-dire qu'il existe une famille $(e_1, \dots, e_r) \in M^r$ telle que le morphisme A-linéaire suivant :

$$\begin{array}{rcl} A^r & \longrightarrow & M \\ (a_1, \dots, a_r) & \longmapsto & \displaystyle\sum_{i=1}^{r} a_i \cdot e_i \end{array}$$

soit surjectif. S'il existe une telle famille telle que le morphisme précédent soit également injectif, alors M est dit *libre* et la famille $(e_1, \dots, e_r)$ est appelée *base* de M.

Tout comme les espaces vectoriels, on a le résultat suivant pour les modules libres de type fini :

Proposition 2.8. Soit M un module libre de type fini. Alors toutes les bases de M ont même cardinal. Ce cardinal commun est appelé *rang* du module libre M.

Remarque 2.2.1. *Attention, cela dit, contrairement au cas des espaces vectoriels, les modules de type fini ne possèdent pas systématiquement une base ! En effet, un module libre est en particulier sans torsion, ce qui signifie que tout module possédant une partie de torsion non-nulle n'est pas libre !*

On a alors un résultat de décomposition matricielle bien connu : la forme normale de Smith.

Théorème 2.9 (Forme normale de Smith)**.** Soit A un anneau commutatif unitaire intègre que l'on suppose principal. Soient $m, n \in \mathbb{N}^*$ et soit $M \in \mathscr{M}_{m,n}(A)$. Alors il existe un entier s et des éléments $d_1, \dots, d_s \in A$ vérifiant les conditions de divisibilité :

$$d_s \mid \dots \mid d_1$$

et des matrices $(P, Q) \in \mathrm{SL}_m(A) \times \mathrm{SL}_n(A)$ tels que :

$$P^{-1}MQ = \begin{pmatrix} d_1 & 0 & \cdots & 0 & \\ 0 & d_2 & \cdots & 0 & \mathbf{O}_{s,n-s} \\ \vdots & \ddots & \ddots & \vdots & \\ 0 & \cdots & 0 & d_s & \\ & \mathbf{O}_{m-s,s} & & & \mathbf{O}_{m-s,n-s} \end{pmatrix}.$$

De plus, le couple $(s, (d_1, \dots, d_s))$ est unique au sens suivant : s'il existe $(t, (d'_1, \dots, d'_t)) \in \mathbb{N}^* \times A^t$ vérifiant les mêmes hypothèses de divisibilité et s'il existe $(P', Q') \in \mathrm{GL}_m(A) \times \mathrm{GL}_n(A)$ tel que :

$$P'^{-1}MQ' = \begin{pmatrix} d'_1 & 0 & \cdots & 0 & \\ 0 & d'_2 & \cdots & 0 & \mathbf{O}_{t,n-t} \\ \vdots & \ddots & \ddots & \vdots & \\ 0 & \cdots & 0 & d'_t & \\ & \mathbf{O}_{m-t,t} & & & \mathbf{O}_{m-t,n-t} \end{pmatrix},$$

alors $s = t$ et pour tout $i \in [\![1, s]\!]$, d_i et d'_i sont associés. La matrice diagonale de ce théorème est appelée *forme normale de Smith* de la matrice A et les coefficients d_i sont appelés *facteurs invariants* de la matrice A.

Remarque 2.2.2. *Il s'agit du pendant "anneau principal" du pivot de Gauss, qui caractérise les matrices à coefficients dans un corps à équivalence près :*

Théorème 2.10. Soit k un corps et $A \in \mathscr{M}_{m,n}(k)$. Alors, il existe un unique entier r et il existe $(P, Q) \in \mathrm{GL}_m(k) \times \mathrm{GL}_n(k)$ tel que :

$$P^{-1}AQ = \begin{pmatrix} I_r & \mathbf{O}_{r,q-r} \\ \mathbf{O}_{p-r,r} & \mathbf{O}_{p-r,q-r}. \end{pmatrix}$$

Cet entier r est le rang de la matrice A et caractérise les orbites de l'action par équivalence : deux matrices A et B sont équivalentes si et seulement si elles ont le même rang.

Dans la preuve de ce théorème, on se base sur le fait que les éléments non-nuls de k sont inversibles pour diviser sans vergogne. Cependant, dans un anneau principal, on ne peut plus effectuer ces divisions. On effectue donc des substituts : si notre anneau est euclidien, on peut effectuer des divisions euclidiennes et donc remplacer l'algorithme du pivot de Gauss par un pivot de Gauss « avec restes » ou, si l'anneau est seulement principal, remplacer la division par l'application d'une relation de Bézout pour remplacer le coefficient que l'on voudrait éliminer par un PGCD.

Ce résultat, couplé au lemme suivant :

Lemme 2.11. Si M est un A-module libre de type fini, alors tout sous-module N de M est libre de type fini. De plus, $\operatorname{rang}(N) \leqslant \operatorname{rang}(M)$.

nous donne le théorème de la base adaptée :

Théorème 2.12 (base adaptée)**.** Soit M un A-module libre de type fini et soit N un sous-module de M. Alors il existe une base $(e_1, \dots, e_n)$ de M et des éléments $d_1, \dots, d_s \in A$ tels que :
— $d_1 \mid \dots \mid d_s$,
— la famille $(d_1 e_1, \dots, d_s e_s)$ forme une base de N.

Démonstration. Étant donné que M est libre et de type fini, il existe une base $(e'_1, \dots, e'_n)$ de M. D'après le lemme précédent, il existe également une base $(\varepsilon'_1, \dots, \varepsilon'_m)$ de N. Soit U la matrice de l'inclusion $N \hookrightarrow M$ dans les bases $(\varepsilon'_1, \dots, \varepsilon'_m)$ et $(e'_1, \dots, e'_n)$. D'après le théorème de forme normale de Smith, il existe deux matrices $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_m(A)$, et des éléments $d_1 \mid \dots \mid d_s \in A$ tels que :

$$PUQ = \begin{pmatrix} d_1 & 0 & \cdots & 0 & \\ 0 & d_2 & \cdots & 0 & \mathbf{O}_{s,n-s} \\ \vdots & \ddots & \ddots & \vdots & \\ 0 & \cdots & 0 & d_s & \\ & & & & \\ & \mathbf{O}_{m-s,s} & & & \mathbf{O}_{m-s,n-s} \end{pmatrix} =: D.$$

Or, U est la matrice d'une application injective. Ainsi, nécessairement, $m = s$ et :

$$D = \begin{pmatrix} d_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_s \\ & & \\ & \mathbf{O}_{m-s,s} & \end{pmatrix}.$$

Soit alors $(e_1, \dots, e_n)$ la base de M telle que P soit égale à la matrice de passage de la base $(e'_1, \dots, e'_n)$ à la base $(e_1, \dots, e_n)$ et $(\varepsilon_1, \dots, \varepsilon_s)$ la base de N telle que Q^{-1} soit égale à la matrice de passage de la base $(\varepsilon'_1, \dots, \varepsilon'_n)$ à la base $(\varepsilon_1, \dots, \varepsilon_n)$. La matrice D correspond alors à la matrice de l'inclusion $N \hookrightarrow M$ dans les nouvelles bases $(\varepsilon_1, \dots, \varepsilon_s)$ et $(e_1, \dots, e_n)$, de sorte que :

$$\forall i \in [\![1, s]\!], \quad \varepsilon_i = d_i e_i,$$

ce qui conclut. □

On en déduit le résultat central de la théorie des modules de type fini :

Théorème 2.13 (Structure des modules de type fini sur un anneau principal)**.** Soit M un A-module de type fini. Alors il existe un unique couple d'entiers (r, s) et d'uniques éléments (à association près) $d_s \mid \dots \mid d_1 \in A \setminus \{0\}$ tels que :

$$M \simeq A^r \times \left(\prod_{i=1}^{s} \frac{A}{(d_i)} \right).$$

Les d_i sont appelés *facteurs invariants* du module M.

Démonstration. Le module M étant supposé de type fini, il possède une famille génératrice finie. Notons-la $(e_1, \dots, e_n)$.

On a alors que le morphisme :

$$\begin{array}{rccc} \Phi & : & A^n & \longrightarrow & M \\ & & (a_1, \dots, a_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} a_i \cdot e_i \end{array}$$

est surjectif. Par théorème d'isomorphisme, on a alors :

$$M \simeq \frac{A^n}{\ker(\Phi)}.$$

Maintenant, par le théorème de la base adaptée appliqué à A^n (qui est un module libre de type fini) et à $\ker(\Phi)$, il existe une base $(f_1, \dots, f_n)$ de A^n, d'un entier s' et d'une suite d'éléments non-nuls $d_{s'} \mid \dots \mid d_1 \in A$ tels que :

$$A^n = \bigoplus_{i=1}^{n} Af_i, \quad \text{et} \quad \ker(\Phi) = \bigoplus_{i=1}^{s'} A(d_i f_i).$$

Ainsi, l'isomorphisme plus haut devient :

$$M \simeq \frac{\displaystyle\bigoplus_{i=1}^{n} Af_i}{\displaystyle\bigoplus_{i=1}^{s'} A(d_i f_i)} \simeq \prod_{i=1}^{s'} \left(\frac{A}{(d_i)} \right) \times \prod_{i=s'+1}^{n} A = A^{n-s'} \times \prod_{i=1}^{s'} \left(\frac{A}{(d_i)} \right).$$

En ne conservant que les d_i non-inversibles (si d_i est inversible, $\dfrac{A}{(d_i)} = \{0\}$), on obtient :

$$M \simeq A^{n-s'} \times \prod_{i=1}^{s} \frac{A}{(d_i)}$$

ce qui donne l'existence de la décomposition. L'unicité des d_i vient de la décomposition en forme normale de Smith. L'unicité de $r := n - s'$ reste à montrer, mais il s'agit du rang de la "partie libre" de M, que l'on peut définir comme étant le module quotient $\dfrac{M}{\mathrm{Tor}(M)}$ où $\mathrm{Tor}(M)$ désigne la partie de torsion de M :

$$\mathrm{Tor}(M) := \{ m \in M \mid \exists a \in A \setminus \{0\}, \quad a \cdot m = 0 \} = \sum_{a \in A \setminus \{0\}} M(a).$$

Ainsi, l'entier r ne dépend que de M et est donc unique, ce qui conclut. □

On a donc la traduction pour les endomorphismes, en prenant $A = K[X]$:

Théorème 2.14. Soit (E, u) un $K[X]$-module. Alors il existe une unique suite de polynômes unitaires $P_r \mid \dots \mid P_1 \in K[X]$ tels que :

$$(E, u) \simeq \prod_{i=1}^{r} \frac{K[X]}{(P_i)}.$$

Les polynômes P_i sont appelés *invariants de similitude* de u.

On a alors que l'endomorphisme u est déterminé, à similitude près, par ces polynômes (c'est pour ça qu'ils s'appellent invariants de similitude !). Pour boucler notre étude, il nous reste à nous intéresser à la description "endomorphisme" des $K[X]$-modules $\dfrac{K[X]}{(P)}$ pour $P \in K[X]$.

2.2.2 Endomorphismes cycliques et matrices compagnon

Proposition 2.15. Soient E un K-espace vectoriel et $u \in \mathscr{L}(E)$. Le $K[X]$-module (E, u) est isomorphe à $\dfrac{K[X]}{(P)}$ si et seulement si P et π_u sont associés et il existe $x \in E$ tel que la famille :

$$\mathscr{B}_x := \big(x, u(x), \dots, u^{n-1}(x)\big)$$

soit une base de E ($n = \deg(P)$). Dans ce cas, on a :

$$\mathrm{Mat}_{\mathscr{B}_x}(u) = C_{\pi_u}$$

la matrice compagnon du polynôme π_u et u est qualifié d'*endomorphisme cyclique.*

Remarque 2.2.3 (Terminologie)**.** *On remarque que $u \in \mathscr{L}(E)$ est cyclique si et seulement si le $K[X]$-module (E, u) est cyclique, c'est-à-dire engendré par un élément $e \in E$, d'où le terme "cyclique" pour l'endomorphisme u !*

Couplé au théorème 2.14, on obtient le théorème de réduction de Frobenius :

Théorème 2.16 (Frobenius)**.** Soient E un K-espace vectoriel et soit $u \in \mathscr{L}(E)$. Alors il existe d'unique polynômes unitaires non-constants $P_r \mid \dots \mid P_1 \in K[X]$ et il existe une base $\mathscr{B}$ de E telle que :

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} C_{P_1} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & C_{P_r} \end{pmatrix}.$$

Dit autrement, il existe des sous-espaces de E stables par u $F_1, \dots, F_r$ tels que :

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

et $u_{|F_i}$ est cyclique, de polynôme minimal P_i. Ces P_i correspondent aux invariants de similitude de u.

Remarque 2.2.4. *Si $u \in \mathscr{L}(E)$ et qu'on note $P_r \mid \dots \mid P_1$ ses invariants de similitude, alors :*
- $\pi_u = P_1$,
- $\chi_u = P_1 \dots P_r$.

Ainsi, u est cyclique si et seulement si $r = 1$ (définition) si et seulement si $\pi_u = \chi_u$.

Cette décomposition de Frobenius donne un moyen effectif de calculer les invariants de similitude de u grâce au fait suivant :

Théorème 2.17. Les invariants de similitude d'une matrice $A \in \mathscr{M}_n(K)$ sont exactement les facteurs invariants non-inversibles de la matrice $XI_n - A \in \mathscr{M}_n(K[X])$. En particulier, deux matrices A et B sont semblables si et seulement si les matrices $XI_n - A$ et $XI_n - B$ sont équivalentes.

Démonstration. Grâce à la décomposition de Frobenius, on est ramené au cas où A est la matrice compagnon C_P d'un polynôme unitaire $P \in K[X]$. Montrons que cette matrice est équivalente dans $K[X]$ à la matrice $\mathrm{diag}(P, 1, \dots, 1)$. Cela montrera que P, qui est l'unique invariant de similitude de C_P est l'unique facteur invariant non-inversible de

$XI_n - C_P$. Pour rappel, on a :

$$XI_n - C_P = \begin{pmatrix} X & 0 & 0 & 0 & \cdots & a_0 \\ -1 & X & 0 & 0 & \cdots & a_1 \\ 0 & -1 & X & 0 & \cdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & -1 & X + a_{n-1} \end{pmatrix}.$$

En effectuant les opérations élémentaires :

$$L_1 \longleftarrow \sum_{i=1}^{n} X^{i-1} L_i \quad \text{et} \quad C_{i+1} \longleftarrow C_{i+1} + XC_i, \quad \text{pour } i \in [\![1, n-1]\!],$$

on obtient que la matrice $XI_n - C_P$ est équivalente à la matrice :

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & P \\ -1 & 0 & 0 & 0 & \cdots & a_1 \\ 0 & -1 & 0 & 0 & \cdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & -1 & a_{n-1} \end{pmatrix}$$

puis, en effectuant l'opération élémentaire $C_n \longleftarrow \sum_{i=1}^{n-1} b_i C_i$, on obtient la matrice :

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & P \\ -1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & -1 & 0 \end{pmatrix}.$$

En effectuant une permutation circulaire des colonnes, on obtient le résultat souhaité ! □

On peut donc calculer les invariants de similitude d'une matrice A en effectuant l'algorithme de mise sous forme normale de Smith de la matrice $XI_n - A$! Cela nous permet d'avoir le théorème suivant :

Théorème 2.18 (Invariances par extension de corps)**.** Soit L une extension de K et soit $A \in \mathscr{M}_n(K)$. Alors les invariants de similitude de A sur le corps K sont également les invariants de similitude de A sur le corps L ! En particulier :

1. le polynôme minimal π_A est invariant par extension de corps,
2. deux matrices $A, B \in \mathscr{M}_n(K)$ semblables sur L sont en fait semblables sur K.

Une autre application de ce fait est le résultat suivant :

Proposition 2.19. Toute matrice $A \in \mathscr{M}_n(K)$ est semblable à sa transposée.

Démonstration. Les invariants de similitude de A^T sont les facteurs invariants de la matrice $XI_n - A^T = (XI_n - A)^T$. Ainsi, ce sont les mêmes que les facteurs invariants de $XI_n - A$. Ainsi, A et A^T ont les mêmes invariants de similitude,

ces deux matrices sont donc semblables. □

2.2.3 Étude détaillée des sous-espaces stables par un endomorphisme cyclique [CG15]

Grâce à la théorie des modules, on peut avoir une description exhaustive des sous-espaces stables par un endomorphisme cyclique :

Théorème 2.20 (Sous-espaces stables par un endomorphisme cyclique)**.** Soit (E,u) un $K[X]$-module avec u cyclique et soit $e \in E$ un vecteur cyclique pour u, c'est-à-dire tel que la famille :

$$\mathscr{B}_e := \big(e, u(e), \dots, u^{n-1}(e)\big)$$

soit une base de E. Notons $\mathscr{S}_u$ l'ensemble des sous-espaces de E stables par u, et $\mathscr{D}_u$ l'ensemble des diviseurs unitaires de π_u. Alors l'application

$$\begin{array}{ccc} \mathscr{D}_u & \longrightarrow & \mathscr{S}_u \\ D & \longmapsto & \mathrm{Im}(D(u)) \end{array}$$

est une bijection. En particulier, u possède un nombre fini de sous-espaces stables (cela caractérise les endomorphismes cycliques sur un corps infini !).

Démonstration. On sait que F est un sous-espace de E stable par u si et seulement si F est un sous-$K[X]$-module de (E,u). Or, u étant cyclique, l'application :

$$\begin{array}{rccc} \Psi & : & \dfrac{K[X]}{(\pi_u)} & \longrightarrow & E \\ & & \overline{P}^{\pi_u} & \longmapsto & P(u)(e) \end{array}$$

est bien définie et est un isomorphisme $K[X]$-linéaire. Ainsi, on a une correspondance entre les sous-$K[X]$-modules de (E,u) et les sous-$K[X]$-modules de $\dfrac{K[X]}{(\pi_u)}$. Or, on a une correspondance entre les sous-$K[X]$-modules de ce quotient et les sous-$K[X]$-modules de $K[X]$ contenant (π_u) via le morphisme de projection π, qui sont les idéaux (D) pour D unitaire divisant π_u. Plus précisément, les sous-$K[X]$-modules de $\dfrac{K[X]}{(\pi_u)}$ sont les $\dfrac{DK[X]}{(\pi_u)}$ pour D parcourant $\mathscr{D}_u$. Ainsi, l'isomorphisme Ψ induit la bijection suivante :

$$\begin{array}{ccc} \mathscr{D}_u & \longrightarrow & \mathscr{S}_u \\ D & \longmapsto & \Psi\left(\dfrac{DK[X]}{(\pi_u)}\right) = \{DP(u)(e),\ P \in K[X]\} = \{D(u)(x),\ x \in E\} = \mathrm{Im}(D(u)). \end{array}$$

La deuxième égalité découle du fait que e est un vecteur cyclique pour u. □

Remarque 2.2.5. *On peut également avoir un point de vue "torsion" et plutôt écrire que l'application :*

$$\begin{array}{ccc} \mathscr{D}_u & \longrightarrow & \mathscr{S}_u \\ D & \longmapsto & \ker\left(\dfrac{\pi_u}{D}(u)\right) \end{array}$$

est une bijection, en remarquant que, si $D \in \mathscr{D}_u$, alors $T := \dfrac{\pi_u}{D} \in \mathscr{D}_u$ et que le sous-module $\dfrac{DK[X]}{(\pi_u)}$ est égal au noyau du morphisme de multiplication par T, et donc :

$$\Psi\left(\frac{DK[X]}{(\pi_u)}\right) = \ker(T(u)).$$

Remarque 2.2.6 (Quelle est la bijection réciproque ?)**.** *Vous pourrez trouver dans [CG15] que si F est un sous-espace de E stable par $u \in \mathscr{L}(E)$, et si u^F désigne l'endomorphisme induit sur le quotient $\dfrac{E}{F}$, alors l'application :*

$$\begin{array}{ccc} \mathscr{S}_u & \longrightarrow & \mathscr{D}_u \\ F & \longmapsto & \pi_{u^F} \end{array}$$

est la bijection réciproque de l'application du théorème 2.20.

2.2.4 Un corollaire important : la réduction de Jordan des endomorphismes nilpotents

On sait que si $u \in \mathscr{L}(E)$ est un endomorphisme nilpotent, alors $\chi_u = X^n$. Ainsi, d'après la remarque 2.2.4, tous les invariants de similitude de u sont de la forme X^{p_i} avec $p_r \leqslant \ldots \leqslant p_1 = \deg(\pi_u)$. Or, la matrice compagnon de ces monômes est la matrice :

$$C_{X^p} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} =: J_p \in \mathscr{M}_p(K).$$

On obtient donc le théorème de réduction de Jordan des endomorphismes nilpotents :

Théorème 2.21 (Jordan-nilpotent)**.** Soient E un K-espace vectoriel et $u \in \mathscr{L}(E)$ un endomorphisme nilpotent. Alors il existe une unique suite d'entiers $1 \leqslant p_r \leqslant \ldots \leqslant p_1 \leqslant n$ telle que :

— $\sum_{i=1}^{r} p_i = n$,

— il existe une base $\mathscr{B}$ de E telle que :

$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} J_{p_1} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & J_{p_r} \end{pmatrix}.$$

Remarque 2.2.7. *Dans certains livres, on définit plutôt le bloc de Jordan de taille p comme étant la transposée de la matrice C_{X^p}, mais au vu de la proposition 2.19, le théorème de Jordan que j'ai donné est rigoureusement équivalent au théorème de Jordan qui ferait intervenir les transposées des matrices C_{X^p}.*

Remarque 2.2.8 (On voit apparaître des partitions !)**.** *Le théorème de Jordan nous montre que l'ensemble des orbites des matrices nilpotentes de taille n sur un corps K est indexée par l'ensemble des partitions de l'entier n. On peut alors représenter ces orbites sous la forme de diagrammes de Ferrers (ou de Young) comme dans l'écrit de maths générales 2023.*

Remarque 2.2.9 (Sous-espaces stables par un endomorphisme nilpotent d'indice maximal)**.** *Si $u \in \mathscr{L}(E)$ est un endomorphisme nilpotent d'indice maximal, alors il est cyclique ($\pi_u = \chi_u = X^n$) et donc, d'après le théorème 2.20, on a une description explicite des sous-espaces de E stables par u. Ce sont exactement les :*

$$\ker\left(u^k\right) = \mathrm{Im}\left(u^{n-k}\right), \quad k \in [\![0, n]\!].$$

2.2.5 Étude détaillée du commutant et du bicommutant d'un endomorphisme

D'après la proposition 1.6, on sait que le commutant d'un endomorphisme $u \in \mathscr{L}(E)$ correspond à l'ensemble des endomorphismes de $K[X]$-modules de (E, u). Grâce à la décomposition de Frobenius, on peut déterminer avec précision la structure du commutant de l'endomorphisme u :

Théorème 2.22 (Structure du commutant de u)**.** Soit (E, u) un $K[X]$-module. Alors, en notant :

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

la décomposition de E en sous-espaces cycliques, alors le commutant de u se décompose en somme directe :

$$\mathscr{C}_u = \bigoplus_{1 \leqslant i,j \leqslant r} \left(\mathscr{L}(F_i, F_j) \cap \mathscr{C}_u\right) = \bigoplus_{1 \leqslant i,j \leqslant r} \mathrm{Hom}_{K[X]}\left((F_i, u), (F_j, u)\right).$$

Remarque 2.2.10. *Ici, les espaces $\mathscr{L}(F_i, F_j)$ sont vus comme des sous-espaces de $\mathscr{L}(E)$ via l'identification :*

$$\varphi_{i,j} \in \mathscr{L}(F_i, F_j) \longhookrightarrow \varphi_{i,j} \circ p_i \in \mathscr{L}(E).$$

où $p_i : E \longrightarrow F_i$ désigne le projecteur sur F_i parallèlement à $\bigoplus_{j \neq i} F_j$.

Démonstration. La deuxième égalité vient de la proposition 1.6. Montrons alors que le commutant de u est égal à la somme directe la plus à droite. Pour cela, on se rappelle que :

$$\mathscr{C}_u = \mathrm{End}_{K[X]}((E, u)).$$

Or, on a la décomposition du module (E, u) en somme directe :

$$(E, u) = \bigoplus_{i=1}^{r} (F_i, u).$$

Ainsi, il suffit juste de montrer le fait général suivant sur les modules :

Proposition 2.23. Soit M un A-module décomposé en somme directe de sous-modules :

$$M = \bigoplus_{i=1}^{r} N_i.$$

Alors on a que $\mathrm{End}_A(M)$ se décompose en somme directe :

$$\mathrm{End}_A(M) = \bigoplus_{1 \leqslant i,j \leqslant r} \mathrm{Hom}_A(N_i, N_j)$$

en identifiant les espaces $\mathrm{Hom}_A(N_i, N_j)$ à des sous-modules de $\mathrm{End}_A(M)$ par l'application injective :

$$\varphi_{i,j} \in \mathrm{Hom}_A(N_i, N_j) \longhookrightarrow \varphi_{i,j} \circ p_i \in \mathrm{End}_A(M).$$

où $p_i : M \longrightarrow N_i$ désigne le morphisme A-linéaire de projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$.

Démonstration. Remarquons pour commencer que la somme du membre de droite est bien une somme directe. En effet, si on a :

$$(\varphi_{i,j})_{1 \leqslant i,j \leqslant r} \in \prod_{1 \leqslant i,j \leqslant r} \mathrm{Hom}_A(N_i, N_j) \quad \text{tel que} \quad \sum_{1 \leqslant i,j \leqslant r} \varphi_{i,j} = 0$$

alors :

$$\forall x \in M, \quad \sum_{1 \leqslant i,j \leqslant r} \varphi_{i,j}(p_i(x)) = 0.$$

Étant donné que les N_j sont en somme directe, on a alors :

$$\forall x \in M, \ \forall j \in [\![1, r]\!], \quad \sum_{i=1}^{r} \varphi_{i,j}(p_i(x)) = 0.$$

En particulier, en prenant, pour $i \in [\![1, r]\!]$, des $x \in N_i$, on a :

$$\forall (i,j) \in [\![1, r]\!]^2, \ \forall x \in N_i, \quad \varphi_{i,j}(x) = 0.$$

On a donc $\varphi_{i,j} = 0$ pour tout $(i,j) \in [\![1, r]\!]^2$, ce qui montre bien que la somme est directe. Maintenant, on se rend compte que :

$$\forall \varphi \in \mathrm{End}_A(M) = \sum_{1 \leqslant i,j \leqslant r} \underbrace{p_j \circ \varphi \circ p_i}_{\in \mathrm{Hom}_A(N_i, N_j)},$$

et donc, on a :

$$\mathrm{End}_A(M) \subset \bigoplus_{1\leqslant i,j\leqslant r} \mathrm{Hom}_A(N_i, N_j),$$

l'inclusion réciproque étant claire. □

En appliquant ce résultat, on a la conclusion. □

Il ne nous reste plus qu'à déterminer la structure des ensembles $\mathrm{Hom}_{K[X]}(F_i, F_j)$, c'est-à-dire trouver la structure de l'ensemble des morphismes de $K[X]$-modules entre deux modules cycliques. Or, un module cyclique (E, u) étant isomorphe au module $\dfrac{K[X]}{(\pi_u)}$, cela revient à déterminer la structure des ensembles :

$$\mathrm{Hom}_{K[X]}\left(\frac{K[X]}{(P)}, \frac{K[X]}{(Q)}\right)$$

pour $P, Q \in K[X]$ unitaire.

Théorème 2.24. Soient $P, Q \in K[X]$ deux polynômes unitaires, $D = P \wedge Q$ leur pgcd et $Q_0 = \dfrac{Q}{D}$. Alors on a les isomorphismes :

$$\mathrm{Hom}_{K[X]}\left(\frac{K[X]}{(P)}, \frac{K[X]}{(Q)}\right) \simeq \frac{Q_0K[X]}{(Q)} \simeq \frac{K[X]}{(D)}.$$

Éléments de démonstration (voir [CG15] pour la preuve complète). On vérifie que le morphisme :

$$\begin{array}{rccc} I & : & \mathrm{Hom}_{K[X]}\left(\dfrac{K[X]}{(P)}, \dfrac{K[X]}{(Q)}\right) & \longrightarrow & \dfrac{Q_0K[X]}{(Q)} \\ & & \varphi & \longmapsto & \varphi\left(\overline{1}^P\right) \end{array}$$

est bien défini et est un isomorphisme. Pour finir, on montre que le morphisme :

$$\begin{array}{ccc} K[X] & \longrightarrow & \dfrac{Q_0K[X]}{(Q)} \\ R & \longrightarrow & \overline{Q_0R}^Q \end{array}$$

passe au quotient en un isomorphisme entre $\dfrac{K[X]}{(D)}$ et $\dfrac{Q_0K[X]}{(Q)}$. □

On peut alors trouver la dimension du commutant et en déduire quelques résultats :

Théorème 2.25. Soit (E, u) un $K[X]$-module avec E de dimension n. Notons $P_s \mid \ldots \mid P_1 \in K[X]$ les facteurs invariants de (E, u) (i.e. les invariants de similitude de u) et $d_s \leqslant \ldots \leqslant d_1$ leur degré. On a alors :

$$\dim\left(\mathscr{C}_u\right) = \sum_{i=1}^{s} (2i-1)d_i.$$

En particulier :

1. $\dim(\mathscr{C}_u) \geqslant n$, avec égalité si et seulement si u est cyclique,
2. $\mathscr{C}_u = K[u]$ si et seulement si u est cyclique.

Démonstration. D'après les théorèmes 2.22 et 2.24, on a la décomposition en somme directe et les isomorphismes suivants :

$$\mathscr{C}_u = \bigoplus_{1\leqslant i,j\leqslant s} \mathrm{Hom}_{K[X]}((F_i, u), (F_j, u)) \simeq \prod_{1\leqslant i,j\leqslant s} \mathrm{Hom}_{K[X]}\left(\frac{K[X]}{(P_i)}, \frac{K[X]}{(P_j)}\right) \simeq \prod_{1\leqslant i,j\leqslant s} \frac{K[X]}{(P_i \wedge P_j)} = \prod_{1\leqslant i,j\leqslant s} \frac{K[X]}{\left(P_{\max(i,j)}\right)}.$$

Ces isomorphismes sont des isomorphismes de $K[X]$-modules. En particulier ce sont des isomorphismes de K-espaces vectoriels et donc :

$$\begin{aligned}\dim(\mathscr{C}_u) &= \sum_{1\leqslant i,j\leqslant s} \dim\left(\frac{K[X]}{(P_{\max(i,j)})}\right) = \sum_{1\leqslant i,j\leqslant s} d_{\max(i,j)} = \sum_{j=1}^{s}\left(\sum_{i=1}^{j} d_j + \sum_{i=j+1}^{s} d_i\right)\\ &= \sum_{j=1}^{s} j d_j + \sum_{i=1}^{s} \underbrace{\sum_{j=1}^{i-1} d_i}_{=(i-1)d_i} = \sum_{j=1}^{s}(2j-1)d_j.\end{aligned}$$

En particulier :

1. Étant donné que pour tout $i \geqslant 1$, on a :
$$2i-1 \geqslant 1,$$
on a :
$$\dim(\mathscr{C}_u) \geqslant \sum_{i=1}^{s} d_i = n,$$
avec égalité si et seulement si :
$$\forall i \in [\![1,s]\!], \quad (2i-1)d_i = d_i, \quad \text{i.e.} \quad \forall i \in [\![1,s]\!], \quad 2i-1=1.$$
Ainsi, $\dim(\mathscr{C}_u) = n$ si et seulement si $s=1$, i.e. u est cyclique.
2. On a déjà que $K[u] \subset \mathscr{C}_u$. Il y a donc égalité entre ces deux espaces si et seulement s'ils ont la même dimension. Or, on a les inégalités :
$$\dim(K[u]) \leqslant n \leqslant \dim(\mathscr{C}_u).$$
Ainsi, $\dim(K[u]) = \dim(\mathscr{C}_u)$ si et seulement si $\dim(K[u]) = \dim(\mathscr{C}_u) = n$, ce qui est vérifié si et seulement si u est cyclique.

□

On a donc pu mener l'étude complète du commutant d'un endomorphisme u assez simplement grâce à la théorie des $K[X]$-modules ! Cette étude du commutant nous permet de mener également l'étude du bicommutant :

Théorème 2.26 (Bicommutant d'un endomorphisme)**.** Soit (E,u) un $K[X]$-module. On note $\mathscr{C}_u^2$ le *bicommutant* de l'endomorphisme u, c'est-à-dire :

$$\mathscr{C}_u^2 := \{v \in \mathscr{L}(E) \mid \forall w \in \mathscr{C}_u, \quad v\circ w = w \circ v\} = \bigcap_{w\in\mathscr{C}_u} \mathscr{C}_w.$$

Alors $\mathscr{C}_u^2 = K[u]$.

Vous pourrez trouver la preuve dans [CG15]. Étant donné que la preuve de ce livre n'utilise pas vraiment de théorie des modules, je ne la détaillerai pas. On peut cependent faire une étude analogue pour le "commutant mixte" (ce terme vient de moi je ne sais pas comment cela s'appelle) de deux endomorphismes :

Définition 2.27. Soient E et G deux K-espaces vectoriels et soient $u \in \mathscr{L}(E)$ et $v \in \mathscr{L}(G)$. J'appelle *commutant mixte* de u et v l'ensemble :

$$\mathscr{C}_{u,v} := \{w \in \mathscr{L}(E,G) \mid w\circ u = v \circ w\}.$$

On sait, d'après la proposition 1.6 que cela correspond aux morphismes de $K[X]$-modules entre (E,u) et (G,v). On a alors un théorème analogue au théorème 2.22, en adaptant simplement la proposition 2.23 :

Théorème 2.28 (Structure du commutant mixte)**.** Soient (E,u) et (G,v) deux $K[X]$-modules. On note :

$$E=\bigoplus_{i=1}^{r} \quad \text{et} \quad G=\bigoplus_{i=1}^{s} H_i$$

les décompositions respectives de E et G en sous-espaces cycliques. Alors on a la décomposition en domme directe suivante :

$$\mathscr{C}_{u,v}=\bigoplus_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant s}} \left(\mathscr{L}(F_i,H_j)\cap\mathscr{C}_{u,v}\right)=\bigoplus_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant s}} \mathrm{Hom}_{K[X]}\left((F_i,u),(H_j,v)\right).$$

On en déduit alors une expression de la dimension du commutant mixte, en réutilisant le théorème 2.24.

Théorème 2.29 (Dimension du commutant mixte)**.** Soient (E,u) et (G,v) deux $K[X]$-modules. Alors, en notant :

$$P_r \mid \ldots \mid P_1 \quad \text{d'une part, et} \quad Q_s \mid \ldots \mid Q_1 \quad \text{d'autre part}$$

les invariants de similitude respectifs de u et v, on a :

$$\dim(\mathscr{C}_{u,v})=\sum_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant s}} \deg\left(P_i\wedge Q_j\right).$$

Je n'ai pas, à ma connaissance, d'expression plus simple pour la dimension de cet espace.

2.3 Sous-espaces simples et réduction d'un endomorphisme semi-simple [CG15]

Reparlons des endomorphismes semi-simples. On a vu que c'étaient des endomorphismes particulièrement adaptés pour la réduction étant donné qu'à partir d'un sous-espace stable, on a immédiatement à disposition un supplémentaire stable. On peut alors décomposer l'espace en somme de sous-espaces stables "indécomposables" au sens où ils n'ont aucun sous-espaces stables non-triviaux. C'est ce que l'on appelle des sous-espaces *simples* :

Définition 2.30. Soient E un K-espace vectoriel et $u\in\mathscr{L}(E)$. On dit que E est u-simple (ou que u est simple sur E) si les seuls sous-espaces de E stables par u sont $\{0\}$ et E.

On a une caractérisation des endomorphismes simples :

Proposition 2.31. Soient E un K-espace vectoriel et $u\in\mathscr{L}(E)$. Alors u est simple sur E si et seulement si son polynôme caractéristique χ_u est irréductible. En particulier, on a dans ce cas $\chi_u=\pi_u$.

Démonstration. $\Leftarrow$: Supposons que u ne soit pas simple sur E. Soit $F\notin\{\{0\},E\}$ un sous-espace stable par u. Dans une base adaptée, on a que la matrice de u s'écrit par blocs :

$$\begin{pmatrix} A & B \\ \mathbf{O} & A' \end{pmatrix}$$

de sorte que :

$$\chi_u=\chi_A\chi_{A'},$$

avec χ_A et $\chi_{A'}$ non constants. Ainsi, χ_u n'est pas irréductible.
$\Rightarrow$: Si χ_u n'est pas irréductible, alors on peut écrire :

$$\chi_u=P_1P_2$$

avec P_1 et P_2 deux polynômes unitaires premiers entre eux non-constants. Ainsi, le lemme des noyaux donne une décomposition de E en sous-espaces stables non-triviaux :

$$E = \ker(P_1(u)) \oplus \ker(P_2(u))$$

et donc u n'est pas simple sur E. □

On peut alors en déduire le fait suivant :

Corollaire 2.32. Si E est un K-espace vectoriel et $u \in \mathscr{L}(E)$ est simple, alors u est cyclique.

Presque par définition des endomorphismes semi-simples, on a alors une version plus forte de la réduction de Frobenius, pour les endomorphismes semi-simples :

Théorème 2.33 (Décomposition en sous-espaces simples)**.** Soit E un K-espace vectoriel et $u \in \mathscr{L}(E)$ un endomorphisme semi-simple. Alors E se décompose ainsi :

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

avec $F_1, \dots, F_r$ des sous-espaces stables par u et u-simples.

Pour prouver ce théorème, il faut vérifier que la propriété de semi-simplicité passe aux sous-espaces stables :

Lemme 2.34. Soient E un K-espace vectoriel, $u \in \mathscr{L}(E)$ un endomorphisme semi-simple et F un sous-espace stable par u. Alors $u_{|F} \in \mathscr{L}(F)$ est également semi-simple.

Démonstration. Soit G un sous-espace de F stable par $u_{|F}$. Il s'agit, en particulier, d'un sous-espace de E stable par u. Par semi-simplicité de u, il existe un supplémentaire G' de G dans E stable par u. Soit alors $\tilde{G} = G' \cap F$. Alors on a :

$$F = G \oplus \tilde{G}$$

En effet, $G \cap \tilde{G} = G \cap (G' \cap F) = (G \cap G') \cap F = \{0\}$ d'une part, et d'autre part, si $x \in F$, alors il existe $(x_G, x_{G'}) \in G \times G'$ tel que :

$$x = x_G + x_{G'} \quad \text{de sorte que} \quad x_{G'} = \underbrace{x}_{\in F} - \underbrace{x_G}_{\in G \subset F} \in F$$

et donc $x_{G'} \in G' \cap F = \tilde{G}$. De plus, $\tilde{G}$ est bien stable par u étant donné que G' et F sont tous deux stables par u. On a donc trouvé un supplémentaire de G dans F stable par u. Ainsi, $u_{|F}$ est bien semi-simple. □

On est prêt à démontrer le théorème 2.33 :

Démonstration. Montrons le résultat par récurrence forte sur $n := \dim(E)$. Pour $n = 1$, E est clairement un espace u-simple, de sorte que le théorème est démontré avec $r = 1$ et $F_1 = E$. Maintenant, si $n \geqslant 2$, alors ou bien E est u-simple et on a terminé, ou bien il existe F un sous-espace de E stable par u qui soit non-trivial. Par semi-simplicité de u, on a également à disposition un sous-espace F' stable par u, non-trivial également tel que :

$$E = F \oplus F'.$$

Ainsi, en appliquant l'hypothèse de récurrence à F muni de $u_{|F}$ qui reste semi-simple d'après le lemme 2.34 et à F' muni de $u_{|F'}$, également semi-simple, on a :

$$E = \underbrace{\left(\bigoplus_{i=1}^{r} F_i\right)}_{=F} \oplus \underbrace{\left(\bigoplus_{i=1}^{r'} F_i'\right)}_{=F'}$$

où $F_1, \dots, F_r, F'_1, \dots, F'_{r'}$ sont des sous-espaces stables par u et u-simples, ce qui conclut. □

Remarque 2.3.1. *Ce résultat peut paraître familier aux habitué.e.s de représentations de groupes : les sous-espaces u-simples étant remplacés, dans le cadre des représentations, par des sous-représentations irréductibles. Il s'agit de la même logique et de la même preuve ! On a tout simplement décomposé un module en somme directe de supplémentaires les plus simples possibles.*

Ce résultat permet alors de donner des caractérisations d'un endomorphisme semi-simple :

Proposition 2.35. Soient E un K-espace vectoriel de dimension finie, avec K un corps parfait et $u \in \mathscr{L}(E)$. Alors les conditions suivantes sont équivalentes :

1. l'endomorphisme u est semi-simple,
2. le polynôme minimal π_u est sans facteur carré,
3. les invariants de similitude de u sont tous sans facteur carré,
4. l'endomorphisme u est diagonalisable dans une extension de K.

L'hypothèse "K est un corps parfait" est absolument nécessaire pour avoir l'implication 2. $\Rightarrow$ 4. : cela vient du fait qu'en passant dans le corps de décomposition de π_u, les facteurs irréductibles de π_u deviennent tous scindés à racines simples, ce qui n'est vrai que dans un corps parfait.

Conclusion

J'ai voulu, dans ce document, compiler tous les liens qu'on pouvait faire entre la théorie des modules et la réduction, et insister le plus possibles sur les éléments de théorie des modules qui peuvent donner davantage de recul sur les notions clefs de la réduction, voire même prouver de manière plus simple ou plus élégante les résultats phares de cette théorie (Frobenius, Jordan, commutant notamment). Dans le H2G2 tome 2 [CG15], vous pourrez trouver un tableau faisant office de "dictionnaire entre les espaces vectoriels et les $K[X]$-modules", que je vous conseille d'aller voir. Par ailleurs, vous remarquerez que la théorie des modules se prête bien pour la réduction d'*un* endomorphisme, mais pas forcément pour la réduction simultanée d'une famille d'endomorphismes qui commute entre eux (en tous cas je n'ai pas trouvé de références bibliographiques là-dessus). En tous cas, j'espère que ce document vous aura aidé et qu'il vous aura donné un éclairage nouveau et inspirant sur la réduction !

Références

[BMP05] Vincent Beck, Jérôme Malick, and Gabriel Peyré. *Objectif agrégation*. Sciences supérieur, 2005.

[CG15] Philippe Caldero and Jérôme Germoni. *Histoires hédonistes de groupes et de géométrie*, volume 2. Calvage & Mounet, 2015.

[DTLQ14] Gema-Maria Díaz-Toca, Henri Lombardi, and Claude Quitté. *Modules sur les anneaux commutatifs - cours et exercices*. Calvage & Mounet, 2014.

[Rom] Matthieu Romagny. Théorème chinois versus lemme des noyaux. `https://agreg-maths.univ-rennes1.fr/documentation/docs/theoreme_chinois_versus_lemme_des_noyaux.pdf`.