Autour du théorème des invariants de similitude

Grégory Vial – Octobre 2005

I. Introduction et notations

Le but de ces quelques pages est de présenter le résultat concernant les invariants de similitude d'un endomorphisme en dimension finie. On considérera deux points de vue qui conduisent à deux démonstrations du théorème : l'une relève de l'algèbre linéaire et de la dualité en dimension finie alors que l'autre utilise la structure de module dont on peut munir un espace vectoriel de dimension finie à l'aide des polynômes d'un endomorphisme. Les techniques employées dans cette deuxième preuve fournissent un algorithme de détermination des invariants de similitude d'un endomorphisme donné.

L'intérêt du théorème des invariants de similitude réside dans ses diverses applications : réduction de matrices, caractérisation des classes de similitude. D'un point de vue plus pragmatique, ce résultat peut constituer un développement dans le cadre d'une leçon d'agrégation : il trouve sa place dans les leçons concernant la réduction des matrices, la dualité en dimension finie, les sous-espaces stables, les polynômes d'endomorphismes, les matrices équivalentes. Enfin les outils développés ici peuvent être utilisés pour les leçons sur les réseaux, les groupes abéliens finis et les opérations élémentaires sur les lignes et les colonnes.

Voici les références bibliographiques dont ce texte est très largement inspiré :

[1] J.-M. Arnaudiès & J. Bertin, *Groupes, algèbres et géométrie*. Ellipses, Paris, 1995.

[2] M. Artin, *Algebra*. Prentice-Hall Inc., Englewood Cliffs, NJ 1991.

[3] R. Goblot, *Algèbre linéaire*. Masson, Paris, 1995.

[4] X. Gourdon, *Les maths en tête, algèbre*. Ellipses, Paris, 1994.

Dans toute la suite, E désignera un espace vectoriel de dimension finie non nulle sur un corps $\mathbb{K}$ et u un endomorphisme de E.

Définition 1 – *Si F est un sous-espace vectoriel de E, stable par u, on dira que u est $F-$cyclique (ou que F est $u-$monogène) ssi il existe $x \in F$ tel que*

$$F = \{f(u)(x) \mid f \in \mathbb{K}[X]\}$$

Notre objet sera de démontrer le résultat suivant :

Théorème 1 – *Il existe $F_1, F_2, \dots, F_r$ sous-espaces vectoriels de E $u-$stables tels que :*
- *$E = F_1 \oplus F_2 \oplus \cdots \oplus F_r$,*
- *F_i est $u-$monogène,*
- *Si P_i désigne le polynôme minimal de $u|_{F_i}$, alors $P_{i+1} \mid P_i$.*

La suite de polynômes $P_1, \dots, P_r$ ne dépend que de u, et non du choix de la décomposition. Elle est appelée suite des invariants de similitude *de u.*

II. L'approche "espace vectoriel"

Commençons par introduire quelques notations concernant les polynômes minimaux : Q_u désigne le polynôme minimal de u, c'est-à-dire le polynôme unitaire de $\mathbb{K}[X]$ tel que :

$$Q_u\mathbb{K}[X] = \{f \in \mathbb{K}[X] \mid f(u) = 0\}$$

Pour $a \in E$, on notera $Q_{u,a}$ le polynôme minimal de u en a, i.e.

$$Q_{u,a}\mathbb{K}[X] = \{f \in \mathbb{K}[X] \mid f(u)(a) = 0\}$$

Enfin on considérera les ppcm normalisés.

Lemme 1 – *Soient $a_1, \ldots, a_p$ des éléments de E tels que les sous-espaces vectoriels $G_i = \{f(u)(a_i) \mid f \in \mathbb{K}[X]\}$ soient en somme directe. On pose $a = \sum_{i=1}^{p} a_i$, alors*

$$Q_{u,a} = \operatorname*{ppcm}_{i=1}^{p} Q_{u,a_i}$$

Démonstration – Soit $M = \operatorname*{ppcm}_{i=1}^{n} Q_{u,a_i}$, alors $Q_{u,a}$ divise M dans $\mathbb{K}[X]$ car pour tout i, $M(u)(a_i) = 0$.

D'autre part, $Q_{u,a}(u)(a) = 0 = \sum_{i=1}^{p} b_i$ avec $b_i = Q_{u,a}(u)(a_i) \in G_i$. L'indépendance des G_i impose que $b_i = 0$ pour tout i, donc que $Q_{u,a_i} \mid Q_{u,a}$ pour tout i. D'où $M \mid Q_{u,a}$. ■

Ce résultat nous permet de démontrer la proposition suivante qui sera fondamentale dans la suite :

Proposition 1 – *Il existe $a \in E$ tel que $Q_u = Q_{u,a}$.*

Démonstration – Le polynôme Q_u n'est pas constant car $E \neq \{0\}$, on peut donc le décomposer en facteurs irréductibles unitaires :

$$Q_u = P_1^{\alpha_1} \cdots P_r^{\alpha_r}, \qquad r \geq 1, \alpha_i \geq 1$$

D'après le lemme des noyaux, $E = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i^{\alpha_i}(u))$.

On a $\mathrm{Ker}(P_i^{\alpha_i - 1}(u)) \subsetneq \mathrm{Ker}(P_i^{\alpha_i}(u))$. En effet s'il y a égalité, le polynôme $g = Q_u/P_i$ vérifie $g(u) = 0$, ce qui contredit la minimalité de Q_u.

Soit donc $a_i \in \mathrm{Ker}(P_i^{\alpha_i}(u)) \backslash \mathrm{Ker}(P_i^{\alpha_i - 1}(u))$. On a $Q_{u,a_i} = P_i^{\alpha_i}$ car P_i est irréductible. De plus, $\{f(u)(a_i) \mid f \in \mathbb{K}[X]\} \subset \mathrm{Ker}(P_i^{\alpha_i}(u))$, donc ces sous-espaces vectoriels sont indépendants.

On peut alors appliquer le lemme 1 : si on pose $a = \sum_{i=1}^{r} a_i$, on a

$$Q_{u,a} = \operatorname*{ppcm}_{i=1}^{r}(Q_{u,a_i}) = \prod_{i=1}^{r} P_i^{\alpha_i} = Q_u$$ ■

Exercice 1 – Montrer l'équivalence de u est $F-$cyclique avec l'égalité des polynômes minimal et caractéristique de $u|_F$.

Proposition 2 – *Si u est $E-$cyclique, alors il existe une base de E telle que la matrice de u dans cette base soit la matrice compagnon*

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

avec $Q_u(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$.

Démonstration – Comme u est cyclique, $\mathrm{d}^\mathrm{o}Q_u = \dim E = n$ (cf exercice 1). De plus, il existe $x \in E$ tel que

$$E = \{f(u)(x) \mid f \in \mathbb{K}[X]\}$$

La famille $(x, u(x), \ldots, u^{n-1}(x))$ est donc libre et, dans cette base, la matrice de u est de la forme annoncée. ■

Nous pouvons maintenant démontrer le théorème des invariants de similitude :

Démonstration du théorème 1 –

Existence – On procède par récurrence sur la dimension de E. La dimension 1 ne pose pas de problème. Supposons donc le résultat acquis pour tout espace vectoriel de dimension inférieure à $n-1$ et soit E de dimension n. D'après la proposition 1, il existe $a \in E$ tel que $Q_{u,a} = Q_u$. Si on note $k = \mathrm{d}^\mathrm{o}Q_u$, alors la famille

$$e_1 = a,\ e_2 = u(a),\ \ldots,\ e_k = u^{k-1}(a)$$

est libre. Soit F le sev engendré par cette famille. Complétons-la en une base $(e_1, \ldots, e_n)$ de E. Soit $(e_1^*, \ldots e_n^*)$ la base duale. On introduit les ensembles

$$\Gamma = \{u^{\top i}(e_k^*) \mid i \in \mathbb{N}\} \subset E^* \quad \text{et} \quad G = \Gamma^\perp = \{x \in E \,|\, \forall i \in \mathbb{N},\ e_k^*(u^i(x)) = 0\} \subset E$$

La notation $u^{\top i}$ désigne le $i^{\text{ème}}$ itéré du transposé de u.
G est un sev de E stable par u. De plus on a $E = F \oplus G$. En effet si $y \in F \cap G$ est non nul, on a

$$y = a_1e_1 + \cdots + a_pe_p \quad \text{avec } a_p \neq 0 \text{ et } p \leq k$$

En composant par $u^{\top k-p}(e_k^*)$, on obtient $a_p = 0$, ce qui est absurde. Donc $F \cap G = \{0\}$.
D'autre part $\dim F + \dim G = \dim E$ car $\dim(\mathrm{Vect}\,\Gamma) = k$. En effet l'application

$$\varphi : \begin{array}{ccc} \{f(u) \mid f \in \mathbb{K}[X]\} & \longrightarrow & \mathrm{Vect}\,\Gamma \\ g & \longmapsto & e_k^* \circ g \end{array}$$

est un isomorphisme (la vérification est immédiate).

Résumons : nous avons trouvé un sous-espace vectoriel F de E, $u-$monogène et un supplémentaire G, stable par u. Si $E = F$, alors le théorème est démontré. Sinon, notons $P_1 = Q_u$ et P_2 le polynôme minimal de $u|_G$. Alors $P_2 \,|\, P_1$. De plus on peut appliquer l'hypothèse de récurrence à $u|_G$ et on obtient ainsi la décomposition voulue.

Unicité – Supposons qu'il existe deux suites $F_1, \dots, F_r$ et $G_1, \dots, G_s$ de sous-espaces $u-$monogènes qui vérifient les conditions du théorème. On note $P_1, \dots, P_r$ et $Q_1, \dots, Q_s$ les deux suites de polynômes associées. Si elles diffèrent, notons j le premier indice pour lequel $P_j \neq Q_j$. Un tel indice existe toujours même si $r \neq s$, car $\sum_{i=1}^{r} \mathrm{d^o} P_i = \sum_{i=1}^{s} \mathrm{d^o} Q_i = \dim E$. De plus $j \geq 2$ car $P_1 = Q_1 = Q_u$. On a alors

$$P_j(u)(E) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_{j-1}) \tag{1}$$

et

$$P_j(u)(E) = P_j(u)(G_1) \oplus \cdots \oplus P_j(u)(G_s) \tag{2}$$

Les sommes sont directes car $P_j(u)(F_i) \subset F_i$ et $P_j(u)(G_i) \subset G_i$.
Or $\dim P_j(u)(F_i) = \dim P_j(u)(G_i)$ pour $1 \leq i \leq j-1$ d'après la proposition 2. En effet les endomorphismes $u|_{F_i}$ et $u|_{G_i}$ sont semblables car semblables à la matrice $C(P_i) = C(Q_i)$ pour $i < j$. On déduit de (1) et (2) que

$$\forall i \in \{j, \dots, s\},\ \dim P_j(u)(G_i) = 0$$

Ce qui prouve que $Q_j \mid P_j$. Par symétrie des rôles, $P_j \mid Q_j$ et donc $P_j = Q_j$, ce qui est une contradiction. On a donc $r = s$ et $P_i = Q_i$ pour tout i. ■

III. Applications

Nous donnons maintenant quelques-unes des applications les plus utiles du théorème des invariants de similitude :

Théorème 2 (réduction de Frobénius) – *Si $P_1, \dots, P_r$ désigne la suite des invariants de similitude de u, alors il existe une base de E dans laquelle u a pour matrice :*

$$\begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

Démonstration – Soit $E = F_1 \oplus \cdots \oplus F_r$ une décomposition associée aux invariants de similitude $P_1, \dots, P_r$. Alors F_i est $u-$monogène, donc d'après la proposition 1, il existe une base $(e_1^i, \dots, e_{n_i}^i)$ dans laquelle la matrice de $u|_{F_i}$ est $C(P_i)$. La matrice de u dans la base $(e_1^1, \dots, e_{n_1}^1, \dots, e_1^r, \dots, e_{n_r}^r)$ est donc de la forme annoncée dans le théorème. ■

Théorème 3 (réduction de Jordan) – *Si le polynôme caractéristique de u est scindé sur $\mathbb{K}$, alors il existe une base de E dans laquelle la matrice de u est de la forme*

$$\begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix}$$

où les blocs de Jordan J_i sont du type

$$J_i = \begin{pmatrix} \lambda_i & 1 & 0 & 0 \\ 0 & \ddots & 1 & 0 \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

Les λ_i sont les valeurs propres (non nécessairement distinctes) de u.

DÉMONSTRATION – On commence par démontrer le résultat dans le cas où u est nilpotent. D'après le théorème 2, le produit des P_i est le polynôme caractéristique de u, c'est-à-dire $(-1)^n X^n$. Donc chaque P_i est de la forme X^{n_i}. Donc $C(P_i)$ est la transposée d'un bloc de Jordan. On applique alors le théorème 2, n'ayant plus qu'à faire une permutation des vecteurs de la base pour obtenir la réduction de Jordan escomptée.

Dans le cas général (u n'est plus supposé nilpotent), on décompose E à l'aide du lemme des noyaux. En effet le polynôme caractéristique de u s'écrit $(x-\lambda_1)^{\alpha_1}\cdots(x-\lambda_s)^{\alpha_s}$. Donc

$$E = \bigoplus_{i=1}^{s} \mathrm{Ker}(u-\lambda_i\cdot\mathrm{id})^{\alpha_i} = \bigoplus_{i=1}^{s} H_i$$

Chaque H_i est $u-$stable et $(u-\lambda_i\cdot\mathrm{id})|_{H_i}$ est nilpotent. On lui applique le résultat démontré plus haut et on obtient la décomposition de Jordan qu'on désirait. ■

On vient d'obtenir deux décompositions importantes d'un endomorphisme : la réduite de Jordan peut-être utilisée pour démontrer des résultats sur les itérés de u. La décomposition de Frobénius, quant à elle, permet d'obtenir un théorème de caractérisation des classes de similitude.

Théorème 4 (caractérisation des classes de similitude) – *Deux endomorphismes sont semblables ssi ils ont les mêmes invariants de similitude.*

DÉMONSTRATION – Si u et v sont semblables, en reprenant la preuve de l'unicité du théorème 1, on montre facilement qu'ils ont mêmes invariants de similitude.

Réciproquement, si u et v ont mêmes invariants de similitude, il existe deux bases dans lesquelles les matrices de u et v sont identiques (cf. théorème 2), donc u et v sont semblables. ■

Ce dernier résultat possède de nombreuses applications dont le corollaire suivant.

Corollaire 1 – *Si $\mathbb{L}$ est une extension de $\mathbb{K}$, et si $A, B \in \mathcal{M}_n(\mathbb{K})$ sont semblables sur $\mathbb{L}$, alors elles sont semblables sur $\mathbb{K}$.*

DÉMONSTRATION – Il suffit, d'après le théorème 4, de démontrer que A et B ont mêmes invariants de similitude sur $\mathbb{K}$. Soient $P_1, \ldots, P_r \in \mathbb{K}[X]$ les invariants de similitude de A sur $\mathbb{K}$. D'après le théorème 2, A est semblable (sur $\mathbb{K}$) à la matrice

$$C = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

Donc les matrices C et A sont semblables sur $\mathbb{L}$, donc ont les mêmes invariants de similitude sur $\mathbb{L}$. Or les invariants de similitude de C sur $\mathbb{L}$ sont les $P_1, \ldots, P_r$, car le polynôme minimal ne dépend pas du corps de base (cf lemme 2). De même les invariants de similitude de B sur $\mathbb{K}$ sont ceux sur $\mathbb{L}$. Donc A et B ont mêmes invariants de similitude sur $\mathbb{K}$ donc sont semblables. ■

Lemme 2 – *Soient $A \in \mathcal{M}_n(\mathbb{K})$ et $\mathbb{L}$ une extension de $\mathbb{K}$, on note $Q_{\mathbb{K}}$ et $Q_{\mathbb{L}}$ les polynômes minimaux de A respectivement sur $\mathbb{K}$ et $\mathbb{L}$. Alors $Q_{\mathbb{K}} = Q_{\mathbb{L}}$.*

Démonstration – Il est clair que $Q_{\mathbb{L}}$ divise $Q_{\mathbb{K}}$. Soit $k = \mathrm{d}^{\mathrm{o}}Q_{\mathbb{K}}$. D'après la proposition 1, il existe $x \in \mathbb{K}^n$ tel que $Q_{\mathbb{K},x} = Q_{\mathbb{K}}$. Ainsi la famille $(x, Ax, \ldots, A^{k-1}x)$ est libre dans le $\mathbb{K}-$ev E. Mais le rang ne dépend pas du corps de base (la détermination du rang par les déterminants mineurs le prouve), donc la famille $(x, Ax, \ldots, A^{k-1}x)$ est libre dans le $\mathbb{L}-$ev E. On en déduit que $\mathrm{d}^{\mathrm{o}}Q_{\mathbb{L}} \geq k$. Donc $Q_{\mathbb{L}} = Q_{\mathbb{K}}$. ■

À titre d'exercice, on donne deux autres applications :

Exercice 2 – Soit $n = 2$ ou 3 et $A, B \in \mathcal{M}_n(\mathbb{R})$. Montrer que A et B sont semblables si et seulement si elles ont même polynôme caractéristique et même polynôme minimal. Trouver un contre-exemple pour $n = 4$.

Exercice 3 – Soit $u \in \mathcal{L}(E)$, montrer que u est cyclique si et seulement si les seuls endomorphismes commutant avec u sont les polynômes en u.

IV. L'approche "module"

Dans cette partie, on donne une autre démonstration du théorème 1, basée sur une idée différente. On va en effet munir E d'une structure de $\mathbb{K}[X]-$module et utiliser la décomposition des modules de type fini sur les anneaux euclidiens.

1. Structure de $\mathbb{K}[X]-$module sur E

Proposition 3 – *Soit $\mathbb{K}$ un corps. La donnée d'un $\mathbb{K}[X]-$module E équivaut à la donnée d'un $\mathbb{K}-$espace vectoriel E et d'un endomorphisme $u \in \mathcal{L}(E)$.*

Démonstration – Si E est un $\mathbb{K}[X]-$module, E est muni d'une structure de $\mathbb{K}-$espace vectoriel. De plus on peut définir un endomorphisme de E par

$$u : \begin{array}{ccc} E & \longrightarrow & E \\ a & \longmapsto & Xa \end{array}$$

Réciproquement, si $u \in \mathcal{L}(E)$, on définit pour $P \in \mathbb{K}[X]$ et $a \in E$, $Pa = (P(u))(a)$. On obtient ainsi une structure de $\mathbb{K}[X]-$module sur E. ■

La proposition précédente permet de considérer E comme module sur l'anneau des polynômes $\mathbb{K}[X]$. On utilisera l'équivalence des structures.

2. Décomposition d'un module de type fini sur un anneau euclidien

Le but de ce paragraphe est de démontrer le théorème de décomposition d'un module quand l'anneau de base est euclidien. La méthode proposée est constructive et l'algorithme utilisé servira plus loin.

Proposition 4 – *Soit A un anneau euclidien et M une matrice de taille $n \times p$ à coefficients dans A. Il existe deux matrices P et Q respectivement dans $\mathrm{GL}_n(A)$ et $\mathrm{GL}_p(A)$ et des éléments $d_1, \ldots, d_s$ de A tels que*

$$M = P \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_s & \\ & & & 0 \end{pmatrix} Q \qquad \text{et} \qquad d_1 \,|\, d_2 \,|\, \cdots \,|\, d_s$$

Démonstration – On procède par opérations élémentaires sur les lignes et les colonnes de la matrice M. Commençons par préciser les opérations licites :

– la permutation de deux lignes ou colonnes,

– l'ajout à une ligne (ou colonne) d'un multiple d'une autre.

En effet l'opération sur les lignes (resp. les colonnes) correspond à la multiplication à gauche (resp. à droite) par une matrice de permutation ou de transvection qui est inversible dans $\mathcal{M}_n(A)$ (voir exercice 4).

L'algorithme qui suit repose sur la division euclidienne dans A (on note ϕ le sthasme associé) ; il utilise les trois étapes suivantes :

Étape 1 –

À l'aide de permutations sur les lignes et les colonnes, on place en position $(1,1)$ le coefficient de M de sthasme minimum : on a alors $\phi(m_{11}) \leq \phi(m_{ij})$.

Étape 2 –

Pour chaque m_{i1} ou m_{1i}, on écrit la division euclidienne par m_{11} :

$$m_{i1} = m_{11}q + r, \qquad \phi(r) < \phi(m_{11})$$

On soustrait alors q fois la première ligne à la i^{e}. On obtient ainsi r à la place de m_{i1}.

Étape 3 –

On suppose que m_{11} est le seul coefficient non nul sur les premieres ligne et colonne. S'il reste un coefficient m_{ij} de M qui n'est pas divisible par m_{11}, on ajoute la i^{e} ligne à la première pour obtenir m_{ij} en position $(1,j)$.

L'algorithme fonctionne alors comme suit : si $M = 0$, on obtient immédiatement le résultat, sinon on effectue l'étape 1, puis l'étape 2. Si tous les restes des divisions euclidiennes sont nuls, on peut passer à l'étape 3. Sinon, on recommence l'étape 1. Quand (enfin) tous les restes sont nuls, on peut passer à l'étape 3. Si m_{11} divise chaque coefficient de M, on s'arrête, sinon on retourne à l'étape 2 qui produira un élément de plus petit sthasme que m_{11} et on effectuera de nouveau l'étape 1.

Il reste à voir que l'algorithme ne boucle pas. À chaque retour en arrière, on passe par l'étape 1 et un élément de plus petit sthasme que le précédent m_{11} est trouvé. Il n'y aura donc qu'un nombre fini de retours en arrière, borné par le sthasme du coefficient $(1,1)$ initial.

On a donc obtenu une décomposition de la forme :

$$M = P \left(\begin{array}{c|c} d_1 & \\ \hline & M' \end{array} \right) Q$$

où P et Q sont inversibles dans $\mathcal{M}_n(A)$ et d_1 divise chaque coefficient de M'. D'après la construction, d_1 est le pgcd des coefficients de M. Il ne reste plus qu'à itérer le procédé pour obtenir la décomposition souhaitée. ■

Exercice 4 – Soit $M \in \mathcal{M}_n(A)$ et K le corps des fractions de A. Montrer que $M \in \mathrm{GL}_n(A)$ si et seulement si $M \in \mathrm{GL}_n(K)$ et $\det M \in A^\times$.

Détaillons sur un exemple la méthode décrite dans la démonstration précédente :

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \xrightarrow{L_2 \leftarrow L_2 - 2L_1} \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix} \xrightarrow{C_2 \leftarrow C_2 - 2C_1} \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix}$$

Si on pose

$$Q = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad P = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

on a

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} = P^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix} Q^{-1}$$

Avant d'énoncer le théorème de décomposition des modules de type fini sur un anneau euclidien, on va démontrer un lemme utile pour la suite.

Lemme 3 – *Soient A un anneau noethérien. A^n est un $A-$module de type fini et si W est un sous-module de A^n, alors W est de type fini.*

Démonstration – Montrons le résultat par récurrence. C'est connu pour $n = 1$, car un sous-module de A est un idéal de A, noethérien par hypothèse. Si $n > 1$, soit la projection

$$\pi : \begin{array}{ccc} A^n & \longrightarrow & A^{n-1} \\ (a_1, \ldots, a_n) & \longmapsto & (a_1, \ldots, a_{n-1}) \end{array}$$

Si W est un sous-module de A^n, on pose $\psi = \pi|_W$. Par hypothèse de récurrence, l'image de ψ est de type fini. De plus, le noyau de ψ est un sous-module de $\mathrm{Ker}\pi \simeq A$, donc est de type fini. Vu l'isomorphisme

$$\frac{W}{\mathrm{Ker}\psi} \simeq \mathrm{Im}\psi$$

W est aussi de type fini. ■

Théorème 5 (Structure des modules de type fini sur un anneau euclidien) – *Soit A un anneau euclidien et V un $A-$module de type fini. Alors il existe $d_1, \ldots, d_r \in A$ et $s \in \mathbb{N}$ tels que $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$ et*

$$V \simeq \frac{A}{(d_1)} \times \cdots \times \frac{A}{(d_r)} \times A^s$$

De plus la suite $(d_1, \ldots, d_r)$ est unique à des inversibles près ; elle est appelée suite des facteurs invariants de V.

Démonstration – V est de type fini, soit $(e_1, \ldots, e_m)$ un système de générateurs de V. Le morphisme

$$f : \left| \begin{array}{ccc} A^m & \longrightarrow & V \\ (\alpha_1, \ldots, \alpha_m) & \longmapsto & \alpha_1 e_1 + \cdots + \alpha_m e_m \end{array} \right.$$

est surjectif. Soit $W = \mathrm{Ker}f$, V est isomorphe au quotient A^m/W.

D'après le lemme 3, W est de type fini. Soit $(f_1, \ldots, f_n)$ un système de générateurs de W. On obtient, comme plus haut, un morphisme surjectif $g : A^n \to W$. En composant g avec l'inclusion de W dans A^m, on construit un morphisme

$$\varphi : A^n \to A^m$$

Soit M la matrice de représentation de φ. Par construction, W est l'image de φ, c'est-à-dire MA^n. Donc V est isomorphe à A^m/MA^n.

Or, d'après la proposition 4, il existe des matrices inversibles P et Q et D diagonale telles que $M = PDQ$. On écrit

$$D = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_s & \\ & & & 0 \end{pmatrix} \qquad \text{avec } d_1 \mid \cdots \mid d_s$$

On remarque qu'on peut omettre les colonnes de 0. On déduit alors l'isomorphisme suivant

$$V \simeq \frac{A^m}{d_1 A \times \cdots \times d_r A} \simeq \frac{A}{(d_1)} \times \cdots \times \frac{A}{(d_r)} \times A^s$$

avec $r = m - s$, ce qui conclut la démonstration de l'existence.

On admet l'unicité des facteurs invariants. ■

Remarque – *Le théorème* 5 *est encore vrai si* A *est seulement principal.*

3. Application au théorème des invariants de similitude

On va maintenant appliquer le théorème 5 dans le cas où $A = \mathbb{K}[X]$ qui est un anneau euclidien, et $V = E$, muni de la structure de $\mathbb{K}[X]-$module décrite au paragraphe IV 1. Le théorème de structure s'applique puisque E est de type fini car de dimension finie comme $\mathbb{K}-$espace vectoriel. On obtient donc

$$E \simeq \frac{\mathbb{K}[X]}{(P_1)} \times \cdots \times \frac{\mathbb{K}[X]}{(P_r)} \times (\mathbb{K}[X])^s$$

Il est immédiat que $s = 0$ puisque E de dimension finie en tant qu'espace vectoriel sur $\mathbb{K}$ (la structure de $\mathbb{K}[X]-$module contient celle de $\mathbb{K}-$espace-vectoriel). On note alors φ l'isomorphisme de $\mathbb{K}[X]-$modules

$$\varphi : \frac{\mathbb{K}[X]}{(P_1)} \times \cdots \times \frac{\mathbb{K}[X]}{(P_r)} \xrightarrow{\simeq} E$$

Posons alors, pour $i = 1, \ldots, r$,

$$F_i = \varphi\left(\{0\} \times \cdots \times \frac{\mathbb{K}[X]}{(P_i)} \times \cdots \times \{0\}\right)$$

F_i est un $\mathbb{K}[X]$-sous-module de E, donc est stable par u. De plus, on a l'isomorphisme de $\mathbb{K}[X]$-modules :

$$F_i \simeq \frac{\mathbb{K}[X]}{(P_i)} \tag{1}$$

ce qui prouve que F_i est u-monogène. Il existe donc $x_i \in F_i$ tel que $F_i = \mathbb{K}[u]x_i$.

L'application $\mathbb{K}[X]$-linéaire

$$\begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & F_i \\ P & \longmapsto & P(u)(x_i) \end{array}$$

est surjective, de noyau $(Q_{u|_{F_i}})$. On obtient donc l'isomorphisme de $\mathbb{K}[X]$-modules

$$F_i \simeq \frac{\mathbb{K}[X]}{(Q_{u|_{F_i}})} \tag{2}$$

Les polynômes P_i et $Q_{u|_{F_i}}$ étant unitaires, on déduit de (1) et (2) qu'ils sont égaux (voir le lemme 4 ci-dessous) .

En conclusion, on a trouvé des sous-espaces F_i u-monogènes, tels que $E = \overset{r}{\underset{i=1}{\oplus}} F_i$ et $P_i = Q_{u|_{F_i}}$ et $P_i \,|\, P_{i+1}$.

On a donc démontré l'existence dans le théorème 1. L'unicité de la suite (P_i) provient de l'unicité dans le théorème 5. On vient de prouver le théorème des invariants de similitude par un autre biais plus complexe. Cependant la proposition 4, qui en est le moteur, conduit à un calcul effectif des invariants de similitude d'un endomorphisme donné.

Lemme 4 – *Soient P et Q deux polynômes unitaires tels qu'il existe un isomorphisme de $\mathbb{K}[X]$-modules*

$$\Phi \,:\, \frac{\mathbb{K}[X]}{(P)} \simeq \frac{\mathbb{K}[X]}{(Q)}.$$

Alors $P = Q$.

Démonstration – Notons $T = \Phi^{-1}(1)$. Alors $PT = 0$ dans $\frac{\mathbb{K}[X]}{(P)}$ et, puisque Φ est $\mathbb{K}[X]$-linéaire,

$$\Phi(PT) = P\,\Phi(T) = P.$$

On en déduit que $P = 0$ dans $\frac{\mathbb{K}[X]}{(Q)}$, si bien que $Q \,|\, P$. En inversant les rôles, on montre que $P \,|\, Q$ et donc $P = Q$, vu que les deux polynômes sont unitaires. ■

Remarquons que la $\mathbb{K}[X]$-linéarité est essentielle : si Φ est seulement un isomorphisme d'anneaux (ou de $\mathbb{K}$-espaces vectoriels), le résultat n'est plus valable :

$$\frac{\mathbb{K}[X]}{(X)} \simeq \frac{\mathbb{K}[X]}{(X-1)} \simeq \mathbb{K} \quad \text{comme anneaux ou } \mathbb{K}\text{-espaces vectoriels.}$$

V. Calcul pratique des invariants de similitude

Le but de ce paragraphe est de démontrer le résultat suivant :

Théorème 6 – *Soit M la matrice de u dans une base de E. Les invariants de similitude de u sont les facteurs invariants différents de 1 de la matrice $M - XI \in \mathcal{M}_n(\mathbb{K}[X])$.*

Démonstration – D'après le théorème 2, la matrice M est semblable à

$$\mathcal{C} = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}$$

Donc $M - XI$ et $\mathcal{C} - XI$ ont mêmes facteurs invariants.

Montrons maintenant que $C(P) - XI$ est équivalente à la matrice

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ 0 & & P \end{pmatrix}$$

par opérations élémentaires sur les lignes et les colonnes :

$$\begin{pmatrix} -X & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & -X & -a_{n-2} \\ & & 1 & -a_{n-1}-X \end{pmatrix} \xrightarrow[+\cdots X^{n-1}L_n]{L_1 \leftarrow L_1 + XL_2} \begin{pmatrix} 0 & \dots & 0 & -P \\ 1 & -X & & \vdots \\ & \ddots & -X & -a_{n-2} \\ & & 1 & -a_{n-1}-X \end{pmatrix}$$

On supprime ensuite les $-X$ de la diagonale par $C_2 \leftarrow C_2 + XC_1, \dots C_n \leftarrow C_n + XC_{n-1}$; on obtient alors

$$\begin{pmatrix} 0 & \dots & 0 & -P \\ 1 & \ddots & & \vdots \\ & \ddots & & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix} \xrightarrow[+\cdots a_{n-1}C_{n-1}]{C_n \leftarrow a_1C_1 + \cdots} \begin{pmatrix} 0 & \dots & 0 & -P \\ 1 & \ddots & & \vdots \\ & \ddots & & 0 \\ & & 1 & 0 \end{pmatrix}$$

Il ne reste plus alors qu'à effectuer une permutation sur les lignes et de multiplier la dernière colonne par -1 pour obtenir le résultat voulu.
On en déduit alors que $\mathcal{C} - XI$ est équivalente à

$$\begin{pmatrix} P_1 & & & & & \\ & \ddots & & & & \\ & & P_r & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

Il s'ensuit que les facteurs invariants différents de 1 de $M - XI$ sont $P_1, \dots, P_r$. ■

Exemple 1 – On veut déterminer les invariants de similitude de la matrice

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

Pour cela, on va effectuer des opérations élémentaires sur la matrice $A - XI$:

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

$C_1 \longleftrightarrow C_2$

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

$C_2 \longleftarrow C_2 - (1-X)C_1$

$$\begin{pmatrix} 1 & 0 & 0 \\ 1-X & -2+2X-X^2 & 1 \\ -2 & 4-2X & -2-X \end{pmatrix}$$

$L_2 \longleftarrow L_2 - (1-X)L_1 \quad$ et $\quad L_3 \longleftarrow L_3 + 2L_1$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2+2X-X^2 & 1 \\ 0 & 4-2X & -2-X \end{pmatrix}$$

$C_3 \longleftrightarrow C_2$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2+2X-X^2 \\ 0 & -2-X & 4-2X \end{pmatrix}$$

$L_3 \longleftarrow -L_3 - (2+X)L_2$

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

$C_3 \longleftarrow C_3 - (-2+2X-X^2)C_2$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3 \end{pmatrix}$$

La matrice A possède donc un seul invariant de similitude, qui est son polynôme minimal et caractéristique : elle est nilpotente et cyclique ; sa réduite de Jordan est

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

Exemple 2 – Pour la matrice

$$B = \begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix}$$

Ici encore on va travailler sur la matrice $B - XI$:

$$\begin{pmatrix} 3-X & 2 & -5 \\ 2 & 6-X & -10 \\ 1 & 2 & -3-X \end{pmatrix}$$

$L_1 \longleftrightarrow L_3$

$$\begin{pmatrix} 1 & 2 & -3-X \\ 2 & 6-X & -10 \\ 3-X & 2 & -5 \end{pmatrix}$$

$L_2 \longleftarrow L_2 - 2L_1 \quad \text{et} \quad L_3 \longleftarrow L_3 - (3-X)L_1$

$$\begin{pmatrix} 1 & 2 & -3-X \\ 0 & 2-X & -4+2X \\ 0 & -4+2X & 4-X^2 \end{pmatrix}$$

$C_2 \longleftarrow C_2 - 2C_1 \quad \text{et} \quad C_3 \longleftarrow C_3 - (-3-X)C_1$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2-X & -4+2X \\ 0 & -4+2X & 4-X^2 \end{pmatrix}$$

$L_3 \longleftarrow L_3 + 2L_2$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2-X & -4+2X \\ 0 & 0 & -(X-2)^2 \end{pmatrix}$$

$C_3 \longleftarrow -C_3 - 2L_2 \quad \text{et} \quad L_2 \longleftarrow C_3 - (-3-X)C_1 - L_2$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$$

La réduite de Jordan de la matrice B est donc

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$