Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

A. Ducros

Quelques compléments concernant les invariants de similitude

Antoine Ducros
Préparation à l'agrégation de mathématiques

17 février 2003

Introduction

Ce texte comprend deux parties. La première vise à expliquer comment calculer *en pratique* les invariants de similitude d'un endomorphisme donné par sa matrice. On commence par faire quelques rappels théoriques, sans donner de démonstration, (elles figurent pour l'essentiel par exemple dans le poly "modules de type fini sur un anneau principal" sur le site), puis l'on donne un algorithme et un exemple sur lequel on le voit fonctionner. Notez que l'algorithme en question, qui concerne en fait les matrices sur un anneau euclidien, est très classique. Il figure par exemple dans le livre *Algèbre Commutative* de Goblot, page 31, à peu près sous la même forme qu'ici ; la condition que Goblot impose au stathme (si y divise x et si $\phi(y) = \phi(x)$ alors x et y sont associés) est superflue. Vous le trouverez également au début de la preuve du théorème 3.8 dans *Basic Algebra I* de Jacobson (page 182).

La deuxième partie vise à vous montrer comment utiliser le point de vue "A-modules" pour traiter deux problèmes d'algèbre linéaire, l'étude du commutant d'un endomorphisme et celle des endomorphismes semi-simples. Ces deux points peuvent bien sûr être abordés de manière plus classique, c'est-à-dire sans parler de modules sur un anneau principal ; c'est ce que fait par exemple Gourdon dans son ouvrage *Algèbre*, p. 179 et p. 282 pour le commutant, p. 220 pour les endomorphismes semi-simples.

Vous êtes bien évidemment libres de choisir le point de vue qui vous convient le mieux. A mon sens celui des A-modules présente deux avantages (mais l'inconvénient de demander un investissement théorique plus important) :

- il permet de dégager réellement ce qui sert dans les démonstrations, en enlevant les hypothèses "parasites" ; ainsi la preuve de Gourdon page 220 utilise essentiellement la bilinéarité de $(P, x) \mapsto P(f)(x)$ et l'identité de Bezout, c'est-à-dire en clair le fait que ...E est un module sur l'anneau principal $k[X]$, et rien d'autre !
- il permet d'alléger considérablement les notations en évitant les écritures du type $(P(f)(Q(f)(x))$ (récurrentes dans la preuve de Gourdon) qui peuvent vite conduire au mieux à ne plus rien voir, au pire à dire des bêtises...

Il faut bien réaliser que dans nombre de cas les preuves des résultats énoncés dans le langage des A-modules sont *exactement les mêmes*, aux notations près, que celles des théorèmes d'algèbre linéaire correspondants ; aucune complication ne vient se greffer. Vous

pourrez par exemple vous convaincre que ce qu'écrit Gourdon dans son livre à propos du commutant page 282 est pratiquement la même chose que la preuve de $i) \Rightarrow ii)$ de la proposition 1 du présent texte. Et sa démonstration de la page 220 est proche de celle des lemmes 1, 2, 3 et 4 ci-dessous.

A vous de voir ce que vous préférez !

1 Exemples de calcul des invariants de similitude

Dans toute la suite, A est un anneau principal.

Quelques rappels

Rappelons quelques résultats vus en cours : si M est un A-module libre de rang fini m et si N est un sous-module de M alors il existe une base $(e_1, \dots, e_m)$ de M dite *adaptée à* N et une famille $\delta_1, \dots, \delta_n$ de scalaires telle que $\delta_1 | \delta_2 | \dots | \delta_n$ et telle que $(\delta_1 e_1, \dots, \delta_n e_n)$ soit une base de N. Les δ_i sont uniques à multiplication par un inversible près. Notons que les facteurs invariants du quotient M/N sont les δ_i *non inversibles* auxquels il faut rajouter en fin de liste $m - n$ termes nuls.

Soit ϕ une application A-linéaire définie entre deux modules libres L et M de rangs finis respectivement notés l et m et soit N son image. Soit $(e_1, \dots, e_m)$ une base de M adaptée à N et $\delta_1, \dots, \delta_n$ la famille de scalaires correspondants. Si l'on se donne pour tout i compris entre 1 et n un antécédent f_i de $\delta_i e_i$ alors la famille des f_i est libre et

$$L = Af_1 \oplus \dots \oplus Af_n \oplus \text{Ker } \phi.$$

Comme Ker ϕ est un sous-module de L il est libre et si l'on en choisit une base quelconque la réunion des f_i et de cette base constitue une base $\mathcal{B}$ de L. La matrice de ϕ dans les bases $\mathcal{B}$ et (e_i) (qui est de taille $m \times l$) se décrit alors simplement : pour tout i compris entre 1 et n son terme d'indice (i, i) est égal à δ_i et ses autres termes sont nuls. Notons $D_{m,l}(\delta_1, \dots, \delta_n)$ cette matrice.

On vient incidemment de démontrer que toute matrice B de taille $m \times l$ à coefficients dans A est équivalente à $D_{m,l}(\delta_1, \dots, \delta_n)$ pour une certaine famille (δ_i) de scalaires non nuls tels que $\delta_1 | \delta_2 | \dots | \delta_n$. Cette propriété caractérise la famille des δ_i *à multiplication par des éléments inversibles près*. Considérons en effet l'application linéaire $\phi : A^l \to A^m$ dont la matrice dans les bases canoniques de ces deux modules est B. Il existe alors une base $(f_1, \dots, f_l)$ de A^l et une base $(e_1, \dots, e_m)$ de A^m telle que la matrice de ϕ dans ces deux bases soit précisément $D_{m,l}(\delta_1, \dots, \delta_n)$. On vérifie immédiatement que $(\delta_1 e_1, \dots, \delta_n e_n)$ est une base de l'image de ϕ, et c'est le théorème de la base adaptée qui fournit l'unicité requise.

Celle-ci peut aussi être déduite du résultat suivant : si B est une matrice de taille $m \times l$ équivalente à $D_{m,l}(\delta_1, \dots, \delta_n)$ pour une certaine famille (δ_i) de scalaires non nuls tels que $\delta_1 | \delta_2 | \dots | \delta_n$ alors pour tout entier k le produit $\delta_1 \dots \delta_k$ est le PGCD des mineurs d'ordre k de B, avec la convention que $\delta_k = 0$ si $k > r$ (notons que "le" PGCD d'une famille d'éléments n'est bien déterminé qu'à un inversible près).

Cette formule fournit un moyen théorique d'obtention des δ_i à partir de B. Toutefois cela demande un grand nombre d'opérations (songez que pour tout k inférieur à m et à l il y a $C_l^k \times C_m^k$ mineurs d'ordre k à calculer et qu'il reste ensuite le PGCD à déterminer...).

Un algorithme simple dans le cas d'un anneau euclidien

Indiquons, dans le cas où A est égal à $\mathbb{Z}$ ou à $k[X]$, ou plus généralement dans le cas où A est euclidien, un algorithme plus rapide : notons $\delta : A - \{0\} \to \mathbb{N}$ un stathme euclidien (par exemple la valeur absolue si $A = \mathbb{Z}$, le degré si $A = k[X]$). Pour toute matrice M non nulle à coefficients dans A notons $\delta(M)$ la valeur minimale de δ sur les coefficients non nuls de M.

Dans ce qui suit on appellera "opération élémentaire" sur une matrice l'une des opérations suivantes : échange de lignes, échange de colonnes, ajout à une ligne d'une combinaison linéaire *d'autres lignes*, ajout à une colonne d'une combinaison linéaire *d'autres colonnes*. On vérifie (petit exercice, faites-le !) que chacune de ces opérations *transforme une matrice en une matrice équivalente*. Le but est de réaliser un nombre fini de telles opérations pour obtenir une matrice sous la forme diagonale souhaitée.

On part donc d'une matrice $M = (m_{i,j})$. Si elle est nulle c'est terminé sinon l'on procède ainsi :

Etape 1 : Par opérations élémentaires on se ramène au cas où $\delta(M) = \delta(m_{1,1})$.

Etape 2 : Si il existe sur la première ligne un élément $m_{1,k}$ non multiple de $m_{1,1}$ on peut, par opérations élémentaires, le remplacer par le reste r de sa division par $m_{1,1}$, lequel reste vérifie $\delta(r) < \delta(m_{1,1})$. On a donc fait chuter strictement $\delta(M)$. On refait alors les étapes 1 et 2. Comme $\delta(M)$ ne peut décroître strictement indéfiniment il arrive un moment où *tous les termes de la première ligne sont multiples de* $m_{1,1}$. On applique le même procédé à la première colonne, et l'on obtient finalement une matrice dont *tous les termes de la première ligne et de la première colonne sont multiples de* $m_{1,1}$. Par opérations élémentaires on obtient une matrice dont tous les coefficents $m_{k,1}$ et $m_{1,k}$ sont nuls pour $k \neq 1$.

Etape 3 : On a ainsi une matrice formée de deux blocs, un bloc 1×1 (le coefficient $m_{1,1}$, qui vérifie $\delta(m_{1,1}) = \delta(M)$) et un bloc $(m-1) \times (l-1)$ que l'on note N. Si l'un des coefficients de N n'est pas multiple de $m_{1,1}$ on additionne la ligne de ce coefficient à la première, puis par opérations élémentaires on remplace l'élément en question (sur la première ligne) par le reste r de sa division euclidienne par $m_{1,1}$. Comme $\delta(r) < \delta(m_{1,1})$ on a fait chuter strictement $\delta(M)$. On refait alors les étapes 1, 2, et 3. Comme $\delta(M)$ ne peut décroître strictement indéfiniment il arrive un moment où tous les coefficients du bloc N sont multiples de $m_{1,1}$. On réapplique alors l'algorithme à N.

Le cas d'un sous-module donné par une famille génératrice

Soit M un A-module libre de rang fini m et soit N un sous-module de M. Soit $C_1, \ldots, C_l$ une famille *génératrice* de N. Soit ϕ l'application linéaire de A^l vers M qui envoie (a_j) sur $\sum a_j C_j$. Comme l'image de ϕ est N il découle de ce qui précède qu'il suffit, pour déterminer la famille de scalaires associée à N par le théorème de la base adaptée (d'où l'on pourra tirer les facteurs invariants du quotient M/N), de choisir une base de A^l, une base de M, d'écrire la matrice de ϕ dans ces deux bases et de lui appliquer l'algorithme vu ci-dessus (si A est euclidien) ou la formule avec le PGCD des mineurs. Notons que si l'on munit M (resp. A^l) d'une base quelconque $(e_1, \ldots, e_m)$ (resp. de sa base canonique) la matrice correspondante de ϕ est simplement la matrice dont les colonnes correspondent aux C_j écrits dans la base $(e_1, \ldots, e_m)$.

Indiquons maintenant comment appliquer cette remarque à la détermination pratique des invariants de similitude d'un endomorphisme. Soit k un corps et soit E un k-espace vectoriel de dimension finie. Donnons-nous un endomorphisme u de E, que l'on munit de la structure de $k[X]$-module correspondante. Soit $(e_1, \dots, e_n)$ une base de E (comme k-espace vectoriel) et $B = (b_{i,j})$ la matrice de u dans cette base. L'application $k[X]$-linéaire de $(k[X])^n$ dans E qui envoie $(P_1, \dots, P_n)$ sur $\sum P_i.e_i$ est surjective (puisqu'elle l'est déjà si l'on se restreint à des P_i constants, la famille des e_i étant en particulier génératrice sur k) ; si l'on appelle N son noyau le $k[X]$-module E est donc isomorphe à $(k[X])^n/N$.

On a vu en cours que N admettait pour base la famille des V_j où pour tout j l'on désigne par V_j le vecteur dont la famille des coordonnées dans la base canonique de $(k[X])^n$ est $(b_{i,j} - \delta_{i,j}X)_i$. Autrement dit, la matrice dont les colonnes sont les V_j exprimés dans la base canonique de $(k[X])^n$ est la matrice $B - X\mathrm{I}_n$.

L'algorithme décrit plus haut permet de mettre cette matrice sous la forme $D_{n,n}(P_1, \dots, P_r)$ pour une certaine famille P_i de polynômes non nuls tels que $P_1|P_2|\dots|P_r$. Les facteurs invariants de E, autrement dit les invariants de similitude de u, sont alors donnés par les P_i *non inversibles* ; comme E est de dimension finie on sait qu'il n'y aura pas de termes nuls à rajouter à la liste (ce qui montre qu'en fait $r = n$).

Donnons maintenant un exemple d'un tel calcul. Partons d'un endomorphisme dont la matrice (dans une base convenable) est égale à

$$\begin{bmatrix} 2 & 4 & -1 \\ 2 & 9 & -2 \\ 3 & 12 & -2 \end{bmatrix}.$$

On retranche à cette matrice XI_3 et l'on trouve donc

$$\begin{bmatrix} 2-X & 4 & -1 \\ 2 & 9-X & -2 \\ 3 & 12 & -2-X \end{bmatrix}.$$

Un échange de la première et de la troisème colonne donne

$$\begin{bmatrix} -1 & 4 & 2-X \\ -2 & 9-X & 2 \\ -2-X & 12 & 3 \end{bmatrix}.$$

On remplace C_2 par $C_2 + 4C_1$ et C_3 par $C_3 + (2-X)C_1$ ce qui donne

$$\begin{bmatrix} -1 & 0 & 0 \\ -2 & 1-X & 2X-2 \\ -2-X & 4-4X & X^2-1 \end{bmatrix}.$$

On remplace L_2 par $L_2 - 2L_1$ puis L_3 par $L_3 - (2-X)L_1$ et l'on obtient :

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1-X & 2X-2 \\ 0 & 4-4X & X^2-1 \end{bmatrix}.$$

On remplace C_3 par $C_3 - 2C_2$, le résultat est

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1-X & 0 \\ 0 & 4-4X & X^2-8X+7 \end{bmatrix}.$$

La dernière opération consiste à remplacer L_3 par $L_3 - 4L_2$, ce qui donne

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1-X & 0 \\ 0 & 0 & X^2-8X+7 \end{bmatrix}.$$

Comme $1 - X$ divise $X^2 - 8X + 7$ c'est terminé. Les invariants de similitude de l'endomorphisme étudié sont donc $X - 1$ et $X^2 - 8X + 7$.

2 Quelques applications des modules de type finis sur un anneau principal à l'algèbre linéaire

Commutant d'un endomorphisme

Proposition 1. *Soit A un anneau principal et M un A-module de type fini. Ecrivons*

$$M \simeq A/d_1 \oplus \ldots \oplus A/d_r$$

où les d_i sont des scalaires non inversibles tels que $d_1|d_2|\ldots|d_r$ (ce sont donc les facteurs invariants de M). Les propositions suivantes sont équivalentes :

i) Tout endomorphisme du A-module M est la multiplication par un scalaire.

ii) L'entier r est égal à 0 ou 1, autrement dit M est nul ou bien n'a qu'un facteur invariant.

Démonstration. Supposons que $i)$ est vraie et considérons la projection de M sur les $r-1$ premiers facteurs de sa décomposition ci-dessus ; c'est un endomorphisme de M, et donc comme $i)$ est supposée vraie c'est la multiplication par un scalaire α. Comme cet endomorphisme restreint au dernier facteur A/d_r est trivial α est nul modulo d_r. Les d_i divisent tous d_r, et donc α est nul modulo tous les d_i ; la multiplication par α est donc l'endomorphisme nul de M, ce qui montre que la somme des $r-1$ premiers facteurs est nulle : en conséquence ou bien M est nul ou bien $r = 1$ et M est alors isomorphe à A/d_1.

Supposons que $ii)$ est vraie. Dans ce cas M est de la forme A/d pour un certain d appartenant à A (éventuellement inversible si M est nul). Soit ϕ un endomorphisme de M. Soit α appartenant à A tel que $\phi(\overline{1}) = \overline{\alpha}$. Considérons un élément x de M. On peut l'écrire $\overline{u}$ pour un certain u dans A. On a alors

$$\phi(x) = \phi(\overline{u}) = \phi(u.\overline{1}) = u.\phi(\overline{1}) = u\overline{\alpha} = \overline{u\alpha} = \alpha\overline{u} = \alpha x$$

et donc ϕ est la multiplication par α. □.

On en déduit la proposition suivante en algèbre linéaire :

Proposition 2. *Soit k un corps, soit E un k-espace vectoriel de dimension finie et soit u un endomorphisme de E. Les proposition suivantes sont équivalentes :*

i) Tout endomorphisme commutant avec u est un polynôme en u.

ii) E est nul ou bien l'endomorphisme u possède un et un seul invariant de similitude.

iii) Le polynôme minimal de u est égal à son polynôme caractéristique.

iv) *Il existe une base de E dans laquelle la matrice de u est une matrice compagnon.*

Démonstration. L'équivalence de *ii*), *iii*) et *iv*) résulte directement du cours sur les modules de type fini sur un anneau principal. Quant à celle de *i*) et *ii*) elle est une simple traduction de la proposition précédente, compte-tenu du fait (vu en cours) que les endomorphismes du $k[X]$-module E sont exactement les applications k-linéaires commutant avec u, et que parmi ces endomorphismes les multiplications par les scalaires (donc par les éléments de $k[X]$) sont exactement les polynômes en u (c'est une conséquence immédiate de la définition de la structure de $k[X]$-module induite sur E par u). □

Remarque. Dans le cas où l'endomorphisme u est supposé diagonalisable on peut prouver le résultat directement, et de manière élémentaire. Voici comment : dire que le polynôme minimal de u est égal à son polynôme caractéristique équivaut alors à dire que les valeurs propres de u sont deux à deux distinctes. Plaçons-nous sous cette hypothèse et montrons que tout endomorphisme commutant avec u est un polynôme en u. Soit $(e_1, \dots, e_n)$ une base de E formée de vecteurs propres de u ; pour tout i on note λ_i la valeur propre correspondant à e_i. Les λ_i sont par hypothèse deux à deux distincts. Pour tout i le sous-espace propre associé à λ_i est donc exactement ke_i. Soit v un endomorphisme commutant avec u. On voit facilement que tout sous-espace propre de u est stable par v. En particulier il existe pour tout i un scalaire μ_i tel que $v(e_i) = \mu_i e_i$. Soit P un polynôme tel que $P(\lambda_i) = \mu_i$ pour tout i (les λ_i étant deux à deux distincts l'existence d'un tel polynôme est assuré par interpolation de Lagrange). Alors $P(u) = v$.

Supposons maintenant que u possède un sous-espace propre F de dimension au moins 2. Comme u est par ailleurs supposé diagonalisable F possède un supplémentaire G dans E stable par u. Soit ϕ un endomorphisme de F qui n'est pas une homothétie (un tel endomorphisme existe car la dimension de F est au moins 2). L'endomorphisme de E dont la restriction à F est ϕ et dont la restriction à G est nulle commute avec u. Or ce n'est pas un polynôme en u car $u_{|F}$ est une homothétie, et donc tout polynôme en $u_{|F}$ en est encore une ; or par hypothèse ϕ n'est pas une homothétie, ce qui achève la démonstration. □

Remarque. Le lecteur à l'aise avec les A-modules et intéressé par ces questions pourra lire avec profit le paragraphe 3.11 de *Basic Algebra I* de Jacobson, consacré à l'étude des endomorphismes d'un A-module de type fini quelconque.

Endomorphismes semi-simples

D'une manière générale on dit qu'un module M sur un anneau (commutatif unitaire) A est *semi-simple* si tout sous-module de M possède un supplémentaire. On va étudier de plus près cette notion lorsque A est principal.

On suppose donc à partir de maintenant que A est un anneau principal.

Un élément m d'un A-module M sera dit *de torsion* s'il existe *a non nul* dans A tel que $am = 0$; on peut l'exprimer également en disant que *l'idéal annulateur de m*, c'est-à-dire

$$\{\alpha \in A \text{ tq } \alpha m = 0\}$$

est non nul. Les éléments de torsion de M forment un sous-module de M ; si *tous* les éléments de M sont de torsion on dit que M est de torsion.

Soit p un élément irréductible de A. On dit qu'un élément m d'un A-module M est *de torsion p-primaire* si son idéal annulateur est de la forme $p^n A$ pour un certain entier n. L'ensemble des éléments de torsion p-primaire d'un A-module M forme un sous-module de M que l'on notera M_p.

Lemme 1. *Soit M un A-module de torsion. Alors*

$$M = \bigoplus_p M_p$$

où p parcourt l'ensemble des éléments irréductibles de A. Si N est un sous-module de M alors

$$N = \bigoplus_p N \cap M_p.$$

Démonstration. Notons que la seconde assertion découle de la première puisqu'il résulte immédiatement des définitions que N est de torsion et que $N_p = N \cap M_p$ pour tout irréductible p.

Pour prouver la première assertion considérons un élément m de M. L'application linéaire ϕ de A vers M qui envoie a sur am a pour noyau l'idéal annulateur de m qui est non nul par hypothèse et qui est donc de la forme bA pour un certain b non nul. On peut donc écrire $b = \prod p_i^{n_i}$ où les p_i sont des irréductibles deux à deux disjoints. L'image de ϕ est isomorphe à A/b donc par le lemme chinois à $\bigoplus A/p_i^{n_i}$. Pour tout i le facteur $A/p_i^{n_i}$ est formé d'éléments de torsion p_i-primaires et m, qui appartient bien sûr à l'image de ϕ, est donc somme de tels éléments.

Supposons maitenant que l'on ait $\sum m_p = 0$ où m_p est un élément de M de torsion p-primaire pour tout p, les m_p étant presque tous nuls. Soit $\mathcal{P}$ un ensemble fini d'éléments irréductibles de A tels que m_p soit nul pour tout p en dehors de $\mathcal{P}$. Soit p_0 appartenant à $\mathcal{P}$. Par le lemme chinois il existe a appartenant à A tel que a soit congru à 1 modulo l'idéal annulateur de m_{p_0} et à 0 modulo l'idéal annulateur de m_p pour tout p élément de $\mathcal{P} - \{\surd\}$. En multipliant l'égalité $\sum m_p = 0$ par a l'on obtient $m_{p_0} = 0$, ce qui achève la preuve du lemme. □

Remarque. Si M est un A-module *de type fini* il est isomorphe à

$$A/d_1 \oplus \ldots \oplus A/d_r$$

pour une certaine famille $(d_1, \ldots, d_r)$ de scalaires non inversibles tels que $d_1 | d_2 | \ldots | d_r$. On voit immédiatement que M est de torsion si et seulement si les d_i sont tous non nuls. La décomposition en irréductibles de chaque d_i et le lemme chinois permettent (voir le cours) de réécrire M sous la forme

$$\bigoplus A/p_i^{n_i}$$

où les p_i sont irréductibles. Pour p fixé M_p est alors égal à

$$\bigoplus_{i \in I_p} A/p^{n_i}$$

où I_p désigne l'ensemble des i tels que $p_i = p$.

Lemme 2. *Soit M un A-module de torsion. Alors M est semi-simple si et seulement si M_p est semi-simple pour tout élément irréductible p de A.*

Démonstration. Supposons que M_p est semi-simple pour tout p et soit N un sous-module de M. On peut alors écrire $N = \bigoplus N \cap M_p$. Fixons p. Comme M_p est semi-simple il existe un supplémentaire N'_p de $N \cap M_p$ dans M_p. Il est alors immédiat que $\bigoplus N'_p$ est un supplémentaire de N dans M.

Réciproquement supposons M semi-simple. Soit p un irréductible de A et N un sous-module de M_p. Comme M est semi-simple N possède un supplémentaire N' dans M. Il est clair que $N \cap (N' \cap M_p)$ est nul. D'autre part soit m un élément de M_p. Alors comme $M = N \oplus N'$ on peut écrire $m = n + n'$ avec n dans N et n' dans N'. Comme m et n appartiennent à M_p il en va de même de n' et donc $M_p = N \oplus (N' \cap M_p)$, ce qui achève la preuve du lemme. □

Fixons maintenant un irréductible p de A. Soit M un module de type fini sur A dont tous les éléments sont de torsion p-primaire. Il s'écrit, d'après ce qui a été vu plus haut, sous la forme

$$\bigoplus A/p^{n_i}.$$

Lemme 3. *Avec les hypothèses et notations ci-dessus, le module M est semi-simple si et seulement si $n_i = 1$ pour tout i.*

Démonstration. Si $n_i = 1$ pour tout i alors M est somme directe de copies de A/p donc sa structure de A-module est en fait induite par une structure de A/p-espace vectoriel (A/p est en effet un corps) et les notions de sous-module et de sous-espace vectoriel de M coïncident. Or il est bien connu que tout sous-espace vectoriel d'un espace vectoriel donné admet un supplémentaire, et donc M est semi-simple.

Supposons que pour un certain j l'on ait $n_j > 1$. Notons N le sous-module

$$\bigoplus_{i \neq j} A/p^{n_i} \oplus pA/p^{n_j}$$

de M. Le quotient M/N est isomorphe à A/p. Si N possédait un supplémentaire dans M ce supplémentaire serait en conséquence isomorphe à A/p, donc formé d'éléments annulés par p. Or les éléments de M annulés par p appartiennent tous à N : en effet si m est un tel élément sa projection sur le facteur A/p^{n_j} est annulée par p, donc est la classe modulo p^{n_j} d'un multiple de $p^{n_j - 1}$. Comme n_j est supposé strictement supérieur à 1 tout multiple de $p^{n_j - 1}$ est multiple de p.

Finalement N n'a pas de supplémentaire dans M et M n'est pas semi-simple. □

Lemme 4. *Soit M un A-module de type fini et de torsion, et soit $d_1, \ldots, d_r$ ses facteurs invariants. Alors M est semi-simple si et seulement si les exposants des facteurs irréductibles dans la décomposition de d_r sont tous égaux à 1.*

Démonstration. D'après le lemme 2 le module M est semi-simple si et seulement si chacun des M_p l'est. Pour tout p le module M_p est de la forme

$$\bigoplus A/p^{n_i}$$

où les n_i sont les exposants de p apparaissant dans les différents d_i. Comme M_p est semi-simple si et seulement si les n_i sont tous égaux à 1 le module M est semi-simple si et seulement si les exposants de la décomposition en facteurs irréductibles de chacun des d_i sont égaux à 1. Comme d_r est multiple de tous les autres d_i il est nécessaire et suffisant, pour que la propriété voulue soit vérifiée, que les exposants des facteurs irréductibles dans la décomposition de d_r soient tous égaux à 1. □

On peut traduire ce dernier résultat dans le langage de l'algèbre linéaire :

Proposition. *Soit k un corps, soit E un k-espace vectoriel de dimension finie et soit u un endomorphisme de E. Les propriétés suivantes sont alors équivalentes :*

i) *Tout sous-espace de E stable par u possède un supplémentaire stable par u.*

ii) *Dans la décomposition en facteurs irréductibles du polynôme minimal de u tous les exposants sont égaux à 1.* □

Un endomorphisme u d'un espace vectoriel de dimension finie qui satisfait ces deux conditions équivalentes est dit *semi-simple*. Notons que si le polynôme caractéristique de u est scindé (ce qui force le polynôme minimal à l'être aussi) la condition *ii*) signifie exactement que le polynôme minimal de u est à *à racines simples*, donc que u est diagonalisable. On en déduit notamment que sur un corps algébriquement clos les notions d'*endomorphisme semi-simple* et d'*endomorphisme diagonalisable* coïncident.