Table des matières

1 Introduction

Dans un article paru 1955, *Faisceaux Algébriques Cohérents* ([5]), Jean-Pierre Serre écrivit : 'On ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libres' (ici $A = k[x_1, \ldots, x_n]$ et k est un corps commutatif).

Ce que Serre présentait alors plutôt comme un problème ouvert fut rapidement considéré comme la 'conjecture de Serre', à savoir :

'Soit k un corps commutatif et A l'anneau de polynômes $A = k[x_1, \ldots, x_n]$. Tout A-module projectif de type fini est libre.'

Certains résultats étaient déjà connus : par exemple, la conjecture est vérifiée lorsque le module projectif est de rang 1, ou lorsque $A = k[x_1]$ est l'anneau des polynômes à une seule variable.

De nombreux mathématiciens s'intéressèrent à ce problème. Ainsi, entre 1955 et 1976, année où il fut entièrement résolu par D.Quillen et A.Suslin (qui prouvèrent de façon indépendante que la conjecture était vérifiée pour tout $n \geq 1$ et tout corps commutatif k), plusieurs résultats intermédiaires furent démontrés (par exemple, le cas de deux variables par Seshradi en 1958).

Après avoir introduit les notions nécessaires et étudié les relations entre module projectif et module libre, nous nous intéresserons plus particulièrement au cas où le module projectif est de rang 1 et celui où le module est gradué (Cartan et Eilenberg, 1956).

Enfin, nous étudierons un résultat démontré par Ojanguren et Sridharan en 1971, à savoir que la conjecture de Serre a une réponse négative dans le cas où $n \geq 2$ et k est un corps gauche.

2 Préliminaires

2.1 Module (module de type fini, module libre)

Les définitions suivantes sont issues de [3].

Définition 1. Soit A un anneau. Un *A-module à gauche* M est un groupe additif abélien muni d'une opération de A sur M vérifiant pour tout $a, b \in A$ et tout $x, y \in M$

$$(a+b)x = ax + bx \qquad a(x+y) = ax + ay$$

Par définition d'une opération, on a $1x = x$. On vérifie de plus que $a(-x) = -(ax)$ et que $0x = 0$.

On définit de façon similaire un *A-module à droite*.

Définition 2. Soit M un A-module à gauche. Un $sous - A - module$ N de M est un sous-groupe additif de M vérifiant $AN \subset N$.

Définition 3. Soit M et M' deux A-modules. Un *morphisme de A-module* ou *A-homomorphisme* est un morphisme de groupes additifs

$$f:\ M \to M'$$

vérifiant pour tout $a \in A$ et $x \in M$

$$f(ax) = af(x)$$

Les définitions suivantes sont analogues à celles correspondant aux groupes abéliens, et seront par conséquent peu détaillées.

Définition 4. Un A-module M est dit *de type fini* s'il a un nombre fini de générateurs.

Définition 5. Un A-module L est dit *libre* s'il est nul ou s'il admet une base.

Afin de définir dans la partie suivante le produit tensoriel, il est nécessaire d'introduire au préalable la notion de *module libre engendré par un ensemble*.

Définition 6. Soit A un anneau et X un ensemble. On note $A^{(X)}$ l'ensemble des applications φ de X dans A à support fini, c'est-à-dire telles que $\varphi(x) = 0$ sauf pour un nombre fini de $x \in X$.

On munit $A^{(X)}$ d'une structure de A-module à gauche en définissant, pour $\varphi, \psi \in A^{(X)}$ et $a \in A$, $\varphi + \psi$ et $a\varphi$ par :

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x)$$
$$(a\varphi)(x) = a\varphi(x)$$

pour tout $x \in X$.

On note α l'application de X dans $A^{(X)}$ qui à $x \in X$ associe l'élément e_x tel que

$$e_x(x) = 1$$
$$e_x(y) = 0 \text{ si } x \neq y$$

Proposition 1. *Un élément φ de $A^{(X)}$ s'écrit de manière unique*

$$\varphi = \sum_{x \in X} a_x e_x$$

où $a_x \in A$ est nul sauf pour un nombre fini de $x \in X$.

Démonstration. Supposons que φ soit de la forme

$$\varphi = \sum_{x \in X} a_x e_x$$

Cela impose, pour tout $y \in X$, $\varphi(y) = a_y$.

On vérifie alors que l'on a bien

$$\varphi = \sum_{x \in X} \varphi(x) e_x$$

puisque pour tout $y \in X$

$$(\varphi - \sum_{x \in X} \varphi(x) e_x)(y) = \varphi(y) - \varphi(y) = 0$$

□

2.2 Produit tensoriel

La définition suivante est issue de [2].

Soit A un anneau commutatif, M et N deux ensembles non vides.

Posons

$$U = A^{(M \times N)}$$

le A-module libre engendré par l'ensemble $M \times N$. Soit V le sous-module de U engendré par les éléments de la forme

$$\begin{aligned}
&e_{(x_1+x_2,y)} - e_{(x_1,y)} - e_{(x_2,y)} \\
&e_{(x,y_1+y_2)} - e_{(x,y_1)} - e_{(x,y_2)} \\
&e_{(ax,y)} - ae_{(x,y)} \\
&e_{(x,ay)} - ae_{(x,y)}
\end{aligned}$$

où $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$ et $a \in A$.

Considérons maintenant le diagramme

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha} & U \\ & & \downarrow p \\ & & U/V \end{array}$$

où

$$\begin{aligned} \alpha : M \times N &\to A^{(M\times N)} \\ (x,y) &\mapsto e_{(x,y)} \end{aligned}$$

et $p : U \to U/V$ est la projection canonique.

Posons

$$M \otimes_A N = U/V$$

et

$$i_{(M,N)} = p \circ \alpha : M \times N \to M \otimes_A N$$

Pour $(x,y) \in M \times N$ on note

$$x \otimes y = i_{(M,N)}(x,y)$$

Définition 7. $M \otimes_A N$ est appelé le *produit tensoriel* de M et N.

Rappel : Un élément de $A^{(M\times N)}$ s'écrit de manière unique

$$\sum_{(x,y)\in M\times N} a_{(x,y)} e_{(x,y)}$$

où $a_{(x,y)} \in A$ est nul sauf pour un nombre fini de (x,y).

Un élément de $M \otimes_A N$ s'écrit (mais sans unicité)

$$\sum_{(x,y)\in M\times N} a_{(x,y)} x \otimes y$$

Par définition de $M \otimes_A N = A^{(M\times N)}/V$, on a pour tout $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$ et $a \in A$:

$$\begin{aligned} (x_1 + x_2) \otimes y &= x_1 \otimes y + x_2 \otimes y \\ x \otimes (y_1 + y_2) &= x \otimes y_1 + x \otimes y_2 \\ (ax) \otimes y = x \otimes (ay) &= a(x \otimes y) \end{aligned}$$

Signalons maintenant une propriété du produit tensoriel fréquemment utilisée.

Proposition 2. *Soit M un A-module. Pour tout $n \in \mathbb{N}$*

$$M \otimes_A A^n \cong M^n$$

Démonstration. Considérons les morphismes de modules

$$\begin{array}{cccc} \Phi : & M \otimes_A A^n & \longrightarrow & M^n \\ & m \otimes \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} & \longmapsto & \begin{pmatrix} m \otimes a_1 \\ \vdots \\ m \otimes a_n \end{pmatrix} \end{array}$$

et

$$\begin{array}{cccc} \Psi : & M^n & \longrightarrow & M \otimes_A A^n \\ & \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} & \longmapsto & m_1 \otimes \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + m_n \otimes \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \end{array}$$

On vérifie que

$$\begin{aligned} \Phi \circ \Psi &= id_{M^n} \\ \Psi \circ \Phi &= id_{M \otimes_A A^n} \end{aligned}$$

D'où le résultat. □

2.3 Rang d'un module de type fini

Soit A un anneau commutatif intègre, K son corps de fractions, et M un A-module de type fini. Alors il existe un sous-module libre L tel que

$$M = M_{\text{tor}} \oplus L$$

Définition 8. On appelle *rang de M* la dimension de ce sous module.

$$\text{rg}\, M := \dim_A L$$

Remarque : Ceci équivaut (dans le cas où la caractéristique de K est nulle, c'est-à-dire si $\mathbb{Q} \subset K$) à

$$\text{rg}\, M = \dim_K (K \otimes_A M)$$

En effet
$$K \otimes_A M = K \otimes_A M_{\text{tor}} \oplus K \otimes_A L$$

Or $K \otimes_A M_{\text{tor}} = 0$. En effet, si $m \in M_{\text{tor}}$, il existe $n \in \mathbb{N}$ tel que $nm = 0$. Mais alors pour tout $k \in K$

$$k \otimes m = \frac{k}{n} \otimes nm = 0$$

D'où
$$K \otimes_A M = K \otimes_A L$$

Or si L est libre, $L \cong A^n$ donc

$$K \otimes_A L \cong K \otimes_A A^n \cong K^n$$

d'après la **Proposition 2**. D'où finalement

$$\dim_K (K \otimes_A M) = \dim_K K^n = n = \dim_A L$$

2.4 Suite exacte scindée de modules

Définition 9. Soit $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ une suite exacte de A-modules (on a donc $Im\, f = ker\, g$, f injective et g surjective).

On dit que la suite est *scindée* s'il existe $\phi : M'' \to M$ homomorphisme tel que $g \circ \phi = id_{M''}$

Proposition 3. *Si la suite exacte* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *est scindée, on a*
$$M \cong M' \oplus M''$$

Démonstration. Soit $x \in M$.

Alors $x - \phi(g(x)) \in \ ker\, g$ d'où

$$M \ = \ ker\, g \ + \ Im\, \phi$$

Montrons que cette somme est directe :

Soit $x \in M$. Alors $x = y + z$ avec $y \in \ ker\ g$ et $z \in \ Im\ \phi$, ou encore $x = y + \phi(w)$ avec $w \in M''$.

En appliquant g on obtient alors $g(x) = g(y) + (g \circ \phi)(w) = w$.

w est donc déterminé de façon unique par x, $z = \phi(w)$ l'est alors également, et y par conséquent l'est aussi.

D'où finalement
$$M \ = \ ker\, g \ \oplus \ Im\, \phi$$

ou encore

$$M \;=\; Im\, f \;\oplus\; Im\, \phi$$

On sait que $g \circ \phi = id_{M''}$, donc ϕ est injective. D'où $Im\, \phi \cong M''$.
De même, f est injective, d'où $Im\, f \cong M'$.
Et, de là :

$$M \cong M' \oplus M''$$

□

2.5 Module projectif

Proposition 4. *Soit A un anneau et P un A-module. Les propositions suivantes sont équivalentes :*

(i) Pour tout homomorphisme $f : P \to M''$ et tout épimorphisme $g : M \twoheadrightarrow M''$, il existe un homomorphisme $h : P \to M$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccc} M & \overset{g}{\twoheadrightarrow} & M'' & \to & 0 \\ h & \nwarrow & \uparrow f & & \\ & & P & & \end{array}$$

(ii) Toute suite exacte de A-modules

$$0 \to M' \to M'' \to P \to 0$$

est scindée.

(iii) Il existe un module M et un module libre L tels que

$$P \oplus M = L$$

Définition 10. Un A-module P vérifiant l'une des propositions précédentes est appelé *module projectif.*

Démonstration de la proposition. $(i) \Rightarrow (ii)$ Soit

$$0 \to M' \to M'' \xrightarrow{g} P \to 0$$

une suite exacte. D'après (i), il existe $\varphi : P \to M''$ tel que le diagramme

$$\begin{array}{cccc} M'' & \overset{g}{\twoheadrightarrow} & \mathrm{P} & \\ \varphi & \nwarrow & \uparrow & id_P \\ & & \mathrm{P} & \end{array}$$

commute, c'est-à-dire tel que $g \circ \varphi = id_P$. La suite est donc scindée.

$(ii) \Rightarrow (iii)$ Représentons P comme le quotient d'un module libre. Pour cela, considérons le morphisme

$$\pi : A^{(P)} \to P$$
$$\sum_{p \in P} a_p e_p \mapsto \sum_{p \in P} a_p p$$

On obtient alors la suite exacte

$$0 \to \ker \pi \hookrightarrow A^{(P)} \twoheadrightarrow A^{(P)}/\ker \pi \to 0$$

Or π est surjectif, donc

$$P \cong A^{(P)}/\ker \pi$$

d'où, en posant $M = \ker \pi$ et $L = A^{(P)}$ on obtient la suite exacte

$$0 \to M \to L \to P \to 0$$

qui d'après (ii) est scindée, d'où :

$$P \oplus M \cong L$$

avec L libre, d'où le résultat.

$(iii) \Rightarrow (i)$ Soit $f : P \to M''$ et $g : M \twoheadrightarrow M''$. On sait par hypothèse que $P \oplus M = L$ est libre. Soit $\{e_i\}_{i \in I}$ une base de L.

Alors tout $p \in P$ s'écrit $p = \sum_{i \in I} a_i e_i$.

Pour tout $i \in I$, $f(e_i) \in M''$. Or g est surjectif, donc il existe un $m_i \in M$ tel que $g(m_i) = f(e_i)$. Posons $h(e_i) := m_i$ et définissons $h : P \to M$ en posant, pour tout $p = \sum_{i \in I} a_i e_i \in P$:

$$h(p) = \sum_{i \in I} a_i h(e_i)$$

On a ainsi construit un morphisme de modules vérifiant pour tout $i \in I$, $f(e_i) = g \circ h(e_i)$ et donc, pour tout $p \in P$

$$f(p) = \sum_{i \in I} a_i f(e_i) = \sum_{i \in I} a_i g \circ h(e_i) = g \circ h(p)$$

□

3 Relations module projectif/module libre - Exemples

3.1 Module libre $\Rightarrow$ module projectif

Proposition 5. *Un module libre est un module projectif.*

Démonstration. Soit A un anneau, et M un A-module libre. Alors

$$M \oplus 0 \cong M$$

où 0 est un A-module et M est libre : M vérifie donc l'assertion (iii) de la **Proposition 4**. $\square$

3.2 Exemples de cas où module projectif $\Rightarrow$ module libre

3.2.1 Cas où l'anneau est un corps

Dans le cas où l'anneau est un corps k, un k-module M est un k-espace vectoriel. Alors, d'après le théorème de la base incomplète, M est de la forme

$$M \cong k^n$$

Ainsi un k-module est toujours libre, a fortiori tout k-module projectif est libre.

3.2.2 Anneau principal, anneau local

Citons pour exemples les deux cas suivants :

Proposition 6. *Un module projectif de type fini sur un anneau principal est libre.*

Proposition 7. *Soit A un anneau commutatif local (c'est-à-dire un anneau ne possédant qu'un seul idéal maximal). Alors tout A-module projectif de type fini est libre.*

([4] p413)

3.3 Contre-exemples

3.3.1 Le $\mathbb{Z}/6\mathbb{Z}$-module $\mathbb{Z}/3\mathbb{Z}$

Remarquons tout d'abord que si l'on a un morphisme d'anneaux commutatifs $\phi : A \to B$, alors B peut-être vu comme un A-module, via l'opération de l'anneau A sur le groupe additif B définie comme suit :

$$a.b = \phi(a) \times b \ \in B$$

Ainsi le morphisme d'anneaux

$$\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$$

nous permet d'affirmer que $\mathbb{Z}/3\mathbb{Z}$ est un $\mathbb{Z}/6\mathbb{Z}$-module.

- Ce module $\mathbb{Z}/3\mathbb{Z}$ est bien projectif, car d'après le théorème chinois :

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

- Mais il n'est pas libre, sinon il serait de la forme

$$\mathbb{Z}/3\mathbb{Z} \cong (\mathbb{Z}/6\mathbb{Z})^n$$

  ce qui est impossible (égalité des cardinaux).

3.3.2 Anneau d'endomorphismes

Considérons l'anneau $A = M_2(\mathbb{R})$ des matrices réelles 2×2, et les deux A-modules

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},\ a, b \in \mathbb{R} \right\}$$
$$B' = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} A = \left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix},\ c, d \in \mathbb{R} \right\}$$

On a l'égalité

$$B \oplus B' = A$$

donc B est un A-module projectif. Il n'est cependant pas libre car s'il l'était, on aurait

$$B \cong A^n$$

or $\dim_{\mathbb{R}} A = 4$ alors que $\dim_{\mathbb{R}} B = 2$.

4 Conjecture de Serre - Etude de certains cas

Toute cette parie a été travaillée à partir des pages 45 à 58 de [2].

Dans les paragraphes **4.1** et **4.2** (où nous travaillerons avec un anneau A commutatif), tous les A-modules considérés sont symétriques. Cela signifie que pour tout $a \in A$ et $m \in M$ on suppose que :

$$am = ma$$

4.1 Modules projectifs de rang 1

Nous allons montrer dans ce paragraphe que sur l'anneau de polynômes $A = R[x_1, \ldots, x_n]$ où R est un anneau factoriel commutatif, tout module projectif de type fini de rang 1 est libre.

Pour ce faire, nous allons au préalable démontrer le lemme suivant :

Lemme 1. *Soit A un anneau intègre commutatif, K son corps de fractions. Soit $P \neq 0$ un A-sous-module de K.*

Alors, si P est projectif, il existe un A-sous-module $Q \subset K$ tel que

$$PQ = A$$

Le A-module P est alors de type fini.

Démonstration du lemme. Puisque P est projectif, il existe un module M et un module libre L tel que

$$P \oplus M \cong L$$

Comme L est libre, on peut l'écrire sous la forme

$$L = \bigoplus_{i \in I} Ae_i$$

où I est un ensemble non vide non nécessairement fini.

Considérons l'épimorphisme canonique $L \overset{f}{\twoheadrightarrow} P$ et l'homomorphisme $id_P : P \to P$.

Puisque P est projectif, il existe un homomorphisme $g : P \to L$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccc} \mathrm{L} & \overset{f}{\twoheadrightarrow} & \mathrm{P} & \\ g & \nwarrow & \uparrow & id_P \\ & & \mathrm{P} & \end{array}$$

autrement dit tel que $f \circ g = id_P$.

Comme $L = \oplus_{i\in I} Ae_i$, tout élément $g(p) \in L$ où $p \in P$ peut s'écrire

$$g(p) = \sum_{i\in I} g_i(p)e_i$$

avec $g_i \in Hom_A(P, A)$.

Chaque g_i induit un morphisme $K \otimes_A P \to K \otimes_A A$, qui, selon Lam ([**2**] p45), induit lui-même un morphisme k-linéaire $\widetilde{g_i} : K \to K$. Pour tout $i \in I$, on peut alors poser $b_i := \widetilde{g_i}(1_A) \ \in K$.

On a alors pout tout $p \in P$:

$$\begin{aligned} g_i(p) &= \widetilde{g_i}(p) \\ &= \widetilde{g_i}(1_A.p) \\ &= \widetilde{g_i}(1_A)p \\ &= b_i p \end{aligned}$$

avec $b_i \in K$ et $b_i P \subset A$.

Notons que l'écriture $g(p) = \sum_{i\in I} g_i(p)e_i$ implique que seul un nombre fini de $g_i(p)$ peuvent être non nuls. Or $g_i(p) = b_i p$ donc cela entraîne que pour chaque $p \neq 0$ seul un nombre fini de b_i peuvent être non nuls, ce qui reste évidemment vrai pour $p = 0$.

Quitte à éliminer $\{i \in I \ / \ b_i = 0\}$, on peut donc supposer désormais que $|I| < \infty$.

Par construction on a $f \circ g = id_P$. D'où, pour tout $p \in P$, $f \circ g(p) = p$. Or

$$\begin{aligned} f(g(p)) &= f(\sum_{i\in I} b_i p\, e_i) \\ &= p \sum_{i\in I} b_i f(e_i) \end{aligned}$$

D'où en posant $a_i := f(e_i) \in P$ (on a alors $\sum_{i\in I} b_i a_i \in A$) on obtient l'égalité $p = p \sum_{i\in I} b_i a_i$ et ce pour tout $p \in P$.

De là

$$\sum_{i\in I} b_i a_i = 1_A$$

Posons maintenant $Q = \sum_{i\in I} Ab_i$.

On obtient alors

$$PQ = A$$

En effet :

On a d'une part $1_A = \sum_{i \in I} b_i a_i = \sum_{i \in I} a_i b_i$. Or pour tout $i \in I$, $a_i \in P$, donc $a_i b_i \in PQ$. D'où :

$$1_A \in PQ$$

Mais alors pour tout $a \in A$, $a = a.1_A \in APQ \subset PQ$ (car P est un A-module). De là :

$$A \subset PQ$$

D'autre part :

$$\begin{aligned} PQ &= P \sum_{i \in I} Ab_i \\ &= \sum_{i \in I} PAb_i \\ &\subset \sum_{i \in I} Pb_i \text{ car } P \text{ est un } A\text{-module} \\ &\subset A \text{ car pour tout } i \in I \ Pb_i \in A \end{aligned}$$

d'où le résultat.

Il apparaît alors que

$$P = \sum_{i \in I} Aa_i$$

donc que P est de type fini (car I est fini).

On a en effet $\sum_{i \in I} Aa_i \subset P$ car pour tout $i \in I$, $a_i \in P$.

De plus pour tout $p \in P$

$$\begin{aligned} p &= p \sum_{i \in I} b_i a_i \\ &= \sum_{i \in I} (b_i p) a_i \end{aligned}$$

avec $b_i p \in A$, d'où $p \in \sum_{i \in I} Aa_i$, d'où le résultat.

□

Nous pouvons maintenant démontrer le théorème suivant :

Théorème 1. *Soit A un anneau factoriel commutatif et P un A-module projectif de type fini de rang 1. Alors*

$$P \cong A$$

Démonstration. Par l'injection

$$\begin{aligned} P &\hookrightarrow K \otimes_A P \\ p &\mapsto 1 \otimes p \end{aligned}$$

on a l'inclusion $P \subset K \otimes_A P$.

Or le rang de P est 1 donc d'après la remarque du **2.3**, on a $\dim_K(K \otimes_A P) = 1$, d'où $K \otimes_A P \cong K$.

Ainsi :

$$P \subset K \otimes_A P \cong K$$

On peut donc voir P comme un A-sous-module de K. On sait de plus que A est factoriel, donc que A est intègre : on peut par conséquent appliquer le lemme précédent.

La preuve de ce lemme nous montre qu'il existe des $a_i \in P$ et $b_i \in K$, où I est un ensemble non vide fini, tels que $\sum_{i \in I} b_i a_i = 1_A$.

On sait alors que P est de type fini et s'écrit $P = \sum_{i \in I} A a_i$.

Pour tout $i \in I$, écrivons $b_i = \frac{c_i}{d_i}$ où $c_i, d_i \in A$ n'ont aucun facteur non-inversible commun.

Puisque pour tout couple $(i, j) \in I^2$ on a

$$b_j a_i = \frac{c_j}{d_j} a_i \ \in A$$

il s'ensuit que $d_j | a_i$ pour tout couple (i, j), par unicité de la décomposition dans l'anneau factoriel A.

Posons $d = \text{ppcm}\,\{d_j\}_{j \in I}$.

Soit $i \in I$. Par définition de d, a_i étant un multiple commmun des d_j, on a $d | a_i$. Ainsi $a_i \in Ad$ et ce pour tout $i \in I$, d'où

$$P = \sum_{i \in I} A a_i \subset Ad$$

D'autre part $\sum \frac{c_i}{d_i} a_i = 1_A$ d'où $d = \sum c_i \frac{d}{d_i} a_i$ avec $\frac{d}{d_i} \in A$. On a donc $d \in P$, ce qui entraîne $Ad \subset P$.

Ainsi

$$P = Ad$$

Or l'homomorphisme $A \to Ad$, $a \mapsto ad$ est clairement surjectif. Il est également injectif car A est intègre et $d \neq 0$. On a donc $Ad \cong A$.

D'où finalement :

$$P \cong A$$

□

On en déduit alors aisément le théorème suivant :

Théorème 2. *Soit R un anneau factoriel commutatif, $A = R[x_1, \ldots, x_n]$, et P un A-module projectif de rang 1.*

Alors

$$P \cong A$$

Démonstration. On sait d'après le théorème de Gauss que R factoriel entraîne $A = R[x_1, \ldots, x_n]$ factoriel.

On obtient alors directement le résultat en appliquant le théorème précédent.

$\square$

4.2 Module gradué

Après avoir introduit les définitions nécessaires, nous allons dans ce paragraphe nous intéresser à un anneau gradué $A = R[x_1, \ldots, x_n]$ et montrer qu'il suffit de savoir que tous les A_0-modules projectifs de type fini sont libres pour montrer que tout A-module projectif de type fini est libre.

Définition 11. Un anneau A est un *anneau* $\mathbb{N}$-*gradué* s'il se décompose en une somme directe de groupes additifs

$$A = A_0 \oplus A_1 \oplus \ldots$$

tels que pour tout $i, j \geq 0$ on ait

$$A_i A_j \subset A_{i+j}$$

Un élément de A_i est dit de *degré* i.

Pour illustrer cette définition, voici un exemple standard d'anneau gradué :
Soit R un anneau. Considérons l'anneau $A = R[x_1, \ldots, x_n]$. Alors

$$A = A_0 \oplus A_1 \oplus \ldots$$

où A_i est le sous-groupe de tous les polynômes homogènes de degré i en $x_1, \ldots, x_n$ (ainsi $A_0 = R$).

L'unicité de la décomposition d'un polynôme de A selon les A_i est claire, et on vérifie aisément l'inclusion $A_i A_j \subset A_{i+j}$ pour tout couple (i, j).

Revenons maintenant à la définition.

Proposition 8. *A_0 est un sous-anneau de A.*

Démonstration. Par hypothèse A_0 est un sous-groupe additif de A vérifiant $A_0 A_0 \subset A_0$, donc stable par multiplication.

De plus $1_A \in A_0$. Démontrons-le :
On peut supposer $A \neq \{0\}$, sinon on aurait $A = A_0$ et il n'y aurait alors rien à montrer.
Ecrivons

$$1 = a_i + a_{i+1} + \ldots$$

avec $a_i \neq 0$ et pour tout $j \geq i$, $a_j \in A_j$.

Comme

$$1 = 1^2 = a_i^2 + \dots$$

et $a_i^2 \in A_{2i}$, cela impose $A_{2i} = A_i$, d'où $i = 0$.

Soit $x \in A_j$. On a l'égalité :

$$1.x = x.1 = x$$

Considérons la composante selon A_j : l'unicité de la décomposition entraîne

$$a_0 x = x a_0 = x$$

Ainsi a_0 est un élément neutre pour A_j, et ce pour tout $j \geq 0$. On en déduit que a_0 est un élément neutre pour A, d'où $a_0 = 1_A$, et de là :

$$1_A \in A_0$$

□

Définition 12. Soit A un anneau gradué. On dit qu'un A-module M est un *module $\mathbb{Z}$-gradué* s'il existe une décomposition de M en somme directe de groupes additifs

$$M = \bigoplus_{j \in \mathbb{Z}} M_j$$

tels que pour tout $i \geq 0$ et $j \in \mathbb{Z}$ on ait

$$A_i M_j \subset M_{i+j}$$

(M_j peut avoir des composants de degré négatif.)

Définition 13. Un A-module gradué M est dit *borné inférieurement* s'il existe un $r \in \mathbb{Z}$ tel que pour tout $j < r$ on ait $M_j = 0$.

Proposition 9. *Tout A-module gradué de type fini est borné inférieurement.*

Démonstration. Soit M un A-module gradué de type fini. Soit $m_1, \dots, m_k$ un ensemble de générateurs de M. Pour tout $i = 1 \dots k$, soit d_i le plus petit degré des composants de m_i.

Posons $r = \min_{i=1\dots k} d_i$.

Alors

$$M = \sum_{i=1}^{k} A m_i \subset \sum_{j \geq r} A M_j$$

d'où

$$M \subset \sum_{j \geq r} M_j$$

□

Pour tout anneau gradué A, il est usuel de poser

$$A^+ = A_1 \oplus A_2 \oplus \dots$$

On vérifie aisément que A^+ est un idéal (à gauche et à droite) gradué de A :

Soit $a \in A$ et $b \in A^+$. Ecrivons $a = a_0 + a_1 + \dots$ et $b = b_1 + b_2 + \dots$ avec pour tout $i \geq 0$, $a_i \in A_i$ et pour tout $j \geq 1$, $b_j \in A_j$.

Il est clair que $a - a_0 \in A^+$, et que $b(a - a_0) \in A^+$. De plus pour tout $j \geq 1$, $b_j a_0 \in A_j$, donc $ba_0 \in A^+$.

D'où $ba \in A^+$. On montre de même que $ab \in A^+$.

Pour tout A-module gradué M, posons

$$\overline{M} = M/A^+M$$

Notons qu'alors

$$\overline{M} \cong A/A^+ \otimes_A M$$

via

$$\begin{aligned} A/A^+ \otimes_A M &\to M/A^+M \\ \widetilde{a} \otimes m &\mapsto \widetilde{a}m \end{aligned}$$

$\overline{M}$ est un module gradué sur $A_0 = A_0 \oplus 0 \oplus \dots$

Proposition 10. *Pour tout A-module gradué M borné inférieurement,*

$$\overline{M} = 0 \Rightarrow M = 0$$

Démonstration. Comme M est borné inférieurement, on peut écrire

$$M = M_r \oplus M_{r+1} \oplus \dots$$

Alors

$$\begin{aligned} A^+M &= (A_1 \oplus A_2 \oplus \dots)(M_r \oplus M_{r+1} \oplus \dots) \\ &\subset M_{r+1} \oplus M_{r+2} \oplus \dots \end{aligned}$$

car $A_i M_j \subset M_{i+j}$.

Par hypothèse $\overline{M} = 0$, donc $M = A^+M$.

D'après ce qui précède, on a donc l'inclusion

$$M_r \oplus M_{r+1} \oplus \dots \subset M_{r+1} \oplus M_{r+2} \oplus \dots$$

ce qui impose $M_r = 0$.

En réitérant ce raisonnement on montre que pour tout $i \geq r$, $M_i = 0$, d'où finalement

$$M = 0$$

□

Or on a vu que tout module gradué de type fini était borné inférieurement. On déduit donc de ce qui précède la proposition suivante :

Proposition 11. *Pour tout A-module gradué M de type fini,*

$$\overline{M} = 0 \Rightarrow M = 0$$

Proposition 12. *Soit A un anneau gradué. Soient P et Q deux A-modules gradués avec P projectif de type fini.*

Soit $\gamma : Q \to P$ un A-homomorphisme conservant les degrés (c'est-à-dire vérifiant pour tout $k \in \mathbb{Z}$ $\gamma(Q_k) \subset P_k$).

Alors on a l'équivalence :

γ est un isomorphisme $\Leftrightarrow \overline{\gamma} :\ \overline{Q} \to \overline{P}$ est un isomorphisme

Démonstration. $\Rightarrow$ Considérons

$$\begin{aligned} \overline{\gamma} : \overline{Q} &\to \overline{P} \\ \overline{q} &\mapsto \overline{\gamma(q)} \end{aligned}$$

Comme γ est surjectif, $\overline{\gamma}$ l'est également.

Montrons que $\overline{\gamma}$ est injectif : soit $\overline{q} \in \overline{Q}$ et $q \in Q$ un de ses représentants. Ecrivons $q = q_0 + q^+$ avec $q_0 \in A_0Q$ et $q^+ \in A^+Q$.

Alors $\gamma(q) = \gamma(q_0) + \gamma(q^+)$ avec $\gamma(q_0) \in A_0P$ et $\gamma(q^+) \in A^+P$, car γ conserve les degrés.

Supposons maintenant que $\overline{\gamma}(\overline{q}) = \overline{\gamma(q)} = 0$, autrement dit que $\gamma(q) \in A^+P$. Cela implique que $\gamma(q_0) = 0$, d'où par injectivité de γ, $q_0 = 0$. On a alors $q \in A^+Q$, donc $\overline{q} = 0$.

D'où l'injectivité de $\overline{\gamma}$.

$\Leftarrow$ Posons $K = \ker\gamma$ et $C = \mathrm{coker}\gamma = P/\mathrm{Im}\gamma$. Ce sont des A-modules gradués.

Montrons tout d'abord que

$$\mathrm{coker}\overline{\gamma} \cong \overline{\mathrm{coker}\gamma}$$

c'est-à-dire montrons que

$$\overline{P}/\mathrm{Im}\overline{\gamma} \cong \overline{P/\mathrm{Im}\gamma}$$

Considérons pour cela l'homomorphisme

$$\begin{aligned} \Phi :\ \overline{P} &\to \overline{P/\mathrm{Im}\gamma} \\ \overline{p} &\mapsto \overline{\widetilde{p}} \end{aligned}$$

Clairement, Φ est surjectif, d'où

$$\overline{P}/\ker \Phi \cong \overline{P/\mathrm{Im}\gamma}$$

On constate d'autre part que $\ker \Phi = \mathrm{Im}\overline{\gamma}$. On a donc

$$\overline{P}/\mathrm{Im}\overline{\gamma} \cong \overline{P/\mathrm{Im}\gamma}$$

d'où le résultat $\mathrm{coker}\overline{\gamma} \cong \overline{\mathrm{coker}\gamma}$.

Or on sait que $\overline{\gamma}$ est surjectif, donc $\mathrm{coker}\overline{\gamma} = 0$, d'où $\overline{C} = \overline{\mathrm{coker}\gamma} = 0$.

Par hypothèse P est de type fini, donc C l'est également. Alors d'après la **Proposition 11**, $\overline{C} = 0$ implique que $C = 0$, d'où γ est surjectif.

D'autre part P est projectif, donc la suite exacte

$$0 \to K \hookrightarrow Q \overset{\gamma}{\twoheadrightarrow} P \to 0$$

est scindée.

On a donc, d'après la **Proposition 3** : $Q = P \oplus K$.

Alors
$$\begin{aligned}\overline{Q} \cong A/A^+ \otimes Q &= A/A^+ \otimes (P \oplus K)\\ &= (A/A^+ \otimes P) \oplus (A/A^+ \otimes K)\end{aligned}$$

Ainsi $\overline{Q} = \overline{P} \oplus \overline{K}$.

Or $\overline{\gamma} : \overline{Q} \to \overline{P}$ est un isomorphisme, donc $\overline{Q} \cong \overline{P}$, ce qui impose $\overline{K} = 0$.

De plus Q est de type fini, donc K aussi. On peut donc appliquer la proposition précédente, ce qui nous donne $K = 0$, autrement dit γ est injectif.

□

Théorème 3. *Soit A un anneau gradué $A = A_0 \oplus A_1 \oplus \dots$ et P un A-module projectif de type fini gradué.*

Alors il existe un isomorphisme de A-modules gradués

$$A \otimes_{A_0} \overline{P} \cong P$$

Démonstration. Remarquons tout d'abord que, P étant un A-module projectif de type fini, $\overline{P}$ est un A_0-module projectif de type fini. En effet, soit $p_1, \dots, p_k$ un ensemble de générateurs de P. Ecrivons $P = \sum_{i=1}^k Ap_i$. Alors $\overline{P}$ est de la forme $\overline{P} = \sum_{i=1}^k A_0\overline{p_i}$, donc un A_0-module de type fini.

De plus, P est projectif donc est facteur direct d'un module libre

$$P \oplus M = L$$

ce qui, comme on l'a vu précédemment, nous permet d'écrire

$$\overline{P} \oplus \overline{M} = \overline{L}$$

d'où $\overline{P}$ est projectif.

Considérons la projection $f : P \twoheadrightarrow \overline{P}$. Comme $\overline{P}$ est projectif, il existe un A_0-homomorphisme $g \in \mathrm{Hom}_{A_0}(\overline{P}, P)$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccc} \mathrm{P} & \overset{f}{\twoheadrightarrow} & \overline{P} & \\ g & \nwarrow & \uparrow & id_{\overline{P}} \\ & & \overline{P} & \end{array}$$

autrement dit tel que $f \circ g = id_{\overline{P}}$.

L'homomorphisme f conserve les degrés, ce qui impose que g les conserve également. En effet, soit $\overline{p} \in \overline{P}_k$. Alors $g(\overline{p}) \in P_{k'}$. Mais f conserve les degrés, donc $\overline{p} = f(g(\overline{p})) \in \overline{P}_{k'}$, d'où $k = k'$ par unicité de la décomposition de $\overline{p}$ sur $\overline{P}$.

Posons $Q = A \otimes_{A_0} \overline{P}$. Alors g induit un A-homomorphisme conservant les degrés

$$\begin{aligned} \gamma :\ Q = A \otimes_{A_0} \overline{P} &\to P \\ a \otimes \overline{p} &\mapsto ag(\overline{p}) \end{aligned}$$

Considérons l'homomorphisme

$$\overline{\gamma} : \overline{Q} \to \overline{P}$$

Or on a

$$\begin{aligned} \overline{Q} = A/A^+ \qquad\qquad & \otimes_A (A \otimes_{A_0} \overline{P}) \\ \cong A/A^+ \otimes_{A_0} \overline{P}) & \\ \cong \overline{P} & \end{aligned}$$

On vérifie que $\overline{\gamma}$ est un isomorphisme. Alors d'après la **Proposition 12** $\gamma :\ Q \to P$ est un isomorphisme, et donc

$$A \otimes_{A_0} \overline{P} \cong P$$

□

De ce théorème on déduit alors le théorème suivant :

Théorème 4. *Soit $A = A_0[x_1, \dots, x_n]$ un anneau gradué. Soit P un A-module gradué projectif de type fini.*

Si tous les modules projectifs de type fini sur A_0 sont libres (par exemple si A_0 est un corps, ou un anneau local commutatif) alors P est libre.

Démonstration. Soit P un A-module gradué projectif de type fini. D'après le théorème précédent

$$A \otimes_{A_0} \overline{P} \cong P$$

Or $\overline{P}$ est un A_0-module projectif de type fini, il est donc libre par hypothèse. Il s'écrit donc

$$\overline{P} = \bigoplus_{i \in I} A_0 e_i$$

Mais alors

$$\begin{aligned} P &\cong A \otimes_{A_0} \bigoplus_{i \in I} A_0 e_i \\ &\cong \bigoplus_{i \in I} A \otimes_{A_0} A_0 e_i \\ &\cong \bigoplus_{i \in I} A e_i \end{aligned}$$

d'où P est un A-module libre.

□

4.3 Contre-exemple : corps gauche

Dans ce paragraphe, nous allons montrer que la conjecture de Serre n'est pas vérifiée dans le cas où l'on considère un anneau $A = k[x_1, \dots, x_n]$ où le corps k n'est pas commutatif (encore appelé *corps gauche*).

Théorème 5. *Soit k un corps gauche et $A = k[x, y]$.*

Alors il existe un A-module à droite P projectif qui n'est pas libre.

Démonstration du théorème. k étant un corps gauche, on peut choisir deux élements inversibles $a, b \in k^\times$ ne commutant pas. Alors $u = ab - ba$ est également inversible.

Posons

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \in A^2$$

et définissons le A-homomorphisme à droite $\Phi : A^2 \to A$ par :

$$\begin{aligned} \Phi(e_1) &= x + a \\ \Phi(e_2) &= -(y + b) \end{aligned}$$

Cet homomorphisme est surjectif car, en posant $U = \begin{pmatrix} y + b \\ x + a \end{pmatrix}$ on obtient :

$$\begin{aligned} \Phi(U) = (x + a, -(y + b)) \begin{pmatrix} y + b \\ x + a \end{pmatrix} &= (x + a)(y + b) - (y + b)(x + a) \\ &= ab - ba \\ &= u \end{aligned}$$

Or u est inversible et tout élément $a \in A$ s'écrit

$$\begin{aligned} a &= uu^{-1}a \\ &= \Phi(U)u^{-1}a \\ &= \Phi(Uu^{-1}a) \end{aligned}$$

car Φ est un A-homomorphisme à droite. Φ est donc bien surjectif.

On a

$$\ker \Phi \oplus \operatorname{Im} \Phi \cong A^2$$

d'où, en posant $P = \ker \Phi$, et sachant que Φ est surjectif, on obtient

$$P \oplus A \cong A^2 \quad \textbf{(1)}$$

On a ainsi obtenu un A-module à droite projectif P.

Montrons maintenant que P n'est pas A-libre. Supposons le contraire, c'est-à-dire

$$P \cong A^n$$

On aurait alors, d'après **(1)** :

$$A^{n+1} \cong A^2$$

En réduisant modulo (x, y), on obtient $kn + 1 \cong k^2$, d'où $n = 1$.

Montrons alors que P n'est pas isomorphe à A.

Nous allons pour cela avoir besoin du lemme technique suivant. Introduisons au préalable les notations suivantes : pour $f \in A$ on notera $\deg f$ le degré total de f.

L'intégrité de k entraîne que $\deg (fg) = \deg f + \deg g$.

Pour $f \in A = k[x, y]$ posons $f(0,0)$ le terme constant de f.

Lemme 2. *(0) P ne contient aucun $\begin{pmatrix} f_0 \\ g_0 \end{pmatrix} \neq 0$ avec $\deg f_0 \leq 1$, $\deg g_0 \leq 1$.*

(1) P contient un $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix}$ tel que $\deg f_1 = \deg g_1 = 2$, avec $f_1(0,0) = 0$.

(2) P contient un $\begin{pmatrix} f_2 \\ g_2 \end{pmatrix}$ tel que $f_2(0,0) \neq 0$.

Une fois ce lemme démontré, il est alors facile de montrer que $P \cong A$ est impossible.

En effet, supposons que l'on ait un isomorphisme $\varphi : \ P \to A$. Posons $\begin{pmatrix} f \\ g \end{pmatrix} = \varphi^{-1}(1_A) \in A^2$ et pour $i = 1, 2$, $h_i = \varphi \begin{pmatrix} f_i \\ g_i \end{pmatrix} \in A$. On a alors d'une part

$$\varphi^{-1}(\varphi \begin{pmatrix} f_i \\ g_i \end{pmatrix}) = \begin{pmatrix} f_i \\ g_i \end{pmatrix}$$

et d'autre part

$$\begin{aligned} \varphi^{-1}(\varphi \begin{pmatrix} f_i \\ g_i \end{pmatrix}) &= \varphi^{-1}(h_i) \\ &= \varphi^{-1}(1_A h_i) \\ &= \varphi^{-1}(1_A) h_i \quad \text{car } \varphi^{-1} \text{ est un } A\text{-homomorphisme à droite} \\ &= \begin{pmatrix} f \\ g \end{pmatrix} h_i \end{aligned}$$

d'où

$$\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} = \begin{pmatrix} f \\ g \end{pmatrix} h_1 \qquad (1)$$
$$\begin{pmatrix} f_2 \\ g_2 \end{pmatrix} = \begin{pmatrix} f \\ g \end{pmatrix} h_2 \qquad (2)$$

De (1) on déduit

$$\begin{aligned} \deg f_1 &= 2 = \deg f + \deg h_1 \\ \deg g_1 &= 2 = \deg g + \deg h_1 \end{aligned}$$

Mais alors si $\deg h_1 = 1$ ou 2 cela impose $\deg f \leq 1$ et $\deg g \leq 1$. Or $\begin{pmatrix} f \\ g \end{pmatrix} \neq 0$ (car $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} \neq 0$), ce qui est donc impossible d'après le (0) du lemme.

Par conséquent $\deg h_1 = 0$, donc $h_1 \in k$. De plus $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} \neq 0$ donc $h_1 \neq 0$.
On a d'autre part $0 = f_1(0,0) = f(0,0)h_1$, d'où $f(0,0) = 0$.
Mais cela contredit alors $0 \neq f_2(0,0) = f(0,0)h_2$.
D'où finalement

$$P \ncong A$$

□

Démontrons maintenant le lemme technique :

Démonstration du lemme. **(0)** Supposons qu'il existe $\begin{pmatrix} f_0 \\ g_0 \end{pmatrix} \neq 0 \in P = \ker\Phi$ avec $\deg f_0 \leq 1$ et $\deg g_0 \leq 1$.

On a donc $f_0 = c + dx + ey$ et $g_0 = c' + d'x + e'y$, avec $c, c', d, d', e, e' \in k$.
Or $\Phi \begin{pmatrix} f_0 \\ g_0 \end{pmatrix} = 0$ d'où

$$(x+a)(c+dx+ey) - (y+b)(c'+d'x+e'y) = 0$$

$$ac - bc' + (c + ad - bd')x + (ae - c' - be')y + dx^2 + (e - d')xy - e'y^2 = 0$$

et donc

$$\begin{aligned} d &= e' = 0 \\ e &= d' \\ c' &= ae \\ c &= bd' \\ ac &= bc' \end{aligned}$$

Mais alors

$$\begin{aligned} ac = bc' &\Rightarrow abd' = bae \\ &\Rightarrow abe = bae \\ &\Rightarrow (ab - ba)e = 0 \\ &\Rightarrow ue = 0 \end{aligned}$$

Or $u \neq 0$ donc $e = 0 = d'$ et ainsi $c = c' = 0$. Mais alors $f_0 = g_0 = 0$, ce qui contredit $\begin{pmatrix} f_0 \\ g_0 \end{pmatrix} \neq 0$.

(1) Essayons de trouver $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} \in P$ tel que $\deg f_1 = \deg g_1 = 2$ et $f_1(0,0) = 0$.

Pour cela écrivons $f_1 = a_1x + a_2y + a_3xy + a_4y^2$ et $g_1 = b_1x + b_2y + b_3xy + b_4x^2$.

La condition $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} \in P$ nous donne

$$(x + a)f_1 = (y + b)g_1$$

d'où, en regroupant les termes de même degré :

$$\begin{aligned} &aa_1x + aa_2y + a_1x^2 + (a_2 + aa_3)xy + aa_4y^2 + a_3x^2y + a_4xy^2 \\ &\qquad = bb_1x + bb_2y + bb_4x^2 + (b_1 + bb_3)xy + b_2y^2 + b_4x^2y + b_3xy^2 \end{aligned}$$

Les b_i sont donc ainsi uniquement déterminés à partir des a_i :

$$\begin{aligned} b_3 &= a_4 \\ b_4 &= a_3 \\ b_2 &= b^{-1}aa_2 \\ b_1 &= b^{-1}aa_1 \end{aligned}$$

On obtient d'autre part les équations

$$\begin{aligned} bb_4 &= a_1 \\ b_2 &= aa_4 \\ b_1 + bb_3 &= a_2 + aa_3 \end{aligned}$$

ce qui d'après les égalités précédentes revient à

$$\begin{aligned} ba_3 &= a_1 \\ b^{-1}aa_2 &= aa_4 \\ b^{-1}aa_1 + ba_4 &= a_2 + aa_3 \end{aligned}$$

Les deux premières équations nous indiquent que a_1 et a_2 sont uniquement déterminés à partir de a_3 et a_4. En effet :

$$\begin{aligned} a_1 &= ba_3 \\ a_2 &= a^{-1}baa_4 \end{aligned}$$

En injectant ces égalités dans la dernière équation, il nous reste alors une unique équation :

$$b^{-1}aba_3 + ba_4 = a^{-1}baa_4 + aa_3$$

ou encore

$$\begin{aligned} b^{-1}aba_3 - aa_3 &= a^{-1}baa_4 - ba_4 \\ b^{-1}(ab - ba)a_3 &= a^{-1}(ba - ab)a_4 \\ b^{-1}ua_3 &= -a^{-1}ua_4 \end{aligned}$$

Ceci peut se résoudre en posant $a_3 = -u^{-1}ba^{-1}ua_4$. En choisissant $a_4 \neq 0$ quelconque dans k, on obtient alors $b_4 = a_3 \neq 0$.

On a donc bien construit un $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} \in P$ avec $\deg f_1 = \deg g_1 = 2$ et $f_1(0,0) = 0$

(2) Essayons de trouver $\begin{pmatrix} f_2 \\ g_2 \end{pmatrix} \in P$ tel que $f_2(0,0) \neq 0$ en écrivant $f_2 = a_1 + a_2y + a_3y^2$ et $g_2 = b_1 + b_2x + b_3y + b_4xy$.

La condition $\begin{pmatrix} f_2 \\ g_2 \end{pmatrix} \in P$ nous impose

$$(x + a)f_2 = (y + b)g_2$$

d'où, en regroupant les termes de même degré :

$$\begin{aligned} &aa_1 + a_1x + aa_2y + a_2xy + aa_3y^2 + a_3xy^2 \\ &\qquad = bb_1 + bb_2x + (b_1 + bb_3)y + (b_2 + bb_4)xy + b_3y^2 + b_4xy^2 \end{aligned}$$

Les a_i sont uniquement déterminés à partir des b_i puisque :

$$\begin{aligned} a_1 &= bb_2 \\ a_2 &= b_2 + bb_4 \\ a_3 &= b_4 \end{aligned}$$

Les équations restantes

$$\begin{aligned} aa_1 &= bb_1 \\ aa_3 &= b_3 \\ aa_2 &= b_1 + bb_3 \end{aligned}$$

sont donc équivalentes aux équations

$$\begin{aligned} abb_2 &= bb_1 \\ ab_4 &= b_3 \\ a(b_2 + bb_4) &= b_1 + bb_3 \end{aligned}$$

Les deux premières équations nous donnent

$$\begin{aligned} b_1 &= b^{-1}abb_2 \\ b_3 &= ab_4 \end{aligned}$$

Il nous reste donc pour seule équation

$$a(b_2 + bb_4) = b^{-1}abb_2 + bab_4$$

soit

$$\begin{aligned} b^{-1}abb_2 - ab_2 &= abb_4 - bab_4 \\ b^{-1}(ab - ba)b_2 &= (ab - ba)b_4 \\ b^{-1}ub_2 &= ub_4 \end{aligned}$$

Posons alors $b_2 = u^{-1}bub_4$ et choisissons $b_4 \neq 0$ quelconque dans k. On a alors $f_2(0,0) = a_1 = bb_2 = bu^{-1}bub_4 \neq 0$.

On a donc bien construit un $\begin{pmatrix} f_2 \\ g_2 \end{pmatrix} \in P$ avec $f_2(0,0) \neq 0$.

$\square$

Références

[1] J.P.Lafon. *Les formalismes fondamentaux de l'algèbre commutative*. Hermann, 1974.

[2] T.Y.Lam. *Serre's Conjecture*. Lecture Notes in Mathematics, 1978.

[3] S.Lang. *Algebra*. Graduate Texts in Mathematics, Springer, 2002.

[4] N. Jacobson. *Basic Algebra II*. Freeman, 1989.

[5] J.P.Serre. *Faisceaux algébriques cohérents*. Ann. of Math. (2) 61, 1955.