Magistère 1ère année
Anne Renardet

Directeur de mémoire :M. Nuss

La conjecture de Serre

Année 2001/2002

Sommaire

<u>Introduction</u>

« Signalons que, lorsque [...] $A = K\left[X_1, X_2, ..., X_n\right]$, on ignore s'il existe des *A*-modules projectifs de type fini qui ne soient pas libres »

…en notant *K* un corps quelconque.

Avec ces quelques mots écrits dans son ouvrage <u>Faisceaux algébriques cohérents</u>, le mathématicien Jean-Pierre Serre ne se doutait sans doute pas qu'il allait occuper de nombreux scientifiques pendant un peu plus de vingt ans.

Lancée en 1955, la conjecture de Serre (comme on continue à l'appeler, et non le résultat de Serre) n'a en effet été prouvée que 21 ans plus tard, en 1976, par Suslin et Quillen, indépendamment l'un de l'autre.

Dans ce mémoire, nous commencerons par définir les notions utilisées par Serre de module libre et projectif, après quelques rappels.

Une fois à même de comprendre la conjecture de Serre, nous étudierons deux des premières preuves de la conjecture qui ont été données dans des cas particuliers. Nous en verrons également un contre-exemple dans le cas où l'on ne considère pas que *K* est un corps mais seulement un corps gauche (c'est-à-dire un anneau non commutatif dont tous les éléments sont inversibles).

Partie I- Rappels

Rappelons tout d'abord la définition suivante : soit A un anneau, un A-*module à gauche* M est la donnée d'un ensemble M et d'une application $\begin{array}{l} A\times M \to M \\ (a,m)\mapsto a.m \end{array}$ vérifiant

- *(M, +)* est un groupe abélien
- Pour tous a et a' éléments de A, pour tous m et m' éléments de M
    i. $(a + a').m = a.m + a'.m$
    ii. $(aa').m = a.(a'.m)$
    iii. $a.(m + m') = a.m + a.m'$
    iv. $0.m = 0$
    v. $1.m = m$

Notons que l'on peut définir de même les notions de A-*module à droite* et de A-*module à droite et à gauche.*
L'application citée est appelée *loi de composition externe* ou *action de A sur M.*

Par exemple, l'anneau A est un A-module en considérant l'application

$$\begin{array}{l} A\times A \to A \\ (a,m)\mapsto a.m \end{array}$$

1-Suites exactes

Nous ne traiterons ici que les *suites exactes courtes*, c'est-à-dire les suites

$$0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$$

telles que f soit un monomorphisme, g un épimorphisme et Ker g= Im f.

La proposition suivante, bien que simple, nous sera utile plus tard.

Proposition : *Soient* (E_i), (F_i) et (G_i) *trois sous-familles de A-modules ayant même ensemble d'indices I. Soient, pour tout i élément de I,* $f_i : E_i \to F_i$ et $g_i : F_i \to G_i$ *deux applications linéaires.*

Alors l'application $f : \prod_{i\in I} E_i \to \prod_{i\in I} F_i$ *telle que* $f\left(\left(x_i\right)_{i\in I}\right) = \left(f_i\left(x_i\right)\right)_{i\in I}$ *est linéaire, tout comme l'application g définie de manière similaire de* $\prod_{i\in I} F_i$ *dans* $\prod_{i\in I} G_i$.

De plus, les suites $0 \to E_i \xrightarrow{f_i} F_i \xrightarrow{g_i} G_i \to 0$ *sont exactes pour tout i élément de I si et seulement si la suite* $0 \to \prod_{i\in I} E_i \xrightarrow{f} \prod_{i\in I} F_i \xrightarrow{g} \prod_{i\in I} G_i \to 0$ *est exacte.*

Preuve : La linéarité de f (respectivement de g) se déduit de la linéarité des f_i (respectivement de celle des g_i).

L'application f est un monomorphisme si et seulement si chaque f_i est un monomorphisme.

L'application g est un épimorphisme si et seulement si chaque g_i est un épimorphisme.

Enfin par définition de f et de g, $\operatorname{Ker} g = \prod_{i\in I} \operatorname{Ker} g_i$ et $\operatorname{Im} f = \prod_{i\in I} \operatorname{Im} f_i$. □

Avant de passer à la proposition suivante, rappelons qu'un sous-module N d'un A-module M est appelé un *facteur direct* s'il possède un supplémentaire dans M, c'est-à-dire s'il existe P sous-module de M tel que $N \oplus P = M$.

Remarquons que *N* est facteur direct si et seulement si il existe un projecteur de *M* dans *M* dont l'image ou le noyau soit *N*.

En effet si un tel projecteur *p* existe, nous pouvons supposer sans nuire à la généralité que *N* est le noyau de ce projecteur. En appliquant la formule $\operatorname{Ker} p \oplus \operatorname{Im} p = M$, nous voyons bien que *N* est un facteur direct dans *M*.
Réciproquement, si *N* est un facteur direct dans *M*, notons *P* un supplémentaire de *N* dans *M*. Appelons *p* la fonction caractéristique de *P* définie sur *M*. Nous voyons alors clairement que la formule $p \circ p = p$ est vérifiée, c'est-à-dire que *p* est un projecteur, dont *N* est le noyau.

Ainsi, en prenant $A = M = V = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ le groupe de Klein et les modules notés *N* et *P* définis par $N = \mathbf{Z}/2\mathbf{Z} \times \{0\}$ et $P = \{0\} \times \mathbf{Z}/2\mathbf{Z}$, nous vérifions la condition ci-dessus : *N* est un facteur direct.

Par contre pour $A = M = \mathbf{Z}$ et $N = \{2k,\ k \in \mathbf{Z}\}$, il n'existe pas de supplémentaire de *N* dans *M* qui soit un sous-module de *M*.

Liées aux suites exactes courtes, nous avons aussi les notions de rétraction et de section.
Soit $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ une suite exacte courte, *f* un monomorphisme et *g* un épimorphisme tels que Ker *g* = Im *f*.
Une *rétraction* est un morphisme $r : F \to E$ tel que $r \circ f \equiv Id_E$.
Une *section* est un morphisme $s : G \to F$ tel que $g \circ s \equiv Id_G$.

Toutes les suites exactes courtes ne possèdent pas une section ou une rétraction. Par exemple il est impossible de trouver une section associée à l'épimorphisme *g* dans la suite exacte courte suivante :

$$0 \to \mathbf{Z}/2\mathbf{Z} \xrightarrow{f} \mathbf{Z}/4\mathbf{Z} \xrightarrow{g} \mathbf{Z}/2\mathbf{Z} \to 0$$

En effet comme *g* est surjectif, on a *g*(0)=0, *g*(1)=1, *g*(2)=0 et *g*(3)=1 dans $\mathbf{Z}/2\mathbf{Z}$.
Mais le seul morphisme non nul de $\mathbf{Z}/2\mathbf{Z}$ dans $\mathbf{Z}/4\mathbf{Z}$ est *s* tel que *s*(0)=0 et *s*(1)=2.
Alors $g \circ s(1) = 0$ et $g \circ s \neq Id_{\mathbf{Z}/2\mathbf{Z}}$.
La suite exacte courte suivante admet quant à elle une section : nous considérons *f* et *g* les injections canoniques, l'injection canonique est elle-même une section associée à *g*.

$$0 \to \mathbf{Z}/2\mathbf{Z} \times \{0\} \xrightarrow{f} \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \xrightarrow{g} \{0\} \times \mathbf{Z}/2\mathbf{Z} \to 0$$

Ces exemples montrent la nécessité de différencier les suites exactes courtes admettant une section (ou une rétraction), dites *suites exactes courtes scindées*, des autres.
La proposition suivante en donne différentes caractérisations.

Proposition : *Une suite exacte* $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ *est dite scindée si elle vérifie l'une des trois propositions équivalentes suivantes :*

i. *Le sous-module f(E) est facteur direct dans F..*
ii. *Il existe une rétraction linéaire* $r : F \to E$ *associée à f.*
iii. *Il existe une section linéaire* $s : G \to F$ *associée à g.*

Dans ce cas, $(f+s) : E \oplus G \to F$ *est un isomorphisme.*

Preuve : $i \Rightarrow ii$ Avec la remarque que nous avons faite sur les facteurs directs, il existe un projecteur *p* de *E* dans *E* tel que *p*(*F*)=*f*(*E*).
L'homomorphisme $r \equiv f^{-1} \circ p$ est alors une rétraction linéaire associée à *f*.

$ii \Rightarrow i$ Soit *r* la rétraction associée à *f*. L'application $f \circ r$ est une projection dans *E* $\left[\text{En effet } (f \circ r)^2 = f \circ r \circ f \circ r = f \circ Id_G \circ r = f \circ r \right]$
Comme $(f \circ r)(F) = f(E)$, *f*(*E*) est un facteur direct.
Donc *i* $\Leftrightarrow$ *ii*.

$i \Rightarrow iii$ Soit *E'* un supplémentaire de *f*(*E*) dans F et soit $j : E' \to F$ l'injection canonique. Alors $g \circ j$ est un isomorphisme de *E'* sur *G* et l'isomorphisme réciproque, considéré comme application de *G* dans *F*, est une section associée à *g*.

$iii \Rightarrow i$ Soit s la section associée à *g*. Alors $s \circ g$ est une projection dans *F* dont *f*(*E*) est le noyau. Avec la remarque portant sur les facteurs directs, nous voyons que *f*(*E*) est un facteur direct.
Donc $i \Leftrightarrow iii$.
Les équivalences sont prouvées.

De plus *s* est une bijection de *G* sur *s*(*G*) et *s*(*G*) est un supplémentaire de *f*(*E*) dans F, donc (*f*+ *s*) est un isomorphisme. ☐

<u>2- Produit tensoriel</u>

Nous allons dans ce paragraphe rappeler la définition du produit tensoriel de deux modules ainsi que ses premières propriétés.
Nous noterons *A* un anneau quelconque, *M* et *N* deux *A*-modules.

Commençons par donner la définition théorique du produit tensoriel de deux *A*-modules.
Notons $C=\mathbf{Z}^{(M\times N)}$ le $\mathbf{Z}$-module des combinaisons linéaires formelles d'éléments de $M\times N$ à coefficients dans $\mathbf{Z}$. On peut considérer qu'une base de *C* est constituée des couples (*x*,*y*) où *x* et *y* sont respectivement des éléments de *M* et *N*.
Notons aussi *D* le sous-$\mathbf{Z}$-module de *C* engendré par les éléments de l'un des types suivants :

$$(x+x',y)-(x,y)-(x',y)$$
$$(x,y+y')-(x,y)-(x,y')$$
$$(x\lambda,y)-(x,\lambda y)$$

où λ est un élément de *A*.

Définition : *On appelle produit tensoriel du A-module à droite M et du A-module à gauche N, et on note* $M\otimes_A N$ *, le* $\mathbf{Z}$*-module quotient* C/D .
Pour x élément de M et y élément de N, on note $x\otimes y$ *et on appelle produit tensoriel de x et de y l'élément de* $M\otimes_A N$ *image canonique de l'élément (x,y) de C.*

Extrait des <u>Elements de Mathématiques</u> de Nicolas Bourbaki, Algèbre, Chapitre 2, page 77.

Une première et évidente propriété des éléments de $M\otimes_A N$ est la suivante :

Propriété : *Les* $x\otimes y$ *éléments de* $M\otimes_A N$ *vérifient les propriétés suivantes :*

$$(x+x')\otimes y=x\otimes y+x'\otimes y$$
$$x\otimes(y+y')=x\otimes y+x\otimes y'$$
$$x\otimes\lambda y=\lambda x\otimes y$$

Preuve : Ceci provient clairement de la définition du produit tensoriel. ☐

Remarque : Les éléments de $M \otimes_A N$ s'écrivent comme combinaisons linéaires finies des $x \otimes y$ où x est un élément de M et y un élément de N.
Toutefois le produit tensoriel de deux modules non réduits à 0 peut se réduire à 0. Par exemple, le produit tensoriel des deux $\mathbf{Z}$-modules $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$ est nul.
En effet, soit $x \in \mathbf{Z}/2\mathbf{Z}$ et soit $y \in \mathbf{Z}/3\mathbf{Z}$. Nous avons les relations suivantes : $2x=0$ et $3y=0$. Alors $x \otimes y = 3(x \otimes y) - 2(x \otimes y) = x \otimes (3y) - (2x) \otimes y = 0$ pour tous x et y.

Nous allons également définir le *produit tensoriel de deux applications linéaires :*
Soient M' et N' deux A-modules.
Soient $u : M \to M'$ et $v : N \to N'$ deux applications A-linéaires.
Il existe une application $\mathbf{Z}$-linéraire et une seule $w : M \otimes_A N \to M' \otimes_A N'$ telle que

$$w(x \otimes y) = u(x) \otimes v(y)$$

Cette application se note $u \otimes v$ et s'appelle le produit tensoriel de u et de v.

Preuve : La preuve de ce résultat est claire. L'application w est entièrement définie par l'image des éléments $\sum_{k=0}^{n} x_k \otimes y_k$ de $M \otimes_A N$, image connue et égale à $\sum_{k=0}^{n} u(x_k) \otimes v(y_k)$.
L'existence et l'unicité de w en découle. □

Nous avons vu également que A est lui-même un A-module. Nous pouvons nous demander à quoi correspond le produit tensoriel $M \otimes_A A$.

Propriété : *Si M est un A-module à droite, l'application* $h : M \to M \otimes_A A$, $x \mapsto x \otimes 1_A$ *est un isomorphisme de A-modules à droite, d'isomorphisme réciproque g défini par* $g(x \otimes \lambda) = x\lambda$ *pour tout x élément de M et tout λ élément de A.*

Preuve : Nous voyons en effet que $g \circ h$ est l'application identité de M.
De même si x est un élément de M et λ un élément de A,

$$(h \circ g)(x \otimes \lambda) = h(x\lambda) = x\lambda \otimes 1 = x \otimes \lambda$$

L'application $h \circ g$ est aussi l'identité de $M \otimes_A A$.
L'application h est bien un isomorphisme. $\square$

La plupart du temps, $M \otimes_A A$ et M sont identifiés.

Remarque : Nous pouvons de même identifier $A \otimes_A N$ et N pour tout A-module à gauche N.

La proposition suivante sera utilisée plus tard :

Proposition : *Soit I un idéal de A. Soit M un A-module.*
Alors l'application $A/I \times M \to M/IM$

$$(i, x) \mapsto ix(\operatorname{mod} IM)$$

est bilinéaire et induit un isomorphisme $A/I \otimes_A M \cong M/IM$.

Preuve : L'application citée est clairement bilinéaire. Elle est également surjective : si x est un représentant de $\bar{x}$ élément de M/IM, alors $(1, x)$ est un antécédent de $\bar{x}$ par cette application, ce pour tout $\bar{x}$ élément de M/IM.

De cette application, nous déduisons une nouvelle application linéaire et surjective de $A/I \otimes_A M$ dans M/IM.
Cette application étant surjective, il nous est possible de construire une application réciproque $M \to A/I \otimes_A M$
Comme IM est clairement contenu dans le noyau de cette dernière application, nous avons donc construit un morphisme de M/IM dans $A/I \otimes_A M$, qui est bien le morphisme réciproque cherché.

L'isomorphisme est démontré. $\square$

Partie II- Modules libres et projectifs

Nous allons définir dans cette partie les notions de module libre et de module projectif, bases même de la conjecture de Serre.
Nous étudierons également leurs premières propriétés.

Dans toute cette partie, nous noterons *A* un anneau quelconque et tout *A*-module sera , à moins d'une précision contraire, indifféremment un module à gauche, à droite ou à droite et à gauche.

1- Modules libres

Rappelons tout d'abord qu'un *A*-module *M* est dit de *type fini* s'il admet une famille génératrice finie.

Par exemple, la famille $\{-2,2\}$ engendre le $\mathbf{Z}$-module $M=\{2k,\ k\in \mathbf{Z}\}$.
Remarquons que l'élément {2} suffit à engendrer *M*.

Ceci nous amène également à rappeler qu'une famille $(e_i)_{i\in I}$ (avec *I* un ensemble quelconque d'indices, fini ou non) est une *base du A-module M* si la famille $(e_i)_{i\in I}$ est libre et engendre *M*.

Ainsi {2} est une base du module *M* précédemment défini.

Définissons également la notion plus précise de *A-module libre* :
un *A*-module *M* est dit *libre* si il admet une base.
Si cette base est finie, on appelle *rang de M* et on note *rg M* son cardinal.

C'est donc le cas de notre module *M*, qui est libre de rang 1.

L'exemple précédent nous montre que *M* est un $\mathbf{Z}$-module libre de base {2}.
Nous voyons également que pour tout n entier naturel, A^n est un *A*-module libre de rang *n*.
Mais un module libre n'a pas forcément une base finie : ainsi le $\mathbf{R}$-module $\mathbf{R}[X]$ est libre de base $\{1,X,X^2,...,X^n,...\}$ dénombrable mais non finie.
L'espace $\mathbf{R}[X]$ est par ailleurs un espace vectoriel et nous avons le résultat suivant : un module *M* sur un corps *K*, c'est-à-dire un *K*-espace vectoriel, possède toujours une base sur *K*.
La preuve de ce résultat est donnée en annexe.
Notons aussi que tout sous-module d'un module libre est libre.

Nous allons étudier maintenant la proposition suivante, qui s'applique à tout *A*-module.

Proposition : *Tout A-module M est isomorphe à un module quotient d'un A-module libre.*

Preuve : Remarquons que pour qu'une famille $(e_i)_{i\in I}$ d'éléments d'un *A*-module *M* soit génératrice, il faut et il suffit que l'application linéaire $A^{(I)} \to M$ définie par cette famille soit surjective.
Notons $(e_i)_{i\in I}$ est une famille de générateurs de *M* (une telle famille existe toujours, quitte à prendre tous les éléments de *E* pour générateurs), la remarque précédente nous dit alors que $\varphi : A^{(I)} \to M$ est surjective.
Les théorèmes d'isomorphie nous donnent le résultat suivant : $M \cong A^{(I)} / \mathrm{Ker}\ \varphi$.
Comme $A^{(I)}$ est un *A*-module libre, nous avons bien le résultat voulu. □

Remarque : Notons que si *M* est un *A*-module de type fini, *M* est isomorphe à un module quotient d'un *A*-module libre de base finie.

Nous allons enfin introduire la notion suivante :
un *A*-module *M* est dit *stablement libre de type m*, avec *m* un entier naturel, si $M \oplus A^m$ est libre.

Un *A*-module *M* est dit *stablement libre* s'il l'est pour un certain entier naturel *m*.

Par exemple, tout *A*-module libre *M* est stablement libre de type 0.
En effet $M \oplus A^0 \cong M$ est bien libre.

Le $\mathbf{Z}$-module $\mathbf{Z}$ est également stablement libre, de type *k* avec *k* un entier naturel quelconque. En effet $\mathbf{Z} \oplus \mathbf{Z}^k \cong \mathbf{Z}^{k+1}$, qui est bien évidemment libre.

2- Modules projectifs

Nous nous attacherons ici à, dans un premier temps, définir la notion de module projectif. Nous étudierons ensuite des caractérisations plus « pratiques » de ces modules que la définition première.

Tout au long de cette partie, nous noterons A un anneau quelconque.

Le A-module M est dit *projectif* si pour toute suite exacte $0 \to F' \to F \to F'' \to 0$ de A-modules, la suite $0 \to \mathrm{Hom}_A(P, F') \to \mathrm{Hom}_A(P, F) \to \mathrm{Hom}_A(P, F'') \to 0$ est exacte.
Ceci en notant $\mathrm{Hom}_{\mathrm{A}}(P, F)$ l'ensemble des homomorphismes du A-module P vers le A-module F.

Notons immédiatement que l'on a la proposition suivante pour des A-modules somme directe d'une famille de A-modules :

Proposition : *Pour qu'un A-module P somme directe d'une famille $(M_i)_{i\in I}$ de A-modules soit projectif, il faut et il suffit que chaque M_i soit projectif.*

Preuve : Ce résultat provient de la définition, de l'identification $\bigoplus_{i\in I} M_i \cong \prod_{i\in I} M_i$ et de la proposition vue page 6. ☐

Mais cette définition ne paraît pas être des plus simples, et il semble bien difficile de s'en servir pour prouver qu'un A-module P est projectif.
La proposition suivante va nous donner d'autres définitions équivalentes des modules projectifs, pour certaines bien plus pratiques.

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

i. *P est projectif.*

ii. *Pour tout homomorphisme surjectif* $u : E \to F$ *de A-modules et pour tout homomorphisme* $f : P \to F$ *il existe un homomorphisme* $g : P \to E$ *tel que* $f \equiv u \circ g$ *(on dit que f se relève en un homorphisme de P dans E).*

iii. *Toute suite exacte* $0 \to E' \to E \xrightarrow{v} P \to 0$ *de A-modules est scindée (et donc P est isomorphe à un facteur direct dans E).*

iv. *P est isomorphe à un facteur direct d'un A-module libre.*

Preuve : $i \Rightarrow ii$ Soit $E' = \mathrm{Ker}\, u$. Considérons la suite exacte $0 \to E' \to E \xrightarrow{u} E'' \to 0$. Remarquons que *ii* équivaut à $\mathrm{Hom}_A(Id_P, u) : \mathrm{Hom}_A(P, E) \to \mathrm{Hom}_A(P, E'')$ est surjectif. Or ceci est vrai car *P* est projectif (d'après la définition donnée à la page 15).

$ii \Rightarrow iii$ Appliquons *ii* à $v : E \to P$ *et à* $Id_P : P \to P$: il existe $g : P \to E$ un homomorphisme tel que $v \circ g \equiv Id_p$. g est une section linéaire associée à v donc la suite exacte $0 \to E' \to E \xrightarrow{v} P \to 0$ est scindée.

$iii \Rightarrow iv$ De la proposition page 8, pour tout *A*-module *M* de *A* il existe *L* un *A*-module libre tel que la suite $0 \to R \to L \to M \to 0$ soit exacte (on sait que *M* est isomorphe à un module quotient L/R où *L* est un module libre).
En prenant *M*=*P* en appliquant *iv* nous obtenons le résultat.

$iv \Rightarrow i$ Il existe *L* un *A*-module libre et *F* un *A*-module tel que $P \oplus F \cong L$.
Or *L* est libre donc projectif (ce résultat sera prouvé page 17), ce qui implique avec la proposition donnée page 15 que *P* et *F* sont projectifs. ☐

Remarque: Avec la caractérisation *iv*, tout module stablement libre est projectif.
La réciproque n'est pas vraie car la définition d'un module stablement libre nous restreint à un entier naturel *m* fini.

Corollaire : *Tout module libre est projectif.*

Preuve : Prenons *P* un module libre et conservons les mêmes notations que dans la proposition précédente, dans *ii*.
Notons $(e_i)_{i \in I}$ une base de *P*, $f(e_i) = f_i$ pour tout i et g_i tels que $u(e_i) = g_i$ pour tout i (ceci est possible car *u* est surjective).
Nous définissons un homomorphisme *g* de *P* dans *E* par $g(e_i) = g_i$ pour tout i. Celui-ci vérifie bien la relation $f \equiv u \circ g$, et donc *P* est projectif. ☐

Corollaire: *Astuce d'Eilenberg*

Si P est un A-module projectif, il existe un A-module libre L tel que $P \oplus L \cong L$.

Preuve: Avec la proposition précédente, dans *iv*, il existe un *A*-module *M* tel que $E = P \oplus M$ soit libre.

Nous prenons alors $L = E \oplus E \oplus E \oplus ...$ qui est libre. Il vient que:

$$P \oplus L \cong P \oplus (M \oplus P) \oplus (M \oplus P) \oplus ...$$

$$\text{Soit } P \oplus L \cong (P \oplus M) \oplus (P \oplus M) \oplus ... \cong E \oplus E \oplus ... \cong L \text{ . } \square$$

Nous allons nous attacher ici à donner divers exemples de modules projectifs ou non.

Nous avons vu que tout module libre est projectif mais la réciproque est fausse (notons que si ce n'était pas le cas, la conjecture de Serre n'aurait pas lieu d'être). Considérons pas exemple $A = \mathrm{M}_2(\mathbf{R})$, l'anneau des matrices 2×2 à coefficients dans $\mathbf{R}$.

Soit $M = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix},\ (\alpha, \beta) \in \mathbf{R}^2 \right\}$. *M* est un *A*-module à droite.

Si nous notons $N = \left\{ \begin{pmatrix} 0 & 0 \\ \gamma & \delta \end{pmatrix},\ (\gamma, \delta) \in \mathbf{R}^2 \right\}$, nous avons $M \oplus N = A$. *M* est alors bien un module projectif dans *A*.

Cependant *M* n'est pas libre. Nous avons $\dim_{\mathbf{R}} A = 4$. Or si *L* était un *A*-module libre, nous aurions

$$\dim_{\mathbf{R}} L = \dim_A L \times \dim_{\mathbf{R}} A$$

$$\text{soit } \dim_{\mathbf{R}} L = \dim_A L \times 4 \text{ .}$$

Mais comme $\dim_{\mathbf{R}} M = 2$, ceci est impossible et *M* n'est pas libre.

Pour le moment nous avons cité uniquement des exemples de modules projectifs. Toutefois tous les modules ne sont pas projectifs. Ainsi le $\mathbf{Z}$-module $\mathbf{Z}/2\mathbf{Z}$ n'est pas projectif.

En effet nous avons vu page 7 que la suite exacte

$$0 \to \mathbf{Z}/2\mathbf{Z} \xrightarrow{f} \mathbf{Z}/4\mathbf{Z} \xrightarrow{g} \mathbf{Z}/2\mathbf{Z} \to O$$

n'est pas scindée. Le *iv* de la proposition nous dit que $\mathbf{Z}/2\mathbf{Z}$ n'est pas projectif.

Nous avons aussi vu que $\underset{i\in I}{\oplus} P_i$ était projectif si et seulement si chaque P_i était projectif. Mais il n'y a pas de proposition équivalente pour le produit direct des P_i, $i \in I$.
Montrons en effet que, bien que $\mathbf{Z}$ soit un $\mathbf{Z}$-module projectif (ceci car c'est un module libre), le $\mathbf{Z}$-module $M = \mathbf{Z}\times\mathbf{Z}\times\mathbf{Z}\times\ldots$ n'est pas projectif.

Afin de vérifier que M n'est pas projectif, nous devons utiliser le fait que tout sous-groupe d'un groupe abélien libre est libre et démontrer le lemme suivant :

Lemme : *Soit* $P = \mathbf{Z}\oplus\mathbf{Z}\oplus\mathbf{Z}\oplus\ldots$ *Alors* $\mathrm{Hom}_{\mathbf{Z}}\left(M/P, \mathbf{Z}\right) = \{0\}$.

Preuve : Soit f un homomorphisme de M dans $\mathbf{Z}$ tel que $f(P)=0$ (c'est-à-dire tel que f passe au quotient).
Considérons les deux sous-groupes suivants de M :

$$B = \left\{ \left(2^n b_n\right)_{n\in\mathbb{N}} \ ,\ b_n \in \mathbf{Z}\ \forall n \in \mathbb{N} \right\}$$

$$\text{et}\, C = \left\{ \left(3^n c_n\right)_{n\in\mathbb{N}} \ ,\ c_n \in \mathbf{Z}\ \forall n \in \mathbb{N} \right\}.$$

Il est clair que

$$B + C = M\ .$$

Soit b un élément de B. On écrit

$$b = \left(2b_1, \ldots, 2^{n-1} b_{n-1}, 0, 0, \ldots\right) + 2^n m,\ m \in M,\ \forall n \in \mathbb{N}\ .$$

Comme $f(P)=0$, on a

$$f\left(b\right) = 2^n f\left(m\right), \forall n \in \mathbb{N}\ .$$

Soit encore $f\left(b\right) \in 2^n \mathbf{Z}\ \forall n \in \mathbb{N}$, c'est-à-dire

$$f(b)=0.$$

Nous avons déjà montré que $f(B)=0$, nous montrons de même que $f(C)=0$. Il en résulte que

$$f(M)=f(B)+f(C)=0.$$

Le résultat voulu est démontré. $\square$

Supposons par l'absurde que M soit projectif.
D'après l'astuce d'Eilenberg, il existe L un $\mathbf{Z}$-module libre de base $\left(e_i\right)_{i\in I}$ tel que

$$M \oplus L \cong L$$

D'où $M \subseteq L$.

Vu que $P = \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z} \oplus ...$ est dénombrable et que l'on a $P \subset M \subseteq L$, nous pouvons écrire $I = I_1 \cup I_2$ où I_1 est dénombrable, tel que $P \subseteq F_1 = \left\{ \sum_{i \in I_1} z_i e_i ,\ z_i \in \mathbf{Z}\ \forall i \in I \right\}$.

Nous avons $M \not\subset F_1$ car F_1 est dénombrable mais pas *M*. Notons *j* un indice de l'ensemble I_2 tel que l'élément e_j soit un élément de *M* (un tel *j* existe, sinon on aurait $M = F_1$).

Soit $f : L \to \mathbf{Z}$ la projection de *L* sur $e_j \mathbf{Z}$.

Par définition de *f*,

$$f(M) \neq 0$$

ce qui est en contradiction avec le lemme précédent.

Nous en déduisons donc que *M* n'est pas un module projectif.

Après ces quelques exemples, nous allons nous intéresser à une proposition plus spécifique aux modules projectifs de type fini :

Proposition : *Pour qu'un A-module soit projectif et de type fini, il faut et il suffit qu'il soit facteur direct d'un A-module libre ayant une base finie.*

Preuve : Cette condition est clairement suffisante.

Inversement, un module projectif de type fini *E* est isomorphe à un quotient d'un module libre *F* ayant une base finie (d'après la remarque page 8). Avec le *iii* de la proposition précédente, *E* est isomorphe à un facteur direct de *F*. □

Partie III- La conjecture de Serre

Après l'étude des notions de modules libres et projectifs, après divers rappels, nous sommes à même de nous consacrer à l'étude de la conjecture de Serre.
Après un rappel historique (21 ans ont étés nécessaires avant de prouver la conjecture de Serre), nous étudierons deux preuves dans des cas particuliers, puis un contre-exemple qui illustrera l'importance de l'hypothèse de considérer un anneau de base qui soit un corps.

1- Historique

En 1955, dans son article Faisceaux algébriques cohérents, le mathématicien Jean-Pierre Serre a écrit ces quelques mots, en notant K un corps :

> Signalons que , lorsque V = K^r (auquel cas A = $K[X_1, \ldots, X_r]$) , on ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libres

(« Signalons que, lorsque […] $A = K[X_1, X_2, ..., X_n]$, on ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libres »)

Cette phrase devint célèbre sous le nom de conjecture de Serre. Bien que prouvée depuis, elle a conservé cette appellation ambiguë.
Entre l'énoncé de la conjecture en 1955 et sa preuve en 1976, les résultats ont fusé de toutes parts, portant sur des preuves dans quelques cas particuliers, des contre-exemples sous des hypothèses restrictives, comme nous allons le découvrir ici.

Nous noterons ici K un corps (sauf indication contraire explicite), $A = K[X_1, X_2, ..., X_n]$ et P un A-module projectif de type fini.
Nous étudierons par la suite les résultats signalés en gras dans l'historique.

- 1955- Jean-Pierre Serre énonce la conjecture.

Les preuves dans les cas particuliers d'un module projectif de rang un et dans **le cas *n*=1** (A=$K[X]$) sont les premières données.

- 1956- Les mathématiciens Cartan et Eilenberg prouvent le résultat dans **le cas où *P* est un module gradué respectant la structure graduée naturelle de *A*.**

- 1957 / 1958- Serre montre que l'on doit avoir, pour que le résultat soit vérifié,

$$P \cong A^r \oplus Q \text{ où } \mathrm{rg}(Q) \leq n.$$

Ceci réduit le problème au cas où $\mathrm{rg}(P) \leq n$.
Le mathématicien Seshadri montre que la conjecture est vraie pour n=2.
Le théorème de Hilbert-Serre implique que P doit être stablement libre, c'est-à-dire que l'on doit avoir $P \oplus A^r \cong A^s$ pour certains r et s éléments de $\mathbb{N} \setminus \{0\}$.
Le problème est donc transformé : un module stablement libre sur A est-il toujours libre ?

- 1963- Bass démontre que tout module projectif n'étant pas de type fini est effectivement libre.

- 1964- Bass prouve que P est libre si $\mathrm{rg}(P) > n$.

- 1969- Pour résoudre le cas n=3, Bass démontre qu'il suffirait de montrer que tout module projectif de type fini de rang 2 est libre sur $K[X_1, X_2, X_3]$.

- 1970- Segre publie un article où il donne une preuve du fait qu'un module projectif de rang 2 ne peut être libre sur $K[X_1, X_2, X_3]$. Ce résultat est très contesté, notamment par Abhyankar.

- 1971- Les mathématiciens Ojanguren et Sridharan prouvent ensemble que **la conjecture est fausse pour $n \geq 2$ si on prend seulement *K* un corps gauche et non un corps.**

- 1974- Murphy et Towber démontrent que la conjecture est vraie pour n=3 en prenant K un corps algébriquement clos. Ceci clos la discussion à propos du résultat de Segre publié en 1970, qui s'avère faux.

Si K est algébriquement clos et si rg(P)=n, Roitman montre que P est libre. L'hypothèse sera même prolongée un peu plus tard à K un corps infini.
A.Suslin et L.N.Vaserstein prouvent que P est toujours libre dans les cas suivants :

1. $\mathrm{rg}(P) \geq \frac{n}{2} + 1$
2. n=3,4, ou 5
3. n=6 et K est un corps fini

- 1976- <u>En janvier, D.Quillen et A.Suslin démontrent en même temps que la conjecture de Serre est vraie dans le cas général, pour tout *n* et tout corps *K*.</u>

2- Cas d'une variable

Dans le cas où K est un corps, l'anneau $K[X]$ est principal et intègre. Il est possible de montrer facilement que la conjecture de Serre est vérifiée dans ce cas.
Nous verrons ici que la conjecture de Serre est également vérifiée dans la cas d'une variable lorsque K est un corps gauche.
Rappelons qu'un *corps gauche* est un anneau dont tous les éléments sont inversibles sauf 0, mais qui n'est pas commutatif, contrairement à un corps.

Commençons par introduire une nouvelle notion : celle d'*anneau héréditaire*.
Un anneau A est dit *héréditaire* à gauche si tout idéal à gauche de A est un A-module projectif.

Par exemple, tout corps est un anneau héréditaire. En effet tout idéal sur un corps est également un module sur ce corps. Il admet par conséquent une base (la preuve en est donnée en annexe), et en tant que module libre il est projectif.

La preuve de la conjecture de Serre dans ce cas particulier découle d'un corollaire du théorème suivant :

Théorème de Kaplansky :
Soit A un anneau héréditaire à gauche. Alors tout sous-module M d'un A-module libre de la forme $F = \bigoplus_{\alpha\in\Lambda} Ae_\alpha$ *est isomorphe à une somme directe d'idéaux à gauche de A.*
En particulier, M est projectif.

Preuve : Ordonnons tout d'abord l'ensemble Λ des indices de la base de F.
Nous posons ensuite les notations suivantes :

F_α est le sous-module engendré par $\{e_\beta,\ \beta < \alpha\}$

$\bar{F}_\alpha$ est le sous-module engendré par $\{e_\beta,\ \beta \le \alpha\}$

$$M_\alpha = M \cap F_\alpha$$
$$\bar{M}_\alpha = M \cap \bar{F}_\alpha$$

Nous avons

$$\bar{M}_\alpha / M_\alpha \subset \bar{F}_\alpha / F_\alpha \cong Ae_\alpha .$$

Le quotient $\bar{M}_\alpha / M_\alpha$ est isomorphe à un idéal à gauche de A. Comme A est un anneau héréditaire, cet idéal est projectif. Donc $\bar{M}_\alpha / M_\alpha$ est projectif.

Considérons la suite exacte $0 \to M_\alpha \to \bar{M}_\alpha \to \bar{M}_\alpha / M_\alpha \to 0$. Sachant que $\bar{M}_\alpha / M_\alpha$ est un module projectif, cette suite exacte est scindée. Nous savons alors que l'on peut écrire

$$\bar{M}_\alpha = M_\alpha \oplus I_\alpha$$

où I_α est isomorphe à $\bar{M}_\alpha / M_\alpha$, idéal à gauche de *A*.

Reste à montrer que $M = \bigoplus_{\alpha \in \Lambda} I_\alpha$.

i. Montrons que la somme est directe.

Supposons que nous ayons $x_1 + x_2 + ... + x_n = 0$, avec x_i élément de I_{α_i} pour tout *i* et $I_{\alpha_i} \subset F_{a_i}$.
Quitte à réordonner, nous pouvons de plus supposer que $\alpha_1 < \alpha_2 < ... < \alpha_n$.
Nous avons alors $\underbrace{x_1 + x_2 + ... + x_{n-1}}_{\in F_{\alpha_n}} = \underbrace{-x_n}_{\in I_{\alpha_n}}$.
Mais comme $F_{\alpha_n} \cap I_{\alpha_n} = \{0\}$, il vient que $x_n = 0$.
En répétant cette opération, nous en déduisons que $x_{n-1} = ... = x_2 = x_1 = 0$.
La somme est donc bien directe.

ii. Montrons maintenant que $M = \bigoplus_{\alpha \in \Lambda} I_\alpha$.

Supposons par l'absurde que $\sum_{\alpha \in \Lambda} I_\alpha \varnothing M$.
Soit β le plus petit indice tel qu'il existe $\bar{a}$ élément de $\bar{M}_\beta \setminus \sum_{\alpha \in \Lambda} I_\alpha$.
Posons alors $\bar{a} = a + x$, avec *a* élément de M_β et *x* élément de I_β ce qui est possible car nous avons $\bar{M}_\beta = M_\beta \oplus I_\beta$.
Il existe $\gamma < \beta$ tel que *a* soit élément de $\bar{M}_\gamma$ (par définitions de M_β et $\bar{M}_\gamma$).
Le choix de β minimal implique que *a* est un élément de $\sum_{\alpha \in \Lambda} I_\alpha$.
Mais alors $\bar{a} = a + x$ est un élément de $\sum_{\alpha \in \Lambda} I_\alpha$ (car *a* et *x* en font partie), ce qui est en contradiction avec le choix de $\bar{a}$. □

Le corollaire suivant sera essentiel pour prouver le résultat dans notre cas :

> **Corollaire :** *Si A est un anneau dont tous les idéaux à gauche sont libres, alors tout sous-module d'un A-module libre est libre.*
> *En particulier, tout A-module projectif est libre.*

Preuve : Tous les idéaux à gauche de *A* sont libres donc projectifs, c'est-à-dire que *A* est un anneau héréditaire à gauche.

Le théorème de Kaplansky nous dit alors que tout sous-module d'un A-module libre est isomorphe à une somme directe d'idéaux à gauche.
Tous ces idéaux étant libres, le résultat est vérifié.

De plus si P est un A-module projectif, il existe F, F' et L des A-modules tels que L soit libre,

$$P \cong F \text{ et } F \oplus F' = L \ .$$

F est libre car c'est un sous-module du module libre L, donc P est libre (par isomorphie). ☐

Le théorème suivant n'est autre que le résultat de Serre énoncé dans le cas particulier d'une seule variable.

Théorème : *Pour tout corps gauche K, tout module projectif sur $A=K[X]$ est libre.*

Preuve : Soit I un idéal à gauche de A.
L'anneau A étant principal, il existe un polynôme f de degré minimal dans A tel que $I=A.f$.
L'anneau A est intègre, il n'a pas de diviseur de zéro. Nous voyons donc que I est isomorphe à A en tant que A-modules.
En appliquant le corollaire précédent (car tout idéal à gauche est libre, d'après ce qui précède), il vient que tout A-module projectif est libre. ☐

La conjecture de Serre est donc prouvée dans le cas où l'on ne considère qu'une variable, et ce même sous l'hypothèse moins forte de K un corps gauche.

3- Cas d’un module gradué

Nous allons montrer dans cette partie que si *P* est un module projectif gradué sur l’anneau *A* défini par $A = K\left[X_1, X_2, ..., X_n\right]$, *P* est libre sur *A*.
La conjecture de Serre est donc vérifiée dans le cas de modules gradués.

Avant toute autre chose, définissons la notion suivante :

Un anneau *A* est dit *gradué* si il existe une décomposition de *A* en somme directe de groupes additifs $A = A_0 \oplus A_1 \oplus ...$ tels que pour tout couple (*m*,*n*) de $\mathbb{N}^2$ on ait $A_m A_n \subseteq A_{m+n}$.
Pour tout *i* entier naturel, A_i est appelée *la composante homogène de A de degré i*.

Par exemple, considérons l’anneau $A = A_0\left[X_1, X_2, ..., X_d\right]$, avec A_0 un corps.
Notons A_i l’ensemble des polynômes homogènes en $X_1, X_2, ..., X_d$ de degré *i*.
Nous avons alors clairement $A = A_0 \oplus A_1 \oplus ...$
De plus, pour tout couple (*m*,*n*) de $\mathbb{N}^2$, pour tout P_m élément de A_m et pour tout P_n élément de A_n, il est évident que $\deg\left(P_m P_n\right) = \deg\left(P_m\right) + \deg\left(P_n\right) = m + n$.
C’est-à-dire que nous avons bien $A_m A_n \subseteq A_{m+n}$, nous avons même en fait l’égalité.

Remarque : Si *A* est un anneau gradué, A_0 est un sous-groupe additif de *A* stable pour la multiplication.

En effet A_0 est par construction un sous-groupe additif de *A*. De plus si *a* et *a’* sont deux éléments de l’anneau A_0, nous avons $aa' \in A_0 A_0 \subseteq A_{0+0} = A_0$. Donc A_0 est bien stable pour la multiplication.

Lemme : *Si A est un anneau gradué, l'élément* 1_A *, neutre pour la multiplication dans l'anneau A, est contenu dans* A_0 .

Preuve : Supposons bien sur que A n'est pas réduit à l'élément nul.
Ecrivons, vu que $A = A_0 \oplus A_1 \oplus \ldots$, $1_A = a_i + a_{i+1} + \ldots$ avec $a_j \in A_j$ pour tout j et a_i non nul.

Nous savons que $1_A{}^2 = 1_A$, ce qui implique que

$1_A = (a_i + a_{i+1} + \ldots) = a_i + \ldots$ $\qquad$ $1_A = (a_i + a_{i+1} + \ldots)^2 = a_i{}^2 + \ldots$

Comme $a_i{}^2 \in A_{2i}$ et $a_i \in A_i$, il faut donc avoir $A_{2i} = A_i$ c'est-à-dire 2i=i.
Il est donc immédiat que i=0.

De plus pour tout x élément de A_i , avec i quelconque dans $\mathbb{N}$, nous avons les équations suivantes :

$$\underbrace{x}_{\in A_i} = 1_A \cdot x = \underbrace{a_0 \cdot x}_{\in A_i} + \underbrace{a_1 \cdot x}_{\in A_{i+1}} + \ldots$$

$$\underbrace{x}_{\in A_i} = x \cdot 1_A = \underbrace{x \cdot a_0}_{\in A_i} + \underbrace{x \cdot a_1}_{\in A_{i+1}} + \ldots$$

Par comparaison des degrés, il vient que $a_0 \cdot x = x = x \cdot a_0$.
Donc a_0 est un neutre pour la multiplication sur A et l'on a

$$1_A = a_0 \in A_0 . \qquad \square$$

Conséquence : *Le groupe* A_0 *, muni de la structure d'anneau induite par A est un sous-anneau de A.*

Preuve : Ceci provient immédiatement de la remarque et du lemme. $\square$

Avant de nous lancer dans la preuve proprement dite du résultat de Serre, nous allons définir de nouveaux objets essentiels ici.

Définition : Soit A un anneau gradué. Un A-module M est dit *gradué* s'il existe une décomposition de M en somme directe de groupes additifs $M = \bigoplus_{j\in\mathbf{Z}} M_j$ tels que pour tout couple (i,j) de $\mathbb{Z}\times\mathbf{Z}$, on ait $A_i M_j \subseteq M_{i+j}$.

Remarquons que M peut avoir des composantes de degré négatif.

Définition : Le A-module gradué M est dit *borné inférieurement* s'il existe un r élément de $\mathbb{Z}$ tel que $M_j = \{0\}$ dès que $j < r$.

La proposition suivante nous donne un cas particulier de modules bornés inférieurement.

Proposition 1 : *Tout A-module gradué M de type fini est borné inférieurement.*

Preuve : Soient $m_1, m_2, ..., m_k$ les générateurs de M.
Choisissons r un entier relatif tel que les composantes homogènes contenant les m_i soient de degrés supérieurs ou égaux à r.
Alors $M = \sum_{i=1}^{k} Am_i \subseteq \sum_{j\geq r} M_j$, donc M est borné inférieurement. $\square$

Remarque : Dans le cas où K est un corps et $A = K[X_1, X_2, ..., X_n]$, tout A-module est non seulement gradué mais aussi de type fini. Nous pourrons donc nous restreindre à l'étude de modules bornés inférieurement.

Nous allons poser ici différentes notations :

- Pour tout anneau gradué A, posons $A^+ = A_1 \oplus A_2 \oplus ...$

Le groupe additif A^+ est un idéal bilatère gradué de A (par construction des A_i)

- Pour tout A-module gradué M posons $\overline{M} = M / A^+M \cong A / A^+ \otimes_A M$.

Le module $\overline{M}$ est un module gradué sur A_0 .

Les propositions suivantes vont nous permettre de prouver un théorème qui nous conduira à la preuve souhaitée.

Proposition 2 : *Pour tout A-module gradué M borné inférieurement,* $\overline{M}$ *={0} implique que M={0}.*

Preuve : Supposons que $M \neq \{0\}$.

Nous écrivons alors $M = M_r \oplus M_{r+1} \oplus ...$ où $M_r \neq \{0\}$.

En conservant ces notations $A^+M \subseteq M_{r+1} \oplus M_{r+2} \oplus ...$

Le fait que $\overline{M}$ soit égal à $\{0\}$ implique alors que $M = A^+M$ car $\overline{M} = M/A^+M$.

Alors $M_r = \{0\}$, ce qui est en contradiction avec l'hypothèse.

Donc *M*={0}. ☐

Proposition 3 : *Soit A un anneau, soient P et Q deux A-modules gradués de type fini, avec P projectif.*

Soit $\gamma : Q \to P$ *un A-homomorphisme préservant les degrés (c'est-à-dire* $\gamma(Q_k) \subset P_k$*, pour tout k élément de* $\mathbf{Z}$*).*

Alors γ *est un isomorphisme si et seulement si* $\overline{\gamma} : \overline{Q} \to \overline{P}$ *est un isomorphisme.*

Preuve : Nous n'utiliserons dans la suite que la condition suffisante, nous nous contenterons donc de montrer celle-ci.

Nous allons poser les notations suivantes :

$$K = \mathrm{Ker}\ \gamma$$

$$C = \mathrm{coker}\ \gamma = P/\mathrm{Im}\,\gamma = P/\gamma(Q)$$

Remarquons que *K* et *C* sont des *A*-modules gradués. En effet, *K* est un sous-module du module gradué *Q* et *C* est isomorphe à un sous-module du module gradué *P*.

De même nous noterons :

$$\overline{K} = \mathrm{Ker}\ \overline{\gamma}$$

$$\overline{C} = \mathrm{coker}\ \overline{\gamma} = \overline{P}/\mathrm{Im}\,\overline{\gamma}$$

Comme $\overline{\gamma}$ est un isomorphisme (par hypothèse), il vient que $\overline{K} = \{0\}$ et que $\overline{C} = \{0\}$.

i. Montrons que γ est surjective.

Comme $C \subset P$, *C* est un module gradué de type fini.

Avec la proposition 1, *C* est borné inférieurement.

Avec la proposition 2 et vu que $\overline{C} = \{0\}$, il vient que $C = \{0\}$.

Donc γ est bien surjective.

ii. Montrons que γ est injective.

De même en utilisant le fait que $\overline{K} = \{0\}$ nous montrons que $K = \{0\}$.

Donc γ est bien injective.

Donc γ est bien un isomorphisme. $\square$

Théorème : *Soit P un module projectif gradué sur l'anneau gradué*

$$A = A_0 \oplus A_1 \oplus ...$$

Il existe un isomorphisme de A-modules gradués $A \otimes_{A_0} \overline{P} \cong P$.

Remarque : Le A_0 -module $\overline{P}$ est gradué. Le produit tensoriel $A \otimes_{A_0} \overline{P}$ est donc gradué de la manière usuelle :

$$\left(A \otimes_{A_0} \overline{P}\right)_k = \sum_{\substack{i \geq 0 \\ j \in \mathbb{Z}, i+j=k}} A_i \otimes_{A_0} \overline{P}_j$$

Preuve : Considérons la projection $f : P \to \overline{P}$.

Le module P est un module projectif, il en est donc de même pour $\overline{P}$ (qui est un A_0 -module).

En effet, la projection f vérifie $\operatorname{Ker} f \oplus \operatorname{Im} f = P \cong F$ où F est un A-module tel qu'il existe deux A-modules F' et L, avec L un module libre, tels que $F \oplus F' = L$ (voir page 10).

Ainsi $\operatorname{Im} f \oplus (\operatorname{Ker} f \oplus F') \cong L$, ce qui implique que $\operatorname{Im} f = \overline{P}$ est un module projectif (il est isomorphe à un facteur direct d'un module libre).

L'homomorphisme f est bien évidemment un épimorphisme.

En considérant $Id_{\overline{P}} : \overline{P} \to \overline{P}$ et en utilisant la proposition de la page 10 qui caractérise les modules projectifs, nous voyons qu'il existe un homomorphisme $g : \overline{P} \to P$ tel que $f \circ g \equiv Id_{\overline{P}}$.

Comme f est un homomorphisme préservant les degrés, nous pouvons supposer que g préserve également les degrés, quitte à modifier quelque peu g.

Nous avons donc vu que g induit un A-homomorphisme préservant les degrés :

$$\gamma : Q = A \otimes_{A_0} \overline{P} \to P$$

L'application $\overline{\gamma} : \overline{Q} \to \overline{P}$ est un isomorphisme.

(En effet $\overline{Q} = A_0 \otimes_{A_0} \overline{P} \cong \overline{P}$ à été vu en rappels)

La proposition 3 nous dit alors que γ est un isomorphisme. Nous avons montré que $A \otimes_{A_0} \overline{P} \cong P$. $\square$

De ce théorème, nous tirons le corollaire suivant qui prouve le résultat dans le cas d'un anneau gradué :

Corollaire : *Soit* $A = A_0[X_1, X_2, ..., X_n]$ *un anneau gradué, en considérant* A_0 *de degré 0 et chaque* $\{X_i\}$ *de degré 1. Soit P un A-module projectif.*
Si tout module projectif de type fini sur A_0 *est libre (par exemple,* A_0 *est un corps) alors P est libre.*

Remarque : Nous savons que si A_0 est un corps, tout module sur A_0 est libre, en particulier tout module projectif de type fini est libre sur A_0 .

Preuve : Soit *P* un module gradué sur $A = A_0[X_1, X_2, ..., X_n]$. Soit $\overline{P}$ le A_0-module associé à *P*, défini comme précédemment.
Nous savons que $\overline{P}$ est un A_0-module gradué. Si A_0 est un corps, $\overline{P}$ est libre.
Or le théorème précédent nous dit que $A \otimes_{A_0} \overline{P} \cong P$, nous en déduisons donc que *P* est libre. $\square$

La conjecture de Serre est donc vérifiée dans le cas particulier d'un anneau gradué.

4- Contre-exemple d’un corps gauche

Nous avons étudié jusqu’ici des preuves de la conjecture de Serre, et nous avons vu qu’il était possible dans le cas particulier d’une variable de se limiter à un corps gauche.
Rappelons que nous nommons ici *corps gauche* un anneau dont tous les éléments sont inversibles sauf zéro mais non commutatif.
Toutefois, hors de ce contexte particulier, l’hypothèse du corps devient essentielle et la restriction au corps gauche n’est plus possible, comme nous allons le voir dans cette partie.

Théorème d’Ojanguren et de Sridharan :

Soit K un corps gauche qui ne soit pas un corps, soit $A = K[X,Y]$.

Il existe un idéal à droite P de A tel que l’on ait $P \oplus A \cong A^2$ *(c’est-à-dire que P est stablement libre de type 1, engendré par deux éléments), mais P n’est pas libre.*

Remarques : • L’idéal *P* est , en lui attribuant la structure associée à *A*, un *A*-module.
• Comme nous avons la relation $P \oplus A \cong A^2$, le module *P* considéré est stablement libre donc projectif.
• Le module considéré est engendré par deux éléments. En effet, il ne peut être engendré par un seul élément, sinon il serait isomorphe à *A*, et donc libre.

Preuve : La preuve du théorème se fait en plusieurs étapes :

i. Propriétés essentielles de *K*
ii. Détermination de *P*
iii. Lemme et sa preuve
iv. Preuve du théorème

i. Propriétés essentielles de *K*

Le corps gauche *K* a certaines propriétés que nous utiliserons par la suite. Nous allons nous attacher ici à les citer et bien sur à les prouver.

Propriété 1 : *Le corps gauche K est intègre.*

Preuve : Soient *a* et *b* deux éléments de *K* tels que *ab*=0.
Supposons par l'absurde que *a* et *b* soient non nuls. Comme *K* est un corps gauche, ceci implique que *a* et *b* sont inversibles.
Le fait que *ab* soit nul implique que :

$$(ab)b^{-1} = 0 \cdot b^{-1} = 0$$

Mais alors :

$$a=0$$

Ceci est en contradiction avec l'hypothèse, *K* est bien intègre. □

Propriété 2 : *Il existe a et b éléments de K, non nuls, tels que u=ab-ba soit inversible.*

Preuve : *K* est un corps gauche qui n'est pas un corps, il existe donc deux éléments au moins *a* et *b* , tous deux non nuls, ne commutant pas.
Mais alors *u=ab-ba* n'est pas nul, c'est-à-dire *u* est inversible vu que *K* est un corps gauche. □

Propriété 3 : *Pour tout couple* (*m*,*n*) *d'éléments de* $\mathbb{N}^2$, K^m *est isomorphe à* K^n *si et seulement si m=n.*

Preuve : Il est clair que si *m=n*, les deux modules K^m et K^n sont égaux, donc isomorphes.
Réciproquement, nous savons que ces deux *K*-modules admettent chacun une base sur *K* (La preuve de ce résultat est donnée en annexe). Il est évident que $\operatorname{rg} K^m = m$ et $\operatorname{rg} K^n = n$. L'isomorphie entre les deux modules implique donc que *m=n*. □

ii. Détermination de *P*

Choisissons *a* et *b* comme dans la propriété 2 de la page précédente.
Nous nommerons *u* l'élément *ab-ba,* qui est inversible.

Dans cette partie, nous allons étudier le morphisme $\Phi : A^2 \to A$ dont la matrice dans la base (e_1, e_2) de A^2 est la suivante :

$$\begin{pmatrix} x+a & -(y+b) \end{pmatrix}$$

Nous avons alors

$$\Phi(e_1) = x+a$$
$$\Phi(e_2) = -(y+b).$$

Montrons que Φ est surjective.
Remarquons tout d'abord que $\Phi\begin{pmatrix} y+b \\ x+a \end{pmatrix} = (x+a)(y+b)-(y+b)(x+a)$

$$\text{Soit } \Phi\begin{pmatrix} y+b \\ x+a \end{pmatrix} = ab-ba = u \; .$$

Posons les notations $v_1 = y+b$ et $v_2 = x+a$.
Soit *v* un élément quelconque de *A*, nous voyons que

$$\Phi\left(v \cdot u^{-1} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \right) = v \cdot u^{-1} \Phi \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

$$\text{D'où } \Phi\left(v \cdot u^{-1} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \right) = v \cdot u^{-1} \cdot u = v$$

Ceci prouve que Φ est surjective.

La surjectivité de Φ nous dit alors que $\mathrm{Im}\,\Phi = A$. Nous avons donc $\mathrm{Ker}\,\Phi \oplus \mathrm{Im}\,\Phi \cong \mathrm{A}^2$.

En posant $P = \mathrm{Ker}\,\Phi$, nous obtenons un *A*-module P tel que $P \oplus A \cong A^2$.

iii. Lemme et sa preuve

Nous noterons désormais *f*, *g*, *h* etc… les éléments de *A*.
De plus si *f* est un élément de *A*, nous notons $\deg f$ le degré total de *f*.
La proposition 1 nous dit que *K* est intègre, donc *A* est également intègre. Si *f* et *g* sont deux éléments de *A*, nous avons alors $\deg fg = \deg f + \deg g$.
Nous utiliserons également la notation $f(0,0)$ pour désigner le terme constant de *f*.

Lemme : *Avec les mêmes notations que celles du théorème :*

i. *P ne contient aucun* $\begin{pmatrix} f_0 \\ g_0 \end{pmatrix}$ non nul tel que $\deg f_0 \leq 1$ et $\deg g_0 \leq 1$.

ii. *P contient un élément* $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix}$ tel que $\deg f_1 = \deg g_1 = 2$ et $f_1(0,0) = 0$.

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

Preuve : i. Considérons un élément $\begin{pmatrix} f_0 \\ g_0 \end{pmatrix}$ de *P* tel que $\deg f_0 \leq 1$ et $\deg g_0 \leq 1$.

Nous noterons :

$$f_0 = c + dx + ey$$
$$g_0 = c' + d'x + e'y$$

Sachant que $P = \operatorname{Ker} \Phi$, il vient que $\Phi\begin{pmatrix} f_0 \\ g_0 \end{pmatrix} = 0$, ce qui équivaut successivement à

$$(x+a) f_0 = (y+b) g_0$$
$$(x+a)(c+dx+ey) = (y+b)(c'+d'x+e'y)$$

$$\begin{cases} d = 0 & \text{termes en } x^2 \\ c + ad = bd' & \text{termes en } x \\ 0 = e' & \text{termes en } y^2 \\ ae = c' + be' & \text{termes en } y \\ e = d' & \text{termes en } xy \\ ac = bc' & \text{termes constants} \end{cases}$$

En résolvant ce système, nous arrivons à la solution unique

$$c = c' = d = d' = e = e' = 0$$

C'est-à-dire $f_0 \equiv 0$ et $g_0 \equiv 0$. Nous avons donc bien démontré le premier point.

ii. Par le même raisonnement, c'est-à-dire en écrivant deux polynômes sous leur forme développée et en résolvant des systèmes d'équations découlant du fait que $P = \operatorname{Ker} \Phi$, nous obtenons les deux polynômes suivants :

$$f_1 = \left(b\left(ab^{-1}u\right)^{-1}\right)x + \left(ab^{-1}u\right)^{-1}xy + \left(a^{-1}ba\left(-u\right)^{-1}\right)y + \left(-u\right)^{-1}y^2$$

$$g_1 = \left(ab^{-1}u\right)^{-1}x^2 + \left(b^{-1}ab\left(ab^{-1}u\right)^{-1}\right)x + \left(-u\right)^{-1}xy + a\left(-u\right)^{-1}y$$

Nous vérifions bien que $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix}$ est un élément de *P* et que l'on a $\deg f_1 = \deg g_1 = 2$ ./

De plus nous avons $f_1(0,0) = 0$.

Il existe bien un élément $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix}$ de *P* ayant les propriétés voulues.

iii. En procédant de même, nous obtenons les deux polynômes suivants :

$$f_2 = v^{-1} + \left(a^{-1}b^{-1}av^{-1} + a^{-1}ba\left(-u\right)^{-1}\right)y + \left(-u\right)^{-1}y^2$$

$$g_2 = b^{-1}av^{-1} + \left(vb\right)^{-1}x + \left(-u\right)^{-1}xy + a\left(-u\right)^{-1}y$$

en posant $v = ab^{-1} - b^{-1}a \neq 0$.

Nous vérifions bien que $\begin{pmatrix} f_2 \\ g_2 \end{pmatrix}$ est un élément de *P* et que nous avons $f_2(0,0) = b^{-1}av^{-1} \neq 0$ (ceci car *K* est intègre et car *a*, *b* et *v* sont non nuls).

Le lemme est donc prouvé. □

iv. Preuve du théorème.

Pour prouver le théorème, il faudrait prouver que P n'est pas libre.
Supposons par l'absurde que P soit libre. Alors P est isomorphe à A^n pour un certain n.
Ceci implique successivement que

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

La propriété 3 nous dit que $n+1=2$, soit $n=1$.
Nous aurions alors $P \cong A$.

Si nous avions $P \cong A$, il existerait $\begin{pmatrix} f \\ g \end{pmatrix}$ élément de P non nul tel que $\begin{pmatrix} f_i \\ g_i \end{pmatrix} = \begin{pmatrix} f \\ g \end{pmatrix} \cdot h_i$, pour i valant 1 ou 2, $\begin{pmatrix} f_1 \\ g_1 \end{pmatrix}$ et $\begin{pmatrix} f_2 \\ g_2 \end{pmatrix}$ étant ceux définis dans le lemme précédent.

Pour i=1, nous aurions $\begin{cases} f_1 = f \cdot h_1 \\ g_1 = g \cdot h_1 \end{cases}$
Ceci impliquerait les égalités suivantes sur les degrés :

$$2 = \deg f_1 = \deg f + \deg h_1$$
$$2 = \deg g_1 = \deg g + \deg h_1$$

Or $\begin{pmatrix} f \\ g \end{pmatrix}$ n'est pas nul, et le *i* du lemme nous dit que nous devons avoir $\deg f \geq 2$ et $\deg g \geq 2$. Ceci implique que $\deg h_1 = 0$, h_1 est une constante.
Comme $2 = \deg f_1 = \deg f \cdot h_1 \neq \deg 0 = -\infty$, nous savons que h_1 est une constant non nulle.

Enfin nous avons vu dans le lemme que $f_1(0,0) = 0 = f(0,0) \cdot h_1$. Comme h_1 n'est pas nulle et que K est intègre, il vient que $f(0,0)$ est nul.

Mais alors pour i=2, nous avons $f_2(0,0) = f(0,0) \cdot h_2(0,0) = 0$ car $f(0,0)$=0. Ceci est en contradiction avec $f_2(0,0) \neq 0$.
Nous ne pouvons donc avoir $P \cong A$. $\square$

Nous avons donc prouvé que le A-module P ainsi déterminé est projectif mais non libre, contre-exemple à la conjecture de Serre dans le cas où l'on considère un corps gauche K qui ne soit pas un corps.

Annexe

Nous allons reprendre ici la preuve de l'existence d'une base de tout module sur un corps gauche ou un corps, qui aurait alourdi inutilement l'exposé.

Théorème : *Soit K un corps gauche, qui soit un corps ou non. Alors tout module sur K admet une base.*

Preuve : Soit *M* un *K*-module non réduit à l'élément nul.
Notons *G* un ensemble de générateurs de *M* sur *K* et *S* un sous-ensemble de *G* dont les éléments sont linéairement indépendants.
Nous allons montrer qu'il existe une base *B* de *M* telle que $S \subset B \subset G$, ce qui est même mieux que le théorème énoncé.

Notons Γ l'ensemble des éléments des sous-ensembles *L* de *G* contenant *S* et dont les éléments sont linéairement indépendants.
L'ensemble Γ est non vide car il contient *S*. Nous savons que Γ est ordonné de manière inductive.
[En effet, si $\{L_i\}_{i\in I}$ est un sous-ensemble de Γ totalement ordonné pour l'inclusion, $\bigcup_{i\in I} L_i$ est également un élément de Γ].
Le lemme de Zorn nous donne alors l'existence d'un élément maximal *B* de Γ. *B* contient en particulier des éléments linéairement indépendants.

Reste à montrer que *B* engendre *M*.
Notons *N* le sous-espace engendré par *B*. Si *N* est différent de *M*, il existe un élément *x* de *G* n'appartenant pas à *N*. Nous allons montrer que $B \cup \{x\}$ ne contient que des éléments indépendants.
[En effet, si nous avions une relation de dépendance linéaire entre les éléments de *B* et *x* de la forme suivante : $\sum_{y\in B} a_y y + bx = 0$, il s'en suivrait que

$$\underbrace{b^{-1}\sum_{y\in B} a_y y}_{\in N} = \underbrace{-x}_{\notin N}$$

(car si *b* est non nul, il est inversible car *K* est un corps gauche), soit *b*=0. Comme les *y* sont tous éléments de *B*, ils sont linéairement indépendants et donc nous avons $a_y = 0$ pour tout *y* de *B*.
Ceci montre que $B \cup \{x\}$ contient uniquement des éléments indépendants.]
Mais alors nous avons construit un nouvel ensemble $B \cup \{x\}$ tel que B Ø $B \cup \{x\} \subset \Gamma$, ce qui est en contradiction avec la maximalité de *B*. Ceci implique que *N*=*M*, et donc *B* est bien une base de *M*.

Le théorème est donc prouvé, que *K* soit un corps gauche ou un corps. □

Bibliographie

- Nicolas BOURBAKI
  Elements de Mathématiques – Algèbre chapitres 1 à 3
  Diffusion TCLS Paris 1970
  Chapitre 2 : p.39, 51, 76 à 95 et 171

- T.Y LAM
  Serre's conjecture
  Lecture notes on mathematics
  Springer-Verlag 1978
  p.5-12 et p.49-58

- T.Y LAM
  Lectures on modules and rings
  Graduate texts in mathematics
  Springer 1999
  p.1-5 et p.21-23

- LAMBEK
  Lectures on rings and modules
  Blaisdell publishing company 1966
  p.84-85

- Serge LANG
  Algebra Second edition
  Addison-Wesley publishing company inc. 1984
  p.60-88, p.92-94, p.101-102, p.255 et p.408-421

- OJANGUREN et SRIDHARAN
  Cancellation of Azumaya algebras
  Journal of algebra 1971
  p.503-504

- Jean-.Pierre SERRE
  Faisceaux algébriques cohérents
  1954
  p.69