Université d'Ottawa • University of Ottawa

LA CONJECTURE DE SERRE

Par

Joseph Khoury

Septembre 1996

Thèse présentée
à l'École des Études Supérieures
de l'Université d'Ottawa
pour l'obtention de la maîtrise ès sciences
en mathémathiques [1]

[1]Le programme de maîtrise est un programme conjoint avec l'université Carleton, administré par l'Institut Ottawa-Carleton de mathématiques et statistiques.

Your file Votre référence
ISBN: 0-612-90094-0
Our file Notre référence
ISBN: 0-612-90094-0

Résumé

Une des grandes réussites de l'algèbre commutatif des années soixante-dix était la preuve de la << conjecture de Serre >>. Dans ces papiers, j'expose deux solutions différentes de cette conjecture. Les deux solutions sont exposées avec beaucoup de détails de façon qu'un lecteur qui n'a pas une connaissance profonde en algèbre commutatif puisse les comprendre sans beaucoup de difficultés.

Introduction

Quand J. P. Serre écrivit dans **[20]** : << On ignore s'il existe des $K[X_1, ..., X_n]$-modules projectifs de type fini qui ne sont pas libres >> (K est un corps), il n'avait pas l'intention de créer une nouvelle "conjecture" et il ne savait pas qu'il faudrait attendre vingt ans avant que A. Suslin **[23]** et D. Quillen **[17]** puissent montrer (séparement) en 1976, que tout module projectif de type fini sur un anneau de polynômes sur un corps est en fait libre.

Dans cette thèse, on expose, avec tous les détails possibles, deux solutions de cette conjecture. La première est celle de Quillen qu'on peut trouver dans **[9]** et qui montre la conjecture de Serre pour les anneaux de polynômes sur un anneau principal. La deuxième est celle de Vaserstein qui se trouve dans **[11]** et qui est une simplification de la preuve de Suslin. On fait enfin une généralisation de la preuve de Vaserstein à un anneau principal.

Avant d'aller plus loin dans notre dissertation du problème en mains, il est peut être normal de se demander si la conjecture de Serre est vraie si l'anneau de base n'est pas un anneau de polynômes. La réponse est << non >>. Un simple contre exemple est le suivant : soient K un corps, $A = K \times K$ et $P = (0) \times K$. Il est clair que A est un anneau commutatif, unitaire qui n'est pas intègre (donc il n'est pas anneau de polynômes) et P est un idéal de A et par suite un A-module qui est de type fini (engendré par l'élément $(0, 1)$) mais qui n'est pas libre car pour tout élément non nul $(0, \alpha)$ de A, on a que $(\alpha, 0).(0, \alpha) = 0$ avec $(\alpha, 0) \neq 0$ dans A. D'autre part, A étant noethérien, P est de présentation finie (voir la définition 1.2.2) et puisque les seuls idéaux premiers de A sont P et $Q = K \times 0$, P est localement libre (définition 1.1.3), ce qui montre que P est projectif sur A (proposition 1.1.13). Un autre exemple moins trivial qu'on peut trouver dans **[9]** consiste à prendre l'anneau $A = \mathbf{R}[X,Y,Z]/ < X^2+Y^2+Z^2-1 >$ comme anneau de base (où $\mathbf{R}$ est le corps des réels) et considérer le A-module $P = AdX \oplus AdY \oplus AdZ/ < xdX + ydY + zdZ >$ où x, y, z sont les images de X, Y, Z dans A et où $AdX \oplus AdY \oplus AdZ$ désigne un A-module libre de rang 3 avec base $\{dX, dY, dZ\}$. Alors on peut montrer que P est projectif et de type fini mais n'est pas libre, bien que l'anneau A possède plusieurs bonnes propriétés. Notons encore que, dans le cas d'une seule variable, la conjecture de Serre est une conséquence immédiate de la théorie élémentaire des modules sur les anneaux principaux.

Pour discuter l'aspect historique du problème, on a besoin de la définition suivante. Soit P un A-module projectif et de type fini. Pour chaque $\wp \in \mathrm{Spec}(A)$, soit $n(\wp)$ le rang du $A_\wp$-module libre $P_\wp$ (il est libre, en vertu du corollaire 1.1.2). Si $n(\wp)$ est indépendant de $\wp$, cet entier est appelé le *rang* de P.

D'après **[10]**, Serre avait deux motivations principales pour poser sa question. D'abord, Serre était occuppé à développer la notion de faisceau cohérent sur un schéma, qui généralise celle de fibré vectoriel sur une variété. Si X est une variété algébrique affine sur un corps K et si A désigne l'anneau de coordonnées de X, alors les fibrés vectoriels (algébriques) sur X correspondent aux A-modules projectifs et de type fini. La question de Serre revient alors à demander si tout fibré sur l'espace affine $\mathbf{A}_K^n$ est trivial.

Pour la deuxième motivation, soit V une sous-variété de $\mathbf{A}_K^n$ qui est irréductible et de codimension 2 et soit $I \subset A = K[t_1, ..., t_n]$ l'idéal de V. On dit que V est une *intersection complète* si I est engendré par deux éléments. Pour que V soit une intersection complète, il faut qu'elle satisfasse à certaines conditions faibles; sous l'hypothèse que ces conditions sont satisfaites, Serre a montré l'existence d'une suite exacte $0 \to A \to P \to I \to 0$ où P est un A-module projectif de rang 2. La << conjecture de Serre >> implique alors que P est engendré par deux éléments, donc I a la même propriété et V est une intersection complète. Citons ensuite les événements principaux dans l'histoire de la conjecture de Serre, par ordre chronologique :

1. En 1957/58, J. P. Serre [**21**] a montré que tout module projectif de type fini P sur $A = K[X_1, ..., X_n]$ admet une décomposition de la forme $P = A^m \oplus P'$ où P' est de rang inférieur ou égal à n. Ceci réduit la conjecture de Serre au cas où P est de rang inférieur ou égal à n.
2. Le cas de deux variables ($A = K[X_1, X_2]$) a été montré par Seshadri [**22**] en 1958.
3. En 1957/58, la question de Serre est devenue : << est-ce que tout $K[X_1, ..., X_n]$-module stablement libre (définition 2.1.3) est libre?>> et ceci après l'apparition du théorème de Hilbert-Serre qui a montré que tout $K[X_1, ..., X_n]$-module projectif de type fini est stablement libre. Dans ce cadre on a une autre formulation de la question de Serre: << est-ce que toute ligne unimodulaire sur A^n ($A = K[X_1, ..., X_n]$) (définition 2.2.1) peut être complétée à une matrice inversible de $\mathcal{M}_n(A)$?>>.
4. En 1963, H. Bass [**2**] a montré que les $K[X_1, ..., X_n]$-modules projectifs qui ne sont pas de type fini sont libres.
5. En 1964, H. Bass [**3**] a montré que tout $K[X_1, ..., X_n]$-module projectif de type fini est libre s'il est de rang strictement plus grand que n.
6. En 1969, H. Bass [**4**] a montré que si A est un anneau commutatif et si tout A-module stablement libre de rang pair est libre, alors A possède la propriété d'extension unimodulaire (définition 2.3.1).
7. En 1973/74, A. Suslin et L. N. Vaserstein [**25**] ont montré que si P est un $K[X_1, ..., X_n]$-module projectif de type fini, alors P est libre si $n = 3, 4, 5$ ou si le rang de P est supérieur ou égal à $\frac{n}{2} + 1$ ou si $n = 6$ et K est un corps fini.
8. En 1974, M. Roitman a montré que si K est un corps algébriquement clos, P un $K[X_1, ..., X_n]$-module projectif de type fini de rang n, alors P est libre. Il a ensuite montré ([**18**]) que l'hypothèse << algébriquement clos >> sur le corps K peut être remplacé par << infini >>.
9. En 1974, R. Swan [**24**] a montré le cas $n = 4$ si le corps K est infini de caractéristique $c \neq 2$.
10. La conjecture de Serre a été montrée en janvier 1976 indépendement par A. Suslin

[23] et D. Quillen **[17]**.
11. S. M. Bhatwadekar et A. Roy **[5]** ont montré en 1984 que si A est un anneau commutatif et noethérien de dimension d et P est un A-module projectif de type fini de rang plus grand ou égale à $d+1$, alors P admet un élément p tel que $\{\phi(p);\ \phi\in \mathrm{Hom}_A(P,A)\} = A$. Ce qui implique que si P est un $A[X_1,...X_n]$-module projectif de type fini et de rang r, alors P est engendré par $r+d$ éléments.
12. I. J. Gubeladze **[7]** a montré en 1984 que si K est un corps, A est un sous-anneau de $K[X_1,...,X_n]$ engendré par K et des monômes et si les trois conditions suivantes sont satisfaites, alors tout A-module projectif et de type fini est libre:

1. L'extension $A \subset K[X_1,...,X_n]$ est entière.
2. Si m_i est le plus petit entier positif tel que $X_i^{m_i} \in A$, alors $X_i^m \in A$ implique que m_i divise m.
3. Si I est l'idéal de $K[X_1,...,X_n]$ engendré par tous les produits X_iX_j $(i\neq j)$, alors $I\cap\overline{A} \subseteq A$, où $\overline{A}$ est la fermeture intégrale de A dans son corps de fractions.

13. En 1987, S. M. Bhatwadekar **[6]** a montré que si A est un anneau commutatif et noethérien de dimension d et si P est un module projectif de type fini sur $A[X,Y]$ et de rang plus grand ou égale à $d+1$, alors P est "simplifiable" dans le sens où si Q est un $A[X,Y]$-module tel que $P\oplus A[X,Y] \approx Q\oplus A[X,Y]$, alors $P \approx Q$.

Notons enfin que les efforts des mathématiciens pour résoudre le problème de Serre depuis l'année 1955 ont contribué, dans les années soixante, à fonder et développer une nouvelle branche de l'algèbre, la K-théorie. Ce qui est étonnant est le fait que la solution finale de la conjecture de Serre n'a pas utilisé du tout cette théorie.

Enfin, sauf mention contraire, tous les anneaux considérés dans ce travail sont commutatifs et unitaires et la lettre A désigne partout un anneau commutatif et unitaire.

Remerciement

Je voudrais exprimer ma sincère reconnaissance au professeur Daniel Daigle qui a dirigé cette thèse et qui a consacré beaucoup de temps à lire et à corriger ces papiers. Ses remarques et son précieux secours ont été essentiels à la réalisation de ce travail.

Dédicace

à celle dont l'amour et la patience ont rendu ce travail possible, à mon épouse Antoinette.

Table des matières

Chapitre 1

Solution de la conjecture de Serre par Quillen

1.1 Propriétés élémentaires

Modules projectifs

Proposition 1.1.1 *Tout A-module est l'image d'un A-module libre.*

Preuve Soit P un A-module. Considérons l'ensemble $A^{(P)}{:=}\{f : P{\rightarrow}A; f(p) = 0$ pour tout sauf un nombre fini d'éléments de P$\}$. On définit une structure de A-module sur $A^{(P)}$ en posant $(f+g)(x) = f(x)+g(x)$ et $(af)(x) = a(f(x))$ pour tous f, g dans $A^{(P)}$, x dans P et a dans A. Pour tout x dans P, on définit $e_x : P{\longrightarrow}A$ par

$$e_x(y) = \begin{cases} 1 & y = x \\ 0 & y{\neq}x \end{cases} .$$

Alors $e_x \in A^{(P)}$ pour tout x dans P, et il est facile de montrer que la famille $(e_x)_{x\in P}$ est une base de $A^{(P)}$ et que l'homomorphisme $\psi : A^{(P)}{\longrightarrow}P$ défini par $\psi(f) = \sum_{x\in P} f(x)x$ (somme finie) est surjectif. ∎

Définition 1.1.1 Un A-module P est dit *projectif* s'il existe un A-module P' tel que $P{\oplus}P'$ est libre.

Théorème 1.1.1 ([9], Proposition 3.2) *Pour un A-module P, les propriétés suivantes sont équivalentes:*

1. *P est un A-module projectif.*

2. *Pour tous A-modules M,N, pour tout épimorphisme $\alpha : M \rightarrow N$ et pour toute application linéaire $\beta : P \rightarrow N$, il existe une application linéaire $\gamma : P \rightarrow M$ telle que $\alpha\gamma = \beta$.*

3. *Toute suite exacte $0 \rightarrow M_1 \rightarrow M_2 \rightarrow P \rightarrow 0$ de A-modules est scindée.*

Preuve 1)⇒2) Supposons que P est projectif.
Soient $\alpha : M \rightarrow N$ un épimorphisme et $\beta : P \rightarrow N$ une application linéaire. Soit P' un A-module tel que $P \oplus P' = F$ libre et considérons l'application linéaire $\beta' : F \rightarrow N$ définie par $\beta' = \beta p_1$ où $p_1 : F \rightarrow P$ est la première projection. Soit $(a_i)_{i \in I}$ une base de F sur A et, pour chaque i $\in$ I, choisissons $c_i \in$ M tel que $\alpha(c_i) = \beta'(a_i)$. Définissons l'homomorphisme $\gamma' : F \rightarrow M$ par $\gamma'(a_i) = c_i$ pour tout i $\in I$, alors on a que $\alpha\gamma'(a_i) = \alpha(c_i) = \beta'(a_i) \forall i \in I$, d'où $\alpha\gamma' = \beta'$. Soit maintenant $\gamma : P \rightarrow M$ l'homomorphisme défini par $\gamma = \gamma' i_1$ où $i_1 : P \hookrightarrow F$ est l'injection canonique. On a que pour tout x dans P, $\alpha\gamma(x) = \alpha\gamma'(x,0) = \beta p_1(x,0) = \beta(x)$, d'où $\alpha\gamma = \beta$.
2)⇒3) Soit $0 \rightarrow M_1 \rightarrow M_2 \xrightarrow{c} P \rightarrow 0$ une suite exacte de A-modules. La condition 2), appliquée à l'épimorphisme c et à l'application $1_P : P \longrightarrow P$, implique l'existence d'une application $c' : P \longrightarrow M_2$ telle que $cc' = 1_P$, ce qui montre que la suite est scindée.
3)⇒1) En vertu de la proposition 1.1.1, on a une suite exacte $0 \rightarrow K \rightarrow L \rightarrow P \rightarrow 0$ de A-modules où L est libre. Par la condition 3), cette suite est scindée, alors $L \approx K \oplus P$, d'où P est projectif. ∎

Proposition 1.1.2 ([9], page 110) *Si M est un A-module projectif et S une partie multiplicativement stable de A, alors M_S est un A_S-module projectif.*

Preuve M étant projectif, il existe un A-module M' tel que $M \oplus M' = F$ est libre. Le A_S-module $L = M_S \oplus M'_S$ est libre car $L \approx F_S$ et F_S est un A_S-module libre (car si

$(a_i)_{i\in I}$ est une base de F sur A on peut vérifier aisément que $(\frac{a_i}{1})_{i\in I}$ est une base de L sur A_S), d'où M_S est un A_S-module projectif. ■

Proposition 1.1.3 ([9], page 110) *Soient $(M_i)_{i\in I}$ une famille de A-modules et $M = \oplus_{i\in I}M_i$. Alors M est projectif si et seulement si M_i est projectif pour tout $i\in I$.*

Preuve ($\Longrightarrow$) M étant projectif, il existe un A-module M' tel que $F = M\oplus M'$ est libre, alors pour tout i $\in$ I on a que $M_i\oplus[(\oplus_{j\neq i}M_j)\oplus M'] = F$ ce qui montre que M_i est projectif.
($\Longleftarrow$) Pour tout $i\in I$, soit M_i' un A-module tel que $M_i\oplus M_i' = F_i$ est libre sur A. Soit $M' = \oplus_{i\in I}M_i'$, alors $M\oplus M' = [\oplus_{i\in I}M_i]\oplus[\oplus_{i\in I}M_i'] = \oplus_{i\in I}F_i$ est libre, d'où M est projectif. ■

Proposition 1.1.4 ([9], page 110) *Si M est un A-module projectif et si $B\subseteq A$ est un sous-anneau de A tel que A est un B-module libre, alors M est un B-module projectif.*

Preuve Soit M' un A-module tel que $M\oplus M' = F$ est libre. Si $(f_i)_i$ est une base de F sur A et $(a_j)_j$ une base de A sur B, il est clair que la famille $(a_jf_i)_{i,j}$ est une base de F sur B. Alors F est libre comme B-module, d'où M est un B-module projectif. ■

Désignons par rad(A) l'intersection de tous les idéaux maximaux de A.

Proposition 1.1.5 (Lemme de Nakayama) *Soient M un A-module de type fini et N un sous-module de M. Si $M = N + JM$ où J est un idéal de A contenu dans* rad(A), *alors $M = N$.*

Une autre version du lemme de Nakayama est donnée par:

Proposition 1.1.6 *Soient M un A-module de type fini et I un idéal de A contenu dans* rad(A). *Si $M = IM$, alors $M = 0$.*

Corollaire 1.1.1 ([9], Corollary 2.4) *Soient (A,Ω) un anneau local, M un A-module de type fini et $\{m_1, ..., m_r\}$ un système minimal de générateurs de M. Alors r est égale à la dimension du A/Ω-espace vectoriel $M/\Omega M$.*

Preuve Puisque l'ensemble $G = \{\overline{m_1}, ..., \overline{m_r}\}$ engendre l'espace vectoriel $M/\Omega M$, il contient une base de cet espace. On arrange les éléments de G de façon que $\{\overline{m_1}, ..., \overline{m_d}\}$ soit une base de $M/\Omega M$ sur A/Ω ($d \leq r$). Il est clair que si F est le sous-module de M engendré par $m_1, ..., m_d$ alors $M = F + \Omega M$, ce qui donne par le lemme de Nakayama que $M = F$. Par le choix de G comme système minimal de générateurs, on aura que $d = r$. ∎

Définition 1.1.2 Un A-module M est dit *de présentation finie* s'il existe une suite exacte $0 \to K \to A^n \to M \to 0$ de A-modules telle que K est de type fini et n un entier naturel.

Proposition 1.1.7 ([9], Corollary 3.3) *Soit P un A-module projectif de type fini, alors on peut trouver un A-module P' de type fini tel que $P \oplus P'$ soit libre de rang fini. En particulier P est de présentation finie.*

Preuve P étant de type fini, on a alors un épimorphisme $\psi : A^n \to P$. Soit $P' = \ker \psi$, on a donc la suite exacte $0 \to P' \hookrightarrow A^n \to P \to 0$ de A-modules. Comme P est projectif, cette suite est scindée, d'où $A^n \approx P' \oplus P$ et P' est de type fini. ∎

Proposition 1.1.8 ([9], Proposition 3.4) *Soient (A, Ω) un anneau local, M un A-module de présentation finie, alors les propriétés suivantes sont équivalentes:*

1. *M est libre.*
2. *Il existe une suite exacte $0 \to K \xrightarrow{\alpha} P \xrightarrow{\beta} M \to 0$ de A-modules où P est projectif et l'application $\overline{\alpha} : K/\Omega K \to P/\Omega P$ induite par α est injective.*

Preuve 1)$\Longrightarrow$2) La condition 2) est satisfaite avec $P = M$, $\beta = 1_P$, $K = 0$.
2)$\Longrightarrow$1) Soit r le plus petit entier positif tel que M peut être engendré par r éléments. Il existe alors une suite exacte $0 \to K_0 \xrightarrow{\alpha_0} F_0 \xrightarrow{\beta_0} M \to 0$ de A-modules où F_0 est libre de rang r ($F_0 \approx A^r$). Considérons aussi une suite exacte $0 \to K \xrightarrow{\alpha} P \xrightarrow{\beta} M \to 0$ de A-modules

où P est projectif. Par le théorème 1.1.1, il existe une application linéaire $\epsilon : P \rightarrow F_0$ telle que $\beta_0\epsilon = \beta$. Considérons le diagramme commutatif

$$\begin{array}{ccc} & F_0/\Omega F_0 & \\ \overline{\epsilon}\nearrow & & \searrow\overline{\beta_0} \\ P/\Omega P & \xrightarrow{\overline{\beta}} & M/\Omega M \end{array} \tag{1.1.1}$$

induit par le diagramme:

$$\begin{array}{ccc} & F_0 & \\ \epsilon\nearrow & & \searrow\beta_0 \\ P & \xrightarrow{\beta} & M \end{array}$$

Notons que $\overline{\beta_0}$ est bijective car elle est surjective (β_0 l'est) et $F_0/\Omega F_0, M/\Omega M$ sont deux espaces vectoriels sur le corps A/Ω de même dimension r (corollaire 1.1.1). Comme $\overline{\beta_0}\overline{\epsilon} = \overline{\beta}$, alors $\overline{\epsilon} = \overline{\beta_0}^{-1}\overline{\beta}$ est surjective, d'où $F_0 = \epsilon(P) + \Omega F_0$. On obtient alors par le lemme de Nakayama que $F_0 = \epsilon(P)$, donc ϵ est surjective. Considérons maintenant le diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{\alpha} & P & \xrightarrow{\beta} & M & \longrightarrow & 0 \\ & & \downarrow\epsilon' & & \downarrow\epsilon & & \downarrow 1_M & & \\ 0 & \longrightarrow & K_0 & \xrightarrow{\alpha_0} & F_0 & \xrightarrow{\beta_0} & M & \longrightarrow & 0 \end{array} \tag{1.1.2}$$

où ϵ' est la restriction de ϵ. L'homomorphism ϵ' est surjectif car si $x_0 \in K_0$, alors $\alpha_0(x_0) = \epsilon(p)$ où $p \in P$ et on a $\beta_0\epsilon(p) = \beta_0\alpha_0(x_0) = 0$, donc $\beta(p) = 0$ et $p \in \ker\beta = \mathrm{Im}\alpha$, alors $p = \alpha(x)$ où $x \in K$, d'où $\epsilon'(x) = x_0$.

Notons que K_0 est de type fini. En effet, M étant de présentation finie, on peut choisir la suite $0 \rightarrow K \rightarrow P \rightarrow M \rightarrow 0$ de sorte que K soit de type fini. Comme $K_0 = \epsilon'(K)$, il s'ensuit que K_0 est de type fini.

Supposons maintenant que la suite $0 \rightarrow K \rightarrow P \rightarrow M \rightarrow 0$ satisfait la condition 2); autrement dit, on suppose que $\overline{\alpha}$ est injective. Posons ensuite $F_1' = \ker\epsilon'$ et $F_1 = \ker\epsilon$, alors pour tout x_1' dans F_1' on a $\epsilon\alpha(x_1') = \alpha_0\epsilon'(x_1') = 0$, d'où $\alpha(x_1') \in \ker\epsilon = F_1$ et par suite $\alpha(F_1') \subseteq F_1$. Réciproquement si $x_1 \in F_1$, alors $\epsilon(x_1) = 0$, d'où $\beta(x_1) = 0$ (par la commutativité du diagramme 1.1.2) ce qui implique que $x_1 \in \ker\beta = \mathrm{Im}\alpha$.

Choisissons $k \in K$ tel que $x_1 = \alpha(k)$, alors $\epsilon'(k) = \epsilon\alpha(k) = \epsilon(x_1) = 0$, d'où $k \in F'_1$ et $F_1 \subseteq \alpha(F'_1)$. Ceci montre que $F_1 = \alpha(F'_1)$ et par suite $F'_1 \overset{\theta}{\approx} F_1$. Considérons le diagramme suivant:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & F'_1 & \xrightarrow{\theta} & F_1 & & & & \\
 & & \downarrow j' & & \downarrow j & & & & \\
0 & \longrightarrow & K & \xrightarrow{\alpha} & P & \xrightarrow{\beta} & M & \longrightarrow & 0 \\
 & & \downarrow \epsilon' & & \downarrow \epsilon & & \downarrow 1_M & & \\
0 & \longrightarrow & K_0 & \xrightarrow{\alpha_0} & F_0 & \xrightarrow{\beta_0} & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Ce diagramme est exact et commutatif . Considérons ensuite ce diagramme modulo Ω:

$$\begin{array}{ccccccccc}
 & & F'_1/\Omega F'_1 & \xrightarrow{\overline{\theta}} & F_1/\Omega F_1 & & & & \\
 & & \downarrow \overline{j'} & & \downarrow \overline{j} & & & & \\
0 & \longrightarrow & K/\Omega K & \xrightarrow{\overline{\alpha}} & P/\Omega P & \xrightarrow{\overline{\beta}} & M/\Omega M & \longrightarrow & 0 \\
 & & \downarrow \overline{\epsilon'} & & \downarrow \overline{\epsilon} & & \downarrow 1_{M/\Omega M} & & \\
 & & K_0/\Omega K_0 & \xrightarrow{\overline{\alpha_0}} & F_0/\Omega F_0 & \xrightarrow{\overline{\beta_0}} & M/\Omega M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array} \qquad (1.1.3)$$

Le foncteur $(A/\Omega \bigotimes_A -)$ étant exact à droite, le diagramme 1.1.3 est alors commutatif et exact. Comme $\overline{\beta_0}$ est un isomorphisme, on peut déduire que $\overline{\alpha_0} = 0$.

Notons que $\overline{j'}$ est surjectif. En effet, pour tout $\overline{k}$ dans $K/\Omega K$, on a $\overline{\epsilon}\ \overline{\alpha}(\overline{k}) = \overline{\alpha_0}\overline{\epsilon'}(\overline{k}) = 0$, d'où $\overline{\alpha}(\overline{k}) \in \ker\overline{\epsilon} = \operatorname{Im}\overline{j}$. Soit $f_1 \in F_1$ tel que $\overline{\alpha}(\overline{k}) = \overline{j}(\overline{f_1}) = \overline{j}(\overline{\theta}(\overline{f'_1})) = \overline{\alpha}\overline{j'}(\overline{f'_1})$ où $f'_1 \in F'_1$ ($\overline{\theta}$ est un isomorphisme), ce qui implique que $\overline{k} = \overline{j'}(\overline{f'_1})$ (car $\overline{\alpha}$ est injective).

Par la surjectivité de $\overline{j'}$ on déduit que $\ker\overline{\epsilon'} = K/\Omega K$, d'où $\overline{\epsilon'} = 0$ et par conséquent $K_0/\Omega K_0 = 0$ (car $\overline{\epsilon'}$ est surjectif) ce qui donne par le lemme de Nakayama que $K_0 = 0$ (K_0 est de type fini). Ainsi $M \approx F_0$ et M est libre. ■

Corollaire 1.1.2 ([9], Corollary 3.5) *Soient (A,Ω) un anneau local, M un A-module de type fini. Alors M est projectif si et seulement si M est libre.*

Preuve Si M est projectif, alors il est de présentation finie (proposition 1.1.7). Considérons la suite exacte $0 \to 0 \to P \to M \to 0$ où $P = M$ est projectif. Le résultat se déduit immédiatement de la proposition précédente. ∎

Notons qu'on peut donner une démonstration du corollaire 1.1.2 qui n'utilise pas la proposition 1.1.8. En effet, soient P un A-module projectif et de type fini ((A,Ω) est local) et $\{x_1, ..., x_r\}$ un système minimal de générateurs de P. Soient $\psi : A^r \longrightarrow P$ l'épimorphisme défini par $\psi(e_i) = x_i$ pour tout i ($\{e_1, ..., e_r\}$ est la base canonique de A^r) et $K = \text{Ker } \psi$. On a que $K \subseteq \Omega A^r$ car s'il existe $a = \sum_{i=1}^{r} \alpha_i e_i$ dans K qui n'appartient pas à ΩA^r, alors il existe un certain j tel que α_j nappartient pas à Ω, d'où α_j est inversible. On a alors

$$x_j = -\alpha_1 \alpha_j^{-1} x_1 - ... - \alpha_r \alpha_j^{-1} x_r,$$

ce qui contredit la minimalité du système $\{x_1, ..., x_r\}$.
D'autre part, la suite de A-modules

$$0 \longrightarrow K \longrightarrow A^r \xrightarrow{\psi} P \longrightarrow 0$$

étant exacte et P projectif, il existe un monomorphisme $\phi : P \longrightarrow A^r$ tel que $\psi\phi = 1_P$ et $A^r = K \oplus \text{ Im } \phi$. Puisque $K \subseteq \Omega A^r$, alors $A^r = K + \text{ Im } \phi$ et le théorème de Nakayama impliquent que $A^r = \text{Im } \phi$ et par suite $P \approx A^r$.

Proposition 1.1.9 *Pour un A-module M, les propriétés suivantes sont équivalentes:*

1. *M_Ω est un A_Ω-module libre pour tout $\Omega \in$ Max(A).*
2. *$M_\wp$ est un $A_\wp$-module libre pour tout $\wp \in$ Spec(A).*

Preuve 1) $\Longrightarrow$ 2) Soit $\wp \in$ Spec(A) et choisissons $\Omega \in$ Max(A) tel que $\wp \subseteq \Omega$. Soit T l'image de $A \backslash \wp$ dans A_Ω, alors l'homomorphisme

$$\begin{array}{ccc} (A_\Omega)_T & \longrightarrow & A_\wp \\ \dfrac{\frac{a}{s}}{\frac{p}{1}} & \longmapsto & \dfrac{a}{sp} \end{array}$$

est un isomorphisme d'anneaux. De même, on a $(M_\Omega)_T \approx M_\wp$. Par la condition 1), M_Ω est un A_Ω-module libre, alors $(M_\Omega)_T$ est libre sur $(A_\Omega)_T$, d'où $M_\wp$ est libre sur $A_\wp$.
2) $\Longrightarrow$ 1) Tout idéal maximal est premier. ∎

Définition 1.1.3 Un A-module est dit *localement libre* s'il vérifie une des deux propriétés équivalentes de la proposition 1.1.9.

Proposition 1.1.10 ([1], Proposition 3.8) *Soit M un A-module. Si $M_\Omega = 0$ pour tout idéal maximal Ω de A, alors $M = 0$.*

Preuve Si $M \neq 0$, choisissons $x \in M$ tel que $x \neq 0$. Soient $\Re =$ ann(x) et $\Omega \in$ Max(A) tel que $\Re \subset \Omega$. Comme $\frac{x}{1} = 0$ dans M_Ω, il existe alors $s \notin \Omega$ tel que $sx = 0$, ce qui implique que $s \in \Re$, d'où la contradiction. ∎

Proposition 1.1.11 *Une suite de A-modules $M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ est exacte si et seulement si pour tout idéal maximal Ω de A, la suite $M_\Omega \xrightarrow{\alpha_\Omega} N_\Omega \xrightarrow{\beta_\Omega} P_\Omega$ est exacte .*

Preuve ($\Longrightarrow$) C'est le fait que la localisation est un foncteur exact.
($\Longleftarrow$) Supposons que $M_\Omega \xrightarrow{\alpha_\Omega} N_\Omega \xrightarrow{\beta_\Omega} P_\Omega$ est exacte pour tout Ω dans Max(A). Soit $Q =$ Im$(\beta\alpha)$; alors $Q_\Omega =$ Im$((\beta\alpha)_\Omega) = 0$ pour tout $\Omega \in$ Max(A), donc $Q = 0$ par la proposition 1.1.10, donc $\beta\alpha = 0$, d'où Im$\alpha \subseteq$ kerβ. D'autre part, pour tout $\Omega \in$ Max(A), on a que $(\ker\beta/ \operatorname{Im}\alpha)_\Omega \approx (\ker\beta)_\Omega/(\operatorname{Im}\alpha)_\Omega \approx \ker\beta_\Omega/ \operatorname{Im}\alpha_\Omega = 0$ car $\operatorname{Im}\alpha_\Omega = \ker\beta_\Omega$, on déduit alors par la proposition précédente que $\ker\beta/\operatorname{Im}\alpha = 0$, d'où $\ker\beta = \operatorname{Im}\alpha$. ∎

Corollaire 1.1.3 *Soient M, N deux A-modules, $f : M \longrightarrow N$ un homomorphisme de A-modules. Alors f est surjective (respectivement injective,respectivement bijective) si et seulement si f_Ω est surjective (respectivement injective,respectivement bijective) pour tout idéal maximal Ω de A.*

Proposition 1.1.12 ([9], Proposition 1.10) *Soient M, N deux A-modules, S une partie multiplicativement stable de A. L'application A-linéaire*

$$\begin{array}{ccc} \mathrm{Hom}_A(M,N) & \xrightarrow{\phi} & \mathrm{Hom}_{A_S}(M_S,N_S) \\ f & \longmapsto & f_S \end{array}$$

induit une application A_S-linéaire

$$\begin{array}{ccc} \mathrm{Hom}_A(M,N)_S & \xrightarrow{h} & \mathrm{Hom}_{A_S}(M_S,N_S) \\ \frac{f}{t} & \longmapsto & \mu_t^{-1} f_S \end{array} \quad \text{où} \quad \begin{array}{ccc} N_S & \xrightarrow{\mu_t^{-1}} & N_S \\ \frac{n}{s} & \longmapsto & \frac{n}{st} \end{array}$$

Sous ces conditions on a que:

1. *Si M est de type fini, alors h est injective.*

2. *Si M est de présentation finie, alors h est bijective.*

Preuve 1) Soient $\{m_1, ..., m_r\}$ un système générateur de M, $f \in \mathrm{Hom}_A(M,N)$ et $s \in S$ tels que $h(\frac{f}{s}) = 0$, alors $\mu_s^{-1} f_S = 0$, d'où pour tout $k = 1, ..., r$ on a $\frac{f(m_k)}{s} = \mu_s^{-1}(\frac{f(m_k)}{1}) = \mu_s^{-1} f_S(\frac{m_k}{1}) = 0$. Choisissons, pour tout $k = 1, ..., r$ un élément s_k de S tel que $s_k f(m_k) = 0$ et soit $s' = \prod_{k=1}^r s_k$, s' est alors dans S et on a $s' f(m_k) = 0$ pour tout $k = 1, ..., r$ ce qui montre que $s'f = 0$ et par suite $\frac{f}{s} = 0$, ce qui montre que h est injectif.
2) Supposons maintenant que M est de présentation finie et choisissons une suite exacte $0 \to K \to A^r \xrightarrow{\epsilon} M \to 0$ avec $\epsilon(e_k) = m_k$ pour tout $k = 1, ..., r$ où $(e_k)_{k=1}^r$ est la base canonique de A^r et K est un A-module de type fini. Par l'énoncé 1), il suffit de montrer que h est surjective. Soient

$$\begin{array}{ccc} M & \xrightarrow{i_M} & M_S \\ m & \longmapsto & \frac{m}{1} \end{array} \quad \text{et} \quad \begin{array}{ccc} N & \xrightarrow{i_N} & N_S \\ n & \longmapsto & \frac{n}{1} \end{array}$$

les A-homomorphismes canoniques et soit $\phi \in \mathrm{Hom}_{A_S}(M_S, N_S)$. Pour tout $k = 1, .., r$ choisissons $p_k \in N$ et $s_k \in S$ tels que $\phi(\frac{m_k}{1}) = \frac{p_k}{s_k}$. Posons $s = \prod_{k=1}^r s_k$, alors $s\phi(\frac{m_k}{1}) = \frac{n_k}{1}$ où $n_k \in N$. Soit $\psi : A^r \longrightarrow N$ l'application linéaire définie par $\psi(e_k) = n_k$

et considérons le diagramme commutatif suivant:

$$\begin{array}{ccc} A^r & \xrightarrow{\psi} & N \\ \epsilon\downarrow & & \downarrow i_N \\ M & \xrightarrow{s\phi i_M} & N_S \end{array}$$

Pour tout x dans K on a $i_N\psi(x) = s\phi i_M\epsilon(x) = 0$, alors $\frac{\psi(x)}{1} = 0$, on peut donc choisir $s' \in S$ tel que $s'\psi(K) = 0$ car K est de type fini sur A. Considérons maintenant l'application $s'\psi : A^r \longrightarrow N$. Comme la réstriction de $s'\psi$ à K est nulle, $s'\psi$ induit alors une application linéaire $f : M \longrightarrow N$ satisfaisant $f\epsilon = s'\psi$, d'où on a $\phi(\frac{m_k}{1}) = \frac{n_k}{s} = \frac{s'n_k}{ss'} = \mu_{ss'}^{-1}(\frac{s'n_k}{1}) = \mu_{ss'}^{-1}(\frac{s'\psi(e_k)}{1}) = \mu_{ss'}^{-1}(\frac{f\epsilon(e_k)}{1}) = \mu_{ss'}^{-1}(\frac{f(m_k)}{1}) = \mu_{ss'}^{-1}f_S(\frac{m_k}{1})$ pour tout $k = 1, .., r$. Alors $\phi = \mu_{ss'}^{-1}f_S = h(\frac{f}{ss'})$, ce qui montre que h est surjectif. ∎

Proposition 1.1.13 ([9], Corollary 3.6) *Pour un A-module P de type fini, les propriétés suivantes sont équivalentes:*

1. *P est projectif.*
2. *P est de présentation finie et localement libre.*

Preuve 1)$\Longrightarrow$2) P est de présentation finie par la proposition 1.1.7. Comme P_Ω est un A_Ω-module projectif pour tout Ω dans $\mathrm{Max}(A)$ (proposition 1.1.2), le résultat se déduit alors du corollaire 1.1.2.

2)$\Longrightarrow$1) Considérons une suite exacte $0 \rightarrow K \xrightarrow{\alpha} F \xrightarrow{\beta} P \rightarrow 0$ où F est libre de rang fini et K est de type fini sur A. Le module P étant localement libre, alors pour tout idéal maximal Ω de A, la suite $0 \rightarrow K_\Omega \xrightarrow{\alpha_\Omega} F_\Omega \xrightarrow{\beta_\Omega} P_\Omega \rightarrow 0$ est exacte et scindée (car P_Ω est libre sur A_Ω et donc projectif), d'où il existe une application linéaire $\beta'_\Omega : P_\Omega \longrightarrow F_\Omega$ telle que $\beta_\Omega\beta'_\Omega = 1_{P_\Omega}$. Ainsi, l'homomorphisme $\mathrm{Hom}_{A_\Omega}(P_\Omega, F_\Omega) \longrightarrow \mathrm{Hom}_{A_\Omega}(P_\Omega, P_\Omega)$ $(\gamma \longmapsto \beta_\Omega\gamma)$ est surjectif pour tout idéal maximal Ω de A. On déduit alors par la proposition 1.1.12 que l'homomorphisme $(\mathrm{Hom}_A(P, F))_\Omega \xrightarrow{\psi_\Omega} (\mathrm{Hom}_A(P, P))_\Omega$ est surjective pour tout Ω dans Max(A), où $\psi : \mathrm{Hom}_A(P, F) \longrightarrow \mathrm{Hom}_A(P, P)$ est l'homomorphisme défini par $\psi(\gamma) = \beta\gamma$. Le corollaire 1.1.3 implique que l'homomorphisme ψ est surjectif. La suite $0 \rightarrow K \xrightarrow{\alpha} F \xrightarrow{\beta} P \rightarrow 0$ est alors scindée, d'où $F \approx K \oplus P$. Le module P est donc projectif. ∎

Produit extérieur

Dans ce qui suit on va montrer quelques propriétés reliées au produit extérieur dans la catégorie des A-modules.

Définition 1.1.4 Soient E, F deux A-modules, r un entier naturel. Une application r-multilinéaire $f : E^r \longrightarrow F$ est dite *alternée* si $f(x_1, ..., x_r) = 0$ chaque fois qu'il existe $i \neq j$ avec $x_i = x_j$. Soit $T^r(E)$ le produit tensoriel

$$\underbrace{E \otimes ... \otimes E}_{r}.$$

et soit $\Re_r$ le sous A-module de $T^r(E)$ engendré par les éléments de la forme $x_1 \otimes ... \otimes x_r$ où $x_i = x_j$ pour un certain $i \neq j$. On définit le *r-ième produit extérieur* de E comme étant $T^r(E)/\Re_r$, c'est un A-module qu'on note par $\bigwedge^r(E)$.

On a un homomorphisme naturel $\psi : E^r \xrightarrow{\phi} T^r(E) \xrightarrow{\pi} \bigwedge^r(E)$ qui est altérné car si $x_i = x_j$ pour $i \neq j$ alors $\psi(x_1, ..., x_r) = 0$.

Le produit extérieur peut être défini par la propriété universelle suivante:

Proposition 1.1.14 ([11], page 732) *Soient E, F deux A-modules, r un entier naturel, et soit $f : E^r \longrightarrow F$ une application multilinéaire alternée sur E^r, alors il existe une application linéaire unique $f_* : \bigwedge^r(E) \longrightarrow F$ telle que le diagramme:*

$$\begin{array}{ccc} E^r & \xrightarrow{f} & F \\ \psi\searrow & & \nearrow f_* \\ & \bigwedge^r(E) & \end{array}$$

est commutatif.

Preuve La donnée d'une application multilinéaire $f : E^r \longrightarrow F$ induit une application linéaire $g : T^r(E) \longrightarrow F$ (propriété universelle du produit tensoriel) unique telle que le diagramme

$$\begin{array}{ccc} E^r & \xrightarrow{f} & F \\ \phi\searrow & & \nearrow g \\ & T^r(E) & \end{array}$$

est commutatif. Mais si $x_1 \otimes ... \otimes x_r$ est un générateur de $\Re_r$, alors $g(x_1 \otimes ... \otimes x_r) = g\phi(x_1, ..., x_r) = f(x_1, ..., x_r) = 0$. Donc g induit une application linéaire $f_* : \bigwedge^r(E) \longrightarrow F$ telle que $f_*\pi = g$ d'où $f_*\psi = f_*\pi\phi = g\phi = f$ et f_* est unique pour cette propriété. ∎

L'image par ψ d'un élément $(x_1, ..., x_r)$ de E^r est notée par $x_1 \wedge ... \wedge x_r$.

Notation 1.1.1 Soient $u : E \longrightarrow F$ une application linéaire, r un entier naturel. On définit une application $\theta : E^r \longrightarrow \bigwedge^r(F)$ par $\theta(x_1, ..., x_r) = u(x_1) \wedge ... \wedge u(x_r)$. Il est clair que θ est multilinéaire et alternée. Elle induit alors par la proposition 1.1.14 une application linéaire notée $\bigwedge^r u$

$$\begin{array}{ccc} \bigwedge^r(E) & \xrightarrow{\bigwedge^r u} & \bigwedge^r(F) \\ x_1 \wedge ... \wedge x_r & \longmapsto & u(x_1) \wedge ... \wedge u(x_r). \end{array}$$

Pour la suite, on a besoin d'un résultat de la théorie des déterminants. On énonce ici le résultat sans le démontrer. Pour la preuve, voir ([**11**], Chapter 13, Corollary 4.12) ou Theorem 2 dans le chapitre 9 de [**13**].

Proposition 1.1.15 *Soient E un A-module libre et $\{v_1, ..., v_n\}$ une base de E. Si $a \in A$, alors il existe une et une seule application n-multilinéaire et alternée $\phi : E^n \longrightarrow A$ telle que $\phi(v_1, ..., v_n) = a$.*

Proposition 1.1.16 ([**11**], chapter 19, Proposition 1.1) *Soit E un A-module libre de rang n. Alors on a*

1. *Si $r > n$, alors $\bigwedge^r(E) = 0$.*
2. *Si $\{v_1, ..., v_n\}$ est une base de E sur A et $1 \leq r \leq n$ alors $\bigwedge^r(E)$ est libre sur A et $\{v_{i_1} \wedge ... \wedge v_{i_r}; i_1 < ... < i_r\}$ est une base de $\bigwedge^r(E)$ sur A.*

Preuve 1. Remarquons tout d'abord que l'ensemble $S := \{v_{i_1} \wedge ... \wedge v_{i_r}; i_1 < ... < i_r\}$ engendre $\bigwedge^r(E)$ (pour voir ceci on utilise la relation $x \wedge y = -y \wedge x$). Alors, si $r > n$, dans chaque produit extérieur $v_{i_1} \wedge ... \wedge v_{i_r}$, on a une répétition, d'où $S = \{0\}$ et par suite $\bigwedge^r(E) = 0$.

2. Supposons maintenant que $1 \leq r \leq n$ et montrons tout d'abord la proposition dans le cas $r = n$. Dans ce cas, il suffit de montrer que $v = v_1 \wedge ... \wedge v_n$ est libre dans $\bigwedge^n(E)$ (car $v_1 \wedge ... \wedge v_n$ engendre $\bigwedge^n(E)$ sur A). Par la proposition 1.1.15, il existe une application multilinéaire et alternée unique $\phi : E^n \longrightarrow A$ telle que $\phi(v_1, ..., v_n) = 1$, ce qui implique (par la proposition 1.1.14) l'existence d'une application linéaire unique $\phi_* : \bigwedge^n(E) \longrightarrow A$ telle que $\phi_*(v) = 1$. Si $\alpha \in A$ est tel que $\alpha v = 0$, alors $\alpha \phi_*(v) = 0$ et par suite $\alpha = 0$. Ceci montre que $\{v\}$ est une base de $\bigwedge^n(E)$.

Supposons maintenant que $r \in \{1, ..., n-1\}$. Il suffit de montrer que l'ensemble $S := \{v_{i_1} \wedge ... \wedge v_{i_r}; i_1 < ... < i_r\}$ est libre. Supposons que $\sum \alpha_{(i)} v_{i_1} \wedge ... \wedge v_{i_r} = 0$ où la somme est prise sur toutes les listes $(i) = (i_1, ..., i_r)$ avec $1 \leq i_1 < ... < i_r \leq n$ et $\alpha_{(i)} \in A$ pour tout (i). Fixons une liste $(i) = (i_1, ..., i_r)$ avec $1 \leq i_1 < ... < i_r \leq n$ et soient $i_{r+1} < ... < i_n$ tels que $\{i_1, ... i_n\} = \{1, 2, ..., n\}$. On a donc que $(\sum \alpha_{(i)} v_{i_1} \wedge ... \wedge v_{i_r}) \wedge v_{i_{r+1}} \wedge ... \wedge v_{i_n} = 0$, alors $\alpha_{(i)} v_{i_1} \wedge ... \wedge v_{i_r} \wedge v_{i_{r+1}} \wedge ... \wedge v_{i_n} = 0$ d'où $\alpha_{(i)} = 0$ par le cas $r = n$. Ainsi $\alpha_{(i)} = 0$ pour tout (i), d'où S est libre, ce qui montre alors que S est une base de $\bigwedge^r(E)$, ce qui montre la proposition dans ce cas. Notons enfin que si r=0, alors $\bigwedge^r(E) = A$ et $\{1\}$ est une base de $\bigwedge^0(E)$. ■

Définition 1.1.5 Soit $\mathcal{A} = (a_{ij})_{i,j} \in \mathcal{M}(A, p \times q)$. Si r, h sont deux entiers positifs, on définit S_r^h comme étant l'ensemble de tous les r-uplets $J = (j_1, ..., j_r)$ où $1 \leq j_1 < j_2 < ... < j_r \leq h$. On choisit un ordre linéaire pour chacun des ensembles S_r^p et S_r^q. Si $1 \leq r \leq \min(p, q)$, $I = (i_1, ..., i_r) \in S_r^p$ et $J = (j_1, ..., j_r) \in S_r^q$, on définit l'élément $\mathcal{A}_{IJ}^{(r)}$ de A comme étant le déterminant:

$$\mathcal{A}_{IJ}^{(r)} = \begin{vmatrix} a_{i_1j_1} & a_{i_1j_2} & \cdots & a_{i_1j_r} \\ a_{i_2j_1} & a_{i_2j_2} & \cdots & a_{i_2j_r} \\ \vdots & \vdots & \cdots & \vdots \\ a_{i_rj_1} & a_{i_rj_2} & \cdots & a_{i_rj_r}. \end{vmatrix}.$$

Si I est le i-ième élément de S_r^p et J est le j-ième élément de S_r^q, on peut regarder $\mathcal{A}_{IJ}^{(r)}$ comme étant la $(i,j)^{ieme}$ composante d'une matrice $\mathcal{A}^{(r)}$ qui sera appelée *la r-ième puissance extérieure* de $\mathcal{A}$.

Une autre manière de décrire la matrice $\mathcal{A}^{(r)}$ est la suivante: soient $\{e_1, ..., e_p\}$ et $\{u_1, ..., u_q\}$ des bases de A^p et A^q respectivement, alors pour tout entier r tel que $1 \leq r \leq \min(p, q)$, l'ensemble $\{e_{j_1} \wedge ... \wedge e_{j_r}; j_1 < ... < j_r\}$ est une base de $\bigwedge^r(A^p)$ et l'ensemble $\{u_{j_1} \wedge ... \wedge u_{j_r}; j_1 < ... < j_r\}$ est une base de $\bigwedge^r(A^q)$ (proposition 1.1.16). $\mathcal{A} \in \mathcal{M}(A, p \times q)$ représente une application linéaire qu'on note encore par $\mathcal{A} : A^q \longrightarrow A^p$. $\mathcal{A}$ induit alors une application linéaire $\bigwedge^r \mathcal{A} : \bigwedge^r(A^q) \longrightarrow \bigwedge^r(A^p)$ (on utilise ici la notation 1.1.1) dont la matrice représentante est $\mathcal{A}^{(r)}$.

Proposition 1.1.17 ([11], Chapter 19, Proposition 2.1) *Si $\mathcal{A} \in \mathcal{M}(A, p \times q)$, $\mathcal{B} \in \mathcal{M}(A, q \times s)$ alors les deux matrices $(\mathcal{A}.\mathcal{B})^{(r)}$ et $\mathcal{A}^{(r)}\mathcal{B}^{(r)}$ sont égales.*

Preuve $\mathcal{A}.\mathcal{B}$ représente l'application linéaire $A^s \xrightarrow{\mathcal{B}} A^q \xrightarrow{\mathcal{A}} A^p$. Par ce qui précède $(\mathcal{A}.\mathcal{B})^{(r)}$ représente l'application $\bigwedge^r A^s \xrightarrow{\mathcal{B}^{(r)}} \bigwedge^r A^q \xrightarrow{\mathcal{A}^{(r)}} \bigwedge^r A^p$, d'où le résultat. ∎

Notation 1.1.2 Soit $\mathcal{A} \in \mathcal{M}(A, p \times q)$. Pour tout entier naturel $r \leq \min(p, q)$ on note par $I_r(\mathcal{A})$ l'idéal de A engendré par les mineurs d'ordre r de $\mathcal{A}$.
Notons que si $\mathcal{B}$ est une matrice carrée inversible d'ordre q, alors pour chaque $r = 1, ..., q$ on a $I_r(\mathcal{B}) = A$ car $\det(\mathcal{B})$ est inversible dans A et $\det(\mathcal{B}) \in I_r(\mathcal{B})$.

Proposition 1.1.18 ([11], page 740) *Si $\mathcal{A} \in \mathcal{M}(A, p \times q)$, $\mathcal{B} \in \mathcal{M}(A, q \times s)$, alors pour tout entier naturel $r \leq \min(p, q, s)$ on a $I_r(\mathcal{AB}) \subseteq I_r(\mathcal{A}) \cap I_r(\mathcal{B})$.*

Preuve Si m est un mineur d'ordre r de $(\mathcal{AB})$, alors m est un coefficient de la matrice $(\mathcal{AB})^{(r)} = \mathcal{A}^{(r)}\mathcal{B}^{(r)}$, ce qui implique que m est une somme des produits des mineurs d'ordre r de $\mathcal{A}$ et de $\mathcal{B}$. Alors $m \in I_r(\mathcal{A}) \cap I_r(\mathcal{B})$. ∎

Proposition 1.1.19 ([11], page 740) *Si $\mathcal{A}$, $\mathcal{B} \in \mathcal{M}(A, p \times q)$ sont deux matrices semblables, alors $I_r(\mathcal{A}) = I_r(\mathcal{B})$ pour tout $r \leq \min(p, q)$.*

Preuve Ecrivons $\mathcal{A} = \mathcal{UBV}$ où $\mathcal{U} \in \mathrm{GL}_p(A)$, $\mathcal{V} \in \mathrm{GL}_q(A)$. Par la proposition 1.1.18, on a que $I_r(\mathcal{A}) \subseteq I_r(\mathcal{UB}) \cap I_r(\mathcal{V}) = I_r(\mathcal{UB})$ (car $I_r(\mathcal{V}) = A$). Comme $I_r(\mathcal{UB}) \subseteq I_r(\mathcal{U}) \cap I_r(\mathcal{B}) = I_r(\mathcal{B})$, alors $I_r(\mathcal{A}) \subseteq I_r(\mathcal{B})$. L'autre inclusion se déduit de la même manière du fait que $\mathcal{B} = \mathcal{U}^{-1}\mathcal{A}\mathcal{V}^{-1}$. ∎

Produit fibré

Une autre notion utilisée par la démonstration de Quillen est celle du produit fibré qui est définie dans une catégorie quelconque. Dans ce qui suit on va définir cette notion dans la catégorie des A-modules et montrer quelques propriétés qui joueront un rôle important dans cette démonstration.

Définition 1.1.6 Soient M_1, M_2, N trois A-modules, $\alpha_i : M_i \longrightarrow N$ $(i = 1, 2)$ deux homomorphismes de A-modules. On définit le *produit fibré* de M_1 et M_2 sur N comme étant un triplet (P, β_1, β_2) où P est un A-module, $\beta_i : P \longrightarrow M_i$ $(i = 1, 2)$ deux homomorphismes tels que $\alpha_1\beta_1 = \alpha_2\beta_2$ avec la propriété universelle suivante: pour tout A-module T, pour chaque couple d'homomorphismes $\gamma_i : T \longrightarrow M_i$ $(i = 1, 2)$ tels que $\alpha_1\gamma_1 = \alpha_2\gamma_2$, il existe un homomorphisme unique $\gamma : T \longrightarrow P$ tel que $\beta_i\gamma = \gamma_i$ $(i = 1, 2)$.

Proposition 1.1.20 ([9], Proposition 5.2) *Le produit fibré existe dans la catégorie des A-modules.*

Preuve Avec les notations de la définition 1.1.6, on désigne par P le sous A-module de $M_1 \oplus M_2$ formé des couples (m_1, m_2) tels que $\alpha_1(m_1) = \alpha_2(m_2)$. Soient $\beta_i : P \longrightarrow M_i$, $(i = 1, 2)$ les restrictions à P des projections canoniques. On a clairement que $\alpha_1\beta_1 = \alpha_2\beta_2$ et il est facile de voir que le triplet (P, β_1, β_2) est le produit fibré de M_1 et M_2 sur N. ∎

Notation 1.1.3 Avec les notations de la définition 1.1.6, le produit fibré de M_1 et M_2 sur N est noté par $(M_1 \prod_N M_2, \beta_1, \beta_2)$.

Proposition 1.1.21 ([9], Rule 5.4) *Avec les notations de la définition 1.1.6 on a les propriétés suivantes:*

1. $\ker(\beta_1) \cap \ker(\beta_2) = 0$.

2. *β_1 induit un isomorphisme* $\ker(\beta_2) \approx (\ker\alpha_1)$ *et de même, β_2 induit un isomorphisme* $\ker(\beta_1) \approx \ker(\alpha_2)$. *En particulier β_2(respectivement β_1) est injectif si et seulement si α_1 (respectivement α_2) est injectif.*

3. *α_2 induit une injection* $\operatorname{coker}(\beta_2) \longrightarrow \operatorname{coker}(\alpha_1)$. *De même, α_1 induit une injection* $\operatorname{coker}(\beta_1) \longrightarrow \operatorname{coker}(\alpha_2)$. *En particulier si α_1 (respectivement α_2) est surjectif alors β_2 (respectivement β_1) est surjectif.*

4. *Si α_1 (respectivement α_2) est un isomorphisme, alors β_2 (respectivement β_1) l'est.*

5. *Si $S \subseteq A$ est multiplicativement stable, le triplet $((M_1 \prod_N M_2)_S, \beta_{1S}, \beta_{2S})$ est alors un produit fibré de $(M_1)_S$ et de $(M_2)_S$ sur N_S (pour $(\alpha_1)_S$ et $(\alpha_2)_S$) et on a $(M_1 \prod_N M_2)_S = (M_1)_S \prod_{N_S} (M_2)_S$.*

Preuve 1. Clair.
2. Rappelons que β_1 est l'homomorphisme suivant

$$\begin{array}{rcl} P & \xrightarrow{\beta_1} & M_1 \\ (m_1, m_2) & \longmapsto & m_1. \end{array}$$

Si $x \in \ker(\beta_2)$ alors $\alpha_1(\beta_1(x)) = \alpha_2\beta_2(x) = 0$, d'où $\beta_1(x) \in \ker(\alpha_1)$ et $\beta_1(\ker(\beta_2)) \subseteq \ker(\alpha_1)$. Réciproquement, si $y \in \ker(\alpha_1)$, posons $Z = (y, 0) \in P$, alors $Z \in \ker(\beta_2)$ et $\beta_1(Z) = y$, d'où $\beta_1(\ker\beta_2) = \ker(\alpha_1)$. Le résultat se déduit maintenant du fait que la restriction de β_1 à $\ker(\beta_2)$ est injective. De la même manière, on montre que β_2 induit un isomorphisme $\ker(\beta_1) \approx \ker(\alpha_2)$.
3. Considérons l'application

$$\begin{array}{rcl} M_2/\operatorname{Im}(\beta_2) & \xrightarrow{\psi} & N/\operatorname{Im}(\alpha_1) \\ \overline{m_2} & \longmapsto & \overline{\alpha_2(m_2)}. \end{array}$$

Notons que ψ est bien définie car si $\overline{m_2} = \overline{m_2'}$, alors $m_2 - m_2' \in \operatorname{Im}(\beta_2)$, d'où $m_2 - m_2' = \beta_2(p_1, p_2) = p_2$ où $(p_1, p_2) \in P$, ceci montre que $\alpha_2(m_2 - m_2') = \alpha_2(p_2)$ et par suite $\overline{\alpha_2(p_2)} - \overline{\alpha_2(m_2')} = \overline{\alpha_2(p_2)} = \overline{\alpha_2\beta_2(p_1, p_2)} = \overline{\alpha_1(p_1)} = 0$.
Si maintenant $\psi(\overline{m_2}) = 0$, alors $\alpha(m_2) \in \operatorname{Im}(\alpha_1)$, on choisit alors $m_1 \in M_1$ tel que $\alpha_2(m_2) = \alpha_1(m_1)$, d'où $(m_1, m_2) \in P$, ce qui donne que $m_2 \in \operatorname{Im}(\beta_2)$ et par suite $\overline{m_2} = 0$. ψ est alors un monomorphisme. De même on montre que α_1 induit une injection $\operatorname{coker}(\beta_1) \longrightarrow \operatorname{coker}(\alpha_2)$. En particulier, si α_1 est surjectif, alors $\operatorname{coker}(\alpha_1) = 0$,

d'où $\operatorname{coker}(\beta_2) = 0$ et β_2 est alors surjectif. De même, si α_2 est surjectif, alors β_1 est surjectif.

4. Clair.

5. Par l'isomorphisme $(M_1)_S \oplus (M_2)_S \approx (M_1 \oplus M_2)_S$, le sous-module de $(M_1)_S \oplus (M_2)_S$ formé des couples $(\frac{m_1}{s_1}, \frac{m_2}{s_2})$ qui satisfont: $(\alpha_1)_S(\frac{m_1}{s_1}) = (\alpha_2)_S(\frac{m_2}{s_2})$ est identifié avec le sous A_S-module de $(M_1 \oplus M_2)_S$ des éléments $\frac{(m_1, m_2)}{s}$ tels que $\alpha_1(m_1) = \alpha_2(m_2)$, d'où $(M_1 \prod_N M_2)_S \approx (M_1)_S \prod_{N_S} (M_2)_S$. ■

Le produit fibré s'utilise pour "coller" des A-modules donnés sur des parties ouvertes de Spec(A). En d'autres termes, soient $f, g \in A$, M_1 un A_f-module, M_2 un A_g-module et supposons qu'il existe un isomorphisme $\alpha : (M_1)_g \longrightarrow (M_2)_f$ de A_{fg}-modules. Posons $N := (M_2)_f$, $\alpha_2 : M_2 \longrightarrow (M_2)_f$ et $\alpha_1 : M_1 \xrightarrow{\theta} (M_1)_g \xrightarrow{\alpha} (M_2)_f$ où θ, α_2 désignent les homomorphismes canoniques. Sous ces hypothèses on a la proposition suivante :

Proposition 1.1.22 ([9], Proposition 5.5) *Si $P = M_1 \prod_N M_2$ est le produit fibré des A-modules M_1 et M_2 sur N (relativement à α_1 et α_2 définis ci-haut), alors les homomorphismes canoniques $\beta_i : P \longrightarrow M_i$ (i=1,2) induisent des isomorphismes $P_f \approx M_1$ et $P_g \approx M_2$ de A_f-modules et A_g-modules respectivement.*

Preuve Considérons le diagramme

$$\begin{array}{ccc} P & \xrightarrow{\beta_1} & M_1 \\ \beta_2 \downarrow & & \downarrow \alpha_1 \\ M_2 & \xrightarrow{\alpha_2} & N := (M_2)_f \end{array}$$

Par la proposition précédente on a que $P_f = (M_1 \prod_N M_2)_f \approx (M_1)_f \prod_{N_f} (M_2)_f$. Comme $(M_2)_f \approx ((M_2)_f)_f$, alors $(M_2)_f \longrightarrow N_f$ est un isomorphisme, l'énoncé 4 implique donc que $P_f \approx (M_1)_f$ (comme des A_f-modules) et comme $(M_1)_f \approx M_1$ (en utilisant l'homomorphisme $\frac{m_1}{f^k} \longmapsto \frac{1}{f^k}.m_1$) on aura que $P_f \approx M_1$ comme des A_f-modules. D'autre part, la proposition précédente donne encore que $P_g \approx (M_1)_g \prod_{N_g} (M_2)_g$. Comme $(M_1)_g \approx (M_2)_f = N$, alors $(M_1)_g \approx N_g$, on déduit par la partie 5 de la proposition 1.1.21 que $P_g \approx (M_2)_g \approx M_2$ (comme A_g-modules). ■

Soit A un anneau, $f \in A$, on écrit $\mathcal{D}(f) = \{\wp \in Spec(A); f \notin \wp\}$. $\mathcal{D}(f)$ est un ouvert de Spec(A) muni de la topologie de Zariski.

Proposition 1.1.23 *Soient $f, g \in$ Spec(A) tels que $\mathcal{D}(f) \cup \mathcal{D}(g) =$ Spec(A). Si M est un A-module tel que M_f est un A_f-module de type fini et M_g est un A_g-module de type fini, alors M est un A-module de type fini.*

Preuve Soient $\{\frac{x_1}{1}, ..., \frac{x_m}{1}\}$ un système générateur du A_f-module M_f et $\{\frac{y_1}{1}, ..., \frac{y_n}{1}\}$ un système générateur du A_g-module M_g. Soit N le sous A-module de M engendré par $\{x_1, ..., x_m, y_1, ..., y_n\}$. Alors pour tout idéal maximal Ω de A on a que $\Omega \in \mathcal{D}(f)$ ou $\Omega \in \mathcal{D}(g)$ d'où $f \notin \Omega$ ou $g \notin \Omega$. Si on suppose que $f \notin \Omega$, alors $M_\Omega \approx (M_f)_\Omega$ et $N_\Omega \approx (N_f)_\Omega$, mais N_f est le sous A_f-module de M_f engendré par $\{\frac{x_1}{1}, ..., \frac{x_m}{1}, \frac{y_1}{1}, ..., \frac{y_n}{1}\}$ donc $N_f = M_f$ et par suite $M_\Omega = N_\Omega$. On obtient le même résultat si on suppose que $\Omega \in \mathcal{D}(g)$, donc $M_\Omega = N_\Omega$ pour tout Ω dans Max(A). En vertu du corollaire 1.1.3, on a $M = N$ et M est de type fini. ∎

Pour la proposition suivante on a besoin du résultat suivant

Lemme 1.1.1 *Soit $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$ une suite exacte de A-modules. Si M et P sont de type fini sur A, alors N l'est aussi.*

Preuve Soient $\{m_1, ..., m_r\}$ et $\{p_1, ..., p_s\}$ deux systèmes générateurs de M et P respectivement. Pour tout $i = 1, ..., r$, posons $x_i = \alpha(m_i)$ et pour tout $j = 1, ..., s$ choisissons $y_j \in N$ tel que $\beta(y_j) = p_j$. Alors pour tout $z \in N$, on a $\beta(z) = a_1p_1 + ... + a_sp_s = \beta(a_1y_1 + ... + a_sy_s)$ où $a_i \in A$ pour tout i. D'où $z - a_1y_1 - ... - a_sy_s \in$ Kerβ et par suite $z - a_1y_1 - ... - a_sy_s = \gamma_1x_1 + ... + \gamma_rx_r$ où $\gamma_i \in A$ pour tout i. Ceci montre que les éléments $x_1, ..., x_r, y_1, ..., y_s$ engendrent N sur A. ∎

Proposition 1.1.24 ([9], Rule 1.14) *Soient f, $g \in A$ avec $\mathcal{D}(f) \cup \mathcal{D}(g) =$ Spec(A), M un A-module tel que M_f est un A_f-module de présentation finie et M_g est un A_g-module de présentation finie. Alors M est un A-module de présentation finie.*

Preuve Considérons une suite exacte de A_f-modules $0 \to \tilde{K} \to (A^n)_f \xrightarrow{\tilde{\alpha}} M_f \to 0$ où $\tilde{K}$ est de type fini sur A_f. Comme $\tilde{\alpha} \in$ Hom$_{A_f}((A^n)_f, M_f)$, il existe alors $\alpha \in$ Hom$_A(A^n, M)$

et $t \in S = \{f^n, n$ entier naturel$\}$ tels que $\tilde{\alpha} = \mu_t^{-1}\alpha_f$ où μ_t^{-1} est l'endomorphisme de M_f défini par: $\mu_t^{-1}(\frac{m}{s}) = \frac{m}{st}$ pour tout m dans M et tout s dans S (proposition 1.1.12). Soit $K =$ kerα. On a alors la suite exacte $0 \to K \to A^n \xrightarrow{\alpha} M$ de A-modules.

Notons que la suite $0 \to K_f \to (A^n)_f \xrightarrow{\alpha_f} M_f \to 0$ est exacte. En effet, α_f est surjectif car $\alpha_f = t\tilde{\alpha}$, $\tilde{\alpha}$ est surjectif et t est une unité de A_f; d'autre part, la suite $0 \to K_f \to (A^n)_f \to M_f$ est exacte car $0 \to K \to A^n \to M$ l'est. On déduit alors que $K_f = \ker(\tilde{\alpha}) = \tilde{K}$ est de type fini sur A_f. Si on refait le même raisonnement pour M_g on obtient une suite exacte $0 \to K' \to A^m \xrightarrow{\alpha'} M$ de A-modules pour laquelle la suite $0 \to K'_g \to (A^m)_g \xrightarrow{\alpha'_g} M_g \to 0$ est exacte et K'_g est de type fini sur A_g. Considérons ensuite l'homomorphisme $(\alpha, -\alpha') : A^n \oplus A^m \longrightarrow M$ défini par $(\alpha, -\alpha')[(x, y)] = \alpha(x) - \alpha'(y)$. Alors pour tout idéal maximal Ω de A on a $(\alpha, -\alpha')_\Omega[\frac{(x,y)}{s}] = \frac{\alpha(x)-\alpha'(y)}{s}$. Comme $\mathrm{Spec}(A) = \mathcal{D}(f) \cup \mathcal{D}(g)$, alors $f \notin \Omega$ ou $g \notin \Omega$. Si on suppose que $f \notin \Omega$, alors $(A_f^n)_\Omega \overset{\theta_1}{\approx} A_\Omega^n$ et $(M_f)_\Omega \overset{\theta_2}{\approx} M_\Omega$. Ceci implique que α_Ω est surjectif car le diagramme

$$\begin{array}{ccc} (A^n)_\Omega & \xrightarrow{\alpha_\Omega} & M_\Omega \\ \theta_1 \downarrow & & \downarrow \theta_2 \\ (A_f^n)_\Omega & \xrightarrow{(\alpha_f)_\Omega} & (M_f)_\Omega \end{array}$$

est commutatif et $(\alpha_f)_\Omega$ est surjectif. Alors pour tout $\frac{m}{t} \in M_\Omega$, il existe $x \in A^n$, $s \notin \Omega$ tels que $\frac{m}{t} = \alpha_\Omega(\frac{x}{s}) = \frac{\alpha(x)}{s} = (\alpha, -\alpha')_\Omega(\frac{(x,0)}{s})$, ce qui implique que $(\alpha, -\alpha')_\Omega$ est surjectif pour tout Ω dans $\mathrm{Max}(A)$. Le corollaire 1.1.3 nous donne maintenant que $(\alpha, -\alpha')$ est surjectif. Soit $\mathcal{U} = \ker(\alpha, -\alpha')$ on a alors la suite exacte $0 \to \mathcal{U} \to A^n \oplus A^m \to M \to 0$.

Il reste à montrer que $\mathcal{U}$ est un A-module de type fini. En vertu de la proposition 1.1.23, il suffit de montrer que $\mathcal{U}_f$ est de type fini sur A_f et que $\mathcal{U}_g$ est de type fini sur A_g. On va le montrer pour $\mathcal{U}_f$, la preuve pour $\mathcal{U}_g$ étant similaire. Fixons $f_1, ..., f_m \in A_f^n$ tels que $\alpha_f(f_i) = \alpha'_f(\frac{e_i}{1})$ pour tout $i = 1, ..., m$ (ceci est possible car α_f est surjectif) où $\{e_1, ..., e_m\}$ est la base canonique de A^m. Soit $\phi : A_f^m \longrightarrow A_f^n$ l'application A_f-linéaire définie par $\phi(\frac{e_i}{1}) = f_i, i = 1, ..., m$. Alors $\alpha_f\phi(\frac{e_i}{1}) = \alpha_f(f_i) = \alpha'_f(\frac{e_i}{1})$ pour tout i, d'où $\alpha_f\phi = \alpha'_f$. Soit $\beta : A_f^n \oplus A_f^m \longrightarrow A_f^n$, l'application A_f-linéaire définie par $\beta(\frac{x}{s}, \frac{y}{t}) = \frac{x}{s} - \phi(\frac{y}{t})$ pour tout $x \in A^n$, $y \in A^m$ et $s, t \notin \{1, f, f^2, ...\}$. Si $(\frac{x}{s}, \frac{y}{t}) \in$

$\mathcal{U}_f$, alors $\alpha_f(\beta(\frac{x}{s},\frac{y}{t})) = \alpha_f(\frac{x}{s} - \phi(\frac{y}{t})) = \alpha_f(\frac{x}{s}) - \alpha'_f(\frac{y}{t}) = (\alpha_f, -\alpha'_f)(\frac{x}{s},\frac{y}{t}) = 0$ (car $\mathcal{U}_f = [\ker(\alpha,-\alpha')]_f = \ker(\alpha,-\alpha')_f \approx \ker(\alpha_f,-\alpha'_f)$), d'où $\beta((\frac{x}{s},\frac{y}{t})) \in \ker(\alpha_f) = K_f$ et par suite $\beta(\mathcal{U}_f) \subseteq K_f$. Réciproquement, si $\frac{x}{s} \in K_f$, alors $\frac{x}{s} = \beta(\frac{x}{s},\frac{0}{1})$, mais $(\alpha_f,-\alpha'_f)(\frac{x}{s},\frac{0}{1}) = \alpha_f(\frac{x}{s}) = 0$ ce qui implique que $(\frac{x}{s},\frac{0}{1}) \in \mathcal{U}_f$, d'où $\beta(\mathcal{U}_f) \supseteq K_f$ et par suite $K_f = \beta(\mathcal{U}_f)$. Soient β' la restriction de β à $\mathcal{U}_f$ et $G = \ker\beta$. Pour tout $(\frac{x}{s},\frac{y}{t}) \in G$, on a $\frac{x}{s} = \phi(\frac{y}{t})$, d'où $(\alpha_f,-\alpha'_f)(\frac{x}{s},\frac{y}{t}) = \alpha'_f(\frac{y}{t}) - \alpha'_f(\frac{y}{t}) = 0$, alors $(\frac{x}{s},\frac{y}{t}) \in \mathcal{U}_f$, ce qui implique que $(\frac{x}{s},\frac{y}{t}) \in \ker\beta'$ et par suite $\ker\beta' \subseteq G$. Comme l'autre inclusion est immédiate, on aura que $G = \ker\beta'$. Considérons le diagramme commutatif suivant de A_f-modules:

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & G & = & G & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathcal{U}_f & \longrightarrow & A_f^n \oplus A_f^m & \longrightarrow & M_f & \longrightarrow & 0 \\
 & & \downarrow\beta' & & \downarrow\beta & & \downarrow 1_{M_f} & & \\
0 & \longrightarrow & K_f & \longrightarrow & A_f^n & \longrightarrow & M_f & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}
\qquad (1.1.4)
$$

Par construction, les colonnes et les lignes du diagramme 1.1.4 sont des suites exactes de A_f-modules. La suite $0 \to G \to A_f^n \oplus A_f^m \to A_f^n \to 0$ étant scindée (A_f^n étant projectif), G est alors l'image de $A_f^n \oplus A_f^m$ par une application linéaire, donc G est de type fini. Comme K_f est encore de type fini sur A_f, $\mathcal{U}_f$ est un A_f-module de type fini (par l'exactitude de la suite $0 \to G \to \mathcal{U}_f \to K_f \to 0$ et le lemme 1.1.1). D'où le résultat. ∎

Dans le cadre de la proposition 1.1.24, il est clair que si M_f est un A_f-module localement libre et M_g est un A_g-module localement libre, alors M est un A-module localement libre. En vertu de la proposition 1.1.13, on a alors:

Corollaire 1.1.4 *Soient f et g deux éléments de A tels que $\mathcal{D}(f) \cup \mathcal{D}(g) =$ Spec(A), et M un A-module tel que M_f est un A_f-module projectif de type fini et M_g est un A_g-module projectif de type fini. Alors M est un A-module projectif de type fini.*

Dimension d'un anneau

Dans ce qui suit on va définir la notion de la dimension d'un anneau et démontrer quelques faits reliés à cette notion et qui seront utilisés dans la preuve de la conjecture de Serre.

Définition 1.1.7 Une suite strictement croissante $\wp_0 \subset \wp_1 \subset ... \subset \wp_n$ d'idéaux premiers de A est appelée une *chaîne première* de A, l'entier n est appelé la *longueur* de la chaîne. La *dimension* de A est définie comme étant le supremum des longueurs des chaînes premières de A. La dimension de A est notée par dimA. Le supremum des longueurs des chaînes premières de A avec $\wp_n = \wp$ où $\wp \in \operatorname{Spec}(A)$ est appelé la *hauteur de* $\wp$ et est noté $\operatorname{ht}(\wp)$.

Proposition 1.1.25 *Si S est une partie multiplicativement stable de A. Alors la dimension de A_S est plus petite ou égale à celle de A.*

Preuve Si $\wp_0 \subset \wp_1 \subset ... \subset \wp_n$ est une chaîne première de A_S de longueur n, alors pour tout $i = 0, ..., n$, $\wp_i = (\wp_i')_S$ où $\wp_i'$ est un idéal premier de A tel que $\wp' \cap S = \emptyset$. Il est immédiat que la suite $\wp_0' \subset \wp_1' \subset ... \subset \wp_n'$ est une chaîne pemière de A, d'où $\dim A_S \leq \dim A$. ■

Proposition 1.1.26 *Si A est un anneau noethérien, alors on a*

1. $\dim A[X] = 1 + \dim A$.
2. *Si* $P \in \operatorname{Spec}(A[X])$ *et* $\wp = P \cap A$, *alors on a*

$$\operatorname{ht}(P) = \begin{cases} \operatorname{ht}(\wp) & \textit{si } P = \wp[X] \\ 1 + \operatorname{ht}(\wp) & \textit{si } \wp[X] \subset P \end{cases}$$

La démonstration de la proposition 1.1.26 nécessite le développement d'une partie de la théorie de dimension. Pour cela on va admettre la proposition. Toutefois, ce résultat est intuitivement acceptable du point de vue qu'on doit s'attendre à ce que la dimension augmente de 1 lorsqu'on passe de A à $A[X]$.

Définition 1.1.8 Un anneau *factoriel* A est un anneau intègre dans lequel:

1. Tout élément non nul et non inversible est un produit fini d'éléments irréductibles de A.

2. Si a est un élément irréductible de A et si a divise le produit bc (b, $c \in A$), alors a divise b ou c.

Proposition 1.1.27 ([9], Examples 1.4) *Soit A un anneau factoriel.*
(1) *Si p est un élément premier de A, alors (p) est un idéal premier et de hauteur* 1.
(2) *Si $\wp$ est un idéal premier et de hauteur* 1, *alors $\wp = (p)$ où p est un élément premier de A.*

Preuve Remarquons tout d'abord que *tout idéal premier et non nul contient un élément premier.* En effet, soit $\wp \in \mathrm{Spec}(A)$, $\wp \neq 0$, alors $\wp$ contient un élément $a \neq 0$ et, comme a n'est pas inversible, on a $a = p_1 ... p_n$ où chaque p_i est un élément premier de A. L'idéal $\wp$ étant premier, un des p_i doit appartenir à $\wp$.

Si p est un élément premier de A, alors il est clair que (p) est un idéal premier et non nul, donc $\mathrm{ht}(\wp) > 0$.

Soit $\wp$ un idéal premier tel que $0 \neq \wp \subseteq (p)$; alors $\wp$ contient un élément premier q de A, donc $(q) \subseteq (p)$, donc $p|q$. Il s'ensuit que p et q sont associés, d'où $\wp = (p)$. Ceci montre que $\mathrm{ht}(p) \leq 1$, donc l'assertion (1) est démontré.

Soit $\wp \in \mathrm{Spec}(A)$, de hauteur 1. Choisissons un élément premier p tel que $p \in \wp$. Alors $0 \neq (p) \subseteq \wp$ et $(p) \in \mathrm{Spec}(A)$, donc $\wp = (p)$ car $\mathrm{ht}(\wp) = 1$. ∎

Proposition 1.1.28 ([9], Examples 1.4) *Si A est principal mais n'est pas un corps, alors* $\dim A = 1$.

Preuve Soient $\wp_1 = (p_1)$ et $\wp_2 = (p_2)$ deux idéaux premiers non nuls de A (p_1, p_2 sont deux éléments premiers de A) tels que $\wp_1 \subseteq \wp_2$. Alors, il existe $\alpha \in A$ tel que

$p_1 = \alpha p_2$, d'où $\alpha \in \wp_1$ ou $p_2 \in \wp_1$. Si $\alpha \in \wp_1$, il existe $\beta \in A$ tel que $\alpha = \beta p_1$, donc $p_1(1-\beta p_2) = 0$, d'où p_2 est inversible (A est intègre), ce qui n'est pas le cas. On a alors que $p_2 \in \wp_1$ et par suite $\wp_1 = \wp_2$. On en déduit que dans $\mathrm{Spec}(A) \setminus \{0\}$, on n'a pas une relation de la forme $\wp_1 \subset \wp_2$, ce qui montre que toute chaîne première de A est de la forme $0 \subset \wp$ (des telles chaînes existent car A n'est pas un corps, il admet alors des idéaux premiers autres que (0)) et par suite la dimension de A est 1. ∎

Proposition 1.1.29 ([16], page 30, Example 3) *Si A est un anneau intègre de dimension zéro, alors A est un corps.*

Preuve Soit $a \in A$ tel que $a \neq 0$, alors a n'appartient à aucun idéal premier, car l'hypothèse dit que 0 est le seul idéal premier. Donc a est inversible. ∎

Lemme 1.1.2 *Soient A un anneau factoriel de dimension 1, $a, b \in A$, d le p.g.c.d de a et b. Alors $(a,b) = (d)$.*

Preuve Notons tout d'abord que le p.g.c.d de a et b est bien défini car A est factoriel. Envisageons les deux cas suivants:
Cas 1 a et b sont relativement premiers. Dans ce cas, $(a,b) = A$ car sinon, on peut choisir un idéal premier $\wp$ de A tel que $(a,b) \subseteq \wp$. Mais comme $\dim(A) = 1$, alors $\wp = (p)$ où p est un élément premier de A (proposition 1.1.27) et par suite $(a,b) \subseteq (p)$, d'où $p|a$ et $p|b$, donc p est inversible dans A, ce qui contredit le fait que $\wp$ est premier. L'assertion est alors vraie dans ce cas.
Cas 2 Dans le cas général $\frac{a}{d}$ et $\frac{b}{d}$ sont relativement premiers, ils engendrent alors, par le cas 1, l'idéal unité. Soient $x, y \in A$ tels que $\frac{a}{d}x + \frac{b}{d}y = 1$, autrement dit $d = ax + by$, ce qui montre que $(d) \subseteq (a,b)$. L'autre inclusion est immédiate. ∎

Proposition 1.1.30 *Soit A un anneau factoriel, de dimension inférieure ou égale à 1. Alors A est principal.*

Preuve Si $\dim(A) = 0$, alors A est un corps (proposition 1.1.29), d'où principal. Supposons pour la suite que $\dim(A) = 1$. Soit I un idéal non nul de A et choisissons

$a_1 \in I$ tel que $a_1 \neq 0$. Si $I \neq (a_1)$, on peut choisir $a'_2 \in I - (a_1)$. Soit a_2 le p.g.c.d de a_1 et a'_2, alors $(a_1) \subset (a_1, a'_2) = (a_2)$ (lemme 1.1.2) $\subseteq I$. Si $(a_2) \neq I$, alors on peut trouver a_3 dans $I - (a_2)$ tel que $(a_2) \subset (a_3) \subseteq I$. On construit ainsi une suite $(a_1) \subset (a_2) \subset ... \subset (a_n) \subset ... \subseteq I$ d' idéaux de A. Comme A est factoriel alors cette suite est stationnaire (dans un anneau factoriel, toute suite d'idéaux principaux est stationnaire), il existe alors un entier n tel que $I = (a_n)$, d'où le résultat. ∎

1.2 Le théorème de Horrocks.

Dans cette section on montrera le résultat suivant (connu sous le nom du théorème de Horrocks): si (A, Ω) est un anneau local, M un $A[X]$-module projectif de type fini et s'il existe un polynôme unitaire $f \in A[X]$ tel que M_f est un $A[X]_f$-module libre, alors M est un $A[X]$-module libre.
On montrera ensuite ce théorème dans le cas général (sans l'hypothèse que A est local). Ce résultat nous aide à mieux comprendre la structure des modules projectifs sur l'anneau des polynômes à une variable. On verra bientôt le rôle crucial qu'il joue dans la démonstration de la conjecture de Serre. Une autre forme de ce résultat se trouve dans le chapitre 2.

Proposition 1.2.1 *Si f est un polynôme unitaire de l'anneau des polynômes $A[X]$ à une variable, alors $A[X]/(f)$ est un A-module libre.*

Preuve Posons $f = X^t + a_{t-1}X^{t-1} + ... + a_1X + a_0$ où $a_i \in A$ pour tout $i = 0, ..., t-1$. Soit $S = \{\overline{1}, ..., \overline{X}^{t-1}\}$ où $\overline{X}^i = X^i + (f)$ pour tout i. L'ensemble S est libre dans $A[X]/(f)$ car si $b_0, ..., b_{t-1} \in A$ sont tels que $b_0\overline{1} + ... + b_{t-1}\overline{X}^{t-1} = 0$, alors le polynôme $b_0 + ... + b_{t-1}X^{t-1}$ appartient à (f), ce qui n'est possible que lorsqu'il est nul. Donc $b_0 = ... = b_{t-1} = 0$.
L'ensemble S engendre $A[X]/(f)$. En effet, soit $g = \alpha_0 + ... + \alpha_s X^s \in A[X]$. On peut supposer que $s \geq t$ (car si $s < t$, on n'a rien à montrer). Le polynôme $g - \alpha_s X^{s-t} f$ a la forme $\beta_{s-1}X^{s-1} + ... + \beta_0$. Si, maintenant $s - 1 \geq t$, le polynôme $g - \alpha_s X^s f - \beta_{s-1}X^{s-1} f$ sera de degré $s - 2$. Si on continue de cette façon, on obtient un polynôme h de $A[X]$

tel que $g - hf = \gamma_r X^r + ... + \gamma_0$ avec $r \leq t-1$, ce qui montre que $\overline{g} = \gamma_r \overline{X}^r + ... + \gamma_0 \overline{1}$ et S est alors une base de $A[X]/(f)$ sur A. ∎

Lemme 1.2.1 *Si A est intègre, S une partie multiplicativement stable de A qui ne contient pas 0 et F un A-module libre, alors l'homomorphisme canonique $f : F \longrightarrow F_S$ est injectif.*

Preuve Soit $(f_i)_{i \in I}$ une base de F sur A et supposons que $x = \sum_{i=1}^n a_i f_i$ ($a_i \in A$ pour tout i) est un élément de F tel que $\frac{x}{1} = 0$ dans F_S. Alors il existe $s \in S$ tel que $sx = 0$, d'où $\sum_{i=1}^n s a_i f_i = 0$ et par suite $s a_i = 0$ pour tout i. Comme A est intègre et $s \neq 0$, alors $a_i = 0$ pour tout i et par suite $x = 0$. ∎

Lemme 1.2.2 *Si F est un A-module libre et B est une algèbre sur A alors $B \otimes_A F$ est un B-module libre.*

Preuve Soit $(a_i)_{i \in I}$ une base de F sur A. Alors $F \approx A^{(I)}$, d'où $B \otimes_A F \approx B \otimes A^{(I)} \approx B^{(I)}$. D'où le résultat. ∎

Lemme 1.2.3 *Si F est un $A[X]$-module libre, Ω un idéal maximal de A, alors $F/\Omega F$ est un $(A/\Omega)[X]$-module libre.*

Preuve Notons tout d'abord que $\Omega F = \Omega[X]F$ (ce qui montre que ΩF est un sous-module de F sur $A[X]$) et que $F/\Omega F$ est un $(A/\Omega)[X]$-module. Comme $F/\Omega F \approx (A/\Omega)[X] \otimes_{A[X]} F$ et $(A/\Omega)[X]$ est une algèbre sur $A[X]$, alors $F/\Omega F$ est libre sur $(A/\Omega)[X]$ (lemme 1.2.2). ∎

Lemme 1.2.4 *Soient $\mathcal{A} \in \mathcal{M}(A, s \times s)$, $\mathcal{B} \in \mathcal{M}(A[X], s \times (t-s))$. Il existe alors deux matrices $\mathcal{B}_0 \in \mathcal{M}(A, s \times (t-s))$ et $\tilde{\mathcal{B}} \in \mathcal{M}(A[X], s \times (t-s))$ telles que $\mathcal{B} = \mathcal{B}_0 + (\mathcal{A} + XE)\tilde{\mathcal{B}}$ où E est la matrice unité $s \times s$.*

Preuve Supposons que $\mathcal{B} = (b_{kj})_{k,j}$ où $b_{kj} \in A[X]$ pour tout k et tout j. Si l est le plus haut degré des polynômes b_{kj}, on peut alors écrire $\mathcal{B}$ sous la forme

$\mathcal{B} = \overline{\mathcal{B}_0} + \overline{\mathcal{B}_1}X + ... + \overline{\mathcal{B}_l}X^l$ où $\overline{\mathcal{B}_i} \in \mathcal{M}(A, s{\times}(t-s))$ pour tout $i = 0, ..., l$. Si on regarde les deux matrices $\overline{\mathcal{B}_0} + \overline{\mathcal{B}_1}X + ... + \overline{\mathcal{B}_l}X^l$ et $\mathcal{A} + EX$ comme étant deux "polynômes" en une seule variable X, on peut alors effectuer la "division" (avec reste) de ces deux polynômes (notons que ceci est possible car le polynôme $\mathcal{A} + EX$ est unitaire dans l'anneau $\mathcal{M}(A, s{\times}s)[X]$). Désignons par $\tilde{\mathcal{B}}$ et $\mathcal{B}_0$ le quotient et le reste de cette division. On a clairement que $\tilde{\mathcal{B}} \in \mathcal{M}(A[X], s{\times}(t-s))$ et $\mathcal{B}_0 \in \mathcal{M}(A, s{\times}(t-s))$ avec $\mathcal{B} = \mathcal{B}_0 + (\mathcal{A} + XE)\tilde{\mathcal{B}}$. ∎

Lemme 1.2.5 *Si $\mathcal{A} \in \mathcal{M}(A, s{\times}t)$ est de la forme:*

$$\mathcal{A} = \begin{pmatrix} \mathcal{A}' & 0 \\ 0 & 1 \end{pmatrix}$$

où $\mathcal{A}' \in \mathcal{M}(A, (s-1){\times}(t-1))$ et si I_s et I'_{s-1} désignent respectivement les idéaux de A engendrés par les mineurs d'ordre s de $\mathcal{A}$ et les mineurs d'ordre s-1 de $\mathcal{A}'$, alors $I_s = I'_{s-1}$.

Preuve Notons tout d'abord que si $s > t$, alors $I_s = I'_{s-1} = 0$. Supposons que $s \leq t$. Si m est un mineur d'ordre s de $\mathcal{A}$, alors $m =$ dét$(\mathcal{H})$ où $\mathcal{H} \in \mathcal{M}(A, s{\times}s)$ est une sous-matrice carrée de $\mathcal{A}$ d'ordre s. Si la s-ième ligne de $\mathcal{H}$ contient des zéros seulement, alors m est nul et par suite appartient à I'_{s-1}. Si, par contre, un coefficient dans la s-ième ligne de $\mathcal{H}$ est 1, alors on développe le déterminant de $\mathcal{H}$ suivant la s-ième ligne et obtient que m est un mineur d'ordre $s-1$ de $\mathcal{A}'$. Dans tous les cas, on a que $m \in I'_{s-1}$ d'où $I_s \subseteq I'_{s-1}$. Réciproquement, si m' est un mineur d'ordre $s-1$ de $\mathcal{A}'$ alors $m' =$ dét$(\mathcal{H}')$ où $\mathcal{H}' \in \mathcal{M}(A, (s-1){\times}(s-1))$ est une sous-matrice carrée de $\mathcal{A}'$. On peut alors écrire:

$$m' = \begin{vmatrix} \mathcal{H}' & 0 \\ 0 & 1 \end{vmatrix}$$

où

$$\begin{pmatrix} \mathcal{H}' & 0 \\ 0 & 1 \end{pmatrix}$$

est une sous-matrice de $\mathcal{A}$ d'ordre $s{\times}s$, d'où m' est un mineur d'ordre s de $\mathcal{A}$. Ceci montre que $I_s = I'_{s-1}$. ∎

Lemme 1.2.6 *Soient R un anneau non commutatif et M un R-module à droite. Soit $M[X]$ le $R[X]$-module à droite dont les éléments sont des polynômes à coefficients dans M. Si $g \in R[X]$ est un polynôme unitaire et $f \in M[X]$, alors il existe deux polynômes uniques q et r de $M[X]$ tels que* $\deg r <$ $\deg g$ *et* $f = qg + r$.

Preuve Par induction sur le degré n de f. ∎

Définition 1.2.1 Soient M un A-module de type fini et $\{m_1, ...m_t\}$ un système générateur de M sur A. Soit $\psi : A^t \longrightarrow M$ l'épimorphisme défini par $\psi(e_i) = m_i$ pour tout i où $(e_i)_{i=1}^t$ est la base canonique de A^t . Si $K =$ $\ker\psi$ est de type fini sur A, alors toute matrice $\mathcal{A} \in \mathcal{M}_{r\times t}(A)$ dont les lignes forment un système générateur de K s'appelle une *matrice de relation* de M par rapport au système générateur $\{m_1, ..., m_t\}$.

Théorème 1.2.1 **(Horrocks)**([9], Theorem 3.11) *Soit (A, Ω) un anneau local, M un $A[X]$-module projectif et de type fini. Supposons qu'il existe un polynôme unitaire f de $A[X]$ tel que M_f est un $A[X]_f$-module libre. Alors M est un $A[X]$-module libre.*

Preuve M étant de type fini sur $A[X]$, alors M_f l'est sur $A[X]_f$ et comme M_f est libre sur $A[X]_f$, on peut choisir une base finie $(\frac{a_i}{1})_{i\in I}$, ($I = \{1, ..., p\}$, $a_i \in M$ pour tout i) de M_f sur $A[X]_f$ (notons que si $(\frac{a_i}{s_i})_{i\in I}$ est une base du $A[X]_f$-module M_f, alors on peut vérifier aisement que la famille $\{\frac{a_i}{1}; i\in I\}$ est encore une base de M_f sur $A[X]_f$). D'autre part, si $f_1, ..., f_p \in A[X]$ sont tels que $f_1a_1 + ... + f_pa_p = 0$ dans M, alors $\frac{f_1}{1}.\frac{a_1}{1} + ... + \frac{f_p}{1}.\frac{f_p}{1} = 0$ dans M_f, ce qui implique que $\frac{f_i}{1} = 0$ pour tout i et par suite, il existe un exposant u tel que $f^u f_i = 0$ pour tout $i = 1, ..., p$, d'où $f_i = 0$ pour tout i car f est un polynôme unitaire de $A[X]$. Ceci montre que la famille $(a_i)_{i\in I}$ est libre sur $A[X]$. Alors le sous-module F de M engendré par les $(a_i)_{i\in I}$ est libre sur $A[X]$. Soit $P := M/F$, on a que $P_f \approx M_f/F_f$, mais $F_f = < \frac{a_i}{1}, i\in I> = M_f$, d'où $P_f = 0$. Comme P est de type fini sur A, il existe alors un entier naturel n tel que $f^n P = 0$ (si $p_1, ..., p_r$ sont des générateurs de P sur A, alors pour tout $k = 1, ..., r$ on peut choisir un entier naturel n_k tel que $f^{n_k} p_k = 0$ car $\frac{p_k}{1} = 0$ dans P_f. Soit $n = \max(n_1, ..., n_r)$, alors $f^n p_k = 0$ pour tout k et par suite $f^n P = 0$).

Soit $\overline{M} = M/f^nM$ et montrons que $\overline{M}$ est libre comme A-module. Posons $S = A[X]/(f^n)$, alors on peut regarder $\overline{M}$ comme S-module (car $(f^n) \subseteq \operatorname{ann}(\overline{M})$) et il est de type fini sur S (car M l'est sur $A[X]$). D'autre part on a que $\overline{M}$ est un S-module projectif car il existe un $A[X]$-module M' tel que $M \oplus M' = L$ est libre, ce qui implique que $(M/f^nM) \oplus (M'/f^nM') \approx L/f^nL$ et L/f^nL est libre sur S (en effet si $(a_i)_{i=1}^r$ est une base de L sur $A[X]$, alors $(a_i + f^nL)_{i=1}^r$ est une base de L/f^nL sur S). Comme S est un A-module libre (proposition 1.2.1), la proposition 1.1.4 implique que M/f^nM est un A-module projectif, donc libre car A est local (corollaire 1.1.2) et il est de rang fini sur A.

Montrons par la suite que, comme A-module, P est de présentation finie. Le foncteur $S \otimes_{A[X]} -$ (qui est exact à droite) appliqué à la suite exacte $0 \to F \to M \to P \to 0$ de $A[X]$-modules donne la suite exacte $S \otimes_{A[X]} F \to \overline{M} \to S \otimes_{A[X]} P \to 0$ de S-modules, qui est aussi exact sur A. Comme $S \otimes_{A[X]} P \approx P/f^nP = P$ (car $f^nP = 0$) et $\overline{M}$ est libre de rang fini sur A, il suffit de montrer que $S \otimes_{A[X]} F \approx F/f^nF$ est de type fini comme A-module. Pour voir ceci, remarquons que F/f^nF est de type fini sur $A[X]$ (F l'est), donc de type fini sur S. Comme S est un A-module de type fini, alors F/f^nF est de type fini sur A. D'où P est un A-module de présentation finie.

L'étape suivante est de montrer que P est libre comme A-module. Tout d'abord, notons que M est projectif sur $A[X]$ et ce dernier est libre comme A-module (ayant $1, X, X^2, \ldots$ comme base), alors la proposition 1.1.4 implique que M est un A-module projectif. Comme on a la suite exacte $0 \to F \overset{\alpha}{\hookrightarrow} M \to P \to 0$ de A-modules, il suffit en vertu de la proposition 1.1.8 de montrer que l'application $\overline{\alpha} : F/\Omega F \longrightarrow M/\Omega M$ est injective. Pour voir ceci, notons que $F/\Omega F$ peut être regardé comme un $(A/\Omega)[X]$-module et si $\overline{f}$ désigne $f + \Omega A[X]$, alors on a $(F/\Omega F)_{\overline{f}} \approx F_f/(\Omega F)_f$ et $M_f/(\Omega M)_f \approx (M/\Omega M)_{\overline{f}}$ (via: $\frac{\overline{x}}{\overline{f}^r} \mapsto \frac{\overline{x}}{f^r}$), mais $M_f = F_f$ et $(\Omega F)_f = (\Omega M)_f$, d'où $(F/\Omega F)_{\overline{f}} \overset{\overline{\alpha}_{\overline{f}}}{\approx} (M/\Omega M)_{\overline{f}}$ (ici $\overline{\alpha}_{\overline{f}}$ est l'homomorphisme induit par $\overline{\alpha}$ en localisant en $\overline{f}$). Considérons le diagramme commutatif suivant de $(A/\Omega)[X]$-modules:

$$
\begin{array}{ccc}
F/\Omega F & \xrightarrow{\overline{\alpha}} & M/\Omega M \\
l_F \downarrow & & \downarrow l_M \\
(F/\Omega F)_{\overline{f}} & \xrightarrow{\overline{\alpha}_{\overline{f}}} & (M/\Omega M)_{\overline{f}}
\end{array}
\tag{1.2.1}
$$

où l_F, l_M sont les localisations. Comme $F/\Omega F$ est libre sur $(A/\Omega)[X]$ (lemme 1.2.3), alors le lemme 1.2.1 implique que l_F est injectif. La commutativité du diagramme 1.2.1 nous donne que $\overline{\alpha}$ est injectif, d'où P est un A-module libre de rang fini (P est de type fini sur A car il est de présentation finie sur A).

Considérons une base $\{\overline{p_1}, ..., \overline{p_s}\}$ de P sur A où $p_i \in M$ pour tout i et une base $\{p_{s+1}, ..., p_t\}$ de F sur $A[X]$. Notons qu'on peut supposer que $s > 0$, car si $s = 0$, alors $P = 0$, d'où $M = F$ qui est libre sur $A[X]$.

Montrons maintenant que chaque élément x de M s'écrit de manière unique sous la forme

$$\sum_{i=1}^{s} \alpha_i p_i + \sum_{j=s+1}^{t} \beta_j p_j, \tag{1.2.2}$$

où $\alpha_i \in A$ et $\beta_j \in A[X]$.
Comme $P = M/F$ est engendré par $\{\overline{p_1}, ..., \overline{p_s}\}$ sur A, il existe α_1,...,$\alpha_s \in A$ tels que $x - \alpha_1 p_1 - ... - \alpha_s p_s \in F$; comme F est engendré par $\{p_{s+1}, ..., p_t\}$ sur $A[X]$, il existe β_{s+1},...,$\beta_t \in A[X]$ tels que la relation 1.2.2 est satisfaite.

Pour montrer l'unicité de l'expression 1.2.2, il suffit de montrer que la relation

$$\sum_{i=1}^{s} \alpha_i p_i + \sum_{j=s+1}^{t} \beta_j p_j = 0 \quad (\alpha_i \in A,\ \beta_j \in A[X])$$

implique $\alpha_i = 0$ et $\beta_j = 0$ pour tout $i = 1, ..., s$ et tout $j = s+1, ..., t$. Mais cette relation implique

$$\sum_{i=1}^{s} \alpha_i \overline{p_i} = 0 \qquad (\text{dans } P)$$

d'où $\alpha_i = 0$ pour tout $i = 1, .., s$. Il s'en suit que $\sum_{j=s+1}^{t} \beta_j p_j = 0$, donc $\beta_j = 0$ pour tout $j = s+1, ..., t$.

En particulier, pour chaque $k = 1, ..., s$, la relation 1.2.2 nous permet d'écrire

$$-Xp_k = \sum_{i=1}^{s} \alpha_{ki} p_i + \sum_{j=s+1}^{t} b_{kj} p_j \tag{1.2.3}$$

où $\alpha_{ki} \in A$ et $b_{kj} \in A[X]$. Considérons les deux matrices

$$\mathcal{A} = (\alpha_{ki})_{k,i} \in \mathcal{M}(A, s{\times}s), \qquad \mathcal{B} = (b_{kj})_{k,j} \in \mathcal{M}(A[X], s{\times}(t-s))$$

et soit $\mathcal{C}$ la matrice $(\mathcal{A} + XE|\mathcal{B})$.

$$\mathcal{C} = \begin{pmatrix} \alpha_{11} + X & \dots & \alpha_{1s} & b_{1s+1} & \dots & b_{1t} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{s1} & \dots & \alpha_{ss} + X & b_{ss+1} & \dots & b_{st} \end{pmatrix}$$

Clairement, $\mathcal{C} \in \mathcal{M}(A[X], s{\times}t)$.

Comme $\{p_1, ..., p_s, p_{s+1}, ..., p_t\}$ est un système de générateurs de M sur $A[X]$, on peut donc considérer un épimorphisme $\psi : A[X]^t \longrightarrow M$ qui envoie e_i à p_i (où les e_i sont les éléments de la base canonique de $A[X]^t$) et dont on note par K son noyau. Montrons que $\mathcal{C}$ est une matrice de relation du $A[X]$-module M, relativement au système générateur $\{p_1, ..., p_t\}$ (en d'autres termes, les lignes de $\mathcal{C}$ forment un système générateur de $K = \ker\psi$). Pour voir ceci, montrons tout d'abord que les lignes de $\mathcal{C}$ sont dans K. Soit $h_i = (\alpha_{i1}, ..., \alpha_{ii} + X, ..., \alpha_{is}, b_{is+1}, ..., b_{it})$ la i-ème ligne de $\mathcal{C}$. Alors $\psi(h_i) = \alpha_{i1}p_1 + ... + (\alpha_{ii} + X)p_i + ... + \alpha_{is}p_s + b_{is+1}p_{s+1} + ... + b_{it}p_t$. Mais $-Xp_i = \alpha_{i1}p_1 + ... + \alpha_{ii}p_i + ... + \alpha_{is}p_s + b_{is+1}p_{s+1} + ... + b_{it}p_t$, d'où $\psi(h_i) = 0$ pour tout $i = 1, ..., s$. Alors $\{h_1, ..., h_s\} \subset K$. Pour montrer que $\{h_1, ..., h_s\}$ engendre K, on prend $M = \mathcal{M}_{1\times s}(A)$ et $R = \mathcal{M}_{s\times s}(A)$ dans le lemme 1.2.6. Alors pour tout $x = (a_1, ..., a_s, b_{s+1}, ..., b_t) \in A[X]^t$, il existe $\mathcal{Q}, \mathcal{R} \in \mathcal{M}_{1\times s}(A[X])$ tels que

$$(a_1, ..., a_s) = \mathcal{Q}(\mathcal{A} + XE) + \mathcal{R} \tag{1.2.4}$$

et $\deg(\mathcal{R}) < \deg(\mathcal{A}+XE)$. Comme $\mathcal{A}+XE$ est de degré 1, $\mathcal{R} = (r_1, ..., r_s)$ est dans $\mathcal{M}_{1\times s}(A)$. La relation 1.2.4 implique que $x = (a_1, ..., a_s, b_{s+1}, ..., b_t) = \mathcal{Q}(\mathcal{A}+XE \mid \mathcal{B}) + (\mathcal{R} \mid (b_{s+1}, ..., b_t) - \mathcal{Q}\mathcal{B})$. Ceci montre que $x = \sum_{i=1}^{s} f_i h_i + (r_1, ..., r_s, b'_{s+1}, ..., b'_t)$ où $r_i \in A$, $b'_j \in A[X]$ et $f_i \in A[X]$ pour tout i et tout j, d'où $\psi(x) = \psi(r_1, ..., r_s, b'_{s+1}, ..., b'_t)$

(car $\psi(h_i) = 0$ pour tout i) $= \sum_{i=1}^{s} r_i p_i + \sum_{j=s+1}^{t} b'_j p_j$. Si, maintenant $x \in K$, alors $r_i = 0$ et $b'_j = 0$ pour tout i et tout j (par un raisonnement fait en haut), d'où $x = \sum_{i=1}^{s} f_i h_i$. Ceci montre que $\{h_1, ..., h_s\}$ engendre K et par suite la matrice $\mathcal{C}$ détermine complètement le $A[X]$-module M car $M \approx A[X]^t / <h_1, ..., h_s>$.

Montrons ensuite que l'idéal $I = I_s(\mathcal{C})$ de $A[X]$ engendré par les mineurs d'ordre $s \times s$ de $\mathcal{C}$ est $A[X]$ lui même. Pour ceci, notons qu'il suffit, en vertu de la proposition 1.1.10, de montrer que $I_\Delta = A[X]_\Delta$ pour tout idéal maximal Δ de $A[X]$ (appliquer la proposition au A-module $A[X]/I$). Soit alors Δ un idéal maximal de $A[X]$, on a que M_Δ est un $A[X]_\Delta$-module projectif (proposition 1.1.3), donc libre sur $A[X]_\Delta$ (corollaire 1.1.2) et comme $M_f = F_f$, alors $(M_f)_\Delta = (F_f)_\Delta$, d'où $(M_\Delta)_f = (F_\Delta)_f$ et par suite le rang de M_Δ est égal à celui de $(F_\Delta)_f$ qui est $t - s$. D'autre part, on a que $(A[X]^t)_\Delta \approx K_\Delta \oplus M_\Delta$ car la suite $0 \rightarrow K_\Delta \rightarrow (A[X]^t)_\Delta \rightarrow M_\Delta \rightarrow 0$ est scindée (M_Δ étant projectif), alors K_Δ est un $(A[X])_\Delta$-module libre de rang s. Ceci montre que $\{\frac{h_1}{1}, ..., \frac{h_s}{1}\}$ forme une base de K_Δ sur $A[X]_\Delta$. Comme cette base peut être complétée à une base de $A[X]_\Delta^t$, au moins un mineur $s \times s$ de l'image de $\mathcal{C}$ est inversible dans $A_\Delta[X]$. D'où $I_\Delta = A[X]_\Delta$ pour tout Δ dans $\mathrm{Max}(A[X])$. Alors $I = A[X]$.

Notons ensuite qu'on peut supposer que $\mathcal{B} = (b_{kj})_{k,j} \in \mathcal{M}(A, s \times (t-s))$. En effet, la relation 1.2.2 peut s'écrire matriciellement comme :

$$-X \begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} = \mathcal{A} \begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} + \mathcal{B} \begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix}. \qquad (1.2.5)$$

Par le lemme 1.2.4, on peut écrire $\mathcal{B} = \mathcal{B}_0 + (\mathcal{A} + XE)\tilde{\mathcal{B}}$ où $\mathcal{B}_0 \in \mathcal{M}(A, s \times (t-s))$ et $\tilde{\mathcal{B}} \in \mathcal{M}(A[X], s \times (t-s))$. La relation 1.2.5 s'écrit alors

$$-X \begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} = \mathcal{A} \begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} + (\mathcal{B}_0 + (\mathcal{A} + XE))\tilde{\mathcal{B}} \begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix}.$$

Ou autrement

$$(\mathcal{A}+XE)\left\{\begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} + \tilde{\mathcal{B}}\begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix}\right\} + \mathcal{B}_0\begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix} = 0. \tag{1.2.6}$$

Si on pose

$$\begin{pmatrix} p'_1 \\ \vdots \\ p'_s \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} + \tilde{\mathcal{B}}\begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix}$$

alors pour tout $k = 1, ..., s$, p'_k est un représentant de $\overline{p_k}$ et la relation 1.2.6 devient

$$(\mathcal{A}+XE)\left\{\begin{pmatrix} p'_1 \\ \vdots \\ p'_s \end{pmatrix}\right\} + \mathcal{B}_0\begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix} = 0.$$

Si on prend pour $\mathcal{B}$ la matrice $\mathcal{B}_0$, on peut supposer que dans la relation 1.2.2 les coefficients b_{kj} sont dans A pour tout k et tout j. Par la suite $\mathcal{B} \in \mathcal{M}(A, s\times(t-s))$.

Soit $g = \det(\mathcal{A} + XE) \in A[X]$ et soit J l'idéal de A engendré par les entrées de la matrice $\mathcal{B}$. Comme $I = A[X]$, alors $A[X] = A[X]g + A[X]J$ car tout mineur d'ordre s de $\mathcal{C}$ est soit g, soit une combinaison linéaire des entrées de $\mathcal{B}$ à coefficients dans $A[X]$. Soit T l'anneau-quotient $A[X]/(g)$. Comme g n'est pas inversible dans $A[X]$, $T \neq 0$. Par la proposition 1.2.1, T est un A-module libre car g est un polynôme unitaire. D'autre part, pour tout $h \in A[X]$, on a $h = gh_1 + jh_2$ où $h_1, h_2 \in A[X]$, $j \in J$, d'où $\overline{h} = h + (g) = \overline{h_2 j} = j\overline{h_2} \in J.T$. Alors $T = J.T$, ce qui donne que $J = A$ car sinon $J \subset \Omega$ et par suite $T = 0$ (par le lemme de Nakayama), ce qui n'est pas le cas. Comme $J = A$, alors un au moins des entrées de la matrice $\mathcal{B}$ est inversible car sinon, toutes ces entrées seront contenues dans Ω (A est local) et par suite toute combinaison linéaire des entrées de $\mathcal{B}$ à coefficients dans A sera contenue dans Ω, ce qui contredit le fait que $1 \notin \Omega$. On peut alors, à l'aide d'une suite des transformations élémentaires sur les lignes et les colonnes, rendre la matrice $(\mathcal{A}+XE|\mathcal{B})$ sous la forme

$$\mathcal{C}' = \begin{pmatrix} \mathcal{A}' + XE'|\mathcal{B}' & 0 \\ 0 & 1 \end{pmatrix}$$

où $\mathcal{A}' \in \mathcal{M}(A,(s-1)\times(s-1))$ et $\mathcal{B}' \in \mathcal{M}(A,(s-1)\times(t-s-1))$ et E' est la matrice unité $(s-1)\times(s-1)$.
Les deux matrices $\mathcal{C}$ et $\mathcal{C}'$ étant semblables on a que $I_s(\mathcal{C}) = I_s(\mathcal{C}')$ où $I_s(\mathcal{C})$, $I_s(\mathcal{C}')$ sont respectivement les idéaux de A engendrés par les mineurs $s\times s$ de $\mathcal{C}$ et de $\mathcal{C}'$ (proposition 1.1.19). Par le lemme 1.2.5, on a que $I_s(\mathcal{C}') = I_{s-1}(\mathcal{A}' + XE'|\mathcal{B}')$. D'où $I_{s-1}(\mathcal{A}'+XE'|\mathcal{B}') = A[X]$. Si on refait le même calcul avec la matrice $(\mathcal{A}'+XE'|\mathcal{B}')$ et on continue de cette façon, on trouve enfin que la matrice $(\mathcal{A}+XE|\mathcal{B})$ est semblable à la matrice $(0|E)$ où E est la matrice unité de $\mathcal{M}(A,s\times s)$. Comme $\mathcal{C} = (\mathcal{A}+XE|\mathcal{B})$ est une matrice des relations du $A[X]$-module M et que toute autre matrice semblable à $\mathcal{C}$ est encore une matrice de relation de M, alors $M \approx A[X]^t/L$ où L est le sous $A[X]$-module de $A[X]^t$ engendré par les lignes de la matrice

$$(0|E) = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \\ 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Considérons l'épimorphisme

$$\begin{array}{ccc} A[X]^t & \xrightarrow{\theta} & A[X]^{t-s} \\ (x_1,\dots,x_t) & \longmapsto & (x_1,\dots,x_{t-s}) \end{array}$$

Il est clair que $\ker\theta$ est engendré par les lignes de la matrices $(0|E)$, d'où $A[X]^{t-s} \approx A[X]^t/L \approx M$. Ceci montre que M est un $A[X]$-module libre. ∎

Dans ce qui suit on va montrer que le théorème de Horrocks s'applique pour n'importe quel anneau commutatif. La démonstration de ce résultat nécessite beaucoup de travail. On commence par montrer quelques propriétés élémentaires.

Lemme 1.2.7 *1.* **(The five lemma)** ([19], Proposition 2.11.15) *Soit*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f} & M_2 & \xrightarrow{g} & M_3 & \xrightarrow{h} & M_4 & \xrightarrow{j} & M_5 \\ \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \downarrow\delta & & \downarrow\epsilon \\ M_1' & \xrightarrow{f'} & M_2' & \xrightarrow{g'} & M_3' & \xrightarrow{h'} & M_4' & \xrightarrow{j'} & M_5' \end{array}$$

un diagramme commutatif de A-modules avec des lignes exactes. Si α, β, δ, ϵ sont des isomorphismes, alors γ l'est aussi.

2. Soit

$$\begin{array}{ccc} M & \xrightarrow{\beta} & N \\ \downarrow f & & \downarrow g \\ M_1 & \xrightarrow{\gamma} & N_1 \end{array} \tag{1.2.7}$$

un diagramme commutatif de A-modules. Alors 1.2.7 induit un diagramme commutatif

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \ker\beta & \longrightarrow & M & \xrightarrow{\beta} & N & \longrightarrow & \mathrm{coker}\beta & \longrightarrow & 0 \\ & & \downarrow f' & & \downarrow f & & \downarrow g & & \downarrow g' & & \\ 0 & \longrightarrow & \ker\gamma & \longrightarrow & M_1 & \xrightarrow{\gamma} & N_1 & \longrightarrow & \mathrm{coker}\gamma & \longrightarrow & 0. \end{array} \tag{1.2.8}$$

Si de plus f, g sont des isomorphismes, alors f', g' le sont encore.

Preuve 1. Prouvons tout d'abord que γ est injective. Soit $x_3 \in M_3$ tel que $\gamma(x_3) = 0$, alors $h'\gamma(x_3) = 0$, d'où $\delta h(x_3) = 0$ et par suite $x_3 \in \ker h$ car δ est injective. Comme $\ker h = \mathrm{Im} g$, il existe $x_2 \in M_2$ tel que $x_3 = g(x_2)$ ce qui implique que $g'\beta(x_2) = \gamma g(x_2) = 0$, alors $\beta(x_2) = f'(x_1')$ où $x_1' \in M_1'$. α étant surjectif, il existe $x_1 \in M_1$ tel que $x_1' = \alpha(x_1)$. Alors on a $\beta f(x_1) = f'\alpha(x_1) = f'(x_1') = \beta(x_2)$, d'où $x_2 = f(x_1)$ (β est injectif). Enfin $x_3 = g(x_2) = gf(x_1) = 0$.
Montrons ensuite que γ est surjectif. Soit $x_3' \in M_3'$, alors il existe $x_4 \in M_4$ tel que $h'(x_3') = \delta(x_4)$, d'où $\epsilon j(x_4) = j'\delta(x_4) = j'h'(x_3') = 0$ ce qui implique que $j(x_4) = 0$ et par suite $x_4 = h(x_3)$ où $x_3 \in M_3$. Alors $h'(x_3' - \gamma(x_3)) = \delta(x_4) - \delta h(x_3) = 0$, d'où $x_3' - \gamma(x_3) = g'(x_2')$ pour un certain $x_2' \in M_2'$. Comme $x_2' = \beta(x_2)$, $x_2 \in M_2$, alors $x_3' = \gamma(x_3) + g'(x_2') = \gamma(x_3) + g'\beta(x_2) = \gamma(x_3 + g(x_2))$.
2. Si $x \in \ker\beta$, alors $\gamma f(x) = g\beta(x) = 0$, d'où $f(\ker\beta) \subseteq \ker\gamma$. On peut donc considérer la réstriction f' de f à $\ker\beta$. D'autre part, si $n_1 \in g(\mathrm{Im}\beta)$, alors $n_1 = g\beta(m)$ $(m \in M) = \gamma f(m) \in \gamma(M_1)$, d'où $g(\mathrm{Im}\beta) \subseteq \gamma(M_1)$, ce qui implique que g induit un homomorphisme $g' : \mathrm{coker}\beta \longrightarrow \mathrm{coker}\gamma$ et il est facile de vérifier la commutativité du diagramme 1.2.8. Si, maintenant, f, g sont des isomorphismes, alors la partie 1 implique que f' et g' sont aussi des isomorphismes. ∎

Définition 1.2.2 Un $A[X]$-module M est dit une *extension* de A s'il existe un A-module N tel que $M \approx N[X]$ (comme $A[X]$-modules). M est dit une *extension locale* de A en $\Omega \in \mathrm{Max}(A)$ si M_Ω est une extension de A_Ω.

Proposition 1.2.2 *Soient M un $A[X]$-module et N un A-module. Si $M = N[X]$, alors $N \approx M/XM$ comme A-modules.*

Preuve Soit

$$\begin{array}{rcl} M & \xrightarrow{\psi} & N \\ f = \sum_{i=0}^{n} \alpha_i X^i & \longmapsto & f(0) = \alpha_0. \end{array}$$

Clairement, ψ est un épimorphisme avec $\ker\psi = XM$. ∎

Proposition 1.2.3 *Si $p \geq 1$, alors $A[X]^p / XA[X]^p \approx A^p$.*

Preuve Soit $A[X]^p \xrightarrow{h} A^p$ l'épimorphisme défini par :
$h(f_1, ..., f_p) = (f_1(0), ..., f_p(0))$. Clairement, $\ker h = XA[X]^p$, d'où le résultat. ∎

Proposition 1.2.4 ([9], Proposition 1.15) *Si $0 \to K_i \xrightarrow{\beta_i} F_i \xrightarrow{\alpha_i} M_i \to 0$ $(i = 1, 2)$ sont deux suites exactes de A-modules avec F_1, F_2 libres sur A, alors on a*

1. *S'il existe un isomorphisme $\mu : M_1 \longrightarrow M_2$, alors il existe $\alpha \in \mathrm{Aut}(F_1 \oplus F_2)$ tel que le diagramme*

$$\begin{array}{ccc} F_1 \oplus F_2 & \xrightarrow{(\alpha_1, 0)} & M_1 \\ \alpha \downarrow & & \downarrow \mu \\ F_1 \oplus F_2 & \xrightarrow{(0, \alpha_2)} & M_2 \end{array} \tag{1.2.9}$$

   est commutatif. De plus, toute application α satisfaisant cette condition satisfait aussi $\alpha[\beta_1(K_1) \oplus F_2] = F_1 \oplus \beta_2(K_2)$.

2. *S'il existe $\alpha \in \mathrm{Aut}(F_1 \oplus F_2)$ avec $\alpha[\beta_1(K_1) \oplus F_2] = F_1 \oplus \beta_2(K_2)$, alors il existe un isomorphisme $\mu : M_1 \longrightarrow M_2$ pour lequel le diagramme 1.2.9 est commutatif.*

Preuve 1. Considérons le diagramme suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 & \xrightarrow{\beta_1} & F_1 & \xrightarrow{\alpha_1} & M_1 & \longrightarrow & 0 \\ & & & & \gamma_1 \downarrow \uparrow \gamma_2 & & \mu \downarrow \uparrow \mu^{-1} & & \\ 0 & \longrightarrow & K_2 & \xrightarrow{\beta_2} & F_2 & \xrightarrow{\alpha_2} & M_2 & \longrightarrow & 0 \end{array}$$

Comme F_1 est projectif (il est libre) et α_2 est surjective, alors il existe $\gamma_1 : F_1 \longrightarrow F_2$ tel que $\alpha_2\gamma_1 = \mu\alpha_1$ (théorème 1.1.1). De même, on trouve $\gamma_2 : F_2 \longrightarrow F_1$ tel que $\mu^{-1}\alpha_2 = \alpha_1\gamma_2$. Considérons les deux homomorphismes

$$\begin{array}{ccc} F_1 \oplus F_2 & \xrightarrow{\alpha'} & F_1 \oplus F_2 \\ (x,y) & \longmapsto & (x, y-\gamma_1(x)) \end{array} \quad \text{et} \quad \begin{array}{ccc} F_1 \oplus F_2 & \xrightarrow{\alpha''} & F_1 \oplus F_2 \\ (x,y) & \longmapsto & (x-\gamma_2(y), y) \end{array}.$$

Une simple vérification montre que α', α'' sont des isomorphismes. Posons $\alpha = \alpha'^{-1}\alpha'' \in \operatorname{Aut}(F_1 \oplus F_2)$. Avec ce choix de α, le diagramme 1.2.9 est commutatif. En effet, pour tout $(x,y) \in F_1 \oplus F_2$ on a $(0,\alpha_2)\alpha(x,y) = (0,\alpha_2)\alpha'^{-1}(x-\gamma_2(y), y) = (0,\alpha_2)(x-\gamma_2(y), y+\gamma_1(x)-\gamma_1\gamma_2(y)) = \alpha_2(y)+\alpha_2\gamma_1(x)-\alpha_2\gamma_1\gamma_2(y) = \alpha_2(y)+\mu\alpha_1(x)-\mu\mu^{-1}\alpha_2(y) = \mu\alpha_1(x) = \mu(\alpha_1, 0)(x,y)$, d'où la commutativité du diagramme 1.2.9. Remarquons que $\beta_1(K_1) \oplus F_2 = \operatorname{Ker}(\alpha_1, 0)$ et $F_1 \oplus \beta_2(K_2) = \operatorname{Ker}(0,\alpha_2)$; comme α et μ sont des isomorphismes et le diagramme 1.2.9 est commutatif, il s'en suit que $\alpha[\beta_1(K_1) \oplus F_2] = F_1 \oplus \beta_2(K_2)$ (notons qu'on peut encore utiliser la deuxième partie du lemme 1.2.7).
2. Soit $\alpha' : \beta_1(K_1) \oplus F_2 \longrightarrow F_1 \oplus \beta_2(K_2)$ la restriction de α. Alors le diagramme

$$\begin{array}{ccccccccc} 0 & \to & \beta_1(K_1) \oplus F_2 & \hookrightarrow & F_1 \oplus F_2 & \overset{(\alpha_1,0)}{\to} & M_1 & \to & 0 \\ & & \alpha' \downarrow & & \alpha \downarrow & & & & \\ 0 & \to & F_1 \oplus \beta_2(K_2) & \hookrightarrow & F_1 \oplus F_2 & \overset{(0,\alpha_2)}{\to} & M_2 & \to & 0 \end{array}$$

est commutatif avec des lignes exactes et α et α' sont des isomorphismes. Par la partie 2 du lemme 1.2.7, il existe un isomorphisme $\mu : M_1 \longrightarrow M_2$ tel que le diagramme 1.2.9 est commutatif. D'où le résultat. ■

Corollaire 1.2.1 ([9], Corollary 1.16) *Soient $F_i' \xrightarrow{\beta_i} F_i \xrightarrow{\alpha_i} M_i \longrightarrow 0$ $(i = 1, 2)$ deux suites exactes de A-modules telles que F_1', F_1, F_2', F_2 sont libres sur A, alors $M_1 \approx M_2$ si et seulement s'il existe $\alpha \in \operatorname{Aut}(F_1 \oplus F_2)$ et $\beta \in \operatorname{Aut}(F_1' \oplus F_2 \oplus F_1 \oplus F_2')$ tel que le diagramme*

$$\begin{array}{ccc} F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \overset{(\beta_1 \oplus 1_{F_2}, 0)}{\longrightarrow} & F_1 \oplus F_2 \\ \beta \downarrow & & \downarrow \alpha \\ F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \overset{(0, 1_{F_1} \oplus \beta_2)}{\longrightarrow} & F_1 \oplus F_2. \end{array} \tag{1.2.10}$$

est commutatif.

Preuve Supposons que $M_1 \overset{i}{\approx} M_2$ et soit $K_i = \ker\alpha_i = \mathrm{Im}\beta_i$ $(i = 1, 2)$. Alors les deux suites $0 \to K_i \hookrightarrow F_i \xrightarrow{\alpha_i} M_i \to 0$ $(i = 1, 2)$ sont exactes, d'où par la proposition précédente, il existe $\alpha \in \mathrm{Aut}(F_1 \oplus F_2)$ tel que le diagramme

$$\begin{array}{ccc} F_1 \oplus F_2 & \xrightarrow{(\alpha_1, 0)} & M_1 \\ \alpha \downarrow & & \downarrow i \\ F_1 \oplus F_2 & \xrightarrow{(0, \alpha_2)} & M_2 \end{array}$$

est commutatif avec $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$. Soit $\alpha' = \alpha/(K_1 \oplus F_2)$. Alors α' établit un isomorphisme entre $K_1 \oplus F_2$ et $F_1 \oplus K_2$. Considérons les deux suites exactes suivantes

$$0 \longrightarrow \ker\beta_1 \oplus 0 \longrightarrow F_1' \oplus F_2 \xrightarrow{\beta_1 \oplus 1_{F_2}} K_1 \oplus F_2 \longrightarrow 0$$
$$0 \longrightarrow 0 \oplus \ker\beta_2 \longrightarrow F_1 \oplus F_2' \xrightarrow{1_{F_1} \oplus \beta_2} F_1 \oplus K_2 \longrightarrow 0$$

La partie 1 de la proposition précédente nous donne l'existence d'un automorphisme $\beta \in \mathrm{Aut}(F_1' \oplus F_2 \oplus F_1 \oplus F_2')$ tel que le diagramme:

$$\begin{array}{ccccc} F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \xrightarrow{(\beta_1 \oplus 1_{F_2}, 0)} & K_1 \oplus F_2 & \longrightarrow & F_1 \oplus F_2 \\ \beta \downarrow & & \downarrow \alpha' & & \downarrow \alpha \\ F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \xrightarrow{(0, 1_{F_1} \oplus \beta_2)} & F_1 \oplus K_2 & \longrightarrow & F_1 \oplus F_2 \end{array}$$

est commutatif, donc le diagramme 1.2.10 est commutatif. Pour la réciproque, on considère le diagramme 1.2.10, on note que $M_1 = \mathrm{coker}(\beta_1 \oplus 1_{F_2}, 0)$ et $M_2 = \mathrm{coker}(0, 1_{F_1})$ et on applique la partie 2 du lemme 1.2.7. ∎

Lemme 1.2.8 *Soient X, Y, M trois A-modules libres tels que X est de rang m et Y est de rang n. Soient $\alpha_1 : X \longrightarrow M$, $\alpha_2 : Y \longrightarrow M$ deux homomorphismes de A-modules et B une base de M sur A. Si $B_1 = \{x_1, ..., x_m\}$ et $B_2 = \{y_1, ..., y_n\}$ sont des bases de X et Y sur A, alors l'ensemble $B_{1,2} := \{(x_1, 0), ..., (x_m, 0), (0, y_1), ..., (0, y_n)\}$ est une base de $X \oplus Y$ sur A et la matrice de (α_1, α_2) par rapport aux bases B et $B_{1,2}$ est*

$$\left([\alpha_1] \mid [\alpha_2] \right)$$

où $[\alpha_i]$ $(i = 1, 2)$ est la matrice de α_i par rapport aux bases B_i et B.

Preuve Il suffit de remarquer que $(\alpha_1, \alpha_2)(x_i, 0) = \alpha_1(x_i)$ et $(\alpha_1, \alpha_2)(0, y_j) = \alpha_2(y_j)$ pour tout i et tout j. ■

De la même façon on montre le lemme suivant

Lemme 1.2.9 *Soient X, Y, M, N quatre A-modules libres et supposons qu'on a deux homomorhismes $\alpha_1 : X \longrightarrow M$, $\alpha_2 : Y \longrightarrow N$. Soient B_1, B_2, B'_1 et B'_2 des bases de X, Y, M et N sur A et considérons les bases correspondantes $B_{1,2}$, $B'_{1,2}$ de $X \oplus Y$ et $M \oplus N$ respectivement sur A. Alors, la matrice représentante de l'homomorphisme $\alpha_1 \oplus \alpha_2 : X \oplus Y \longrightarrow M \oplus N$ par rapport aux bases $B_{1,2}$ et $B'_{1,2}$ est:*

$$\begin{pmatrix} [\alpha_1] & 0 \\ 0 & [\alpha_2] \end{pmatrix}$$

où $[\alpha_i]$ est la matrice représentant α_i relativement aux bases B_i et B'_i.

Lemme 1.2.10 ([9], Lemma 1.17) *Si $\mathcal{A}_1 \in \mathcal{M}(A[X], r \times s)$, $\mathcal{A}_2 \in \mathcal{M}(A[X], s \times t)$ et $\mathcal{A}_3 \in \mathcal{M}(A[X], r \times t)$ sont trois matrices et S une partie multiplicativement stable de A, l'homomorphisme canonique $A[X] \longrightarrow A_S[X]$ induit un homomorphisme*

$$\begin{array}{rcl} \mathcal{M}(A[X], u \times v) & \longrightarrow & \mathcal{M}(A_S[X], u \times v) \\ (f_{ij})_{i,j} & \longmapsto & \left(\dfrac{f_{ij}}{1}\right)_{i,j} . \end{array}$$

Soit $\overline{\mathcal{A}_i}$ l'image de $\mathcal{A}_i$ par cet homomorphisme et supposons que $\overline{\mathcal{A}_1} \cdot \overline{\mathcal{A}_2} = \overline{\mathcal{A}_3}$ et que $\mathcal{A}_1(0)\mathcal{A}_2(0) = \mathcal{A}_3(0)$. Alors, il existe $s \in S$ tel que $\mathcal{A}_1(sX) \cdot \mathcal{A}_2(sX) = \mathcal{A}_3(sX)$.

Preuve Comme $\mathcal{A}_1(0).\mathcal{A}_2(0) - \mathcal{A}_3(0) = 0$, alors tous les coefficients a_{ij} de la matrice $\mathcal{A} = \mathcal{A}_1.\mathcal{A}_2 - \mathcal{A}_3$ sont dans l'idéal (X) de $A[X]$. D'autre part $\overline{\mathcal{A}} = \overline{\mathcal{A}_1}.\overline{\mathcal{A}_2} - \overline{\mathcal{A}_3} = 0$. Il existe alors $s_{ij} \in S$ tel que $s_{ij}a_{ij} = 0$. Soit $s = \prod_{i,j} s_{ij} \in S$, alors on a $\mathcal{A}(sX) = 0$ et par suite $\mathcal{A}_1(sX).\mathcal{A}_2(sX) = \mathcal{A}_3(sX)$. ■

Lemme 1.2.11 *Soient S une partie multiplicativement stable de A, $\mathcal{U}(Y)$ une matrice de $\mathrm{GL}_n(A_S[Y])$ telle que $\mathcal{U}(0) = I$. Alors, il existe s dans S et $\mathcal{U}'(Y) \in \mathrm{GL}_n(A[Y])$ tels que $\overline{\mathcal{U}'(Y)} = \mathcal{U}(sY)$ et $\mathcal{U}'(0) = I$.*

Preuve Soit $\mathcal{V}(Y) = \mathcal{U}(Y)^{-1}$ dans $\mathrm{GL}_n(A_S[Y])$, et écrivons

$$\mathcal{U}(Y) = \mathcal{U}_0 + \mathcal{U}_1 Y + \ldots + \mathcal{U}_p Y^p$$

$$\mathcal{V}(Y) = \mathcal{V}_0 + \mathcal{V}_1 Y + \ldots + \mathcal{V}_q Y^q$$

où $\mathcal{U}_i$, $\mathcal{V}_j \in \mathcal{M}_{n\times n}(A_S)$ et $\mathcal{U}_0 = \mathcal{V}_0 = I$.
Soit $s' \in S$ tel que pour tout i et pour tout j, $s'\mathcal{U}_i$ et $s'\mathcal{V}_j$ sont des images d'éléments de $\mathcal{M}_{n\times n}(A)$; alors il existe $\mathcal{U}^*(Y)$, $\mathcal{V}^*(Y) \in \mathcal{M}_{n\times n}(A[Y])$ qui satisfont $\overline{\mathcal{U}^*(Y)} = \mathcal{U}(s'Y)$ et $\overline{\mathcal{V}^*(Y)} = \mathcal{V}(s'Y)$, et ces matrices peuvent être choisies de telle sorte que $\mathcal{U}^*(0) = I$ $= \mathcal{V}^*(0)$, On a alors $\overline{\mathcal{U}^*(Y)}.\overline{\mathcal{V}^*(Y)} = \overline{I}$ et $\mathcal{U}^*(0).\mathcal{V}^*(0) = I$, donc, par le lemme 1.2.8, il existe $s'' \in S$ tel que $\mathcal{U}^*(s''Y).\mathcal{V}^*(s''Y) = I$. En prenant $s = s's'' \in S$ et $\mathcal{U}'(Y) = \mathcal{U}^*(s''Y)$, on obtient le résultat voulu. ∎

Définition 1.2.3

1. On dit que deux matrices $\mathcal{A}_1$, $\mathcal{A}_2 \in \mathcal{M}(A, r\times s)$ sont *semblables* (et on note $\mathcal{A}_1 \sim \mathcal{A}_2$) s'il existe deux matrices inversibles $\mathcal{U} \in \mathrm{GL}(A, r\times r)$ et $\mathcal{V} \in \mathrm{GL}(A, s\times s)$ telles que $\mathcal{A}_1 = \mathcal{U} \cdot \mathcal{A}_2 \cdot \mathcal{V}$.

2. Si S est une partie multiplicativement stable de A, on dit que les deux matrices $\mathcal{A}_1$, $\mathcal{A}_2 \in \mathcal{M}(A[X], r\times s)$ sont *localement semblables* en S, si les images de $\mathcal{A}_1$ et $\mathcal{A}_2$ dans $\mathcal{M}(A_S[X], r\times s)$ sont semblables. Si $\mathcal{A}_1$, $\mathcal{A}_2$ sont localement semblables en $S = A\backslash\Omega$ où Ω est un idéal maximal de A, on dit aussi qu'elles sont *localement semblables en* Ω.

Dans ce qui suit, si $\mathcal{A} \in \mathcal{M}(A[\underline{X}], r\times s)$ et si S est une partie multiplicativement stable de A, on désigne par $\overline{\mathcal{A}}$ l'image de $\mathcal{A}$ dans $\mathcal{M}(A_S[\underline{X}], r\times s)$ où $\underline{X}$ est un ensemble de variables.

Proposition 1.2.5 (théorème de Vaserstein) ([9], Theorem 1.18) *Soit $\mathcal{A} \in \mathcal{M}(A[X], r\times s)$. Alors, $\mathcal{A}$ et $\mathcal{A}(0)$ sont semblables si et seulement si $\mathcal{A}$ et $\mathcal{A}(0)$ sont localement semblables en tout $\Omega \in \mathrm{Max}(A)$.*

Preuve ($\Longrightarrow$) Clair.
($\Longleftarrow$) Supposons que $\mathcal{A}$ et $\mathcal{A}(0)$ sont localement semblables en tout $\Omega \in \mathrm{Max}(A)$ et

soit $I = \{a \in A$ tel que $\mathcal{A}(f)$ et $\mathcal{A}(g)$ sont globalement semblables pour tout $f,\ g \in A[X]$ avec $f - g \in aA[X]\ \}$.

I est un idéal de A. En effet, il est tout d'abord clair que $0 \in I$. Si $a_1,\ a_2 \in I$ et si $f,\ g \in A[X]$ tels que $f - g \in (a_1 - a_2)A[X]$, alors $f - g = (a_1 - a_2)\phi$ où $\phi \in A[X]$, d'où $f - (g - a_2\phi) \in a_1A[X]$, par suite $\mathcal{A}(f) \sim \mathcal{A}(g - a_2\phi)$. D'autre part, $g - (g - a_2\phi) = a_2\phi \in a_2A[X]$ et $a_2 \in I$, ce qui implique que $\mathcal{A}(g) \sim \mathcal{A}(g - a_2\phi)$, donc $\mathcal{A}(f) \sim \mathcal{A}(g)$, ce qui montre que $a_1 - a_2 \in I$. Si maintenant, $a_1 \in I$, $a \in A$ et si $f,\ g \in aa_1A[X]$, alors $f - g = aa_1\phi$ où $\phi \in A[X]$ et par suite $f - g \in a_1A[X]$, d'où $\mathcal{A}(f) \sim \mathcal{A}(g)$. Ceci montre que I est un idéal de A.

Montrons ensuite que $I = A$. Pour ceci, on va montrer que pour tout idéal maximal Ω de A, il existe un élément de I qui n'est pas dans Ω. Soit alors $\Omega \in \mathrm{Max}(A)$. Comme $\overline{\mathcal{A}}$ et $\overline{\mathcal{A}(0)}$ sont deux matrices semblables dans $\mathcal{M}(A_\Omega[X], r\times s)$, il existe $\mathcal{C} \in \mathrm{GL}(A_\Omega[X], r)$ et $\mathcal{D} \in \mathrm{GL}(A_\Omega[X], s)$ telles que $\overline{\mathcal{A}(X)} = \mathcal{C}(X).\overline{\mathcal{A}(0)}.\mathcal{D}(X)$. Si Y est une autre indétérminée, alors on peut écrire $\overline{\mathcal{A}(X+Y)} = \mathcal{C}(X+Y).\overline{\mathcal{A}(0)}.\mathcal{D}(X+Y)$ $= \mathcal{C}(X+Y).\mathcal{C}^{-1}(X).\overline{\mathcal{A}(X)}.\ \mathcal{D}^{-1}(X).\mathcal{D}(X+Y)$. Posons $\mathcal{C}^* = \mathcal{C}(X+Y).\mathcal{C}^{-1}(X)$ et $\mathcal{D}^* = \mathcal{D}^{-1}(X).\mathcal{D}(X+Y)$. Alors $\overline{\mathcal{A}(X+Y)} = \mathcal{C}^*(X,Y).\overline{\mathcal{A}(X)}.\mathcal{D}^*(X,Y)$. Comme $\mathcal{C}^*(X,Y) \in \mathrm{GL}_r(A_\Omega[X][Y])$ et $\mathcal{D}^*(X,Y) \in \mathrm{GL}_s(A_\Omega[X][Y])$ satisfont à $\mathcal{C}^*(X,0) = I_r$ et $\mathcal{D}^*(X,0) = I_s$, on peut leur appliquer le lemme 1.2.11. Ainsi, il existe $\alpha_1 \in A\backslash\Omega$, $\mathcal{N}(X,Y) \in \mathrm{GL}_r(A[X,Y])$ et $\Delta(X,Y) \in \mathrm{GL}_s(A[X,Y])$ tels que $\mathcal{N}(X,0) = I_r$, $\Delta(X,0) = I_s$, $\overline{\mathcal{N}(X,Y)} = \mathcal{C}^*(X,\alpha_1Y)$ et $\overline{\Delta(X,Y)} = \mathcal{D}^*(X,\alpha_1Y)$. On a alors

$$\overline{\mathcal{A}(X+\alpha_1Y)} = \mathcal{C}^*(X,\alpha_1Y).\overline{\mathcal{A}(X)}.\mathcal{D}^*(X,\alpha_1Y)$$

$$= \overline{\mathcal{N}(X,Y)}.\overline{\mathcal{A}(X)}.\overline{\Delta(X,Y)}$$

et

$$\mathcal{A}(X+\alpha_1.0) = \mathcal{N}(X,0).\mathcal{A}(X).\Delta(X,0).$$

En vertu de lemme 1.2.8, il existe alors $\alpha_2 \in A\backslash\Omega$ tel que

$$\mathcal{A}(X+\alpha Y) = \mathcal{N}(X,\alpha_2Y).\mathcal{A}(X).\Delta(X,\alpha_2Y)$$

où $\alpha = \alpha_1\alpha_2 \in A\backslash\Omega$. Si f, g sont tels que $f - g = \alpha\phi$ où $\phi \in A[X]$, alors $\mathcal{A}(f) = \mathcal{A}(g+\alpha\phi) = \mathcal{N}(g, \alpha_2\phi).\mathcal{A}(g).\Delta(g, \alpha_2\phi)$ où $\mathcal{N}(g, \alpha_2\phi)$ et $\Delta(g, \alpha_2\phi)$ sont deux matrices inversibles, ceci montre que $\mathcal{A}(f) \sim \mathcal{A}(g)$ et par suite $\alpha \in I$. Enfin $I = A$, en d'autres termes, $\mathcal{A}(f) \sim \mathcal{A}(g)$ pour tout f et tout $g \in A[X]$. En particulier $\mathcal{A}(X) \sim \mathcal{A}(0)$. ∎

Théorème 1.2.2 ([**9**], Theorem 1.20) *Soit M un $A[X]$-module de présentation finie. Alors M est une extension de A si et seulement si M est une extension locale de A en tout $\Omega \in$ Max(A).*

Preuve Supposons que M est une extension de A et soit N un A-module tel que $M \approx N[X]$. Pour tout $\Omega \in$ Max(A), on a que $M_\Omega \approx (N[X])_\Omega \approx N_\Omega[X]$, ce qui montre que M_Ω est une extension de A_Ω.

Supposons maintenant que M est une extension locale de A en tout $\Omega \in$ Max(A) et montrons que M est une extension de A. Comme M est de présentation finie, on peut considérer une suite exacte

$$A[X]^m \xrightarrow{\beta_1} A[X]^n \xrightarrow{\alpha_1} M \rightarrow 0.$$

Si on considère cette suite modulo X, on obtient par la proposition 1.2.3 une suite exacte de A-modules

$$A^m \xrightarrow{\overline{\beta_1}} A^n \xrightarrow{\overline{\alpha_1}} M/XM \longrightarrow 0. \tag{1.2.11}$$

Si $\mathcal{B}$ désigne la matrice de β_1 par rapport aux bases canoniques de $A[X]^m$ et $A[X]^n$, alors $\mathcal{B}(0)$ est la matrice représentante de $\overline{\beta_1}$ également par rapport aux bases canoniques.

Définissons maintenant l'application linéaire $\overline{\beta_1}[X] : A^m[X] \longrightarrow A^n[X]$ par

$$\begin{aligned}\overline{\beta_1}[X]((\alpha_{01}, ..., \alpha_{0m}) + ... + (\alpha_{r1}, ..., \alpha_{rm})X^r) = \\ \overline{\beta_1}(\alpha_{01}, ..., \alpha_{0m}) + ... + \overline{\beta_1}(\alpha_{r1}, ..., \alpha_{rm})X^r\end{aligned}$$

De même on définit l'homomorphisme $\overline{\alpha_1}[X] : A^n[X] \longrightarrow M/XM[X]$. Il est facile de vérifier que la suite $A^m[X] \xrightarrow{\overline{\beta_1}[X]} A^n[X] \xrightarrow{\overline{\alpha_1}[X]} N[X] \longrightarrow 0$ où $N = M/XM$ est une suite exacte de $A[X]$-modules. Comme on peut identifier $A^p[X]$ avec $A[X]^p$ pour tout $p \geq 1$, on aura alors une suite exacte de $A[X]$-modules:

$$A[X]^m \xrightarrow{\beta_2} A[X]^n \xrightarrow{\alpha_2} N[X] \longrightarrow 0.$$

où $\beta_2(f_1, ..., f_m) = \overline{\beta_1}[X]((\alpha_{01}, ..., \alpha_{0m}) + ... + (\alpha_{r1}, ..., \alpha_{rm})X^r)$ où $f_i = \alpha_{0i} + ... + \alpha_{r_i i}X^{r_i}$ et r est le maximum des degrés des pôlynomes f_i $(i = 0, ..., m)$. Comme $\beta_2(e_i) = \overline{\beta_1}[X](e_i) = \overline{\beta_1}(e_i)$, alors β_2 est encore représentée par la matrice $\mathcal{B}(0)$.
Soit $R = A[X]$ on a alors les deux suites exactes de R-modules

$$R^m \xrightarrow{\beta_1} R^n \xrightarrow{\alpha_1} M \longrightarrow 0. \tag{1.2.12}$$

$$R^m \xrightarrow{\beta_2} R^n \xrightarrow{\alpha_2} N[X] \longrightarrow 0. \tag{1.2.13}$$

Pour montrer que $M \approx N[X]$, il suffit, en vertu du corollaire 1.2.1, de montrer qu'il existe $\alpha \in \operatorname{Aut}(R^m \oplus R^n)$ et $\beta \in \operatorname{Aut}(R^m \oplus R^n \oplus R^m \oplus R^n)$ tels que le diagramme

$$\begin{array}{ccc} R^m \oplus R^n \oplus R^m \oplus R^n & \xrightarrow{(\beta_1 \oplus 1_{R^n}, 0)} & R^n \oplus R^n \\ \beta \downarrow & & \downarrow \alpha \\ R^m \oplus R^n \oplus R^m \oplus R^n & \xrightarrow{(0, \beta_2 \oplus 1_{R^n})} & R^n \oplus R^n \end{array}$$

est commutatif. La matrice représentant $(\beta_1 \oplus 1_{R^n}, 0)$ est

$$\mathcal{A} = \left(\ [\beta_1 \oplus 1_{R^n}] \ \mid \ 0 \ \right) = \left(\begin{array}{cc|c} [\beta_1] & 0 & \\ 0 & I_n & 0 \end{array} \right) = \left(\begin{array}{cc|c} \mathcal{B} & 0 & \\ 0 & I_n & 0 \end{array} \right)$$

et la matrice représentant $(0, \beta_2 \oplus 1_{R^n})$ est

$$\mathcal{C} = \left(\ 0 \ \mid \ [\beta_2 \oplus 1_{R^n}] \ \right) = \left(\begin{array}{c|cc} & [\beta_2] & 0 \\ 0 & 0 & I_n \end{array} \right) = \left(\begin{array}{c|cc} & \mathcal{B}(0) & 0 \\ 0 & 0 & I_n \end{array} \right)$$

On voit clairement que la matrice $\mathcal{C}$ est semblable à la matrice $\mathcal{A}(0)$ (par une suite des transformations élémentaires sur les lignes et les colonnes). La démonstration se termine alors si on montre que $\mathcal{A} \sim \mathcal{A}(0)$. Il suffit, en vertu de la proposition 1.2.5, de montrer ceci localement. Soit alors $\Omega \in \operatorname{Max}(A)$ et localisons les deux suites 1.2.12 et 1.2.13 en Ω. On obtient alors les deux suites exactes de $A_\Omega[X]$-modules

$$A_\Omega[X]^m \xrightarrow{\beta_{1\Omega}} A_\Omega[X]^n \xrightarrow{\alpha_{1\Omega}} M_\Omega \longrightarrow 0 \tag{1.2.14}$$

$$A_\Omega[X]^m \xrightarrow{\beta_{2\Omega}} A_\Omega[X]^n \xrightarrow{\alpha_{2\Omega}} N_\Omega[X] \longrightarrow 0. \tag{1.2.15}$$

Comme M_Ω est une extension de A_Ω, il existe un A_Ω-module H tel que $M_\Omega \approx H[X]$. Par la proposition 1.2.3 on a que $M_\Omega/XM_\Omega \approx H$. D'autre part $N = M/XM$, alors $N_\Omega \approx M_\Omega/XM_\Omega \approx H$, d'où $M_\Omega \approx N_\Omega[X]$, ce qui implique qu'il existe $\alpha \in \mathrm{Aut}(A_\Omega[X]^n \oplus A_\Omega[X]^n)$ et $\beta \in \mathrm{Aut}(A_\Omega[X]^m \oplus A_\Omega[X]^n \oplus A_\Omega[X]^n \oplus A_\Omega[X]^m)$ tels que le diagramme

$$\begin{array}{ccc} A_\Omega[X]^m \oplus A_\Omega[X]^n \oplus A_\Omega[X]^n \oplus A_\Omega[X]^m & \overset{(\beta_{1\Omega}\oplus 1,0)}{\longrightarrow} & A_\Omega[X]^n \oplus A_\Omega[X]^n \\ \beta\downarrow & & \downarrow\alpha \\ A_\Omega[X]^m \oplus A_\Omega[X]^n \oplus A_\Omega[X]^n \oplus A_\Omega[X]^m & \overset{(0,1\oplus\beta_{2\Omega})}{\longrightarrow} & A_\Omega[X]^n \oplus A_\Omega[X]^n \end{array}$$

est commutatif. On peut alors déduire que les matrices représentant les applications $(\beta_{1\Omega} \oplus 1_{R^n_\Omega}, 0)$ et $(0, 1_{R^n_\Omega} \oplus \beta_{2\Omega})$ sont semblables. Ceci montre que $\overline{\mathcal{A}(0)} \sim \overline{\mathcal{A}(X)}$ pour tout Ω dans $\mathrm{Max}(A)$, d'où le résultat. ■

Lemme 1.2.12 *1. Soit u un élément inversible de A. Alors, pour tout A-module M l'homomorphisme canonique $f : M \longrightarrow M_u$ est un isomorphisme de A-modules.*

2. Si $a \in A$, alors $A_a \approx A_{au}$ et $M_a \approx M_{ua}$ (comme A_a-modules).

Preuve 1. f est injective car si $m \in M$ est tel que $\frac{m}{1} = 0$, il existe alors un entier naturel positif n tel que $u^n m = 0$, d'où $m = 0$ (u est inversible). D'autre part, si $\frac{m}{u^k} \in M_u$, alors $f(u^{-k}m) = \frac{m}{u^k}$, d'où la surjectivité de f.
2. Il est facile de voir que $\frac{m}{a^k} \longmapsto \frac{mu^k}{(ua)^k}$ est l'isomorphisme voulu. ■

Théorème 1.2.3 ([9], Theorem 3.14) *Si M est un $A[X]$-module projectif et de type fini et s'il existe un polynôme unitaire f dans $A[X]$ tel que M_f est un $A[X]_f$-module libre alors M est un $A[X]$-module libre.*

Preuve Commençons par montrer que M est une extension de A. Pour ceci, notons qu'en vertu du théorème 1.2.2, il suffit de le montrer localement. Soit $\Omega \in \mathrm{Max}(A)$. Comme M est projectif et de type fini sur $A[X]$, M_Ω est encore projectif et de type fini sur $(A[X])_\Omega = A_\Omega[X]$ et on a que $(M_\Omega)_f \approx (M_f)_\Omega$ est libre sur $(A_\Omega[X])_f$, d'où par le théorème 1.2.1 M_Ω est un $A[X]_\Omega$-module libre de rang fini, ce qui implique qu'il existe un entier positif n tel que $M_\Omega \approx (A_\Omega[X])^n \approx A_\Omega^n[X]$. Soit V le A_Ω-module A_Ω^n, alors $M_\Omega \approx V[X]$. Alors M_Ω est une extension de A_Ω et par suite M est une extension de A.

Soit N un A-module tel que $M \approx N[X]$, alors $N \approx M/XM$ comme A-modules (proposition 1.2.2). D'autre part considérons l'homomorphisme suivant

$$\begin{array}{ccc} N[X] & \xrightarrow{\psi} & N \\ \alpha_0 + \alpha_1 X + \ldots + \alpha_r X^r & \longmapsto & \alpha_0 + \alpha_1 + \ldots + \alpha_r \end{array}$$

Il est clair que ψ est un épimorphisme pour lequel $\ker\psi = (X-1)N[X]$, ce qui montre que $N[X]/(X-1)N[X] \approx N$. Alors, pour montrer que M est libre comme $A[X]$-module, il suffit de montrer que $M/(X-1)M$ l'est sur A (si $\{a_1, ..., a_n\}$ est une base de N sur A, alors elle est encore une base de $N[X]$ sur $A[X]$).

Notre objectif maintenant est alors de montrer que $M/(X-1)M$ est un A-module libre. Désignons par X^{-1} l'inverse de $\frac{X}{1}$ dans l'anneau $A[X]_X$ et considérons le sous-anneau $A[X^{-1}]$ de $A[X]_X$. Puisque X^{-1} est un élément inversible de $A[X]_X$, le localisé $A[X^{-1}]_{X^{-1}}$ est un sous-anneau de $A[X]_X$; en fait, on voit facilement que $A[X^{-1}]_{X^{-1}}$ est égal à $A[X]_X$ et que $A[X^{-1}]_{X^{-1}} = A[X, X^{-1}] = A[X]_X$.
Si $f = X^n + a_1X^{n-1} + \ldots + a_n$, posons $g = 1 + a_1X^{-1} + \ldots + a_nX^{-n}$ où $a_i \in A$ pour tout $i = 1, ..., n$. Notons que $g = X^{-n}f$, alors $\frac{g}{1} = \frac{X^{-n}}{1}.\frac{f}{1}$ dans $A[X, X^{-1}]$. Comme $\frac{X^{-n}}{1}$ est inversible dans $A[X, X^{-1}]$, le lemme 1.2.12 implique que $A[X, X^{-1}]_f \approx A[X, X^{-1}]_g$ et $(M_X)_f \approx (M_X)_g$, c'est alors un $A[X, X^{-1}]_g$-module libre car M_f est libre sur $A[X]_f$. D'autre part, on a que $g - (a_1 + a_2X^{-1} + \ldots + a_nX^{-n+1})X^{-1} = 1$, alors l'idéal $< X^{-1}, g >$ de $A[X^{-1}]$ engendré par g et X^{-1} est $A[X^{-1}]$, ce qui donne que $\mathrm{Spec}(A[X^{-1}]) = \mathcal{D}(X^{-1}) \cup \mathcal{D}(g)$. Soit r le rang de M_f sur $A[X]_f$ et $W = (A[X^{-1}]_g^r)_{X^{-1}}$. On considère le diagramme de $A[X^{-1}]$-modules:

$$\begin{array}{ccc} & & A[X^{-1}]_g^r \\ & & \downarrow\alpha_2 \\ M_X & \xrightarrow{\alpha_1} & W \end{array}$$

où α_2 est l'homomorphisme de localisation et α_1 est la composition

$$M_X \xrightarrow{\text{loc.}} (M_X)_g \xrightarrow{\approx} A[X, X^{-1}]_g^r \xrightarrow{\approx} W.$$

Soit M' le $A[X^{-1}]$-module $M_X \prod_W A[X^{-1}]_g^r$ (produit fibré). Par la proposition 1.1.22, on a alors $M'_{X^{-1}} \approx M_X$ (comme $A[X, X^{-1}]$-modules) et $M'_g \approx A[X^{-1}]_g^r$ (comme $A[X^{-1}]_g$-modules). D'autre part, M_X est projectif et de type fini sur $A[X, X^{-1}]$ car M l'est sur $A[X]$, donc $M'_{X^{-1}}$ est un $A[X^{-1}]_{X^{-1}}$ projectif et de type fini. Comme M'_g est projectif et de type fini sur $A[X^{-1}]_g$, alors le corollaire 1.1.4 montre que M' est projectif et de type fini sur $A[X^{-1}]$.
Soit $\Omega \in \operatorname{Max}(A)$. Comme $(M_\Omega)_f$ est libre sur $A_\Omega[X]_f$ et f est unitaire, alors le théorème de Horrocks implique que M_Ω est libre sur $A_\Omega[X]$ et par suite $(M_X)_\Omega$ est libre sur $A_\Omega[X, X^{-1}]$. D'autre part, M'_Ω est un $A_\Omega[X^{-1}]$-module projectif et de type fini et on a que $(M'_\Omega)_{X^{-1}} \approx (M_X)_\Omega$ et X^{-1} est un polynôme unitaire de l'anneau $A_\Omega[X^{-1}]$, alors le théorème de Horrocks montre que M'_Ω est un $A_\Omega[X^{-1}]$-module libre de rang fini. Alors M'_Ω est une extension de A_Ω pour tout $\Omega \in \operatorname{Max}(A)$, donc M' est une extension de l'anneau A par le théorème 1.2.2. Considérons alors un A-module N' tel que $M' = N'[X^{-1}]$. Par la proposition 1.2.2, on a que $N' \approx M'/X^{-1}M' \approx M'/(X^{-1} - 1)M'$ et comme M'_g est un $A[X^{-1}]_g$-module libre et que $g \equiv 1 \mod(X^{-1})$ dans $A[X^{-1}]$, alors $M'_g/X^{-1}M'_g \approx M'/X^{-1}M'$ est un A-module libre, d'où $M'/(X^{-1} - 1)M'$ est encore un A-module libre. D'autre part, $M/(X-1)M \approx M_X/(X-1)M_X \approx M'_{X^{-1}}/(X^{-1} - 1)M'_{X^{-1}} = M'/(X^{-1} - 1)M'$ alors $M/(X-1)M$ est un A-module libre, d'où le résultat. ■

Corollaire 1.2.2 *Soient M un $A[X]$-module projectif et de type fini et S une partie multiplicativement stable de $A[X]$ qui est contenue dans l'ensemble des polynômes unitaires de $A[X]$. Si M_S est un $A[X]_S$-module libre, alors M est libre sur $A[X]$.*

Preuve Soit $\{\frac{w_1}{1}, \ldots, \frac{w_r}{1}\}$ une base de M_S sur $A[X]_S$ (où $w_i \in M$) et soit $\alpha : A[X]^r \to M$ l'application $A[X]$-linéaire qui envoie e_i sur w_i, où $\{e_1, \ldots, e_r\}$ est la base canonique de $A[X]^r$. Soient N et C le noyau et le conoyau de α respectivement. Puisque la suite

$$0 \to N \to A[X]^r \xrightarrow{\alpha} M \to C \to 0$$

est exacte et la localisation est un foncteur exacte, alors la suite

$$0 \to N_S \to A[X]^r_S \xrightarrow{\alpha_S} M_S \to C_S \to 0$$

est exacte. Par définition α_S est un isomorphisme, donc $N_S = 0$ et $C_S = 0$. Comme C est un $A[X]$-module de type fini, il existe $f \in S$ tel que $C_f = 0$. Alors la suite

$$0 \to N_f \to A[X]^r_f \xrightarrow{\alpha_f} M_f \to 0$$

est exacte; en fait, cette suite est scindée car M_f est un $A[X]_f$-module projectif. Ainsi, $A[X]^r_f \approx N_f \oplus M_f$ et N_f est donc un $A[X]_f$-module de type fini. Comme $(N_f)_S = 0$, il existe $g \in S$ tel que $(N_f)_g = 0$. Posons $h = f.g \in S$, alors $N_h = 0$ et $C_h = 0$; par l'exactitude de la suite

$$0 \to N_h \to A[X]^r_h \xrightarrow{\alpha_h} M_h \to C_h \to 0$$

on en déduit que M_h est libre sur $A[X]_h$. Par le théorème 1.2.3, M est un $A[X]$-module libre. ■

1.3 la solution de la conjecture de Serre

Proposition 1.3.1 ([8], Theorem 3.7) *Soient A un anneau principal, F un A-module libre de rang n. Alors tout sous-module de F est libre de rang $m \leq n$.*

Preuve Si $n = 0$, la proposition est vraie si on adopte la convention que le module nul est libre de rang 0. Supposons maintenant que la proposition est vraie jusqu'à l'ordre $n-1$ où $n > 0$, c.à.d, on suppose que dans un A-module libre de rang inférieur ou égal à $n-1$, tout sous-module est libre et de rang inférieur ou égal à $n-1$. Soient F un A-module libre de rang n et $\{ e_1,...,e_n \}$ une base de F sur A et désignons par F' le sous-module de F engendré par $e_2,...,e_n$. Soit K un sous-module de F. Si $K \subseteq F'$, on termine par l'hypothèse d'induction. Si K n'est pas inclu dans F', on dénote par I l'idéal de A de tous les éléments a tel que $ae_1 + y \in K$ pour un certain $y \in F'$. Il est clair que $0 \in I$. Si a, $b \in I$, il existe alors y_1, $y_2 \in F'$ tels que $ae_1 + y_1 \in K$

et $be_1 + y_2 \in K$, d'où $(a+b)e_1 + y_1 + y_2 \in K$, donc $a+b \in I$. D'autre part, si $\alpha \in A$ et $a \in I$, alors il existe $y \in F'$ tel que $ae_1 + y \in K$, d'où $\alpha a e_1 + \alpha y \in K$ et par suite $\alpha a \in I$. Ceci montre que I est un idéal de A. Si $I = 0$, alors pour tout $k \in K$ écrivons $k = \alpha_1 e_1 + by$ où α_1, $b \in A$ ($\{ e_1, ..., e_n \}$ est une base de F), d'où $\alpha_1 = 0$ et $k \in F'$, ce qui contredit notre supposition. Comme A est principal, on peut choisir un élément $d \in A$ tel que $d \neq 0$ et $I = (d)$. Choisissons $y_1 \in F'$ tel que $k_1 = de_1 + y_1 \in K$ et posons $L = K \cap F'$. Alors, L est un A-module libre de rang $m - 1 \leq n - 1$ (c'est l'hypothèse d'induction). Soit $\{ k_2,...,k_m \}$ une base de L sur A.

Motrons ensuite que $B = \{ k_1,...,k_m \}$ est une base de K sur A. Soit $k \in K$ et écrivons $k = ae_1 + y$ où $a \in I$ et $y \in F'$, alors $a = b_1 d$ où $b_1 \in A$, d'où $k - b_1 k_1 = b_1 de_1 + y - b_1(de_1 + y_1) = y - b_1 y_1 \in L$, d'où $k = b_1 k_1 + ... + b_m k_m$, ce qui montre que B engendre K. Pour montrer la liberté de B, on suppose que $b_1 k_1 + ... + b_m k_m = 0$, alors $b_1 de_1 + b_1 y_1 + b_2 k_2 + ... + b_m k_m = 0$. Si on écrit y_1 et $b_2 k_2 + ... + b_m k_m$ comme combinaisons linéaires des e_i, $i = 2, ..., m$, on obtient une relation de la forme $b_1 de_1 + \sum_{i=2}^{m} \alpha_i e_i = 0$ où $\alpha_i \in A$ pour tout $i = 2, ..., m$, ce qui implique que $b_1 d = 0$ et par suite $b_1 = 0$ car $d \neq 0$. Donc, $\sum_{i=2}^{m} b_i k_i = 0$, ce qui montre que $b_i = 0$ pour tout $i = 2, ..., m$. Alors K est libre du rang inférieur ou égale à n. ∎

Proposition 1.3.2 *Soient B une A-algèbre et S une partie multiplicativement stable de A. Alors $B_S \approx A_S \otimes_A B$ comme A_S-modules.*

Preuve Notons tout d'abord qu'on peut munir $A_S \otimes_A B$ d'une structure de A_S-module par l'application

$$\begin{array}{rcl} A_S \times (A_S \otimes_A B) & \longrightarrow & A_S \otimes_A B \\ (\frac{\alpha}{s}, \frac{\alpha'}{s'} \otimes b) & \longmapsto & \frac{\alpha\alpha'}{ss'} \otimes b. \end{array}$$

Considérons l'application

$$\begin{array}{rcl} A_S \times B & \xrightarrow{\phi} & B_S \\ (\frac{\alpha}{s}, b) & \longmapsto & \frac{\alpha . b}{s}. \end{array}$$

Il est facile de vérifier que ϕ est A-bilinéaire, alors par la propriété universelle du produit tensoriel, il existe une application A-linéaire unique $\psi : A_S \otimes_A B \longrightarrow B_S$ telle que le diagramme

$$\begin{array}{ccc} A_S \times B & \xrightarrow{\phi} & B_S \\ g\searrow & & \nearrow\psi \\ & A_S \otimes_A B & \end{array}$$

est commutatif, où

$$\begin{array}{ccc} A_S \times B & \xrightarrow{g} & A_S \otimes_A B \\ (\dfrac{\alpha}{s}, b) & \longmapsto & \dfrac{\alpha}{s} \otimes b. \end{array}$$

Si on regarde $A_S \otimes_A B$ et B_S comme des A_S-modules, on aura que ψ est A_S-linéaire. En effet, pour tout $\alpha \in A$ et $s \in S$, on a $\psi[\frac{\alpha}{s}.\sum_{i=1}^{n}(\frac{\alpha_i}{s}\otimes b_i)] = \psi[\sum_{i=1}^{n}\frac{\alpha\alpha_i}{ss_i}\otimes b_i] = \sum_{i=1}^{n}\frac{\alpha\alpha_i b_i}{ss_i} = \frac{\alpha}{s}\sum_{i=1}^{n}\frac{\alpha_i b_i}{s_i} = \frac{\alpha}{s}.\psi(\sum_{i=1}^{n}\frac{\alpha_i}{s_i}\otimes b_i)$. Notons ensuite que ψ est bijectif. En effet, pour tout $\frac{b}{s} \in B_S$, $\frac{b}{s} = \phi(\frac{1}{s}, b)$, d'où $\psi(\frac{1}{s}\otimes b) = \frac{b}{s}$, ce qui montre que ψ est surjectif. D'autre part, pour tout $x \in A_S \otimes_A B$, $x = \sum_{i=1}^{n}\frac{\alpha_i}{s_i}\otimes b_i$, soit $s = \prod_{i=1}^{n} s_i$ et $t_i = \prod_{j\neq i} s_j$, on a alors $x = \sum_{i=1}^{n}\frac{\alpha_i t_i}{s}\otimes b_i = \sum_{i=1}^{n}\frac{1}{s}\otimes \alpha_i t_i b_i = \sum_{i=1}^{n}\frac{1}{s}\otimes m_i = \frac{1}{s}\otimes\sum_{i=1}^{n} m_i = \frac{1}{s}\otimes m$ où m_i, $m \in B$. On déduit que si $\psi(x) = 0$, alors $\psi(\frac{1}{s}\otimes m) = 0$, d'où $\frac{1}{s}.\frac{m}{1} = 0$, ce qui donne l'existence d'un élément t de S tel que $tm = 0$. Donc, $x = \frac{1}{s}\otimes m = \frac{1}{st}\otimes tm = 0$. Ceci montre que ψ est injectif. ■

Proposition 1.3.3 ([1], Proposition 2.14) *Soit M un A-module, alors $A \otimes_A M \approx M$ comme A-modules.*

Preuve L'homomorphisme $a\otimes m \longmapsto am$ établit l'isomorphisme voulu. ■

Proposition 1.3.4 ([1], Exercice 2.15) *Soient A, B deux anneaux, M un A-module, P un B-module et N un (A, B)-bimodule (c.à.d un A-module et un B-module en même temps et les deux structures sont compatibles dans le sens que $a(bx) = b(ax)$ pour tout a dans A, b dans B et x dans N). Alors on a $(M\otimes_A N)\otimes_B P \approx M\otimes_A(N\otimes_B P)$ comme A-modules et comme B-modules.*

Preuve Notons tout d'abord qu'on peut munir $M\otimes_A N$ d'une structure de B-module en posant $b.\sum_{i=1}^{n} x_i\otimes y_i = \sum_{i=1}^{n} x_i\otimes by_i$. De la même manière, on peut munir $N\otimes_B P$ d'une structure de A-module. De même, $(M\otimes_A N)\otimes_B P$ est un A-module par la loi $a.\sum_{i=1}^{n}(x_i\otimes y_i)\otimes z_i = \sum_{i=1}^{n}(ax_i\otimes y_i)\otimes z_i$ et encore $M\otimes_A(N\otimes_B P)$ est un B-module.
Fixons z dans P. Soit $\phi : M\times N\longrightarrow M\otimes_A(N\otimes_B P)$ l'application A-bilinéaire définie par $\phi(x,y) = x\otimes(y\otimes z)$. Par la propriété universelle du produit tensoriel, il existe alors une application A-linéaire $f_z : M\otimes_A N\longrightarrow M\otimes_A(N\otimes_B P)$ telle que $f_z(x\otimes y) = x\otimes(y\otimes z)$. D'autre part, l'application B-linéaire

$$\begin{array}{ccc} M\otimes_A N\times P & \xrightarrow{\psi} & M\otimes_A(N\otimes_B P) \\ (x\otimes y, z) & \longmapsto & (x\otimes y)\otimes z. \end{array}$$

induit une application B-linéaire $f : (M\otimes_A N)\otimes_B P\longrightarrow M\otimes_A(N\otimes_B P)$ avec la propriété $f((x\otimes y)\otimes z) = x\otimes(y\otimes z)$. De même on peut montrer l'existence d'une application A-linéaire $g : M\otimes_A(N\otimes_B P)\longrightarrow(M\otimes_A N)\otimes_B P$ telle que $g(x\otimes(y\otimes z)) = (x\otimes y)\otimes z$. Notons que g est B-linéaire. En effet, pour tout $b \in B$, $x_i \in M$, $y_i \in N$, $z_i \in P$ $(i = 1, ..., n)$, on a $g(b.\sum_{i=1}^{n} x_i\otimes(y_i\otimes z_i)) = g(\sum_{i=1}^{n} x_i\otimes(y_i\otimes bz_i)) = \sum_{i=1}^{n}(x_i\otimes y_i)\otimes bz_i = b.g(\sum_{i=1}^{n}(x_i\otimes y_i)\otimes z_i)$.
On peut vérifier aisement que $f^{-1} = g$ et $g^{-1} = f$. Ceci montre que les deux B-modules $M\otimes_A(N\otimes_B P)$ et $(M\otimes_A N)\otimes_B P$ sont isomorphes. De la même manière, on montre qu'ils sont isomorphes comme A-modules. ∎

Proposition 1.3.5 *Si B est une A-algèbre, alors on a l'isomorphisme suivant de A-modules $B\otimes_A A[X_1, ..., X_n] \approx B[X_1, ..., X_n]$.*

Preuve Montrons tout d'abord le cas $n = 1$. Considérons l'application bilinéaire

$$\begin{array}{ccc} B\times A[X] & \xrightarrow{\phi} & B[X] \\ (b, \sum_{i=0}^{n} \alpha_i X^i) & \longmapsto & \sum_{i=0}^{n} \alpha_i bX^i. \end{array}$$

Par la proporiété universelle du produit tensoriel, il existe une application A-linéaire $\theta : B\otimes_A A[X]\longrightarrow B[X]$ telle que le diagramme

$$\begin{array}{ccc} B\times A[X] & \xrightarrow{\phi} & B[X] \\ g\searrow & & \nearrow\theta \\ & B\otimes_A A[X] & \end{array}$$

est commutatif. Montrons que θ est un isomorphisme de A-modules. Pour tout $h = \sum_{i=0}^{n} b_i X^i \in B[X]$, on a que $h = \theta(\sum_{i=0}^{n} b_i \otimes X^i)$, d'où la surjectivité de θ. D'autre part, tout $x \in B\otimes_A A[X]$ s'écrit comme $x = \sum_{i=1}^{r} b_i \otimes f_i$ où $b_i \in B$ et $f_i = \sum_{k=1}^{n_i} \alpha_{ki} X^k \in A[X]$, d'où $x = \sum_{i=1}^{r}(b_i \otimes \sum_{k=1}^{n_i} \alpha_{ki} X^k)$, donc $\theta(x) = \sum_{i=1}^{r} \sum_{k=1}^{n_i} b_i \alpha_{ki} X^k$. Si $\theta(x) = 0$, alors $\sum_{k=1}^{n_i}(\sum_{i=1}^{r} b_i \alpha_{ki}) X^k = 0$ et par suite $\sum_{i=1}^{r} b_i \alpha_{ki} = 0$ pour tout k, ce qui montre que $x = \sum_{k=1}^{n_i}(\sum_{i=1}^{r} b_i \alpha_{ki}) \otimes X^k = 0$. D'où l'injectivité de θ. Ceci montre le cas $n = 1$. Supposons ensuite que la proposition est vraie jusqu'à l'ordre $n - 1$ ($n \geq 1$), alors $B\otimes_A A[X_1, ..., X_n] \approx B\otimes_A (A[X_1, ..., X_{n-1}] \otimes_{A[X_1,...,X_{n-1}]} A[X_1, ..., X_n])$ (par la proposition 1.3.3) $\approx B[X_1, ..., X_{n-1}] \otimes_{A[X_1,...,X_{n-1}]} A[X_1, ..., X_n]$ (par la proposition 1.3.4 et par l'hypothèse d'induction) $\approx B[X_1, ..., X_n]$ (par le cas $n = 1$ et le fait que $B[X_1, ..., X_{n-1}]$ est une $A[X_1, ..., X_{n-1}]$-algèbre). ∎

Proposition 1.3.6 ([**14**], Proposition 1.12) *Soient A un anneau factoriel, S une partie multiplicativement stable de A. Alors A_S est un anneau factoriel.*

Preuve Comme A est intègre (factoriel), l'homomorphisme canonique $f : A \longrightarrow A_S$ est injectif. Soit $\mathcal{H}$ l'ensemble de tous les éléments irréductibles de A . Soit $\mathcal{Q}$ l'ensemble de tous les éléments de $\mathcal{H}$ qui ne divisent aucun élément de S. Alors pour tout élément p de $\mathcal{Q}$, $\frac{p}{1}$ n'est pas inversible dans A_S et s'il existe a, $b \in A$, s, $t \in S$ tels que $\frac{p}{1} = \frac{a}{s}.\frac{b}{t}$, alors $ab = pst$, d'où p divise a ou b (A est factoriel), ce qui montre que $\frac{p}{1}$ est irréductible dans A_S. D'autre part, pour tout élément $\frac{a}{s} \in A_S$, on a que $a = p_1 ... p_n$ où $p_i \in \mathcal{H}$. S'il existe un i tel que p_i divise un élément de S, alors $\frac{p_i}{1}$ sera inversible dans A_S et par suite on peut écrire $\frac{a}{s} = \gamma \frac{q_1}{1} ... \frac{q_r}{1}$ où γ est inversible dans A_S et $q_i \in \mathcal{Q}$ pour tout $i = 1, ..., r$. Ceci montre que l'image de $\mathcal{Q}$ dans A_S est l'ensemble de tous les éléments irréductibles de A_S à la multiplication par un élément inversible de A_S près. Il reste à vérifier la condition 2) de la définition 1.1.8. Pour ceci, on considère un élément $\frac{q}{1}$ où $q \in \mathcal{Q}$ et on suppose que $\frac{q}{1}$ divise un produit $\frac{a}{s}\frac{b}{t}$, alors $\frac{a}{s}\frac{b}{t} = \frac{q}{1}\frac{x}{v}$ où $x \in A$ et $v \in S$. D'où $abv = qxst$, mais q ne divise pas v, alors q divise ab et par suite q divise a ou b, d'où le résultat. ∎

Lemme 1.3.1 ([**9**], Lemma 3.16) *Soient K un anneau principal et S l'ensemble multiplicativement stable de tous les polynômes unitaires de $K[X]$. Alors l'anneau $K[X]_S$ est principal.*

Preuve Notons par R l'anneau $K[X]_S$. Par la proposition 1.3.6, on a que R est un anneau factoriel car $K[X]$ l'est. D'autre part, K étant intègre, on peut le regarder comme un sous anneau de R à cause de l'injection $K \hookrightarrow K[X] \xrightarrow{\theta} K[X]_S$. Si on montre que R est de dimension au plus 1, on termine alors par la proposition 1.1.30. Pour ceci, il suffit de montrer que tout idéal premier de R est de hauteur au plus 1.
Soit $\wp$ un idéal premier de R et supposons tout d'abord que $\wp \cap K = 0$. Notons que la composition des deux localisations

$$K[X] \hookrightarrow R \hookrightarrow R_\wp$$

est elle-même une localisation : si on pose

$$\wp_1 = \wp \cap K[X] \in \mathrm{Spec}(K[X])$$

alors $R_\wp = K[X]_{\wp_1}$. Remarquons qu'on a aussi $\wp_1 = \mathcal{R} \cap K[X]$ où $\mathcal{R} = \wp R_\wp$ (l'idéal maximal de $R_\wp$).

Puisque $\wp \cap K = 0$, chaque élément non nul de K est un élément inversible de $R_\wp$ et, conséquement, le corps des fractions Q de K est un sous-anneau de $R_\wp$. On a donc

$$K[X] \subseteq Q[X] \subseteq R_\wp.$$

Si on pose $\wp_2 = \mathcal{R} \cap Q[X] \in \mathrm{Spec} Q[X]$ alors on obtient

$$K[X]_{\wp_1} \subseteq Q[X]_{\wp_2} \subseteq R_\wp.$$

Puisque $K[X]_{\wp_1} = R_\wp$, on a donc $R_\wp = Q[X]_{\wp_2}$ et enfin

$$\mathrm{ht} \wp = \dim R_\wp = \dim Q[X]_{\wp_2} \leq \dim Q[X] = 1.$$

Notons que l'égalité $\dim Q[X] = 1$ provient du fait que $Q[X]$ est un anneau principal mais qui n'est pas un corps (proposition 1.1.28).

Supposons ensuite que $\wp \cap K \neq 0$, alors $\wp \cap K = (p)$ où p est un élément premier de K (car $\wp \cap K$ est un idéal premier de K qui est principal). Désignons par L le corps $K/(p)$ et notons que

$$R/pR = S^{-1}(K[X]/pK[X]) = S^{-1}L[X] = L(X)$$

d'où pR est un idéal maximal de R. Comme $pR \subseteq \wp$, on a donc $\wp = pR$. En vertu de la proposition 1.1.27, on a $\mathrm{ht}\wp = 1$. ∎

On est maintenant prêt à confirmer la conjecture de Serre

Théorème 1.3.1 ([9], Theorem 3.15) *Soient K un anneau principal, $X_1, ..., X_n$ des variables indépendantes. Alors tout $K[X_1, ..., X_n]$-module projectif et de type fini est libre.*

On va montrer ce théorème par induction sur n. Si $n = 0$, alors M est un K-module projectif et de type fini. Considérons un K-module M' de type fini tel que $L = M \oplus M'$ est libre et de rang fini (ceci est possible par la proposition 1.1.7). D'où M peut être vu comme un sous-module de L. La proposition 1.3.1 montre que M est libre. Supposons que le théorème reste vrai jusqu'à l'ordre $n - 1 \geq 0$, c.à.d, si G est un anneau principal, tout $G[X_1, ..., X_{n-1}]$-module projectif et de type fini est libre.

Soit M un $K[X_1, ..., X_n]$-module projectif et de type fini. Si on pose

$$S = \{f \in K[X_n] \text{ tel que } f \text{ est unitaire}\}$$

alors M_S est un $(K[X_n]_S)[X_1, ..., X_{n-1}]$-module projectif et de type fini; comme $K[X_n]_S$ est un anneau principal (lemme 1.3.1), l'hypothèse d'induction implique que M_S est libre sur $(K[X_n]_S)[X_1, ..., X_{n-1}]$.

Ecrivons $A = K[X_1, ..., X_{n-1}]$; alors M est un $A[X_n]$-module projectif et de type fini et M_S est libre sur $A[X_n]_S = (K[X_n]_S)[X_1, ..., X_{n-1}]$.
Comme S est contenue dans $\{f \in A[X_n] \text{ tel que } f \text{ est unitaire}\}$, le corollaire 1.2.2 implique que M est libre sur $A[X_n] = K[X_1, ..., X_n]$. ∎

Chapitre 2

Solution de la conjecture de Serre par Suslin et Vaserstein

Ce chapitre présente la preuve de Vaserstein (qu'on peut trouver dans [**11**]), qui est une simplification de celle de Suslin. Notons que la preuve de Suslin démontre la conjecture de Serre dans le cas général, c'est à dire sur un anneau principal, tandis que la version donnée dans [**11**] (et ici) est valide sur un corps seulement (voir le théorème 2.3.4).

Dans la section 2.4, on fait une généralisation de la preuve de Vaserstein à un anneau principal. Cette généralisation utilise des résultats qui se trouvent dans [**10**].

2.1 Le théorème de Serre

Dans cette section on va montrer le résultat suivant (connu sous le nom du théorème de Serre): si A est un anneau principal, $X_1, ..., X_n$ des variables indépendantes et si M est un $A[X_1, ..., X_n]$-module projectif et de type fini, alors il existe un $A[X_1, ..., X_n]$-module libre de rang fini F tel que $M \oplus F$ est un $A[X_1, ..., X_n]$-module libre de rang fini (on dit que M est stablement libre). Ce résultat suggère que l'on étudie les modules stablement libres pour voir sous quelles conditions ces modules deviennent libres.

Proposition 2.1.1 *Étant donnée une suite exacte* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *de A-modules de type fini, alors on peut construire un diagramme:*

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M_1' & \xrightarrow{g_1} & M_1 & \xrightarrow{g_2} & M_1'' & \to & 0 \\ & & \downarrow j' & & \downarrow j & & \downarrow j'' & & \\ 0 & \to & E' & \xrightarrow{i} & E & \xrightarrow{p} & E'' & \to & 0 \\ & & \downarrow \psi' & & \downarrow \psi & & \downarrow \psi'' & & \\ 0 & \to & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

qui soit commutatif et exact (lignes et colonnes exactes) et tel que E, E', E'' *sont des A-modules libres de rang fini.*

Preuve M', M'' étant de type fini sur A, on peut considérer deux épimorphismes $E' \xrightarrow{\psi'} M'$ et $E'' \xrightarrow{\psi''} M''$ où E', E'' sont deux A-modules libres de rang fini. Posons $E = E' \oplus E''$. Alors E est libre de rang fini. Considérons la suite exacte $0 \to E' \xrightarrow{i} E \xrightarrow{p} E'' \to 0$ où i est l'injection canonique et p est la deuxième projection. Comme $g : M \longrightarrow M''$ est surjectif et E'' est projectif (libre), on a alors un homomorphisme $\phi : E'' \longrightarrow M$ tel que $g\phi = \psi''$ (théorème 1.1.1). Considérons l'homomorphisme suivant

$$\begin{array}{ccc} E & \xrightarrow{\psi} & M \\ (x', x'') & \longmapsto & f\psi'(x') + \phi(x'') \end{array}$$

On a que ψ est surjectif car si $m \in M$, il existe $x'' \in E''$ tel que $g(m) = \psi''(x'') = g\phi(x'')$, donc $m - \phi(x'') \in \ker g = \operatorname{Im} f$, d'où $m = \phi(x'') + f\psi'(x')$ où $x' \in E'$. Soient maintenant M_1' le noyau de ψ', M_1 celui de ψ et M_1'' celui de ψ'' et soient $M_1' \xrightarrow{j'} E'$, $M_1 \xrightarrow{j} E$, $M_1'' \xrightarrow{j''} E''$ les inclusions. On construit ainsi les trois colonnes du diagramme voulu. L'existence de g_1 et g_2 est une conséquence de la partie 2 du lemme 1.2.7. Il est facile de voir que le diagramme ainsi construit est commutatif et exact. ■

Proposition 2.1.2 ([15], (7.B)) *Soient M un A-module non nul et $\mathcal{F}$ la famille de tous les idéaux I de A tels que $I =$ ann(x) pour un certain x non nul dans M. Alors, tout élément maximal de $\mathcal{F}$ (pour l'inclusion) est un idéal premier de A.*

Preuve Soit $\wp$ un élément maximal de $\mathcal{F}$ et choisissons $x \in M \setminus \{0\}$ tel que $\wp =$ ann(x), ceci implique que $\wp \neq A$. Soient $\alpha, \beta \in A$ tels que $\alpha.\beta \in \wp$ et supposons que $\alpha \notin \wp$, alors on a $(\alpha.\beta)x = 0$ et $\alpha x \neq 0$. Pour tout $p \in \wp$, on a que $p(\alpha x) = \alpha(px)$ $= 0$, d'où $p \in$ ann(αx) et par suite $\wp \subseteq$ ann(αx). Comme ann$(\alpha x) \in \mathcal{F}$ $(\alpha x \neq 0)$, alors $\wp =$ ann(αx) par la maximalité de $\wp$, d'où $\beta \in \wp$ car $\beta(\alpha x) = 0$. Donc $\wp$ est premier. ∎

Définition 2.1.1 Soient M un A-module, $\wp$ un idéal premier de A. On dit que $\wp$ est *associé* à M s'il existe un élément x de M tel que $\wp =$ ann(x).

Proposition 2.1.3 ([15], (7.A)) *Si M est un A-module, $\wp$ un idéal premier associé à M, alors il existe un sous-module N de M tel que $N \approx A/\wp$.*

Preuve Choisissons un élément x de M tel que $\wp =$ ann(x) et soit $\phi : A \longrightarrow M$ l'homomorphisme défini par $\phi(a) = ax$. Il est clair que ker$\phi =$ ann(x). La proposition est alors vraie pour $N =$ Imϕ. ∎

Proposition 2.1.4 *Si A est noethérien, alors tout A-module non nul admet un idéal premier associé.*

Preuve La famille $\mathcal{F}$ définie dans la proposition 2.1.2 admet un élément maximal $\wp$ comme étant une famille d'idéaux dans un anneau noethérien. Par cette même proposition 2.1.2, $\wp$ est premier, donc associé à M par la définition de la famille $\mathcal{F}$. ∎

Définition 2.1.2 Soit M un A-module, une *filtration finie* de *longueur* n de M est une suite $0 = M_1 \subseteq M_2 \subseteq ... \subseteq M_n = M$ de sous-modules de M.

Proposition 2.1.5 ([15], Chapter 3, Theorem 10) *Si A est noethérien, M un A-module non nul de type fini, alors M admet une filtration finie $M_1 = 0 \subset M_2 \subset ... \subset M_n = M$ telle que $M_i/M_{i-1} \approx A/\wp_i$ où $\wp_i$ est un idéal premier de A pour tout $i = 2, ..., n$.*

Preuve Soit $\mathcal{F}$ la famille de tous les sous-modules N de M tel que N admet une filtration finie $0 = N_1 \subset ... \subset N_r = N$ avec $N_i/N_{i-1} \approx A/\wp_i$ pour un certain $\wp_i$ dans $\mathrm{Spec}(A)$ pour tout $i = 2, ..., r$. Comme M admet un idéal premier associé $\wp$ (proposition 2.1.4), il existe un sous-module N de M tel que $N \approx A/\wp$ (proposition 2.1.3). La filtration $0 \subset N$ satisfait $N/0 \approx A/\wp$, d'où $\mathcal{F} \neq \emptyset$. M étant noethérien (il est de type fini sur un anneau noethérien), la famille $\mathcal{F}$ admet un élément maximal N_0. Si $M \neq N_0$, alors M/N_0 est un A-module non nul, ce qui implique que M/N_0 admet un idéal premier associé $\Re$ (proposition 2.1.4) et par suite, il existe un sous-module P de M contenant strictement N_0 tel que $P/N_0 \approx A/\Re$ (proposition 2.1.3). Etant un élément de $\mathcal{F}$, N_0 admet une filtration $H_1 = 0 \subset H_2 \subset ... \subset H_r = N_0$ telle que $H_i/H_{i-1} \approx A/\wp_i$ où $\wp_i \in \mathrm{Spec}(A)$ pour tout $i = 2, ..., r$. Alors $H_1 = 0 \subset H_2 \subset ... \subset H_r \subset P = H_{r+1}$ est une filtration de P satisfaisant $H_i/H_{i-1} \approx A/\wp_i$ où $\wp_i \in \mathrm{Spec}(A)$ pour tout $i = 2, ..., r+1$, d'où $P \in \mathcal{F}$, ce qui contredit la maximalité de N_0 dans $\mathcal{F}$. On déduit alors que $M = N_0 \in \mathcal{F}$. ∎

Définition 2.1.3 Un A-module M est dit *stablement libre* s'il existe un A-module libre de rang fini F tel que $M \oplus F$ est un A-module libre de rang fini. En particulier M est alors projectif et de type fini.

Définition 2.1.4 On dit qu'un A-module M admet une *résolution libre finie* (qu'on note par RLF) de *longueur* n, s'il existe une suite exacte $0 \rightarrow F_n \rightarrow ... \rightarrow F_0 \rightarrow M \rightarrow 0$ de A-modules où les F_i sont libres de type fini.

Pour les A-modules projectifs, cette définition est joue un rôle exceptionel. En effet, on a la proposition suivante:

Proposition 2.1.6 ([11], Chapter XXI, Theorem 2.1) *Pour un A-module projectif M, les deux propriétés suivantes sont équivalentes:*

1. M est stablement libre.

2. M admet une RLF.

Preuve Supposons que M soit stablement libre, il existe alors un A-module libre de rang fini E_1 tel que $E_2 = M \oplus E_1$ est un A-module libre de rang fini. On a alors la suite exacte $0 \rightarrow E_1 \xrightarrow{i} E_2 \xrightarrow{p} M \rightarrow 0$ où i est l'injection canonique et p est la deuxième projection. Ceci montre que M admet une RLF. Réciproquement, supposons que $0 \rightarrow F_n \xrightarrow{f_n} \ldots \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \rightarrow 0$ soit une RLF de M de longueur n et montrons, par récurrence sur n que M est stablement libre. Si $n = 1$, on a la suite exacte $0 \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0$ qui est scindée car M est projectif. Alors $F_0 \approx M \oplus F_1$, ce qui montre que M est stablement libre. La proposition est alors vraie dans le cas où $n = 1$. Supposons par la suite qu'elle reste vraie pour le rang $n-1$, c.à.d, on suppose que tout A-module projectif qui admet une RLF de longueur $n-1$ est stablement libre. Soit K_0 le noyau de f_0. K_0 est alors projectif car la suite $0 \rightarrow K_0 \rightarrow F_0 \rightarrow M \rightarrow 0$ est scindée, d'autre part, comme $K_0 = \ker f_0 = \operatorname{Im} f_1$, la suite $0 \rightarrow F_n \rightarrow \ldots F_1 \xrightarrow{f_1} K_0 \rightarrow 0$ est exacte et par suite elle est une RLF de longueur $n-1$ de K_0, ce qui donne, par l'hypothèse d'induction, que K_0 est stablement libre. On peut donc trouver un A-module libre de rang fini E_1 tel que $E_2 = E_1 \oplus K_0$ est libre de rang fini. Comme $F_0 \approx K_0 \oplus M$, alors $E_1 \oplus F_0 \approx E_1 \oplus K_0 \oplus M \approx E_2 \oplus M$. Ceci montre que M est stablement libre. ■

Définition 2.1.5 On dit qu'un A-module M possède une *résolution stablement libre finie* (qu'on note par RLS) de *longueur* n s'il existe une suite exacte de A-modules $0 \rightarrow E_n \rightarrow \ldots \rightarrow E_0 \rightarrow M \rightarrow 0$ où E_i est un A-module stablement libre pour tout $i = 0, \ldots, n$.

Proposition 2.1.7 ([**11**], Chapter XXI, Proposition 2.2) *Soient M un A-module et n un entier naturel strictement positif. Alors M admet une RLF de longueur n si et seulement si M admet une RLS de longueur n.*

Preuve ($\Longrightarrow$) Toute RLF est en particulier une RLS.
($\Longleftarrow$) Soit $0 \rightarrow E_n \xrightarrow{f_n} \ldots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M \rightarrow 0$ une RLS de longueur $n \geq 1$. Montrons qu'on peut supposer que deux modules consécutifs E_i, E_{i+1} de cette suite sont libres. Pour ceci,

fixons i dans $\{0, ..., n-1\}$. Comme E_i, E_{i+1} sont stablement libres, on peut considérer deux A-modules libres avec des rangs finis F_i, F_{i+1} tels que $E_i \oplus F_i$ et $E_{i+1} \oplus F_{i+1}$ sont libres de rang fini. Soit $F = F_i \oplus F_{i+1}$, F est alors libre et de rang fini sur A. Considérons la suite

$$0 \rightarrow E_n \rightarrow ... \rightarrow E_{i+3} \xrightarrow{f_{i+3}} E_{i+2} \xrightarrow{g_{i+2}} E_{i+1} \oplus F \xrightarrow{g_{i+1}} E_i \oplus F \xrightarrow{g_i} E_{i-1} \xrightarrow{f_{i-1}} ... \rightarrow E_0 \rightarrow M \rightarrow 0 \qquad (2.1.1)$$

où g_i, g_{i+1}, g_{i+2} sont des homomorphismes de A-modules définis par $g_{i+2}(x_{i+2}) = (f_{i+2}(x_{i+2}), 0)$, $g_{i+1}(x_{i+1}, y) = (f_{i+1}(x_{i+1}), y)$ et $g_i(x_i, y) = f_i(x_i)$ où $x_{i+2} \in E_{i+2}$, $x_{i+1} \in E_{i+1}$, $x_i \in E_i$ et $y \in F_i \oplus F_{i+1}$. Montrons par la suite l'exactitude de 2.1.1

<u>Exactitude en E_{i+2}.</u> $\mathrm{Ker} g_{i+2} = \mathrm{Ker} f_{i+2} = \mathrm{Im} f_{i+2}$.

<u>Exactitude en $E_{i+1} \oplus F$.</u> $\mathrm{Ker} g_{i+1} = \mathrm{Ker} f_{i+1} \oplus 0 = \mathrm{Im} f_{i+2} \oplus 0 = \mathrm{Im} g_{i+2}$.

<u>Exactitude en $E_i \oplus F$.</u> $\mathrm{Ker} g_i = \mathrm{Ker} f_i \oplus F = \mathrm{Im} f_{i+1} \oplus F = \mathrm{Im} g_{i+1}$.

<u>Exactitude en E_{i-1}.</u> $\mathrm{Ker} f_{i-1} = \mathrm{Im} f_i = \mathrm{Im} g_i$.

La suite 2.1.1 est alors exacte avec $E_{i+1} \oplus F$, $E_i \oplus F$ libres de rang fini. En appliquant n fois cette opération à la RLS: $0 \rightarrow E_n \rightarrow ... \rightarrow E_0 \rightarrow M \rightarrow 0$, on obtient une RLF de même longueur. ∎

Définition 2.1.6 On dit que deux A-modules M_1 et M_2 sont *stablement isomorphes* s'il existe deux A-modules libres de rang fini F_1 et F_2 de sorte que $M_1 \oplus F_1 \approx M_2 \oplus F_2$.

Proposition 2.1.8 (Lemme de Schanuel) ([11], Chapter XXI, Lemma 2.4) *Si on a deux suites exactes de A-modules $0 \rightarrow K \xrightarrow{i} P \xrightarrow{s} M \rightarrow 0$ et $0 \rightarrow K' \xrightarrow{i'} P' \xrightarrow{s'} M \rightarrow 0$ avec P, P' projectifs, alors $K \oplus P' \approx K' \oplus P$.*

Preuve Comme P est projectif et $s' : P' \longrightarrow M$ est surjectif, il existe $u \in \mathrm{Hom}(P, P')$ tel que $s = s'u$ (théorème 1.1.1). Soit $v : K \longrightarrow K'$ la restriction de u à K. On a alors le diagramme commutatif suivant:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{s} & M & \longrightarrow & 0 \\ & & \downarrow v & & \downarrow u & & \downarrow 1_M & & \\ 0 & \longrightarrow & K' & \xrightarrow{i'} & P' & \xrightarrow{s'} & M & \longrightarrow & 0 \end{array} \qquad (2.1.2)$$

Considérons ensuite les deux homomorphismes de A-modules suivants

$$\begin{array}{ccc} K & \xrightarrow{\phi} & P\oplus K' \\ x & \longmapsto & (i(x), v(x)) \end{array} \quad \text{et} \quad \begin{array}{ccc} P\oplus K' & \xrightarrow{\psi} & P' \\ (x,y) & \longmapsto & u(x) - i'(y) \end{array}$$

Montrons ensuite que la suite $0 \longrightarrow K \xrightarrow{\phi} P\oplus K' \xrightarrow{\psi} P' \longrightarrow 0$ est exacte.

<u>ϕ est injectif</u> Si $\phi(x) = 0$, alors $i(x) = 0$, d'où $x = 0$ (car i est injectif).

<u>Exactitude en $P\oplus K'$</u> Pour tout $x \in K$, $\psi\phi(x) = \psi(i(x), v(x)) = ui(x) - i'v(x) = 0$ (par la commutativité du diagramme 2.1.2), alors $\text{Im}\phi \subseteq \ker\psi$. Réciproquement, si $(x, y) \in \ker\psi$, alors $u(x) = i'(y)$, d'où $s(x) = s'u(x) = s'i'(y) = 0$, donc $x = i(h)$ où $h \in K$ (car $\ker s = \text{Im} i$). D'autre part, $u(x) = i'(y)$, alors $i'v(h) = ui(h) = i'(y)$, d'où $y = v(h)$ (i' est injectif). Donc $(x, y) = (i(h), v(h)) = \phi(h)$ et par suite $\ker\psi \subseteq \text{Im}\phi$.

<u>ψ est surjective</u> Soit $z \in P'$, il existe $x \in P$ tel que $s'(z) = s(x)$ (s est surjectif), alors $s'(z) = s'u(x)$, d'où $z - u(x) \in \ker s' = \text{Im} i'$. Choisissons $y \in K'$ tel que $z = u(x) + i'(y)$, on obtient que $z = \psi(x, -y)$.

Comme P' est projectif, la suite $0 \to K \xrightarrow{\phi} P\oplus K' \xrightarrow{\psi} P' \to 0$ est scindée, par suite $P\oplus K' \approx P'\oplus K$. D'où le résultat. ∎

Lemme 2.1.1 ([11], Chapter XXI, Lemma 2.3) *Soient* $0 \to N_i \xrightarrow{j_i} E_i \xrightarrow{s_i} M_i \to 0$ $(i = 1, 2)$ *deux suites exactes de A-modules où M_1 et M_2 sont stablement isomorphes et E_1, E_2 sont deux modules stablement libres. Alors N_1 et N_2 sont stablement isomorphes.*

Preuve Soient F_1, F_2 deux A-modules libres de rang fini tels que $M_1\oplus F_1 \approx M_2\oplus F_2$. Considérons les quatre homomorphismes suivants

$$\begin{array}{ccc} N_i & \xrightarrow{\phi_i} & E_i\oplus F_i \\ x & \longmapsto & (j_i(x), 0) \end{array} \quad \text{et} \quad \begin{array}{ccc} E_i\oplus F_i & \xrightarrow{\psi_i} & M_i\oplus F_i \\ (x,y) & \longmapsto & (s_i(x), y) \end{array} \quad (i = 1, 2)$$

Clairement, ϕ_i est injectif et ψ_i est surjectif $(i = 1, 2)$. D'autre part, pour $i = 1$ ou $i = 2$, la suite $0 \to N_i \xrightarrow{\phi_i} E_i\oplus F_i \xrightarrow{\psi_i} M_i\oplus F_i \to 0$ est exacte. En effet, il suffit de montrer l'exactitude en $E_i\oplus F_i$. Pour ceci, soit $(x, y) \in \ker\psi_i$, alors $(s_i(x), y) = 0$, d'où $x \in \ker s_i = \text{Im} j_i$ et $y = 0$, donc $(x, y) = (j_i(x'), 0)$ (où $x' \in N_i$) $= \phi_i(x')$ et par suite

$\ker\psi_i \subseteq \mathrm{Im}\phi_i$. Comme l'autre inclusion est immédiate, l'exactitude de la suite est montrée.

Pour $i = 1$ ou 2, E_i et F_i sont projectifs, alors $E_i \oplus F_i$ est projectif. Comme $M_1 \oplus F_1 \approx M_2 \oplus F_2$, la proposition précédente implique que $N_1 \oplus E_2 \oplus F_2 \approx N_2 \oplus E_1 \oplus F_1$. Soient L_1, L_2 deux A-modules libres de rang fini tels que $E_1 \oplus L_1$, $E_2 \oplus L_2$ sont libres de rangs finis (E_1, E_2 sont stablement libres). Si $P_1 = E_2 \oplus F_2 \oplus L_2$ et $P_2 = E_1 \oplus F_1 \oplus L_1$, alors P_1 et P_2 sont libres de rang fini et on a $N_1 \oplus P_1 \approx N_2 \oplus P_2$, ce qui montre que N_1 et N_2 sont stablement isomorphes. ∎

Définition 2.1.7 Soit M un A-module qui admet une RLS, on définit *la dimension de liberté stable* de M (qu'on note par DLS(M)) comme étant l'infimum des longueurs de toutes les résolutions stablement libres finies de M.

Notons que DLS(M) $= 0$ si et seulement si M est stablement libre.

Proposition 2.1.9 ([11], Chapter XXI, Theorem 2.5) *Soit M un A-module qui admet une RLS de longueur $n \geq 1$. Alors, toute suite exacte de A-modules de la forme $F_m \xrightarrow{g_m} \ldots \xrightarrow{g_1} F_0 \xrightarrow{g_0} M \to 0$, où $m < n$ et F_i est stablement libre pour tout $i = 0, \ldots, m$, peut être complétée à une RLS de M de longueur n.*

Preuve Soit $0 \to E_n \xrightarrow{f_n} \ldots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M \to 0$ une RLS de M de longueur $n \geq 1$. Pour tout $i = 0 \ldots, m$, posons $K_i = \ker f_i$ et $K'_i = \mathrm{Ker} g_i$ et montrons que K_i, K'_i sont stablement isomorphes. Pour $i = 0$, on a les deux suites exactes

$$0 \to K_0 \hookrightarrow E_0 \xrightarrow{f_0} M \to 0.$$
$$0 \to K'_0 \hookrightarrow F_0 \xrightarrow{g_0} M \to 0.$$

Comme E_0, F_0 sont stablement libres, ils sont en particulier projectifs. Alors, la proposition 2.1.8 implique que $K_0 \oplus F_0 \approx K'_0 \oplus E_0$. Soient L_0, P_0 deux A-modules libres de rang fini tels que $E_0 \oplus L_0$ et $F_0 \oplus P_0$ sont libres de rang fini, alors $K_0 \oplus F_0 \oplus L_0 \oplus P_0 \approx K'_0 \oplus E_0 \oplus L_0 \oplus P_0$, ce qui montre que K_0 et K'_0 sont stablement isomorphes. Supposons maintenant que K_{i-1} et K'_{i-1} ($i \geq 1$) sont stablement isomorphes. On a les deux suites exactes

$$0 \to K_i \hookrightarrow E_i \xrightarrow{f_i} \mathrm{Im} f_i = K_{i-1} \to 0.$$
$$0 \to K'_i \to F_i \xrightarrow{g_i} \mathrm{Im} g_i = K'_{i-1} \to 0.$$

Comme K_{i-1} et K'_{i-1} sont stablement isomorphes et E_i, F_i sont stablement libres, la proposition 2.1.8 implique que K_i et K'_i sont stablement isomorphes. Ceci montre que K_i et K'_i sont stablement isomorphes pour tout $i = 0, ..., m$. En particulier, il existe deux A-modules libres de rang fini F et F' tels que $K_m \oplus F \overset{\rho}{\approx} K'_m \oplus F'$.
Si $m < n-1$, considérons l'homomorphisme suivant

$$\begin{array}{ccc} E_{m+1}\oplus F & \xrightarrow{\psi} & K_m \oplus F \\ (x,y) & \longmapsto & (f_{m+1}(x), y) \end{array}$$

Pour tout $(x,y) \in K_m \oplus F$, on a $x = f_{m+1}(x')$ où $x' \in E_{m+1}$, d'òu $(x,y) = (f_{m+1}(x'), y)$ $= \psi(x', y)$. Alors ψ est surjectif. Soient $p_1 : K'_m \oplus F' \longrightarrow K'_m$ la première projection et $g_{m+1} : E_{m+1} \oplus F \longrightarrow K'_m$ la composition $p_1 \rho \psi$. Posons $F_{m+1} = E_{m+1} \oplus F$, alors F_{m+1} est stablement libre. La suite

$$F_{m+1} \xrightarrow{g_{m+1}} F_m \xrightarrow{g_m} \ldots \xrightarrow{g_1} F_0 \xrightarrow{g_0} M \longrightarrow 0$$

est exacte car $\ker g_m = K'_m = g_{m+1}(E_{m+1} \oplus F) = \operatorname{Im} g_{m+1}$. On est alors ramené à montrer le cas ou $m = n-1$. Dans ce cas, $K_m = \ker f_m = \operatorname{Im} f_n \approx E_n$ car f_n est injectif. Comme $K_m \oplus F \approx E_n \oplus F$ est stablement libre, alors $K'_m \oplus F'$ l'est encore. Il existe alors un A-module L' libre de rang fini tel que $K'_m \oplus F' \oplus L'$ est libre de rang fini, ce qui montre que K'_m est stablement libre. On prend $F_{m+1} = K'_m$ et le résultat se déduit immédiatement. ■

Corollaire 2.1.1 *Soit* $0 \rightarrow M_1 \xrightarrow{f} E \xrightarrow{g} M \rightarrow 0$ *une suite exacte de A-modules où E est stablement libre.*

1. *Si M admet une RLS de longueur $n \geq 1$, alors M_1 admet une RLS de longueur $n-1$.*

2. *Si M_1 admet une RLS de longueur $r \geq 0$, alors M admet une RLS de longueur $r+1$.*

3. *M admet une RLS si et seulement si M_1 admet une RLS.*

4. Si M admet une RLS, alors

$$DLS(M_1) = \begin{cases} DLS(M) - 1, & si\, DLS(M) > 0 \\ 0, & si\, DLS(M) = 0 \end{cases}$$

Preuve Comme les parties (3) et (4) sont des conséquences immédiates de (1) et (2), nous allons montrer seulement les deux premiers énoncés.
1. Soit $0 \to E_n \xrightarrow{f_n} \ldots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M \to 0$ une RLS de longueur n de M. Comme la suite $E \xrightarrow{g} M \to 0$ est exacte et E est stablement libre, cette suite peut être complétée à une RLS $0 \to F_n \xrightarrow{g_n} \ldots \to F_1 \xrightarrow{g_1} E \xrightarrow{g} M \to 0$ de M de longueur n (proposition 2.1.9). Comme $\mathrm{Im} g_1 = \ker g = \mathrm{Im} f$, alors pour tout $x_1 \in F_1$, on a $g_1(x_1) = f(y_1)$ où $y_1 \in M_1$, ce qui nous perment de définir l'homomorphisme

$$\begin{array}{ccc} F_1 & \xrightarrow{\psi} & M_1 \\ x_1 & \longmapsto & f^{-1}(g_1(x_1)) \end{array}$$

Si $y_1 \in M_1$, alors $f(y_1) = g_1(x_1)$ où $x_1 \in F_1$ (car $\mathrm{Im} f = \mathrm{Im} g_1$), d'où $y_1 = \psi(x_1)$, ce qui implique que ψ est surjectif. La suite

$$0 \longrightarrow F_n \xrightarrow{g_n} \ldots \xrightarrow{g_2} F_1 \xrightarrow{\psi} M_1 \longrightarrow 0 \tag{2.1.3}$$

est exacte. En effet, il suffit de montrer l'exactitude en F_1. Pour ceci, prenons un élément x_2 dans F_2, on a $g_1 g_2(x_2) = 0 = f(0)$, alors $\psi g_2(x_2) = 0$, d'où $\mathrm{Im} g_2 \subseteq \ker \psi$. Inversement, si $x_1 \in \ker \psi$, alors $g_1(x_1) = f\psi(x_1) = 0$, d'où $x_1 \in \ker g_1 = \mathrm{Im} g_2$. La suite 2.1.3 est alors une RLS de longueur $n-1$ de M_1.
2. Si $0 \to E_r \xrightarrow{f_r} \ldots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M_1 \to 0$ est une RLS de M_1 de longueur $r \geq 0$, alors on peut montrer sans difficulté que la suite $0 \to E_r \xrightarrow{f_r} \ldots \xrightarrow{f_i} E_0 \xrightarrow{ff_0} E \xrightarrow{g} M \to 0$ est une RLS de M de longueur $r+1$. ■

Proposition 2.1.10 ([11], Chapter XXI, Theorem 2.7) *Soit $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ une suite exacte de modules sur A. Alors on a:*

1. *Si M' et M admettent des RLF, il en est de même pour M''.*

2. *Si M' et M'' admettent des RLF, il en est de même pour M.*

3. *Si A est noethérien et si M, M'' admettent des RLF, il en est de même pour M'.*

Preuve 1. Supposons que M' et M admettent des RLF, alors M, M' sont de type fini et par suite M'' l'est ($M'' = g(M)$). Par la proposition 2.1.1, on a un diagramme commutatif et exact de la forme :

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \rightarrow & M_1' & \xrightarrow{g_1} & M_1 & \xrightarrow{g_2} & M_1'' & \rightarrow & 0 \\ & & \downarrow j' & & \downarrow j & & \downarrow j'' & & \\ 0 & \rightarrow & E' & \xrightarrow{i} & E & \xrightarrow{p} & E'' & \rightarrow & 0 \\ & & \downarrow \psi' & & \downarrow \psi & & \downarrow \psi'' & & \\ 0 & \rightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \rightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \tag{2.1.4}$$

où E, E', E'' sont libres de rang fini. Faisons la démonstration par induction sur $n = \mathrm{DLS}(M)$. Si $n = 0$, M est stablement libre. Le corollaire 2.1.1 appliqué à la suite

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

implique alors que M'' admet une RLS. Par la proposition 2.1.7, M'' admet une RLF. Supposons que la proposition est vraie jusqu'à l'ordre $n-1$ et que $\mathrm{DLS}(M) = n \geq 1$. Le corollaire 2.1.1 appliqué aux suites

$$0 \rightarrow M_1' \rightarrow E' \rightarrow M' \rightarrow 0, \qquad 0 \rightarrow M_1 \rightarrow E \rightarrow M \rightarrow 0$$

implique que M_1' et M_1 admettent des RLS (donc aussi des RLF, par la proposition 2.1.7) et que $\mathrm{DLS}(M_1) < \mathrm{DLS}(M)$. L'hypothèse d'induction (appliquée à la suite $0 \rightarrow M_1' \rightarrow M_1 \rightarrow M_1'' \rightarrow 0$) implique alors que M_1'' admet une RLF, et le corollaire 2.1.1 (appliqué à la suite $0 \rightarrow M_1'' \rightarrow E'' \rightarrow M'' \rightarrow 0$) implique que M'' admet une RLS, donc aussi une RLF.

2. Supposons maintenant que M', M'' admettent des RLF et montrons que c'est

le cas pour M. Notons tout d'abord que par le lemme 1.1.1, on a que M est de type fini sur A. La proposition 2.1.1 nous permet alors de considérer un diagramme commutatif et exact du type 2.1.4. Soit $n = \max(\text{DLS}(M'),\text{DLS}(M''))$ et faisons une preuve par induction sur n. Si $n = 0$, alors $\text{DLS}(M') = \text{DLS}(M'') = 0$, ce qui donne que M' et M'' sont stablement libres, donc projectifs. La suite $0 \to M' \to M \to M'' \to 0$ est alors scindée, d'où $M \approx M' \oplus M''$, ce qui implique que M est encore stablement libre et par suite il admet une RLF. Supposons ensuite que la proposition soit vraie jusqu'à l'ordre $n-1$ (où $n > 0$). D'après le corollaire 2.1.1, on a que $\max(\text{DLS}\ (M_1'),$ $\text{DLS}(M_1'')) = n-1$, alors par l'hypothèse d'induction, on déduit que M_1 admet une RLF et le corollaire 2.1.1 implique alors que M admet une RLS, donc aussi une RLF.
3.M, M'' sont de type fini sur A (car ils admettent des RLF) et $M' \approx f(M')$ qui est un sous-module d'un A-module de type fini sur un anneau noethérien, donc de type fini. On peut alors considérer un diagramme du type 2.1.4 et on fait une preuve par induction sur $n = \max(\text{DLS}(M),\text{DLS}(M''))$. Si $n = 0$, alors $\text{DLS}(M) = \text{DLS}(M'') =$ 0, ce qui implique que M, M'' sont stablement libres, d'où M' l'est encore car la suite $0 \to M' \to M \to M'' \to 0$ est scindée. Donc M' admet une RLF. Supposons maintenant que $n \geq 1$, le corollaire 2.1.1 nous donne que $\text{DLS}(M_1) \leq n-1$ et $\text{DLS}(M_1'') \leq n-1$. On déduit alors par l'hypothèse d'induction que M_1' admet une RLF, ce qui montre que M' admet une RLF, en vertu du corollaire 2.1.1 et de la proposition 2.1.7. ∎

Lemme 2.1.2 *Soit $0 = M_1 \subset M_2 \subset \ldots \subset M_n = M$ une filtration d'un A-module M telle que M_i/M_{i-1} admet une RLF pour tout $i = 2, \ldots, n$. Alors M admet une RLF.*

Preuve Montrons que M_i admet une RLF pour tout $i = 1, \ldots, n$. Si $i = 1$, $M_1 =$ 0 est libre (ayant $\emptyset$ comme base par convention), donc admet une RLF. Supposons que M_{i-1} ($i \geq 2$) admet une RLF. On a la suite exacte $0 \to M_{i-1} \hookrightarrow M_i \to M_i/M_{i-1} \to 0$ où M_{i-1}, M_i/M_{i-1} admettent des RLF. La partie 2 de la proposition précédente montre que M_i admet une RLF. Alors M_i admet une RLF pour tout $i = 1, \ldots, n$. En particulier pour $M_n = M$. ∎

Théorème 2.1.1 ([**11**], Chapter XXI, Theorem 2.8) *Soit A un anneau noethérien. Si tout A-module de type fini admet une RLF, alors tout $A[X]$-module de type fini admet une RLF.*

Preuve Soit M un $A[X]$-module de type fini. Comme $A[X]$ est noethérien, la proposition 2.1.5 nous donne que M admet une filtration $0 = M_1 \subset M_2 \subset \ldots \subset M_n = M$ avec $M_i/M_{i-1} \approx A[X]/P_i$ où $P_i \in \operatorname{Spec}(A[X])$. Alors, il suffit (par le lemme 2.1.2) de montrer le théorème dans le cas où $M = A[X]/P$ avec $P \in \operatorname{Spec}(A[X])$.

Supposons par l'absurde que l'ensemble

$$\mathcal{J} = \{\, P \in \operatorname{Spec}(A[X]) \text{ tel que } A[X]/P \text{ n'admet pas une RLF}\}$$

est non vide; alors l'ensemble $\mathcal{J}' = \{\, P \cap A$ tel que $P \in \mathcal{J}\,\}$ est non vide et admet un élément maximal $\wp_0$; soit aussi $P_0 \in \mathcal{J}$ tel que $P_0 \cap A = \wp_0$.
On considère l'anneau intègre $A_0 = A/\wp_0$ et les $A[X]$-modules

$$\wp_0[X], \qquad A[X]/\wp_0[X] \approx A_0[X], \qquad Q_0 = P_0/\wp_0[X] \subset A_0[X].$$

Pour tout A-module H, on peut considérer le $A[X]$-module $H[X]$ dont les éléments sont les polynômes en X à coefficients dans H; on a alors un isomorphisme de $A[X]$-modules, $H[X] \approx A[X] \otimes_A H$. Si H admet une RLF alors, en appliquant le foncteur $A[X] \otimes_A -$ à cette RLF, on obtient une RLF du $A[X]$-module $H[X]$ (en effet, $A[X]$ étant un A-module libre, le foncteur $A[X] \otimes_A -$ est exacte). On voit ainsi que si H est un A-module de type fini alors le $A[X]$-module $H[X]$ admet une RLF (car H admet une RLF). En particulier, les $A[X]$-modules $\wp_0[X]$ et $A_0[X]$ admettent des RLF.

Le fait que $A[X]/\wp_0[X] \approx A_0[X]$ admette une RLF implique que $P_0 \neq \wp_0[X]$, car $A[X]/P_0$ n'admet pas de RLF. L'idéal premier Q_0 de $A_0[X]$ est donc non nul; on peut alors choisir $f \in Q_0 \backslash \{0\}$ de degré minimal et considérer les $A[X]$-modules

$$(f) = f.A_0[X] \qquad \text{et} \qquad N = Q_0/(f).$$

Notons que les $A[X]$-modules (f) et $A_0[X]$ sont isomorphes, car ils sont isomorphes comme $A_0[X]$-modules; donc (f) admet une RLF.

Il est clair que le $A[X]$-module N satisfait $\operatorname{ann}_A(N) \supseteq \wp_0$ lorsqu'on le considère comme un A-module; montrons que $\operatorname{ann}_A(N) \supset \wp_0$ (inclusion stricte).

Soient $S = A_0 \backslash \{0\}$ et $K_0 = S^{-1}A_0$ (le corps des fractions). Puisque f est un élément non nul et de degré minimal de l'idéal $S^{-1}Q_0 = Q_0.K_0[X]$ de $K_0[X]$, on a $S^{-1}Q_0 = f.K_0[X] = S^{-1}(f)$. On a donc $S^{-1}N = S^{-1}Q_0/S^{-1}(f) = 0$ et puisque N est de type fini, il existe $s \in S$ tel que $sN = 0$. Soit $d_0 \in A$ tel que $s = d_0 + \wp_0[X]$ alors $d_0 \in \mathrm{ann}_A(N)$ et $d_0 \notin \wp_0$ car $s \neq 0$.

La condition $\mathrm{ann}_A(N) \supset \wp_0$ implique que le $A[X]$-module N admet une RLF. En effet, N admet une filtration finie

$$0 = N_1 \subset N_2 \subset ... \subset N_n = N,$$

avec $N_i/N_{i-1} \approx A[X]/Q_i$, $Q_i \in \mathrm{Spec}(A[X])$ pour tout $i = 2, ..., n$ (proposition 2.1.5). On a alors pour chaque $i = 2, ..., n$

$$Q_i \cap A = \mathrm{ann}_A\,(A[X]/Q_i) = \mathrm{ann}_A\,(N_i/N_{i-1}) \supseteq \mathrm{ann}_A(N_i) \supseteq \mathrm{ann}_A(N) \supset \wp_0$$

donc $Q_i \cap A \notin \mathcal{J}'$ par maximalité de $\wp_0$, donc $Q_i \notin \mathcal{J}$ et $N_i/N_{i-1} \approx A[X]/Q_i$ admet une RLF. Par le lemme 2.1.2, N admet donc une RLF.

On a les trois suites exactes de $A[X]$-modules

$$\begin{aligned} &0 \to (f) \to Q_0 \to N \to 0 \\ &0 \to \wp_0[X] \to P_0 \to Q_0 \to 0 \\ &0 \to P_0 \to A[X] \to A[X]/P_0 \to 0 \end{aligned}$$

où (f), N, $\wp_0[X]$ et $A[X]$ admettent des RLF. En appliquant la proposition 2.1.10 à ces suites on obtient successivement que Q_0, P_0 et $A[X]/P_0$ admettent des RLF. Ceci contredit le fait que $P_0 \in \mathcal{J}$. Cette contradiction découle de notre supposition de l'existence d'un idéal premier P de $A[X]$ tel que $A[X]/P$ n'admet pas une RLF. D'où le résultat. ∎

Théorème 2.1.2 (Serre) ([**11**], Chapter XXI, Theorem 2.7) *Soient A un anneau principal, $X_1,...,X_n$ des variables indépendantes. Alors tout $A[X_1, ..., X_n]$-module projectif et de type fini est stablement libre.*

Preuve Motrons ce théorème par induction sur n. Si $n = 0$, alors M est un A-module projectif de type fini, on peut construire un épimorphisme $\psi : L \longrightarrow M$ où L est un A-module libre de rang fini. Soit K le noyau de ψ. Par la proposition 1.3.1, K est libre de rang fini sur A. La suite

$$0 \longrightarrow K \longrightarrow L \longrightarrow M \longrightarrow 0$$

étant exacte et M projectif, alors $L \approx M \oplus K$, ce qui montre que M est stablement libre. Supposons ensuite que $n \geq 1$ et soit M un $A[X_1, ..., X_n]$-module projectif de type fini. Par le théorème 2.1.1 et l'hypothèse d'induction, M admet une RLF. Comme il est projectif sur $A[X_1, ..., X_n]$, le résultat se déduit immédiatement de la proposition 2.1.6. ∎

2.2 Le théorème de Horrocks

Définition 2.2.1 1. On dit que $(f_1, ..., f_n) \in A^n$ est une *ligne unimodulaire* sur A^n si l'idéal de A engendré par les f_i $(i = 1, ..., n)$ est A.

2. On dit qu'une ligne unimodulaire $f = (f_1, ..., f_n)$ sur A^n *possède la propriété d'extension unimodulaire* (qu'on note par PEU) s'il existe une matrice $\mathcal{A} \in \mathrm{GL}_n(A)$ telle que f est la première ligne de $\mathcal{A}$.

Pour tout idéal I de $A[X]$ et tout entier positif m, on note par I_m l'ensemble de tous les éléments $\alpha \in A$ tels qu'il existe $h \in I$ avec $h = \alpha X^m + \alpha_{m-1}X^{m-1} + ... + \alpha_0$.

Lemme 2.2.1 *I_m est un idéal de A pour tout m.*

Preuve Evident. ∎

Proposition 2.2.1 (Lemme de Suslin) *Soit I un idéal de $A[X]$ contenant un polynôme unitaire f de degré $m + 1$. Alors les coefficients d'un polynôme g appartenant à I tel que* $\deg g \leq m$ *appartiennent à I_m.*

Preuve Posons $f = X^{m+1} + a_1X^m + ... + a_{m+1}$ où $a_i \in A$ pour tout i. Soit $g = b_0X^m + b_1X^{m-1} + b_{m-1}X + b_m$ un polynôme de degré m dans I. On a que $b_0 \in I_m$ par définition de I_m. Supposons que pour tout polynôme $h = \sum_{k=0}^{m} c_k X^{m-k}$ de I, on a que $c_k \in I_m$ pour tout $k = 0, ..., i$ où $i < m$. Posons $g' = Xg - b_0f \in I$. Alors g' est le polynôme $(b_1 - b_0a_1)X^m$ +...+ $(b_i - b_0a_i)X^{m-i+1}$ + $(b_{i+1} - b_0a_{i+1})X^{m-i}$ +...+ $(b_m - b_0a_m)X + (0 - b_0a_{m+1})$. On déduit par l'hypothèse d'induction que $b_{i+1} - b_0a_{i+1} \in I_m$, d'où $b_{i+1} \in I_m$ car $b_0 \in I_m$, ce qui termine la preuve. ∎

Théorème 2.2.1 (Horrocks) ([11], Chapter XXI, Theorem 3.1) *Soit* (A, Ω) *un anneau local,* $S = A[X]$. *Si*

$$f = (f_1, ..., f_n), \qquad n \geq 1$$

est une ligne unimodulaire de S^n *telle que un des* f_i *est unitaire, alors* f *possède la PEU.*

Preuve Faisons la preuve par induction sur n. Si $n = 1$, alors $f = f_1$ avec $f_1A[X] = A[X]$. Il existe alors $g_1 \in A[X]$ tel que $f_1g_1 = 1$, ce qui montre que la matrice (f_1) est inversible dans $\mathcal{M}_1(A[X])$. Montrons aussi le cas $n = 2$. Dans ce cas $f = (f_1, f_2)$ avec $< f_1, f_2 > = A[X]$. Il existe alors g_1, $g_2 \in A[X]$ tels que $f_1g_1 + f_2g_2 = 1$. Considérons les deux matrices

$$\mathcal{A} = \begin{pmatrix} f_1 & f_2 \\ g_2 & -g_1 \end{pmatrix}, \mathcal{B} = \begin{pmatrix} g_1 & f_2 \\ g_2 & -f_1 \end{pmatrix}$$

On a clairement que $\mathcal{A}.\mathcal{B} = \mathcal{B}.\mathcal{A} = I_2$. Ce qui montre que $\mathcal{A}$ est inversible, d'où $f = (f_1, f_2)$ possède la PEU. (Remarquons que pour montrer les cas $n = 1, 2$, on n'a pas besoin du fait que A est local). Supposons que $n \geq 3$. Soit f_i la composante unitaire de f de plus faible degré d. Par une permutation convenable des indices, on peut supposer que $i = 1$ et on fait la preuve dans ce cas par induction sur d. Si $d = 0$, alors $f_1 = 1$. Soit la matrice

$$\mathcal{A} = \begin{pmatrix} 1 & f_2 & ... & f_n \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & ... & \vdots \\ 0 & 0 & ... & 1 \end{pmatrix}.$$

Il est clair qu'on peut, par une suite d'opérations élémentaires sur les colonnes, ramener $\mathcal{A}$ à la matrice unité I_n, ce qui montre que $\mathcal{A}$ est inversible et f possède la PEU. Supposons ensuite que $d \geq 1$. Soit $j \in \{2, ..., n\}$. Si $\deg f_j < d$, on pose $g_j = f_j$. Si $\deg f_j \geq d$, on peut trouver (par l'algorithme d'Euclide) q_j, $r_j \in A[X]$ avec $f_j = q_j f_1 + r_j$ et $\deg r_j < \deg f_1 = d$, on pose dans ce cas $g_j = r_j$. Ecrivons $g_1 = f_1$ et $g = (g_1, ..., g_n)$. Comme les vecteurs f et g peuvent être obtenus l'un de l'autre au moyen d'opérations élémentaires sur les colonnes, on voit que g est unimodulaire, et que g admet la PEU si et seulement si f admet la PEU. On peut alors supposer que $f = (f_1, ..., f_n)$ est une ligne unimodulaire telle que f_1 est unitaire et $\deg f_i < \deg f_1 = d$ pour tout $i = 2, ..., n$. Montrons ensuite que les coefficients des f_i $(i = 2, ..., n)$ ne peuvent pas être tous dans Ω. Pour voir ceci on choisit des éléments $v_1, ..., v_n$ dans $A[X]$ tels que

$$v_1 f_1 + ... + v_n f_n = 1 \tag{2.2.1}$$

Si tous les coefficients des f_i sont dans Ω, alors dans $A[X]/\Omega[X]$ la relation 2.2.1 sera $\overline{v_1}.\overline{f_1} = 1$ (car $\overline{f_i} = 0$ pour tout $i = 2, ..., n$), ce qui montre que $\overline{f_1}$ est inversible dans $A[X]/\Omega[X] = (A/\Omega)[X]$, d'où $\overline{f_1} = \overline{\alpha}$ où $\alpha \in A \backslash \Omega$ et par suite $f_1 - \alpha \in \Omega[X]$, ce qui implique que tous les coefficients de f_1 sauf celui de X^0 sont dans Ω. Ceci est impossible car f_1 est unitaire et de degré $d \geq 1$.

Soit $i \in \{2, ..., n\}$ tel que f_i admet au moins un coefficient n'appartenant pas à Ω. On peut supposer, par une permutation des indices, que $i = 2$. Posons $f_1 = X^d + a_1 X^{d-1} + ... + a_{d-1} X + a_d$ et $f_2 = b_s X^s + ... + b_1 X + b_0$ où un des b_i n'appartient pas à Ω, donc inversible. Soit $I = < f_1, f_2 >$. I est un idéal de $A[X]$ contenant un polynôme unitaire de degré $d > 0$ (qui est f_1) et $f_2 \in I$ avec $\deg f_2 \leq d - 1$. On déduit par le lemme de Suslin que tous les coefficients de f_2 sont dans I_{d-1}, d'où $I_{d-1} = A$, ce qui implique qu'il existe un polynôme unitaire $g = g_1 f_1 + g_2 f_2 \in I$ (g_1, $g_2 \in A[X]$) tel que $\deg g = d - 1$.

Soit f' la ligne unimodulaire $(f'_1, ..., f'_n)$ où $f'_i = f_i$ pour tout $i \neq 3$ et $f'_3 = f_3 + g_1 f_1 + g_2 f_2$. Clairement, on a que f' possède la PEU si et seulement si f possède la PEU. Si f_3 est unitaire (avec $\deg f_3 < d$), alors le plus petit degré d'une composante unitaire de f est inférieur ou égale $d - 1$, alors f possède la PEU par l'hypothèse d'induction. Si f_3 n'est pas unitaire, alors le coefficient directeur de f_3 est dans Ω (car il n'est pas inversible) et on a deux cas à envisager :

Cas1 Si $\deg f_3 < d-1$, alors le coéfficient directeur de f_3' est celui de $g_1f_1+g_2f_2$. Donc f_3' est unitaire et par suite le degré minimal d'une composante unitaire de f' est inférieur ou égale au degré de f_3' qui est $d-1$. Le résultat se déduit alors par l'hypothèse d'induction.

Cas2 Si $\deg f_3 = d-1$, alors le coefficient directeur de f_3' est dans $1+\Omega$, donc inversible. On peut alors supposer que f_3' est unitaire de degré $d-1$. L'hypothèse d'induction nous permet de conclure que f' (et par suite f) admet la PEU. ∎

On définit $E_n(A)$ comme étant le sous-groupe de $\mathrm{GL}_n(A)$ engendré par les matrices de $\mathrm{GL}_n(A)$ qui sont de la forme $I+ae_{ij}$, $i \neq j$ où $a \in A$ et e_{ij} est la matrice dont toutes les entrées sont nulles sauf celle de la i-ème ligne et la j-ème colonne qui est égale à 1. Notons que si $\mathcal{A} \in \mathcal{M}(A, n\times n)$, alors multiplier $\mathcal{A}$ à gauche par $I+ae_{ij}$ revient à ajouter le produit de la j-ème ligne de $\mathcal{A}$ par a à la i-ème ligne et multiplier $\mathcal{A}$ à droite par $I+ae_{ij}$ revient à ajouter un produit de la i-ème colonne de $\mathcal{A}$ par a à la j-ème colone.

Le sous-groupe $E_n(A)$ jouit d'une propriété exceptionnelle qui le rend très utile dans ce qui suit. Pour le moment, on a le lemme suivant

Lemme 2.2.2 ([10], Chapter I, page 36) *Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux commutatifs et notons par $E_n(f) : E_n(A) \longrightarrow E_n(B)$ l'homomorphisme de groupes induit par f. Alors, si f est surjectif, $E_n(f)$ l'est aussi.*

Preuve Notons tout d'abord que si $a \in A$ et $i \neq j$, alors $E_n(f)(I+ae_{ij}) = I'+f(a)e_{ij}'$ où I' est l'élément neutre de $\mathrm{GL}_n(B)$ et e_{ij}' est définie de la même manière que e_{ij}. Considérons un générateur $I'+be_{ij}'$ de $E_n(B)$, où $b \in B$ et $i \neq j$. Comme f est surjectif, il existe $a \in A$ tel que $f(a) = b$; alors $I'+be_{ij}' = I'+f(a)e_{ij}' = E_n(f)(I+ae_{ij}) \in \mathrm{Im}E_n(f)$, d'où $E_n(f)$ est surjectif. ∎

Définition 2.2.2 Soient $f = (f_1, ..., f_n)$ et $g = (g_1, ..., g_n)$ deux vecteurs de A^n. On dit que f est *équivalent* à g sur A et on écrit $f \sim g$ s'il existe une matrice inversible $\mathcal{A} \in \mathrm{GL}_n(A)$ telle que $f = g.\mathcal{A}$.

Si G est un sous-groupe de $\mathrm{GL}_n(A)$, on dit que f et g sont *équivalentes relativement à G* et on note $f \sim_G g$ si $f = g.\mathcal{A}$ avec $\mathcal{A} \in G$.

Remarque Soient f, $g \in A^n$ deux vecteurs.

1. f admet la PEU si et seulement si $f \sim (1, 0, ..., 0)$.

2. $f \sim_{E_n(A)} g$ si et seulement si g peut être obtenu de f (ou vice-versa) au moyen d'une suite d'opérations élémentaires sur les colonnes (par une transformation élémentaire, on veut dire ici une transformation dont la seule opération permise est la multiplication d'une colonne i d'une certaine matrice par une constante et l'ajouter à la colonne j de cette matrice où $i \neq j$).

Lemme 2.2.3 ([10], Chapter I, Proposition 5.2) *Si* $(a_1, ..., a_n)$ *est un vecteur de* A^n *où* $n \geq 2$*, alors pour* $i < j$ *on a* $(a_1, ..., a_i, ..., a_j, ..., a_n) \sim_{E_n(A)} (a_1, ..., a_j, ..., -a_i, ..., a_n)$.

Preuve Faisons la preuve par induction sur n. Si $n = 2$, on a que la matrice

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

appartient à $E_2(A)$ car on a la suite suivante de transformations élémentaires :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Comme

$$\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} b & -a \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

pour tout (a, b) dans A^2, on déduit que $(a, b) \sim_{E_2(A)} (-b, a)$.
Si $n \geq 3$, supposons que i, $j \neq 1$. Par l'hypothèse d'induction, il existe une matrice $\mathcal{A} \in E_{n-1}(A)$ telle que $(a_2, ..., a_i, ..., a_j, ..., a_n) = (a_2, ..., a_j, ..., -a_i, ..., a_n)\mathcal{A}$. Ceci implique que $(a_1, ..., a_i, ..., a_j, ..., a_n) = (a_1, ..., a_j, ..., -a_i, ..., a_n).\mathcal{A}'$ où

$$\mathcal{A}' = \begin{pmatrix} 1 & 0 \\ 0 & \mathcal{A} \end{pmatrix}.$$

Clairement $\mathcal{A}' \in E_n(A)$. D'où le résultat. ■

Lemme 2.2.4 *Soit $a = (a_1, ..., a_n)$ $(n > 1)$ une ligne unimodulaire sur A^n qui admet une sous-ligne unimodulaire de longueur $m < n$. Alors $a \sim_{E_n(A)} (1, 0, ..., 0)$.*

Preuve On peut supposer que $(a_1, ..., a_m)$ est la sous-ligne unimodulaire de a. On a dans A une relation de la forme $b_1 a_1 + ... + b_m a_m = 1$ où $b_i \in A$. Par une suite de transformations élémentaires sur les colonnes, on peut ramener a_{m+1} à $a_{m+1} - (b_1 a_1 + ... + b_m a_m)(a_{m+1} - 1) = 1$ et par suite on peut ramener a à la forme $(0, ..., 0, 1, 0, ..., 0)$. Le résultat se déduit maintenant du lemme 2.2.3. ∎

On termine cette section par un corollaire du théorème de Horrocks :

Corollaire 2.2.1 *Soient (A, Ω) un anneau local, f une ligne unimodulaire sur $A[X]^n$ qui admet une composante unitaire. Alors $f(X) \sim f(0)$ sur $A[X]$.*

Preuve Soit $g = (g_1, ..., g_n)$ un vecteur de $A[X]^n$ tel que $\sum_{i=1}^n f_i g_i = 1$, ce qui donne que

$$\sum_{i=1}^{n} f_i(0) g_i(0) = 1. \tag{2.2.2}$$

Ceci montre que les composantes de $f(0)$ ne peuvent pas être toutes dans Ω car sinon l'équation 2.2.2 devient $0 = 1$ modulo Ω. Donc $f(0)$ a une composante inversible, ce qui implique que $f(0) \sim e_1$. Par le théorème de Horrocks on a $f(X) \sim e_1$. D'où le résultat. ∎

2.3 La solution dans le cas d'un corps.

Lemme 2.3.1 ([11], Chapter XXI, lemme 3.3) *Soient A un anneau intègre, S une partie multiplicativement close de A, $f(X) = (f_1, ..., f_n)$ un vecteur de $A[X]^n$ et $\overline{f(X)}$ le vecteur $(\frac{f_1}{1}, ..., \frac{f_n}{1})$ dans $A_S[X]^n$. Si $\overline{f(X)} \sim \overline{f(0)}$ sur $A_S[X]$, alors il existe $c \in S$ tel que $f(X + cY) \sim f(X)$ sur $A[X, Y]$ où Y est une variable indépendante.*

Preuve Comme A est un anneau intègre, on peut prendre A comme sous-anneau de A_S et alors (pour chaque p, q) l'homomorphisme

$$\begin{array}{ccc} \mathcal{M}(A[X,Y], p \times q) & \longrightarrow & \mathcal{M}(A_S[X,Y], p \times q) \\ \mathcal{U} & \mapsto & \overline{\mathcal{U}} \end{array}$$

est tout simplement l'inclusion (c'est-à-dire $\mathcal{U} = \overline{\mathcal{U}}$). Ainsi, quand des matrices $\mathcal{U} \in \mathcal{M}(A[X,Y], p\times q)$, $\mathcal{V} \in \mathcal{M}(A[X,Y], q\times r)$ et $\mathcal{W} \in \mathcal{M}(A[X,Y], p\times r)$ satisfont à $\overline{\mathcal{U}}.\overline{\mathcal{V}} = \overline{\mathcal{W}}$, on peut conclure que $\mathcal{U}.\mathcal{V} = \mathcal{W}$.

Soit $\mathcal{A}(X)$ une matrice inversible d'ordre n à entrées dans $A_S[X]$ telle que $\overline{f(X)} = \overline{f(0)}.\mathcal{A}(X)$, d'où $\overline{f(0)} = \overline{f(X)}.\mathcal{A}(X)^{-1}$. Posons $G(X,Y) = \mathcal{A}(X+Y)^{-1}.\mathcal{A}(X) \in \mathrm{GL}_n(A_S[X,Y])$. Si on développe l'expression de $G(X,Y)$ on obtient

$$G(X,Y) \;=\; G_0(X) + G_1(X)Y + ... + G_r(X)Y^r$$

où $G_i(X) \in \mathcal{M}(A_S[X], n\times n)$ pour tout i et $G_0(X) = I_n$.
Soit t le produit de tous les dénominateurs des entrées de toutes les matrices $G_i(X)$ ($i = 0, ..., r$), alors $t \in S$. D'autre part on a $\overline{f(X+Y)}.G(X,Y) = \overline{f(0)}.\ \mathcal{A}(X) = \overline{f(X)}$, ce qui implique que $\overline{f(X+tY)}.G(X,tY) = \overline{f(X)}$. Comme $G(X,tY)$ est l'image d'une matrice $N(X,Y) \in \mathcal{M}(A[X,Y], n\times n)$, $\overline{f(X+tY)}.\overline{N(X,Y)} = \overline{f(X)}$ et conséquement $f(X+tY).N(X,Y) = f(X)$.

Soit $\mathcal{H}(X,Y) \in \mathrm{GL}_n(A_S[X,Y])$ telle que $G(X,Y).\mathcal{H}(X,Y) = \overline{I_n}$. En suivant le même raisonnement que précédement, on peut trouver $t' \in S$ tel que $\mathcal{H}(X,t'Y) = \overline{Q(X,Y)}$ où $Q(X,Y) \in \mathcal{M}(A[X,Y], n\times n)$. Comme $\overline{N(X,t'Y)}.\overline{Q(X,tY)} = \overline{I_n}$, il s'ensuit que $N(X,t'Y).Q(X,tY) = I_n$, d'où $N(X,t'Y) \in \mathrm{GL}_n(A[X,Y])$. Posons $c = tt'$, alors $f(X+cY).N(X,t'Y) = f(X)$, d'où $f(X+cY) \sim f(X)$. ■

Lemme 2.3.2 *Soit $\phi : A \longrightarrow B$ un homomorphisme d'anneaux. Si $\mathcal{A} = (a_{ij})_{i,j} \in \mathrm{GL}_n(A, n\times n)$, alors $\phi(\mathcal{A}) \in \mathrm{GL}_n(B, n\times n)$ où $\phi(\mathcal{A})$ est la matrice $(\phi(a_{ij}))_{i,j}$.*

Preuve Soit $\mathcal{B} \in \mathrm{GL}_n(A)$ telle que $\mathcal{A}.\mathcal{B} = \mathcal{B}.\mathcal{A} = I_n$. Alors $\phi(\mathcal{A}).\phi(\mathcal{B}) = \phi(\mathcal{A}.\mathcal{B}) = I_n$. Alors $\phi(\mathcal{A}) \in \mathrm{GL}_n(B)$. ■

Théorème 2.3.1 ([11], Chapter XXI, Theorem 3.4) *Soient A un anneau intègre, $f(X) = (f_1(X), ..., f_n(X))$ une ligne unimodulaire sur $A[X]^n$ qui admet au moins une composante unitaire. Alors $f(X) \sim f(0)$ sur $A[X]$.*

Preuve Soit $\mathcal{J}$ l'ensemble de tous les éléments $c \in A$ qui vérifient $f(X+cY) \sim f(X)$ où Y est une variable indépendante. On a que $\mathcal{J}$ est un idéal de A. En effet, soient c, $c' \in \mathcal{J}$ et $\mathcal{A} \in \mathrm{GL}_n(A[X,Y])$ telle que $f(X+cY) = f(X).\mathcal{A}$. Par la propriété universelle de l'anneau de polynômes sur A, il existe un unique homomorphisme de A-algèbres $\phi : A[X,Y] \longrightarrow A[X,Y]$ tel que $\phi(X) = X + c'Y$ et $\phi(Y) = Y$. On a que $\phi(f(X+cY)) = \phi(f(X).\mathcal{A}) = f(X+c'Y).\phi(\mathcal{A})$ avec $\phi(\mathcal{A}) \in \mathrm{GL}_n(A[X,Y])$ (lemme 2.3.2). D'où $f(X+c'Y+cY) = f(X+c'Y).\phi(\mathcal{A})$. Comme $c' \in \mathcal{J}$, $f(X+c'Y) = f(X).\mathcal{A}'$ où $\mathcal{A}' \in \mathrm{GL}_n(A[X,Y])$, ce qui implique que $f(X+(c+c')Y) = f(X).\mathcal{A}'.\phi(\mathcal{A})$. Donc $f(X+(c+c')Y) \sim f(X)$ et par suite $c+c' \in \mathcal{J}$. D'autre part, soient $c \in \mathcal{J}$ et $\alpha \in A$, alors $f(X+cY) = f(X).\mathcal{B}$ où $\mathcal{B} \in \mathrm{GL}_n(A[X,Y])$. Soit $\psi : A[X,Y] \longrightarrow A[X,Y]$ l'homomorphisme unique tel que $\psi(X) = X$ et $\psi(Y) = \alpha Y$. Comme $\psi(f(X+cY)) = \psi(f(X)).\psi(\mathcal{B})$, alors $f(X+\alpha cY) = f(X).\psi(\mathcal{B})$ avec $\psi(\mathcal{B}) \in \mathrm{GL}_n(A[X,Y])$, ce qui montre que $\alpha c \in \mathcal{J}$.
Montrons ensuite que $\mathcal{J} = A$. Pour tout $\wp \in \mathrm{Spec}(A)$, l'anneau $A_\wp$ est local et $\overline{f(X)} = (\frac{f_1}{1}, ..., \frac{f_n}{1})$ est une ligne unimodulaire de $A_\wp[X]^n$ qui admet une composante unitaire, alors $\overline{f(X)} \sim \overline{f(0)}$ (corollaire 2.2.1). Soit S la partie multiplicativement close $A \backslash \wp$ de A, il existe alors $c \in S$ (donc $\notin \wp$) tel que $f(X+cY) \sim f(X)$ sur $A[X,Y]$ où Y est une variable indépendante (lemme 2.3.1), ce qui montre que $c \in \mathcal{J}$. Alors $\mathcal{J}$ n'est contenu dans aucun idéal premier de A, d'où $\mathcal{J} = A$ et par suite $f(X+Y) \sim f(X)$. Soit $G(X,Y) \in \mathrm{GL}_n(A[X,Y])$ telle que $f(X+Y) = f(X).G(X,Y)$, alors $f(Y) = f(0).G(0,Y)$ avec $G(0,Y) \in \mathrm{GL}_n(A[Y])$ car c'est l'image de $G(X,Y)$ par l'homomorphisme $A[X,Y] \longrightarrow A[Y]$ qui envoie X sur 0 et Y sur Y. D'où $f(X) \sim f(0)$. ■

Lemme 2.3.3 ([11], Chapter VIII, Theorem 2.1) *Soient $X_1,...,X_r$, r variables indépendantes et F un polynôme non constant de $A[X_1, ..., X_r]$. Posons $Y_i = X_i - X_r^{n_i}$ pour $i = 1, ..., r-1$ (n_i est entier positif pour tout i) et $Y_r = X_r$. Alors $A[X_1, ..., X_r] = A[Y_1, ..., Y_r]$ et, pour un choix convenable des n_i, F prend la forme $\alpha Y_r^m + \beta_{m-1} Y_r^{m-1} + ... + \beta_1 Y_r + \beta_0$ où m est un entier positif, $\alpha \in A\backslash\{0\}$, $\beta_i \in A[Y_1, ..., Y_{r-1}]$ pour tout $i \in \{ 0,...,m-1 \}$.*

Preuve Posons $F = \sum \alpha_{(\nu)} X_1^{\nu_1} ... X_r^{\nu_r}$ où $\alpha_{(\nu)} \in A$ ne sont pas tous nuls (car F n'est pas constant) et la somme est prise sur un nombre fini des r-tuplet $(\nu) = (\nu_1, ..., \nu_r)$ qui sont distincts et non nuls. Comme $X_r = Y_r$ et $X_i = Y_i + Y_r^{n_i}$ $(1 \leq i \leq r-1)$, on aura $F = \sum \left(\alpha_{(\nu)} Y_r^{n_1\nu_1 + ... + n_{r-1}\nu_{r-1} + \nu_r} + f_{(\nu)}(Y_1, ..., Y_r) \right)$ où $f_{(\nu)}(Y_1, ..., Y_r)$ est un polynôme de $A[Y_1, ..., Y_{r-1}, Y_r]$ dans lequel Y_r apparaît avec un degré inférieur à $n_1\nu_1 + ... + n_{r-1}\nu_{r-1} + \nu_r$.
Soit $\mathcal{F}$ la famille de tous les entiers positifs ν_i tels que ν_i est une composante d'un r-tuplets $(\nu) = (\nu_1, ..., \nu_r)$ pour lequel $\alpha_{(\nu)}$ est non nul. Soit $k = \operatorname{Sup}(\mathcal{F})$. Prenons un entier positif $d > k$ et posons $n_i = d^i$ pour $i = 1, ..., r-1$.
Soit $m = \max\{n_1\nu_1 + ... + n_{r-1}\nu_{r-1} + \nu_r \mid \alpha_{(\nu)} \neq 0\}$. Rappelons que tout entier naturel x s'écrit de manière unique sous forme de somme finie $x = \sum_{i \geq 0} x_i d^i$ avec x_i entier et $0 \leq x_i \leq d$. Ceci étant vrai pour $x = m$, il existe un et un seul (ν^*) tel que $\alpha_{(\nu^*)} \neq 0$ et $n_1\nu_1^* + ... + n_{r-1}\nu_{r-1}^* + \nu_r^* = m$. On a alors $F = \alpha Y_r^m + \beta_{m-1} Y_r^{m-1} + ... + \beta_0$ avec $\alpha = \alpha_{(\nu^*)} \in A \backslash \{0\}$ et $\beta_i \in A[Y_1, ..., Y_{r-1}]$. ■

Théorème 2.3.2 (Quillen-Suslin) ([11], Chapter XXI, Theorem 3.5) *Soient K un corps, $X_1, ..., X_r$ des variables indépendantes. Alors, toute ligne unimodulaire sur $K[X_1, ..., X_r]^n$ admet la PEU.*

Preuve Faisons la preuve par induction sur le nombre r des variables indépendantes. Soit $f(X) = (f_1, ..., f_n)$ une ligne unimodulaire sur $K[X_1, ..., X_r]^n$. Si $r = 0$, on a rien à montrer. Si $r = 1$, alors f est une ligne unimodulaire sur $K[X]^n$ et K est en particulier un anneau intègre, de plus, on peut supposer que toutes les composantes f_i non nulles sont unitaires, d'où $f(X) \sim f(0)$ (théorème 2.3.1). Comme toutes les composantes non nulles de $f(0)$ sont inversibles, $f(0) \sim e_1 = (1, ..., 0)$. Donc $f(X)$ admet la PEU. Supposons ensuite $r \geq 2$. Sans perdre de généralité, on peut supposer que $f_1 \neq 0$. Si $f_1 \in K$ alors f_1 est inversible et, par conséquent, f possède la PEU. Si $f_1 \notin K$ alors, en vertu du lemme 2.3.3, on peut choisir un système de variables $Y_1, ..., Y_r$ tel que $K[X_1, ..., X_r] = K[Y_1, ..., Y_r]$ et $f_1 = \alpha Y_r^m + \beta_{m-1} Y_r^{m-1} + ... + \beta_0$, où $\alpha \in K \backslash \{0\}$ et $\beta_i \in K[Y_1, ..., Y_{r-1}]$. Ecrivons $R = K[Y_1, ..., Y_{r-1}]$, alors f est une ligne unimodulaire sur $R[Y_r]^n$ et le coefficient directeur de f_1 est un élément inversible de R; en vertu du théorème 2.3.1, $f = f(Y_1, ..., Y_r) \sim f(Y_1, ..., Y_{r-1}, 0)$. Soit $\mathcal{N} \in \mathrm{GL}_n(R[Y_r])$ telle que

$f(Y_1,...,Y_r) = f(Y_1,...,Y_{r-1},0).\mathcal{N}$. On voit facilement que $f(Y_1,...,Y_{r-1},0)$ est une ligne unimodulaire sur R^n, donc $f(Y_1,...,Y_{r-1},0)$ possède la PEU (par l'hypothèse d'induction). D'où $f(Y_1,...,Y_{r-1},0) = e_1.\mathcal{M}$ où $e_1 = (1,0,...,0)$ et $\mathcal{M} \in \mathrm{GL}_n(R)$, ce qui montre que $f = f(Y_1,...,Y_r) = e_1.\mathcal{M}.\mathcal{N}$ avec $\mathcal{M}.\mathcal{N} \in \mathrm{GL}_n(R[Y_r])$. Donc f possède la PEU. ∎

Définition 2.3.1 On dit qu'un anneau A *possède la proporiété d'extension unimodulaire* (on dit aussi que A est *Hermitien*) si toute ligne unimodulaire f sur A^n admet la PEU pour tout entier positif n.

Théorème 2.3.3 ([**11**], Chapter XXI, Theorem 3.6) *Soit A un anneau qui admet la propriété d'extension unimodulaire. Alors tout A-module stablement libre est libre.*

Preuve Soient n, r deux entiers positifs tels que $E \oplus A^r \approx A^n$. On fait une démonstration par induction sur r. Si $r = 1$, alors $E \oplus A \overset{\theta}{\approx} A^n$. Soient $p : A^n \longrightarrow A$ la deuxième projection et $\{u\}$ une base du A-module A et considérons les injections canoniques:

$$\begin{array}{ccc} A & \xrightarrow{\psi} & E\oplus A \\ a & \longmapsto & (0,a) \end{array} \qquad \text{et} \qquad \begin{array}{ccc} E & \xrightarrow{\phi} & E\oplus A \\ x & \longmapsto & (x,0) \end{array}$$

Puisque $\{u\}$ est une base de A, u est inversible. Il existe alors $v \in A$ tel que $uv = 1$, ce qui montre que (u) est une ligne unimodulaire sur A, d'où $\theta\psi(u) = (a_{11}, a_{12}, ..., a_{1n})$ est une ligne unimodulaire sur A. en effet, soit Ω un idéal maximal de A, il suffit de montrer que a_{11},...,a_{1m} n'appartiennent pas tous à Ω. Soit $K = A/\Omega$ et $\overline{E} = E/\Omega E$, alors θ induit un isomorphisme d'espaces vectoriels sur K,

$$\overline{E} \oplus K \overset{\overline{\theta}}{\approx} K^n$$

Si $\overline{a_{1j}} = a_{1j} + \Omega \in K$ alors $(\overline{a_{11}}, ..., \overline{a_{1n}}) = \overline{\theta}(\overline{u}) \neq (0, ..., 0)$, donc il existe un j tel que $\overline{a_{1j}} \neq 0$, donc $a_{1j} \notin \Omega$.
Puisque A possède la propriété d'extension unimodulaire, $(a_{11}, a_{21}, ..., a_{1n})$ est alors la première ligne d'une matrice inversible $\mathcal{A} = (a_{ij})_{i,j}$. Pour tout $j \geq 2$, on a $p(e_j)$ $= c_j u$ où $c_j \in A$. La matrice $\mathcal{B}$ dont les lignes sont les $u_j = (e_j - c_j e_1).\mathcal{A}$ a le même déterminant que $\mathcal{A}$ car elle est obtenue de $\mathcal{A}$ par une suite des tranformations

élémentaires sur les lignes. Alors $\mathcal{B}$ est inversible et par suite elle représente un automorphisme $f : A^n \longrightarrow A^n$. D'autre part on a que $p(u_j) = 0$, ce qui montre que $u_j = (x_j, 0)$ et $f(e_j) = \mathcal{B}.e_j = u_j$. Soit H le sous-module libre de A^n engendré par $\{e_2, ..., e_n\}$, alors $f(H)$ est un sous-module de E engendré par $n-1$ éléments. D'où $f(H) = E$ et par suite E est libre.
Supposons maintenant que $r > 1$. Comme $E \oplus A^r \approx A^n$, alors $E \oplus A^{r-1}$ est libre (car il est stablement libre de type 1), d'où E est libre par l'hypothèse d'induction. ∎

On arrive maintenant à la solution de la conjecture de Serre dans le cas d'un corps.

Théorème 2.3.4 ([**11**], Chapter XXI, Theorem 3.7) *Soient K un corps et M un $K[X_1, ..., X_n]$-module projectif de type fini. Alors M est libre.*

Preuve Par le théorème 2.1.2, on sait que tout $K[X_1, ..., X_n]$-module projectif de type fini est stablement libre. Comme l'anneau $K[X_1, ..., X_n]$ possède la propriété d'extension unimodulaire (par le théorème 2.3.2), le théorème 2.3.3 donne le résultat. ∎

2.4 Généralisation à un anneau principal.

Définition 2.4.1 Si I est un idéal de A, on définit la *hauteur* de I (qu'on note par $\mathrm{ht}(I)$) comme étant le minimum de l'ensemble $\{\ \mathrm{ht}(\wp)$ tel que $\wp \in \mathrm{Spec}(A)$ avec $I \subseteq \wp\ \}$. Par convention $\mathrm{ht}(A) = +\infty$.

Proposition 2.4.1 ([**10**], Chapter II, Lemma 7.4) *Soient I un idéal de A, $\wp_1, ..., \wp_r \in \mathrm{Spec}(A)$. Pour tout $x \in A$, si $x + I \subseteq \cup_{i=1}^{r} \wp_i$, alors l'idéal $J_{x,I}$ engendré par x et I est contenu dans un des $\wp_i$ $(i = 1, ..., r)$.*

Preuve Si $r = 1$, alors pour tout $x \in A$ tel que $x + I \subseteq \wp_1$, on a $x \in \wp_1$ et par suite $I \subseteq \wp_1$, d'où $J_{x,I} \subseteq \wp_1$. Supposons ensuite que la proposition cesse d'être vraie pour un certain rang et choisissons un entier positif r qui soit minimal pour la propriété que la proposition n'est pas vraie. Alors $r > 1$ et il existe $x_0 \in A$ tel que $x_0 + I \subseteq \cup_{i=1}^{r} \wp_i$ et $J_{x_0,I}$ n'est pas contenu dans $\wp_i$ pour tout $i = 1, ..., r$. Notons que pour tout

$i \neq j$, $\wp_i$ n'est pas inclus dans $\wp_j$ car sinon, ceci contredirait la minimalité de r. Notons ensuite que $x_0 \in \cap_{i=1}^{r}\wp_i$. En effet, s'il existe i tel que $x_0 \notin \wp_i$, alors $(x_0 + \wp_i I) \cap \wp_i = \emptyset$ (car si $z \in \wp_i$ est tel que $z = x_0 + p_i\alpha$ où $p_i \in \wp_i$ et $\alpha \in I$, alors $x_0 = z - p_i\alpha \in \wp_i$, d'où la contradiction). Comme $x_0 + \wp_i I \subseteq x_0 + I \subseteq \cup_{i=1}^{r}\wp_i$, alors $x_0 + \wp_i I \subseteq \cup_{i\neq j}\wp_j$, ce qui implique qu'il existe $j \neq i$ tel que $J_{x_0,\wp_i I} \subseteq \wp_j$ (par notre choix de r), d'où $x_0 \in \wp_j$ et $\wp_i I \subseteq \wp_j$. Comme $\wp_i$ n'est pas contenu dans $\wp_j$, on peut considérer un élément $y \in \wp_i \backslash \wp_j$. Alors pour tout $\alpha \in I$, on a $y\alpha \in \wp_j$, d'où $\alpha \in \wp_j$ ($\wp_j$ est premier), ce qui implique que $I \subseteq \wp_j$ et par suite $J_{x_0,I} \subseteq \wp_j$, d'où la contradiction.

Comme $x_0 + I \subseteq \cup_{i=1}^{r}\wp_i$ et $x_0 \in \wp_i$ pour tout i, alors $I \subseteq \cup_{i=1}^{r}\wp_i$. D'autre part, pour tout $i = 1, ..., r$ on a que I n'est pas contenu dans $\cup_{i\neq j}\wp_j$ (car sinon on aura que $x_0 + I \subseteq \cup_{j\neq i}\wp_j$ et $J_{x_0,I}$ n'est pas contenu dans $\wp_j$ pour tout $j \neq i$, ce qui contredit la minimalité de r). Pour tout $i = 1, ..., r$, choisissons un élément $y_i \in I\backslash\cup_{j\neq i}\wp_j$, alors $y_i \in \wp_j$ si et seulement si $i = j$. Soit $y = z_1 + ... + z_r$, où $z_i = y_1...y_{i-1}y_{i+1}...y_r$; on a alors $z_i \in \wp_j$ si et seulement si $i{\neq}j$ et conséquement y n'appartient à aucun $\wp_i$. Ainsi on a $y \in I$ et $y \notin \cup_{i=1}^{r}\wp_i$, donc I n'est pas contenu dans $\cup_{i=1}^{r}\wp_i$, ce qui est une contradiction. ■

Lemme 2.4.1 ([1], Proposition 1.11) *Soient $I_1,...,I_r$ des idéaux de A, $\wp \in$ Spec(A) tel que $\wp \supseteq \cap_{i=1}^{r}I_i$. Alors, il existe i tel que $\wp \supset I_i$.*

Preuve Supposons que $\wp$ ne contient aucun idéal I_i $(i = 1, ..., r)$. Alors, pour tout i on peut choisir un élément x_i de A tel que $x_i \in I_i$ et $x_i \notin \wp$. Soit $x = x_1.x_2...x_r$, alors $x \in \prod_{i=1}^{r}I_i \subseteq \cap_{i=1}^{r}I_i$, mais $x \notin \wp$ (car $\wp$ est premier) alors $\wp$ ne contient pas $\cap_{i=1}^{r}I_i$, d'où la contradiction. ■

Proposition 2.4.2 *1. Tout idéal premier de A contient un idéal premier minimal.*

2. Si A est noethérien, alors A amet un nombre fini d'idéaux premiers minimaux.

Preuve 1. Soient $\wp$ un idéal premier de A et $\mathcal{J}_\wp$ l'ensemble de tous les idéaux premiers de A qui sont contenus dans $\wp$. Ordonnons $\mathcal{J}_\wp$ par la relation de contenance

$\supseteq$ et montrons que toute chaîne (sous-ensemble totalement ordonné) de $\mathcal{J}_\wp$ admet une borne supérieure dans $\mathcal{J}_\wp$. Soit donc $(\wp_i)_{i\in I}$ une chaîne de $\mathcal{J}_\wp$ et posons $\wp_0 = \cap_{i\in I}\wp_i$. Comme $\wp \supseteq \wp_i$ pour tout i, alors $\wp \supseteq \wp_0$, il suffit de montrer alors que $\wp_0$ est un idéal premier de A. Soient x, $y \in A$ tels que $x, y \notin \wp_0$, il existe alors i_1, $i_2 \in I$ tels que $x \notin \wp_{i_1}$ et $y \notin \wp_{i_2}$. Supposons que $\wp_{i_1} \subseteq \wp_{i_2}$, alors x, $y \notin \wp_{i_1}$ et par suite $xy \notin \wp_{i_1}$, donc $xy \notin \wp_0$. Ceci montre que $\wp_0$ est une borne supérieure de la chaîne $(\wp_i)_{i\in I}$ dans $\mathcal{J}_\wp$. On peut déduire par le lemme de Zorn que l'ensemble $\mathcal{J}_\wp$ admet un élément maximal Ψ pour la relation de contenance. Ψ est minimal dans Spec(A) pour la relation $\subseteq$ et $\Psi \subseteq \wp$.

2. Supposons maitenant que A est noethérien et montrons que l'ensemble d'idéaux minimaux de Spec(A) est fini. Soit $\mathcal{I}$ l'ensemble de tous les idéaux radicaux (c.à.d $\sqrt{I} = I$) de A qui ne s'écrivent pas comme intersection finie d'idéaux premiers de A. Si $\mathcal{I}$ était non vide, on pourrait alors considérer un élément maximal $\Omega \in I$ pour l'inclusion (ceci est possible car A est noethérien). Comme $\Omega \in \mathcal{I}$, alors Ω n'est pas premier, d'où l'existence de deux éléments a et b de A tels que $a \notin \Omega$ et $b \notin \Omega$, mais $a.b \in \Omega$. Soient I_a et I_b les idéaux de A engendrés par a et Ω, b et Ω respectivement et montrons que $\Omega = \sqrt{I_a} \cap \sqrt{I_b}$. On a $\Omega \subset I_a$ et $\Omega \subset I_b$, d'où $\Omega \subset \sqrt{I_a}$ et $\Omega \subset \sqrt{I_b}$, ce qui implique que $\Omega \subseteq \sqrt{I_a} \cap \sqrt{I_b}$. Réciproquement, si $x \in \sqrt{I_a} \cap \sqrt{I_b}$, alors il existe deux entiers positifs m et n tels que $x^n \in I_a$ et $x^m \in I_b$, d'où $x^n = \alpha a + x_1$ et $x^m = \beta b + x_2$ où α, $\beta \in A$ et x_1, $x_2 \in \Omega$, ce qui implique que $x^{m+n} = \alpha\beta ab + \alpha a x_2 + \beta b x_1 + x_1 x_2 \in \Omega$, d'où $x \in \sqrt{\Omega} = \Omega$. Alors $\Omega = \sqrt{I_a} \cap \sqrt{I_b}$, ce qui montre que $\sqrt{I_a}$ ou $\sqrt{I_b} \in \mathcal{I}$ car sinon ils seraient tous les deux intersections finies d'idéaux premiers de A et par suite Ω le serait aussi, contredisant le fait que $\Omega \in \mathcal{I}$. Supposons que $\sqrt{I_a} \in \mathcal{I}$. Comme $\Omega \subseteq \sqrt{I_a}$ et $\Omega \neq \sqrt{I_a}$ ($a \in I_a \backslash \Omega$), on a une contradiction. On en déduit alors que $\mathcal{I} = \emptyset$ et par suite tout idéal radical de A s'écrit comme intersection finie d'idéaux premiers. Soit $\mathfrak{R}$ le nilradical de A. $\mathfrak{R}$ est l'ensemble de tous les éléments nilpotents de A et c'est encore l'intersection de tous les idéaux premiers de A. Comme $\mathfrak{R}$ est un idéal radical de A, alors on peut écrire $\mathfrak{R} = \cap_{i=1}^r \wp_i$ où $\wp_i \in$ Spec(A) pour tout i. Soit $\wp$ un idéal premier minimal de A, alors $\wp \supseteq \mathfrak{R}$, d'où il existe i tel que $\wp \supseteq \wp_i$ (lemme 2.4.1) et par suite $\wp = \wp_i$. L'ensemble des idéaux premiers minimaux de A est alors fini. ∎

Corollaire 2.4.1 *Soient A un anneau noethérien et $I \neq A$ un idéal de A. Alors l'ensemble des idéaux premiers qui contiennent I admet un nombre fini déléments minimaux.*

Preuve On applique la partie (2) de la proposition 2.4.2 à l'anneau noethérien A/I. ∎

Lemme 2.4.2 ([10], Chapter I, Proposition 5.6) *Soit $(a_1, ..., a_r, b_1, ..., b_s)$ une ligne unimodulaire sur A^{r+s} $(s \geq 1)$. Si I est l'idéal de A engendré par les a_i, $i = 1, ..., r$, et $\overline{A} = A/I$ et si $(\overline{b_1}, ..., \overline{b_s}) \sim_{E_s(\overline{A})} (\overline{1}, \overline{0}, ..., \overline{0})$, alors $(a_1, ..., a_r, b_1, ..., b_s) \sim_{E_{r+s}(A)}$ $(1, 0, ..., 0)$.*

Preuve Soit $\pi : A \longrightarrow \overline{A}$ l'épimorphisme canonique. Le lemme 2.2.2 nous donne que l'homomorphisme induit $E_s(\pi) : E_s(A) \longrightarrow E_s(\overline{A})$ est encore surjectif, ce qui nous permet de faire une marche inverse dans la suite des transformations élémentaires qui ramènent $(\overline{b_1}, ..., \overline{b_s})$ à $(\overline{1}, ..., \overline{0})$ et par suite trouver des éléments $b'_1, ..., b'_s \in A$ tels que $b'_1 \equiv 1$ et $b'_k \equiv 0 \pmod I$ pour tout $k = 2, ..., s$ et

$$(a_1, ..., a_r, b_1, ..., b_s) \sim_{E_{r+s}(A)} (a_1, ..., a_r, b'_1, ..., b'_s).$$

Une autre suite des transformations élémentaires ramène la ligne $(a_1, ..., a_r, b'_1, ..., b'_s)$ à $(a_1, ..., a_r, 1, ..., 0)$ qui admet une sous-ligne unimodulaire $(1, ..., 0)$. Le résultat se déduit maintenant du lemme 2.2.4. ∎

Proposition 2.4.3 ([10], Chapter II, Theorem 7.5) *Si A est noethérien de dimension finie d et si $a = (a_1, ..., a_n)$ est une ligne unimodulaire sur A^n avec $n \geq d + 2$, alors $a \sim_{E_n(A)} (1, 0, ..., 0)$. En particulier, a possède la PEU.*

Preuve Par la proposition 2.4.2, A possède un nombre fini d'idéaux premiers minimaux $\wp_1, ..., \wp_r$. Soit $I = < a_2, ..., a_n >$ l'idéal de A engendré par $a_2, ..., a_n$. Si $J_{a_1,I}$ est l'déal de A engendré par a_1 et I, alors $J_{a_1,I} = < a_1, a_2, ..., a_n > = A$, d'où $J_{a_1,I}$ n'est pas contenu dans $\wp_i$ pour tout $i = 1, ..., r$, la proposition 2.4.1 montre que $a_1 + I$ n'est pas contenu dans $\cup_{i=1}^{r} \wp_i$. Soit $a'_1 \in (a_1 + I) \backslash \cup_{i=1}^{r} \wp_i$ et écrivons $a'_1 = a_1 + b_2 a_2 + ... + b_n a_n$ où $b_i \in A$ pour tout $i = 2, ..., n$. Donc il suffit de montrer que la

ligne unimodulaire $(a'_1, a_2, ..., a_n)$ est équivalente à $(1, 0, ..., 0)$ relativement à $E_n(A)$. Pour ceci, on fait un argument par induction sur la dimension d de A.
Si $d = 0$, alors tout idéal premier de A sera minimal car dans Spec(A), on n'a pas de relation de la forme $\wp_1 \subset \wp_2$. Alors Spec$(A) = \{ \wp_1, ..., \wp_r \}$. Comme $a'_1 \notin \cup_{i=1}^r \wp_i$, alors a'_1 est inversible dans A et par suite $(a'_1, ..., a_n) \sim_{E_n(A)} (1, 0..., 0)$. Supposons ensuite que $d \geq 1$ et posons $\overline{A} = A/(a'_1)$, alors la dimension δ de l'anneau $\overline{A}$ est plus petite ou égale à $d-1$. En effet, soit $Q_0 \subset Q_1 \subset ... \subset Q_s$ une chaîne première de $\overline{A}$ avec $Q_i = P_i/(a'_1)$ où P_i est un idéal premier de A contenant a'_1. Il est clair que $P_0 \subset P_1 \subset ... \subset P_s$ est une chaîne première de A et comme $a'_1 \in P_0$, alors P_0 n'est pas minimal, d'où l'existence d'un idéal premier minimal $\wp_0$ tel que $\wp_0 \subset P_0$, ce qui montre que $\dim A \geq 1 + s$, d'où $\delta \leq d - 1$.
Comme il est clair que $(\overline{a_2}, ..., \overline{a_n})$ ($\overline{a_i}$ désigne $a_i + (a'_1)$) est une ligne unimodulaire de $\overline{A}$ avec $n - 1 \geq d + 1 \geq \delta + 2$, l'hypothèse d'induction montre que $(\overline{a_2}, ..., \overline{a_n})$ est équivalente à $(1, 0, ..., 0)$ relativement à $E_n(A)$. Le lemme 2.4.2 termine la preuve. ■

Si I est un idéal de $A[X]$, on note $C(I) = \{ a \in A$ tel que a est le coefficient directeur d'un polynôme f de $I \} \cup \{0\}$.

Lemme 2.4.3 *$C(I)$ est un idéal de A et si I, J sont deux idéaux de $A[X]$, alors $C(I).C(J) \subseteq C(I.J)$.*

Preuve Le fait que $C(I)$ est un idéal de A provient simplement du fait que I est un idéal de $A[X]$. Soient I, J deux idéaux de $A[X]$. Si $\alpha \in C(I)$ et $\beta \in C(J)$, il existe alors $f \in I$, $g \in J$ tels que $f = \alpha X^m + ... + a_0$ et $g = \beta X^n + ... + b_0$, d'où $fg = \alpha\beta X^{m+n} + ... + a_0 b_0 \in I$, ce qui montre que $\alpha\beta \in C(I.J)$. Comme tout élément de $C(I).C(J)$ s'écrit de la forme $\sum_{i=1}^r \alpha_i \beta_i$ où $\alpha_i \in C(I)$ et $\beta_i \in C(J)$ pour tout $i = 1, ..., r$, alors $C(I).C(J) \subseteq C(I.J)$. ■

Lemme 2.4.4 **[10]**, Chapter III, Lemma 3.2) *Si A est noethérien, alors* $\mathrm{ht}(C(I)) \geq \mathrm{ht}(I)$ *pour tout idéal I de $A[X]$.*

Preuve Supposons tout d'abord que I est un idéal premier de $A[X]$ et soit $\wp = I \cap A$. Si $I = \wp[X]$, alors $C(I) = \wp$ car $C(I) \supseteq I \cap A = \wp$ et si $\alpha \in C(I)$, alors il existe

$f \in \wp[X]$ tel que $f = \alpha X^n + ... + a_0$, d'où $\alpha \in \wp$. La proposition 1.1.26 implique que $\mathrm{ht}(C(I)) = \mathrm{ht}(\wp) = \mathrm{ht}(\wp[X]) = \mathrm{ht}(I)$. Si maintenant $\wp[X] \subset I$, alors $\wp \subset C(I)$, ce qui implique que $\mathrm{ht}(C(I)) > \mathrm{ht}(\wp) = \mathrm{ht}(I) - 1$ (proposition 1.1.26), d'où $\mathrm{ht}(C(I)) \geq \mathrm{ht}(I)$.

Dans le cas général, soient $\wp_1,...,\wp_r$ les idéaux premiers de $A[X]$ qui contiennent I et qui sont minimaux relativement à cette condition. Si $r = 0$, alors $I = A[X]$, d'où $C(I) = A$ et par suite $\mathrm{ht}(C(I)) = \mathrm{ht}(I) = +\infty$. Si $r \geq 1$, on a $\mathrm{rad}(I) = \cap_{\wp \in \mathcal{V}(I)} \wp$ $= \cap_{i=1}^r \wp_i$, d'où $\prod_{i=1}^r \wp_i \subseteq \mathrm{rad}(I)$. Soient $\alpha_1,...,\alpha_p$ des générateurs de $\prod_{i=1}^r \wp_i$ (comme étant un idéal de A, $\prod_{i=1}^r \wp_i$ est de type fini) et choisissons pour tout i un entier naturel n_i tel que $\alpha_i^{n_i} \in I$ ($\alpha_i \in \mathrm{rad}(I)$). Soit $n = \max\{ n_1,...,n_r \}$, alors $\alpha_i^n \in I$ pour tout $i = 1,...,p$, ce qui montre que $(\prod_{i=1}^r \wp_i)^n \subseteq I$ et par suite $C(\prod_{i=1}^r \wp_i)^n \subseteq C(I)$, d'où $(\prod_{i=1}^r C(\wp_i))^n \subseteq C(I)$ (lemme 2.4.3). Soit $\wp \in \mathcal{V}(C(I))$ tel que $\mathrm{ht}(C(I))$ $= \mathrm{ht}(\wp)$. Comme $(\prod_{i=1}^r C(\wp_i))^n \subseteq C(I) \subseteq \wp$, alors il existe $i \in \{1,...,r\}$ tel que $C(\wp_i)$ $\subseteq \wp$, d'où $\mathrm{ht}(C(\wp_i)) \leq \mathrm{ht}(\wp) = \mathrm{ht}(C(I))$ et par suite $\mathrm{ht}(I) \leq \mathrm{ht}(\wp_i) \leq \mathrm{ht}(C(\wp_i))$ (la troisième inégalité provient du fait que $\wp_i$ est premier) $\leq \mathrm{ht}(\wp) = \mathrm{ht}(C(I))$. ■

Théorème 2.4.1 (Suslin Monic Polynominal Theorem) ([**10**], Chapter III, Theorem 3.3) *Soient A un anneau noethérien de dimension d ($d < \infty$) et I un idéal de l'anneau $A[X_1,...,X_n]$ avec $\mathrm{ht}(I) > d$. Alors, il existe des éléments algébriquement indépendants $Y_1,...,Y_n$ de $A[X_1,...,X_n]$ tels que $A[X_1,...,X_n] = A[Y_1,...,Y_n]$ et I contient un polynôme unitaire en tant qu'élément de $A[Y_2,...,Y_n][Y_1]$.*

Preuve On fait la preuve par induction sur le nombre n des variables indépendantes. Si $n = 0$, I est un idéal de A. Comme $\mathrm{ht}(I) > d$, alors $I = A$ et par suite I contient un élément inversible, ce qui montre le théorème dans ce cas. Supposons ensuite que $n \geq 1$ et soit $R = A[X_1,...,X_n]$. Posons $B = A[X_1,...,X_{n-1}]$, alors $R = B[X_n]$ et on peut regarder I comme un idéal de $B[X_n]$, alors par le lemme 2.4.4, on déduit que $\mathrm{ht}(C(I)) \geq \mathrm{ht}(I) > d$, d'où $\mathrm{ht}(C(I)) \geq d-1$ et $C(I) \subseteq A[X_1,...,X_{n-1}]$. L'hypothèse d'induction nous donne l'existence de $n-1$ éléments $Y_1,...,Y_{n-1}$ de $A[X_1,...,X_{n-1}]$ tels que $A[X_1,...,X_{n-1}] = A[Y_1,...,Y_{n-1}]$ et $C(I)$ contient un polynôme unitaire f (par rapport à Y_1). Posons $f = Y_1^t + f_{t-1}Y_1^{t-1} + ... + f_1Y_1 + f_0$ où $f_i \in A[Y_2,...,Y_{n-1}]$. Comme $f \in C(I)$, il existe alors $g \in I$ tel que f est le coefficient directeur de g. Soit alors $g = fX_n^s + g_{s-1}X_n^{s-1} + ... + g_1X_n + g_0$ où $g_i \in A[X_1, ..., X_{n-1}]$ et soit δ le plus haut degré de Y_1 qui figure dans g_{s-1},...,g_0. Posons $Y_n = X_n - Y_1^k$ pour un certain entier naturel k, alors dans l'expression $g_{s-1}X_n^{s-1} + ... + g_1X_n + g_0$, on a que Y_1 apparaît avec une puissance inférieure ou égale à $\delta + k(s-1)$ et $f.X_n^s$ est un polynôme unitaire en Y_1 de degré $ks + t$. Si on choisit k de sorte que $ks + t > \delta + k(s-1)$, alors g sera un polynôme unitaire de I en Y_1. Enfin, il est clair que $A[X_1, ..., X_n] = A[Y_1, ..., Y_n]$. ∎

Proposition 2.4.4 ([**10**], Chapter III, Lemma 3.4) *Si A est noethérien, $(a_1, ..., a_n)$ une ligne unimodulaire sur A^n, alors il existe une ligne unimodulaire $(a_1', ..., a_n')$ telle que $(a_1, ..., a_n) \sim_{E_n(A)} (a_1', ..., a_n')$ où pour tout $r \leq n$, on a* $\mathrm{ht}(< a_1', ..., a_r' >) \geq r$.

Preuve Supposons qu'on a construit a_1',...,a_r' (où $0 < r \leq n$) de telle manière que $(a_1, ..., a_n) \sim (a_1', ..., a_r', a_{r+1}, ..., a_n)$ et $\mathrm{ht}(< a_1', ..., a_r' >) \geq r$. Soit $\overline{A}$ l'anneau-quotient $A/ < a_1', ..., a_r' >$, alors $\overline{A}$ est noethérien et $(\overline{a_{r+1}}, ..., \overline{a_n})$ est une ligne unimodulaire de $\overline{A}^{n-r}$. Comme dans la preuve de la proposition 2.4.3, on peut trouver un élément $\overline{a_{r+1}'} = \overline{a_{r+1}} + \overline{b_{r+2}}.\overline{a_{r+2}}$ +...+ $\overline{b_n}.\overline{a_n}$ où $\overline{b_i} \in \overline{A}$ pour tout i et $\overline{a_{r+1}'} \notin \overline{\wp}$ pour tout idéal premier minimal $\overline{\wp}$ de $\overline{A}$. Soit $a_{r+1}' = a_{r+1} + b_{r+2}a_{r+2} + ... + b_na_n$, alors on a $(a_1, ..., a_n) \sim (a_1', ..., a_{r+1}', ..., a_n)$. D'autre part, soit $\wp$ un idéal premier minimal de A contenant l'idéal $< a_1', ..., a_r', a_{r+1}' >$. Comme l'idéal premier $\wp/ < a_1', ..., a_r' >$ ne peut pas être minimal dans $\overline{A}$ (car il contient $\overline{a_{r+1}'}$), il existe un idéal premier $\wp'$ de A tel que $< a_1', ..., a_r' > \subseteq \wp' \subset \wp$, d'où $\mathrm{ht}(\wp) > \mathrm{ht}(\wp') \geq \mathrm{ht}(< a_1', ..., a_r' >) \geq r$ et par suite $\mathrm{ht}(\wp) \geq r + 1$. Ceci montre que $\mathrm{ht}(< a_1', ..., a_{r+1}' >) \geq r + 1$, ce qui termine la preuve. ∎

Théorème 2.4.2 ([**10**], Chapter III, Theorem 3.5) *Si A est intègre et noethérien de dimension $d < \infty$ et si $R = A[X_1, ..., X_s]$ où X_1,...,X_s sont s variables indépendantes, alors si $n \geq d + 2$, toute ligne unimodulaire sur R^n admet la PEU .*

Preuve On fait une preuve par induction sur s. Si $s = 0$, le théorème se déduit dans ce cas de la proposition 2.4.3. Supposons ensuite que $s \geq 1$ et prenons une ligne unimodulaire $f = (f_1, ..., f_n)$ sur R^n avec $n \geq d + 2$. Par la proposition 2.4.4, il existe une ligne unimodulaire $f' = (f_1', ..., f_n')$ sur R^n telle que $f \sim f'$ et $\mathrm{ht}(< f_1', ..., f_r' >)$

$\geq r$ pour tout $r \leq n$. En particulier, $\mathrm{ht}(I) \geq n-1 > d$ où $I = < f_1', ..., f_{n-1}' >$.
Par le théorème 2.4.1, il existe des éléments Y_1,...,$Y_s \in R$ tels que $R = A[Y_1, ..., Y_s]$ et I contient un polynôme unitaire ϕ en Y_1. Soient g_1,...,$g_{n-1} \in R$ tels que $\phi = g_1 f_1' + g_2 f_2' + ... + g_{n-1} f_{n-1}'$ et soit t le plus haut degré de Y_1 qui figure dans l'expression de f_n', comme étant un élément de $A[Y_2, ..., Y_s][Y_1]$. Alors $f_n' + Y_1^{t+1}(f_1' g_1 + ... + f_{n-1}' g_{n-1})$ est unitaire comme étant un polynôme en Y_1 et on a que $(f_1', ..., f_n') \sim (f_1', ..., f_n' + Y_1^{t+1}.\phi)$, ce qui nous permet de supposer que f_n' est unitaire en Y_1.
Soit $B = A[Y_2, ..., Y_s]$. B est alors un anneau intègre et $(f_1', ..., f_n')$ est une ligne unimodulaire sur $B[Y_1]^n$. Le théorème 2.3.1 implique que

$$(f_1'(Y_1, ..., Y_s), ..., f_n'(Y_1, ..., Y_s)) \quad \sim \quad (f_1'(0, Y_2, ..., Y_s), ..., f_n'(0, Y_2, ..., Y_s)).$$

Puisque $h = (f_1'(0, Y_2, ..., Y_s), ..., f_n'(0, Y_2, ..., Y_s))$ est une ligne unimodulaire avec $n \geq d+2$ sur $A[Y_2, ..., Y_s]^n$, l'hypothèse d'induction montre que h (et par suite f) admet la PEU. ∎

On est maintenant capable de généraliser la solution de la conjecture de Serre à un anneau principal :

Théorème 2.4.3 *Si A est principal et X_1,...,X_s des variables indépendantes, alors tout $A[X_1, ..., X_s]$-module projectif de type fini est libre.*

Preuve Notons tout d'abord que toute ligne unimodulaire $f = (f_1, ..., f_n)$ sur B^n où $B = A[X_1, ..., X_s]$ admet la PEU. En effet, les cas $n = 1$, 2 sont vrais, même sans l'hypothèse que A est principal et le cas $n \geq 3$ est encore vrai par le théorème 2.4.2. Ceci montre que B possède la PEU.
D'autre part, si P est un B-module projectif de type fini, le théorème de Serre implique que P est stablement libre. Donc P est libre (théorème 2.3.3). ∎

Bibliographie

[1] Atiyah M and Macdonald I.G, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[2] H. Bass, *Big projective module are free*, Ill. J. Math. **7** (1963), 24-31.

[3] H. Bass, *Projective modules over free groups are free*, J. Algebra **13** (1964), 367-373.

[4] H. Bass, *Modules which support non-singular forms*, J. Algebra **13** (1969), 246-252.

[5] S. M. Bhatwadekar et A. Roy, *Some theorems about projective modules over polynomial rings*, J. Algebra **86**(1984), 150-158.

[6] S. M. Bhatwadekar, *A note on projective modules over polynominal rings*, Math. Z. **194** (1987), 285-291.

[7] I. J. Gubeladze, *On projective modules over seminormal rings generated by monominals*, Bulletin of the academy of sciences of the Georgian SSR **114**(1984), no **3**, 473-475.

[8] N. Jacobson, *Basic Algebra I*, second edition, Freeman, 1985.

[9] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhauser, Boston, 1985.

[10] T. Y. Lam, *Serre's conjecture*, Springer Lecture Notes in Mathematics **635** (1978).

[11] S. Lang, *Algebra*, third edition, Addison-Wesley, 1993.

[12] H. Lindel, *Unimodular elements in projective modules*, Journal of Algebra **172** (1995), 301-319.

[13] S. Mac Lane, G. Birkhoff, *Algebra*, Macmillan, 1967.

[14] M. -P. Malliavin, *Algèbre commutative, application en géométrie et théorie des nombres*, Masson, 1985.

[15] H. Matsumura, *Commutative algebra*, second edition, The Benjamin and Cummings publishing company, 1980.

[16] H. Matsumura, *Commutative ring theory*, Cambridge studies in Adv. Math. 8, Cambridge University Press, 1986.

[17] D. Quillen, *Projective modules over polynominal rings*, Invent. Math. **36** (1976), 167-171 .

[18] M. Roitman, *On Serre's problem on projective modules*, Proc. Amer. Math. Soc. **50** (1975), 245-52.

[19] L. H. Rowen, *Ring theory*, student edition, Academic press, Inc, 1991.

[20] J. P. Serre, *Faisceaux algébriques cohérents*, Ann. Math. **65** (1955), 191-278.

[21] J. P. Serre, *Modules projectifs et espaces fibrés à fibre vectorielle*, séminaire Dubreil-Pisot, no. **23**, 1957/58.

[22] C. S. Seshadri, *Triviality of vector bundles over the affine space* K^2, Proc. Nat'l. Acad. Sci. U. S. A **44** (1958), 456-458.

[23] A. Suslin, *Projective modules over polynominal ring are free*, Soviet Math. Dokl. **17** (1976), no. **4**, 1160-1164.

[24] R. Swan, *A cancellation theorem for projective modules in the metastable range*, Invent. Math. **27** (1974), 23-43.

[25] L. N. Vaserstein et A. A. Suslin, *The Serre problem on projective modules over polynominal rings and algebraic K-theory*, Functional Analysis and its Applications **8** (1974), 148-150.