Les modules projectifs sur les anneaux de polynômes

Mohammad Hadi Hedayatzadeh

15 juin 2004

École Polytechnique Fédérale de Lausanne

Dans cet article on va montrer que tout module projectif sur un anneau de polynômes à coefficients dans un anneau principal est libre. Avant cela, on doit définir quelques notions et montrer ou citer certains résultats d'algèbre commutative. On note que tous les anneaux dans ce traité sont commutatifs avec l'unité. On note encore que selon la simplicité on utilise les notations suivantes pour la localisé d'un A-module M, à l'ensemble multiplicatif $U \subset A$:

$$U^{-1}M \ , \ \ M[U^{-1}] \text{ et } M_U$$

et si $f \in A$ est un élément non-nul, on note par M_f la localisé de M à l'ensemble multiplicatif $\{f, f^2, f^3, \ldots\}$.

Définition 1. *Deux éléments f, g d'un anneau A sont dits* comaximaux *si l'idéal engendré par eux est l'anneau A ou de manière équivalente il existe $a, b \in A$ tels que $af + bg = 1$.*

Définition 2. *Soit $\mathcal{C}$ une catégorie et soient A, B, C trois objets de $\mathcal{C}$ un* pull-back *du diagramme*

$$\begin{tikzcd} & A \arrow[d, "f"] \\ B \arrow[r, "g"'] & C. \end{tikzcd}$$

est un objet D de $\mathcal{C}$ avec deux morphismes $\hat{g} : D \to A, \hat{f} : D \to B$ tels que le diagramme suivant commute

$$\begin{tikzcd} D \arrow[r, "\hat{g}"'] \arrow[d, "\hat{f}"] & A \arrow[d, "f"] \\ B \arrow[r, "g"'] & C. \end{tikzcd}$$

et tels qu'ils sont uniques à isomorphisme près c-à-d que pour tout objet D' de $\mathcal{C}$ et toute paire de morphismes $g' : D' \to A, f' : D' \to B$ qui ont la même propriété que $D, \hat{f}, \hat{g}$, il existe un unique morphisme $\theta : D' \to D$ tel que le diagramme suivant est commutatif :

$$\begin{tikzcd}
D' \arrow[dr, "\theta"] \arrow[drr, "g'"] \arrow[ddr, "f'"'] & & \\
& D \arrow[r, "\hat{g}"'] \arrow[d, "\hat{f}"] & A \arrow[d, "f"] \\
& B \arrow[r, "g"'] & C.
\end{tikzcd}$$

Remarque 3. Parfois par l'abus de notation on dit que le deuxième diagramme de la définition précédente est un pull-back.

Remarque 4. Il existe des catégories qui ne possèdent pas tous les pull-backs. Toutefois la catégorie des A-modules pour tout anneau A possède toutes les colimites et limites et en particulier tous les pull-backs. On donne une construction d'un pull-back dans la catégorie des A-modules. Supposons donc que l'on a un diagramme :

$$\begin{tikzcd}
& M \arrow[d, "f"] \\
N \arrow[r, "g"'] & P
\end{tikzcd}$$

où M, N, P sont des A-modules. On peut facilement verifier que le sous-A-module $Q := \{(m,n) \in M \oplus N | f(m) = g(n)\}$ de $M \oplus N$ avec $\overline{f} : Q \longrightarrow N$ et $\overline{g} : Q \longrightarrow M$ les projections naturelles, est un pull-back pour le diagramme donnée.

Soient M un A-module et f un élément de A, $M \longrightarrow M_f$ désigne l'application canonique qui envoie m sur $\frac{m}{1} \in M_f$.

Proposition 5. *Soit M un A-module, et soient f, g deux éléments comaximaux dans A. Alors le diagramme suivant est un pull-back dans la catégorie de A-modules :*

$$\begin{tikzcd}
M \arrow[r] \arrow[d] & M_g \arrow[d] \\
M_f \arrow[r] & M_{fg}
\end{tikzcd}$$

Preuve. On remarque d'abord que l'anneau A_{fg} est canoniquement isomorphe à $A_{f,g} \simeq (A_f)_g \simeq (A_g)_f$, de même le A_{fg}-module M_{fg} est canoniquement isomorphe à $(A_{f,g}$-module $M_{f,g} \simeq (M_f)_g \simeq (M_g)_f$. On remarque également que f^n, g^m sont aussi comaximaux pour tout $n, m \geq 0$, en effet f, g sont comaximal, implique qu'il existe $a, b \in A$ tels que $af + bg = 1$, alors $1 = (af+bg)^{n+m+1} = a'f^n + b'g^m$. On pose $S = \{f^n | n \geq 0\}$ et $T = \{g^n | n \geq\}$, et de ce que l'on vient de remarquer toute paire $(s, t) \in S \times T$ est comaximale. Soit maintenant N un A-module avec deux morphismes $\phi : N \longrightarrow M_g$ et $\psi : N \longrightarrow M_f$ tels que le diagramme suivant commute :

$$\begin{tikzcd} N \arrow[r, "\psi"] \arrow[d, "\phi"'] & M_g \arrow[d] \\ M_f \arrow[r] & M_{fg}. \end{tikzcd}$$

Soit n un élément de N alors $\psi(n) = \frac{m}{s} \in M_f = M_S$, $\phi(n) = \frac{n}{t} \in M_g = M_T$ pour certains $s \in S, t \in T, n, m \in M$, et on a $\phi(n) = \psi(n)$ dans M_{fg}. On peut supposer que $sn = tm$, en effet on a $(s't')(tm - sn) = 0$ pour certains $s' \in S, t' \in T$, alors $(tt')(s'm) = (ss')(t'n)$ et donc on peut remplacer $\frac{m}{s}$ par $\frac{s'm}{s's}$, et $\frac{n}{t}$ par $\frac{t'n}{t't}$. s, t sont comaximaux, on peut écrire $xs + yt = 1$ avec $x, y \in A$ et on pose $q = xm + yn$. Alors

$$sq = (xs)m + y(sn) = (xs)m + (yt)m = m$$

et de façon similaire, $tq = n$, on en tire alors que $q = \frac{m}{s} \in M_S$ et $q = \frac{n}{t} \in M_T$. Ce q est unique, car si $q = q'$ dans M_T et M_S alors il existe $s \in S, t \in T$ tels que $s(q - q') = 0$ et $t(q - q') = 0$, s, t sont comaximaux, il existe $a, b \in A$ avec $as + bt = 1$, alors

$$q - q' = 1.(q - q') = (as + bt)(q - q') = as(q - q') + bt(q - q') = 0 + 0 = 0.$$

On définit l'application $\theta : N \longrightarrow M$ qui associe à $n \in N$ $q \in M$ défini en haut. Il est facile à voir que cette application soit en fait un A-homomorphisme et qu'elle soi t unique. Donc M est bien le pull-back du diagramme. $\square$

Définition 6. *Soient A un anneau et M un A-module. On dit que M est un module plat si pout toute suite exacte courte*

$$0 \longrightarrow K \longrightarrow N \longrightarrow Q \longrightarrow 0$$

de A-module la suite

$$0 \longrightarrow K \otimes_A M \longrightarrow N \otimes_A M \longrightarrow Q \otimes_A M \longrightarrow 0$$

est courte.

Proposition 7. *Soient A un anneau et $U \subset A$ un ensemble multiplicatif. Alors le A-module $A[U^{-1}]$ est plat.*

Proposition 8 (Lemme de cinq). *Soient R un anneau et $A_i, B_i, C_i, D_i, F_i, i = 1, 2$ des R-modules. Supposons que l'on a un diagramme commutatif à lignes exactes :*

$$\begin{array}{ccccccccc}
A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\
\downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} & & \downarrow{\scriptstyle \phi_5} \\
A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & D_2 & \longrightarrow & E.
\end{array}$$

Si ϕ_i,$i = 1, 2, 4, 5$ sont des isomorphismes, alors ϕ_3 l'est aussi.

Proposition 9. *Soient A un anneau, et S un A-module plat. Soit encore $\{M_i\}_{i\in I}$ une famille de A-module. Alors il existe un isomorphisme canonique*

$$S \otimes_A (\oplus_{i\in I} M_i) \simeq \oplus_{i\in I}(S \otimes_A M_i).$$

Proposition 10. *Soient A un anneau et N un A-module et $\{M_i\}_{i\in I}$ une famille de A-module. Alors il existe un isomorphisme canonique*

$$Hom_A(\oplus_{i\in I} M_i, N) \simeq \prod_{i\in I} Hom_A(M_i, N).$$

En particulier si l'ensemble d'indices I est fini on a un isomorphisme canonique

$$Hom_A(\oplus_{i\in I} M_i, N) \simeq \oplus_{i\in I} Hom_A(M_i, N).$$

Proposition 11. *Le foncteur $Hom(-, N)$ est un foncteur contravariant exact à gauche.*

Proposition 12. *Soient A un anneau et B un A-algèbre. Si M et N sont des A-modules, alors il y a un unique homomorphisme de B-modules*

$$\alpha_M : B \otimes_A Hom_A(M, N) \longrightarrow Hom_B(B \otimes_A M, B \otimes_A N)$$

qui envoie l'élément $1 \otimes \phi \in B \otimes_A Hom_A(M, N)$ sur le B-homomorphisme $id \otimes_A \phi : B \otimes_A M \longrightarrow B \otimes_A N$ dans $Hom_B(B \otimes_A M, B \otimes_A N)$. Si B est plat sur A et M est de présentation finie, alors α_M est un isomorphisme. En particulier, si M est de présentation finie, alors $Hom_A(M, N)$ localise dans le sens que l'application α fournit un isomorphisme naturel

$$Hom_{A[U^{-1}]}(M[U^{-1}], N[U^{-1}]) \simeq Hom_A(M, N)[U^{-1}]$$

pour tout ensemble multiplicatif $U \subset A$.

Preuve. Par la Proposition 7 la dernière assertion est un cas particulier des premières.

Il est facile de voir que l'application ensembliste

$$\alpha' : Hom_A(M, N) \longrightarrow Hom_B(B \otimes_A M, B \otimes_A N)$$

qui envoie un homomorphisme ϕ sur l'homomorphisme $id \otimes \phi$ soit un homomorphisme de A-module. Puisque le but est un B-module, α' s'étend à un unique homomorphisme $\alpha = \alpha_M$ de B-modules avec la propriété voulue.

Supposons maintenant que B soit plat et M soit de présentation finie et montrons que α_M est un isomorphisme. Supposons d'abord que $M = A$. On peut identifier $Hom_A(A, N)$ avec N en envoyant un homomorphisme ϕ sur l'élément $\phi(1)$. On a également $B \otimes_A A = B$, et la même remarque montre que $Hom_B(B \otimes_A A, B \otimes_A N) = B \otimes_A N$. Il est facile de voir que l'application $\alpha_A : B \otimes_A N \longrightarrow B \otimes_A N$ après ces identifications soit l'identité.

On suppose ensuite que $M = \oplus_1^m A$ soit un module libre de rang fini. Un calcul direct montre que le diagramme suivant commute :

$$\begin{tikzcd}
B \otimes_A Hom_A(\oplus_1^m A, N) \arrow[r, "\alpha_{\oplus_1^m A}"] \arrow[d, "\simeq"'] & Hom_B(B \otimes_A \oplus_1^m A, B \otimes_A N) \arrow[d, "\simeq"] \\
\oplus_1^m B \otimes_A Hom_A(A, N) \arrow[r, "\oplus_1^m \alpha_A"'] & \oplus_1^m Hom_B(B \otimes_A A, B \otimes_A N)
\end{tikzcd}$$

où les isomorphismes verticals indiqués proviennent des Propositions 9,10.

Enfin, supposons que M soit de présentation finie et choisissons une présentation finie libre :

$$F \longrightarrow G \longrightarrow M \longrightarrow 0.$$

Puisque B est plat sur A, et F, G et par conséquent $B \otimes_A F, B \otimes_A G$ sont libres,en tensorisant cette présentation finie de M on trouve une présentation finie de B-modules pour $B \otimes_A M$.

Pour simplifier la notation, on note M' pour le B-module $B \otimes_A M$,de même pour les autres modules et applications. En appliquant le foncteur $Hom(-, N)$ sur la présentation finie de M et $Hom(-, N')$ sur celle de M' et en utilisant la Proposition 11, on obtient les suites exactes

$$0 \longrightarrow Hom_A(M, N) \longrightarrow Hom_A(G, N) \longrightarrow Hom_A(F, N)$$

et

$$0 \longrightarrow Hom_A(M', N') \longrightarrow Hom_A(G', N') \longrightarrow Hom_A(F', N').$$

Puisque B est plat sur A, on peut tensoriser la première suite par B et avoir encore une suite exacte

$$0 \longrightarrow Hom_A(M, N)' \longrightarrow Hom_A(G, N)' \longrightarrow Hom_A(F, N)'.$$

L'application que l'on a définie dans la proposition est, avec cette notation, une application $\alpha_M : Hom_A(M, N)' \longrightarrow Hom_B(M', N')$, on veut montrer que α_M est un isomorphisme. Par les arguments faits en haut, α_F et α_G sont des isomorphismes. Si on met tout ceci ensemble on trouve le diagramme commutatif suivant :

$$\begin{tikzcd}
0 \arrow[r] & Hom_A(M,N)' \arrow[r] \arrow[d, "\alpha_M"'] & Hom_A(G,N)' \arrow[r] \arrow[d, "\alpha_G"'] & Hom_A(F,N)' \arrow[d, "\alpha_F"'] \\
0 \arrow[r] & Hom_B(M',N') \arrow[r] & Hom_B(G',N') \arrow[r] & Hom_B(F',N').
\end{tikzcd}$$

Par le Lemme de cinq, on trouve que α_M est un isomorphisme. En effet on ajoute "$0 \longrightarrow$" à gauche aux deux lignes de ce diagramme pour avoir cinq termes en chaque lignes. $\square$

Proposition 13. *Soient M, N deux A-modules, f, g deux éléments comaximaux. Supposons que l'on a deux homomorphismes $\beta_f : M_f \longrightarrow N_f$, $\beta_g : M_g \longrightarrow N_g$ qui localisent en même homomorphisme $M_fg \longrightarrow N_fg$. Alors il existe un unique A-homomorphisme $\beta : M \longrightarrow N$ qui localisent en β_f et β_g. De plus β est un isomorphisme si et seulement si β_f et β_g sont des isomorphismes.*

Preuve. L'existence est une conséquence du fait que la construction de pull-back est fonctorielle et que M et N sont des pull-backs. On le peut constater dans le diagramme suivant :

$$\begin{tikzcd}
M \arrow[rr] \arrow[dd] \arrow[dr, dashed, "\beta"] & & M_g \arrow[dd] \arrow[dr, "\beta_g"] & \\
& N \arrow[rr] \arrow[dd] & & N_g \arrow[dd] \\
M_f \arrow[rr] \arrow[dr, "\beta_f"'] & & M_fg \arrow[dr] & \\
& N_f \arrow[rr] & & N_fg.
\end{tikzcd}$$

Le fait que β_f et β_g localisent en homomorphisme $M_fg \longrightarrow N_fg$ fait les carrés de ce diagramme commuter et puisque N est un pull-back implique l'existence et l'unicité de β. Le sens "seulement si" est trivial et pour montrer dans l'autre sens il faut juste utiliser la propriété universelle de pull-back. En effet s'il existe des inverses α_f pour β_f et α_g pour β_g par la première partie il existe un homomorphisme $\alpha : N \longrightarrow M$ qui localisent à α_f et α_g, on a alors le diagramme commutatif suivant :

$$\begin{tikzcd}
N \arrow[rr] \arrow[dr, dashed, "\theta"] \arrow[dd] & & N_g \arrow[dd] \arrow[dr, "\alpha_g \circ \beta_g = id"] & \\
& N \arrow[rr] \arrow[dd] & & N_g \arrow[dd] \\
N_f \arrow[rr] \arrow[dr, "\alpha_f \circ \beta_f = id"'] & & N_f g \arrow[dr] & \\
& N_f \arrow[rr] & & N_f g.
\end{tikzcd}$$

où θ peut être l'identité ou la composition $\alpha \circ \beta$, mais ce homomorphisme est unique, vue que N est un pull-back, donc $\alpha \circ \beta = id$. On montre de même manière que $\beta \circ \alpha = id$ et par conséquent β est un isomorphisme. □

Remarque 14. En fait dans la proposition précédente β est un monomorphisme (resp. epimorphisme) si et seulement si β_f et β_g sont des monomorphismes (resp. épimorphismes).

Proposition 15. *Soient f, g deux éléments comaximaux dans un anneau A. Soient Y un A_f-modules et Z un A_g-module tels que $Y_g \simeq Z_f$ comme A_{fg}-modules. Alors il existe à isomorphisme près un unique A-module X tel que $X_f \simeq Y$ et $X_g \simeq Z$. De plus on a les propriétés suivantes :*

1. *X est de type fini si et seulement si Y et Z sont de type fini.*
2. *X est de présentation finie si et seulement si Y et Z sont de présentation finie.*
3. *X est projectif si et seulement si Y et Z sont projectifs.*

Preuve. On identifie Y_g avec Z_f en utilisant l'isomorphisme donné, et on pose X le pull-back du diagramme suivant (dans la catégorie des A-modules) :

$$\begin{tikzcd}
X \arrow[r, dashed, "j"] \arrow[d, dashed, "i"'] & Z \arrow[d] \\
Y \arrow[r] & Y_g \simeq Z_f.
\end{tikzcd}$$

X possède une structure naturelle de A-module, et on va montrer que X est notre candidat unique. En fait on suppose que X soit le pull-back construit dans la Remarque 4. Soit $i' : X_f \longrightarrow Y$ le A_f-homomorphisme induit par $i : X \longrightarrow Y$. on prétend que i' est en fait un isomorphisme. Il est injectif : En effet si $i'(\frac{x}{f^n}) = \frac{i(x)}{f^n} = 0$ pour un $x \in X$, alors $i(x) = 0$ et en particulier $i(x)$ localise en zéro dans $Y_g \simeq Z_f$, et donc $j(x)$ aussi localise en zéro dans ce module. Il implique que $f^m j(x) = j(f^m x) = 0$ pour un $m \geq 0$. Puisque l'on a aussi $i(f^m x) = 0$, $f^m x$ doit être nul dans X, car X est le pull-back (défini dans la Remarque

4). Par conséquent $\frac{x}{f^n} = 0 \in X_f$. i' est surjectif : Soit $y \in Y$ donné, et soit $\frac{z}{f^r} \in Z_f$ qui correspond à $\frac{y}{1}$ sous l'isomorphisme $Y_g \simeq Z_f$. Alors $f^r y \in Y$ et $z \in Z$ localisent au même élément dans $Y_g \simeq Z_f$, il s'en suit qu'il existe un élément $x \in X$ avec $i(x) = f^r y$ et $j(x) = z$. Alors $i'(\frac{x}{f^r}) = y$.

On a donc montré que $X_f \simeq Y$ et par la symétrie $X_g \simeq Z$. Ceci démontre l'unicité à isomorphisme près de cette construction. En effet d'après la proposition précédente et les faits que les localisés d'un tel module global doivent être isomorphes à Y et Z tous les candidats sont isomorphes. Pour les trois propriétés, les implications "$\Rightarrow$" sont triviales, car toutes les propriétés citées sont invariantes par la localisation. On les prouve donc dans l'autre sens :

1. Supposons que Y et Z soient de type fini. Choisissons $x_1, \ldots, x_s \in X$ tels que $i(x_1), \ldots, i(x_s)$ forment un système de A_f-générateurs pour $Y \simeq X_f$, et $j(x_1), \ldots, j(x_s)$ forment un système de A_g-générateurs pour $Z \simeq X_g$. Soit X' le sous-A-module de X engendré par les $x_k, k = 1, \ldots, s$. Alors l'inclusion $X' \subseteq X$ induit des isomorphismes $X'_f \longrightarrow X_f$ et $X'_g \longrightarrow X_g$, on a donc par la proposition précédente $X = X'$ et donc X est également de type fini.
2. Supposons que Y et Z soient de présentation finie, ils sont donc en particulier de type fini et par le point précédent X est de type fini, alors il existe une surjection $F \longrightarrow X \longrightarrow 0$ avec F un A-module libre de rang fini. Soit K le noyau de cette surjection. En localisant en f on obtient

$$0 \longrightarrow K_f \longrightarrow F_f \longrightarrow X_f(\simeq Y) \longrightarrow 0.$$

Montrons que K_f est de type fini. En effet puisque $X_f \simeq Y$ est de présentation finie, il existe une présentation

$$A_f^n \longrightarrow A_f^m \longrightarrow X_f \longrightarrow 0.$$

Par la liberté de A^n, A^m on peut trouver des homomorphismes ϕ, ψ qui font commuter le diagramme suivant :

$$\begin{tikzcd} & A_f^n \arrow[r] \arrow[d, "\psi"'] & A_f^m \arrow[r] \arrow[d, "\phi"'] & X_f \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & K_f \arrow[r] & F_f \arrow[r] & X_f \arrow[r] & 0. \end{tikzcd}$$

Une chasse au diagramme facile, montre que $coker\psi = coker\phi$. Ce dernier étant un quotient de module libre et de rang fini F, on a que $coker\psi = K_f/im(\psi)$ est de type fini. $im(\psi)$ est aussi de type fini, et en conséquence le module K_f l'est aussi. De façon similaire K_g est aussi de type fini. Par le point (1), K est également de type fini. X est donc de présentation finie sur A.

3. Supposons que Y et Z soient projectifs. Pour voir que X est projectif, on montre que l'application induite $\varepsilon_* : Hom_A(X,M) \longrightarrow Hom_A(X,N)$ est surjective pour toute A-surjection $\varepsilon : M \twoheadrightarrow N$. La source et le but de cette application sont des A-modules, on peut donc utiliser la proposition précédente et la remarque qui la suit, et montrer seulement que $(\varepsilon_*)_f$ et $(\varepsilon_*)_g$ sont surjectifs. En localisant en f, on obtient

$$(\varepsilon_*)_f : (Hom_A(X,M))_f \longrightarrow (Hom_A(X,N))_f.$$

Puisque X est de présentation finie d'après le point (2), (en effet Y, Z projectifs implique qu'ils sont de présentations finie, et on utilise (2)), on peut identifier la source et le but de $(\varepsilon_*)_f$ avec $Hom_{A_f}(X_f, M_f)$ et $Hom_{A_f}(X_f, N_f)$, en appliquant la Proposition 12. Via ces identifications on voit que $(\varepsilon_*)_f$ est surjectif, parce que $X_f \simeq Y$ est projectif. De même on a $(\varepsilon_*)_g$ est surjectif, et la démonstration est terminée.

$\square$

Proposition 16. *Soient A un anneau $U \subset A$ un ensemble multiplicatif, et M, N deux A-modules de présentation finie. Soit encore $\phi : M[U^{-1}] \longrightarrow N[U^{-1}]$ un isomorphisme. Alors il existe un élément $f \in U$ et un isomorphisme $M_f \longrightarrow N_f$ qui localise à ϕ.*

Preuve. Soit $\psi : N[U^{-1}] \longrightarrow M[U^{-1}]$ l'inverse de ϕ. Par la Proposition 12 il existe $\theta : M \longrightarrow N$ et $g_1 \in U$ tels que $\phi = \frac{\theta_U}{g_1}$ et il existe $\gamma : N \longrightarrow M$ et $g_2 \in U$ tels que $\psi = \frac{\gamma_U}{g_2}$ où θ_U, γ_U sont les localisés de θ, γ. On pose $g = g_1 g_2$ et

$$\phi' := \frac{1}{g_1}\theta_g, \quad \psi' := \frac{1}{g_2}\gamma_g.$$

Alors $\psi'\phi' \in End_{A_g}(M_g)$ localise à l'identité dans $End_{A[U^{-1}]}(M[U^{-1}])$. Mais on sait que $(End_{A_g}(M_g))[U^{-1}] \simeq End_{A[U^{-1}]}(M[U^{-1}])$, donc $f_1(\psi'\phi' - 1) = 0$ pour un $f_1 \in U$. Par conséquent, $\psi'\phi' = id$ dans M_{gf_1}. De façon similaire, on obtient $f_2 \in U$ tel que $\phi'\psi' = id$ dans N_{gf_2}. Si on pose $f = gf_1f_2 \in U$, ϕ' définit un isomorphisme $M_f \longrightarrow N_f$ qui localise à ϕ. $\square$

Proposition 17. *Soient P un module projectif de type fini sur un anneau A, et $U \subset A$ un ensemble multiplicatif. Si $P[U^{-1}]$ est un $A[U^{-1}]$-module libre de rang r, alors il existe un $f \in U$ tel que P_f est un A_f-module libre de rang r.*

Preuve. Pour simplifier la notation on écrit P_U au lieu de $P[U^{-1}]$ et A_U au lieu de $A[U^{-1}]$, ainsi pour tous les modules qui interviennent . Supposons que le rang de P_U soit r, et que $\frac{p_1}{b_1}, \dots, \frac{p_r}{b_r}$ forment une base pour P_U, alors $\frac{p_1}{1}, \dots, \frac{p_r}{1}$ forment également une base pour P_U. Considérons l'application $F \longrightarrow P$ qui envoie $e_i \mapsto p_i, i = 1, \dots, r$ où $F := A^r$ et $\{e_1, \dots, e_r\}$ est la base canonique de $F = A^r$. Soient K, C le noyau et le conoyau de cette application (resp.). On a alors une suite exacte

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow C \longrightarrow 0$$

qui localise à

$$0 \longrightarrow K_U \longrightarrow F_U \longrightarrow P_U \longrightarrow C_U \longrightarrow 0.$$

Or P_U est libre de rang r, donc $C_U = 0 = K_U$. On montre maintenant qu'il existe $s \in U$ tel que $C_s = 0$, en effet puisque P est de type fini et P surjecte sur C, C est aussi de type fini avec disons $\{c_1, \ldots, c_l\}$ un système de générateurs. pour tout $i = 1, \ldots, l$ $\frac{c_i}{1} = 0 \in C_U$ donc il existe $s_i \in U$ tels que $s_i c_i = 0$. En posant $s := s_1 \ldots s_l$ on a que $C_s = 0$. Par conséquent on a la suite exacte courte suivante si l'on localise en s :

$$0 \longrightarrow K_s \longrightarrow F_s \longrightarrow P_s \longrightarrow 0.$$

P est projectif, et alors P_s l'est aussi et donc cette suite est scindée, i.e., $F_s \simeq K_s \oplus P_s$ et alors F_s surjecte sur K_s, donc K_s est de type fini et comme on l'a dit en haut $K_U = 0$. Un argument similaire pour C, montre qu'il existe $t \in U$ tel que $K_{st} = 0$, et si l'on pose $f := st$ on a $K_f = C_f = 0$ et l'exactitude de la suite $0 \longrightarrow K_f = 0 \longrightarrow F_f \longrightarrow P_f \longrightarrow C_f = 0 \longrightarrow 0$ montre qu'en fait $F_f \simeq P_f$ et donc P_f est libre de rang r. □

Définition 18. *Soit $A \longrightarrow B$ une extension des anneaux . Un B-module M est dit* étendu *de A (ou tout simplement un module étendu) si $M \simeq N \otimes_A B$ pour un A-module N. Dans la suite on s'interresse au cas où B est un anneau de polynôme sur A.*

Proposition 19. *Soit $R = A[x]$ un anneau de polynômes sur l'anneau noetherien A et soit M un R-module de type fini étendu de A, i.e., $M \simeq N \otimes_A R$ pour un A-module N. Alors $N \simeq M/xM$. En conséquence $M \simeq \overline{M} \otimes_A A[x]$ où $\overline{M} = M/xM$.*

Preuve. Puisque M est étendu, il existe un A-module N tel que $M \simeq N \otimes_A A[x]$. Alors $\overline{M} = M/xM \simeq M \otimes_R R/xR \simeq (N \otimes_A A[x]) \otimes_{A[x]} A[x]/(x) \simeq (N \otimes_A A[x]) \otimes_{A[x]} A \simeq N \otimes_A (A[x] \otimes_{A[x]} A) \simeq N \otimes_A A \simeq N$. □

Remarque 20. Avec les hypothèses de la proposition précédente si $\phi : M \longrightarrow N \otimes_A R$ est un isomorphisme, et si l'on note l'isomorphisme induit entre M/xM et N par $\overline{\phi}$ on obtient un isomorphisme $M \xrightarrow{\phi} N \otimes_A R \xrightarrow{(\overline{\phi})^{-1} \otimes id} M/xM \otimes_A R$ et si l'on tensorise les deux cotés par $R/xR = A[x]/(x)$ (c.à.d. le passage aux quotients) on trouve l'identité de M/xM.

Proposition 21 (Lemme de Quillen). *Soient A un anneau et R un A-algèbre (pas nécessairement commutative). Soient $f \in A$ et x un variable et θ une unité de $R_f[x]$ appartenant à l'ensemble $1 + xR_f[x]$. Alors il existe un entier $k \geq 0$ tel que pour tout $g_1, g_2 \in A$ avec $g_1 - g_2 \in f^k A$, il y a une unité $\psi \in R[x]$ appartenant à l'ensemble $1 + xR[x]$ telle que $\psi_f(x) = \theta(g_1 x)\theta(g_2 x)^{-1}$.*

En général on note par α_f, l'image de α sous l'application induite par la localisation $A \longrightarrow A_f$.

PREUVE. Soit $\theta(x) = \sum_{i=0}^{p} a_i x^i$ et $\theta(x)^{-1} = \sum_{i=0}^{p} b_i x^i$ avec $a_i, b_i \in R_f$ et $a_0 = b_0 = 1$. Soient r un entier non-négatif et y, z des variables. Alors par un calcul direct on obtient

$$\theta((y + f^r z)x)\theta(yx)^{-1} = 1 + [\theta((y + f^r z)x) - \theta(yx)]\theta(yx)^{-1}$$
$$= 1 + zx \sum_{i=1}^{p} \sum_{j=0}^{p} \sum_{n=0}^{i-1} f^r a_i b_j (y + f^r z)^{i-1-n} y^{n+j} x^{i-1+j}.$$

Si r est assez grand alors il existe des éléments $c_{ij} \in R$ tels que $(c_{ij})_f = f^r a_i b_j$. Par conséquent il y a $\phi \in 1 + zxR[y, z, x]$ tel que $\phi_f(y, z, x) = \theta((y + f^r z)x)\theta(yx)^{-1}$. En remplaçant y, z par $y + f^r z, -z$ on voit qu'il existe $\phi' \in 1 + zxR[y, z, x]$ tel que $\phi'(y, z, x) = \theta(yx)\theta((y + f^r z)x)^{-1}$. On a alors $(\phi\phi')_f = (\phi'\phi)_f = 1$ et donc si l'on écrit $\phi\phi' = 1 + zxh_1$ et $\phi'\phi = 1 + zxh_2$, il existe un entier non-négatif s tel que $f^s h_1 = f^s h_2 = 0$. Il s'en suit que $\phi(y, f^s z, x)$ est une unité. La proposition découle posant $k := r + s$ et $\psi(x) := \phi(g_2, f^s w, x)$ où $g_1 = g_2 + f^k w$. □

REMARQUE 22. Si M est un $A[x]$-module et $f : M \longrightarrow M$ est un homomorphisme qui réduit modulo x à l'identité de M/xM, alors $f = 1 + xh$ où $h : M \longrightarrow M$ est un homomorphisme. En effet la réduction de f est l'homomorphisme $f : M/xM \longrightarrow M/xM$ qui envoie $xM + t$ sur $xM + f(t)$, et dire que $\overline{f}$ est identité équivaut à dire que pour tout $t \in M, f(t) - t \in xM$, et donc $f(t) - t = xh(t)$.

THÉORÈME 23 (Quillen). *Soit M un $A[x]$-module de présentation finie. Si pour tout idéal maximal m de A, le $A_m[x]$-module M_m est étendu, alors M est également étendu.*

PREUVE. Soit S l'ensemble de f dans A tel que M_f est un $A_f[x]$-module étendu. On veut montrer que 1 appartient à S qui termine la preuve. Posons $N = M/xM$. Puisque M_m est un $A_m[x]$-module étendu par la Proposition 19 et la Remarque 20 on a un isomorphisme

$$A_m[x] \otimes_A N = A_m[x] \otimes_{A_m} A_m \otimes_A N = A_m[x] \otimes_{A_m} N_m \simeq M_m$$

qui réduit modulo x à l'isomorphisme canonique entre $A_m \otimes_A N$ et M_m/xM_m. M est de présentation finie, alors par la Proposition 16 il existe un élément $f \in A$ et un isomorphisme $A_f[x] \otimes_A N \simeq M_f$ qui réduit à l'isomorphisme canonique $A_f \otimes_A N \simeq M_f/xM_f$ et donc $f \in S$. On a donc montré que pour tout idéal maximal m de A il existe un élément $f \in S$. Ceci montre que S et par conséquent l'idéal engendré par lui, ne sont inclus dans aucun idéal maximal de A et alors idéal engendré par S est A tout entier. Or si l'on montre que cet idéal est S, i.e., S est un idéal on finit la démonstration. Pour ce faire il suffit de prouver que si $v = af_0 + bf_1$ avec $f_i \in S, i = 0, 1$, alors $v \in S$. En remplaçant A, M par A_v, M_v on peut supposer que $v = 1$.

Supposons que $u_i : A_{f_i}[x] \otimes_A N \simeq M_{f_i}, i = 0, 1$ soient deux isomorphismes réduisant modulo x aux isomorphismes canoniques $A_{f_i} \otimes_A N = M_{f_i}/xM_{f_i}$. Les localisés des u_i, i.e., $(u_1)_{f_0}$ et $(u_0)_{f_1}$ ont aussi la propriété qu'ils réduisent aux isomorphismes canoniques $A_{f_0 f_1}[x] \otimes_A N \simeq$

$M_{f_0f_1}/xM_{f_0f_1}$ en conséquence la composition $\theta := (u_0)_{f_1}^{-1}(u_1)_{f_0} : A_{f_0f_1}[x] \otimes_A N \longrightarrow A_{f_0f_1}[x] \otimes_A N$ réduit modulo x à l'identité de $A_{f_0f_1} \otimes_A N$, et alors par la Remarque 22 elle est de la forme $1+xh$ où $h : A_{f_0f_1}[x] \otimes_A N \longrightarrow A_{f_0f_1}[x] \otimes_A N$ est un $A_{f_0f_1}[x]$-homomorphisme.

M est de présentation finie et donc N l'est aussi. En effet si

$$F \longrightarrow G \xrightarrow{\gamma} M \longrightarrow 0$$

est une présentation finie de M, la suite exacte

$$F \longrightarrow G \xrightarrow{\pi\circ\gamma} N \longrightarrow 0$$

est une présentation finie de N où $\pi : M \longrightarrow N$ est la projection naturelle. En utilisant la Proposition 7 et en appliquant la Proposition 12 on trouve

$$Hom_{A_f[x]}(A_f[x] \otimes_A N, A_f[x] \otimes_A N) = A_f[x] \otimes_A Hom_A(N,N) = A_f[x] \otimes_A R = R_f[x]$$

où $R = End_A(N)$. Alors θ est une unité appartenant à l'ensemble $1+xR_{f_o f_1}[x]$. f_0, f_1 sont comaximaux et comme on a vu dans la preuve de la Proposition 5, pour tout entier $k \geq 0$, f_0^k, f_1^k le sont aussi, et on donc peut trouver un $g \in A$ tel que $g \in f_0^k A$ et $1 - g \in f_1 A^k$. Considérons maintenant la factorisation, avec $\theta(0x) = \theta(0) = 1$:

$$\theta(x) = [\theta(x)\theta(gx)^{-1}][\theta(0x)\theta(gx)^{-1}]^{-1}.$$

En appliquant la Proposition 21 à l'algèbre R_{f_0} sur A_{f_0} et l'élément f_1, on voit que le premier facteur est de la forme $(\psi_0)_{f_1}$ avec ψ_0 une unité dans l'ensemble $1 + xR_{f_0}[x]$, si k est choisi assez grand. De même, le deuxième facteur est de la forme $(\psi_1)_{f_0}^{-1}$ avec ψ_1 une unité dans l'ensemble $1 + xR_{f_1}[x]$. En remplaçant u_i par $u_i\psi_i$, on obtient $(u_0)_{f_1} = (u_1)_{f_0}$, et par la Proposition 13 ces deux isomorphismes nous fournissent un isomorphisme global $A[x] \otimes_A N \simeq M$, et la preuve est achevée. $\square$

Définition 24. *Soit A un anneau. On note l'ensemble des idéaux premiers de A par $Spec(A)$ et on l'appelle* le spectre de A. *Si I est un idéal de A on définit $V(I) := \{\mathfrak{p} \in Spec(A) | \mathfrak{p} \supseteq I\}$. On peut facilement vérifier les relations suivantes :*

1. *Si I, J sont deux idéaux de A, alors $V(I) \cup V(J) = V(IJ)$.*
2. *Si $\{I_i\}_{i\in T}$ est une famille d'idéaux de A, alors $\cap_{i\in T} V(I_i) = V(\sum_{i\in T} I_i)$.*

Donc si l'on définit les fermés de $Spec(A)$, l'ensemble $\{V(I) | I$ est un idéal de $A\}$, on obtient une topologie sur A qui s'appelle la topologie de Zariski. *On définit également pour un $f \in A$, l'ensemble $D(f) = Spec(A) \backslash V((f)) = \{\mathfrak{p} \in Spec(A) | f \notin \mathfrak{p}\}$, et on l'appelle un ouvert fondamental de $Spec(A)$. En fait on peut montrer que ces ouverts engendrent la topologie de Zariski de $Spec(A)$.*

Proposition 25 (Nakayama). *Soit A un anneau et soit $\Re$ l'intersection de tous les idéaux maximaux de A que l'on appelle le radical de A. Soient I est un idéal de A inclus dans $\Re$ et M un A-module de type fini tel que $IM = M$, alors $M = 0$. De plus si $x_1 + IM, \ldots, x_n + IM$ engendrent M/IM, alors $x_1, \ldots, x_n$ engendrent M.*

Proposition 26. *Soit P un module projectif sur l'anneau local A, avec l'idéal maximal $\mathfrak{m}$. Alors P est libre.*

Preuve. On remarque que le radical de A, $\mathfrak{R} = \mathfrak{m}$,et que $P/\mathfrak{m}P$ est un $A/\mathfrak{m}$-espace vectoriel de dimension finie, car P est de type fini. Alors il existe un $n \in \mathbb{N}$ tel que $P/\mathfrak{m}P \simeq (A/\mathfrak{m})^n$. Soit $\{\overline{e}_1, \dots, \overline{e}_n\}$ une $A/\mathfrak{m}$-base de $P/\mathfrak{m}P$ ($\overline{e}_i = \mathfrak{m}P + e_i$ pour $e_i \in P$). On considère l'application $\phi : A^n \longrightarrow P$ qui envoie la base canonique de A^n sur $\{e_1, \dots, e_n\}$ et on note son noyau et conoyau par K et C respectivement. On a donc une suite exacte :

$$0 \longrightarrow K \longrightarrow A^n \longrightarrow P \longrightarrow C \longrightarrow 0.$$

Si on tensorise cette suite par $A/\mathfrak{m}$ on trouve la suite exacte

$$0 \longrightarrow K/\mathfrak{m}K \longrightarrow (A/\mathfrak{m})^n \longrightarrow P/\mathfrak{m}P \longrightarrow C/\mathfrak{m}C \longrightarrow 0.$$

Mais $P/\mathfrak{m}P \simeq (A/\mathfrak{m})^n$, qui implique que $K/\mathfrak{m}K = 0 = C/\mathfrak{m}C$, donc $K = \mathfrak{m}K$ et $C = \mathfrak{m}C$. Puisque P est de type fini, C l'est aussi, et on tire par Nakayama que $C = 0$, donc on a la suite exacte courte $0 \longrightarrow K \longrightarrow A^n \longrightarrow P \longrightarrow 0$. P étant projectif, cette suite est scindée, i.e., $A^n \simeq K \oplus P$. Donc K est également de type fini et de nouveau par Nakayama, $K = \mathfrak{m}K$ implique $K = 0$. Par conséquent $A^n \simeq P$. $\square$

Un corollaire immédiat de cette proposition est la proposition suivante :

Proposition 27. *Tout module projectif est localement libre, i.e., si P est un module projectif sur l'anneau A et si $\mathfrak{p}$ est un idéal premier de A, alors le $A_\mathfrak{p}$-module $P_\mathfrak{p}$ est libre.*

Remarque 28. En fait l'inverse de cette proposition est aussi vraie, donc on a cette caractérisation des modules projectifs : Un module est projectif si et seulement s'il est localement libre.

Cette proposition nous permet de donner la définition suivante :

Définition 29. *Pour tout A-module projectif P on a une application $rang_P : Spec(A) \longrightarrow \mathbb{N}$, qui à chaque idéal premier $\mathfrak{p} \in Spec(A)$ associe le rang de $A_\mathfrak{p}$-module $P_\mathfrak{p}$. On dit qu'un A-module projectif est de rang n, si l'application $rang_P$ ne prend que la valeur n.*

Proposition 30. *L'application $rang_P$ définie ci-dessus est une application continue où $Spec(A)$ et $\mathbb{N}$ sont munis de la topologie de Zariski et la topologie discrète respectivement.*

Preuve. Soit $\mathfrak{p} \in Spec(A)$, et $n = \mathrm{rang}_P(\mathfrak{p})$, i.e., $P_\mathfrak{p} \simeq (A_\mathfrak{p})^n$. Alors par la Proposition 17, il existe $f \in A$ tel que $P_f \simeq (A_f)^n$, donc pour tout $\mathfrak{q} \in D(f)$ on a $P_\mathfrak{q} \simeq (A_\mathfrak{q})^n$, c.à.d. $\mathrm{rang}_P(D(f)) = n$, ce qui implique la continuité de rang_P. $\square$

Proposition 31. *Soit A un anneau. Alors il ne possède aucun élément idempotent non-trivial, i.e., différent de $0, 1$ si et seulement si $Spec(A)$ est un espace topologique connexe. En particulier, dans un tel cas l'application $rang_P$ est constante pour tout A-module projectif P.*

Preuve. Supposons d'abord que $Spec(A)$ est connexe, et $f \in A$ un élément idempotent, i.e., $f(f-1) = 0$. Donc tout idéal premier de A, contient $f(f-1)$. Il implique que $D(f) \cap D(f-1) = \emptyset$, mais on aussi que $D(f) \cup D(f) = Spec(A)$, car sinon il existe un idéal premier qui contient f et $f-1$, qui contradictoire. Puisque $D(f)$ et $D(f-1)$ sont des ouverts disjoints qui recouvrent tout l'espace on a soit $D(f) = Spec(A)$ soit $D(f-1) = Spec(A)$. Le premier cas implique que f est une unité et avec $f = f^2$ on a $f = 1$. L'autre cas implique pareillement que $f = 0$.

On suppose donc que A ne possède aucun élément idempotent non-trivial et on montre que $Spec(A)$ est connexe. Soit $Spec(A) = V(I) \cup V(J) = V(IJ)$ et $V(I) \cap V(J) = V(I+J) = \emptyset$ avec I, J des idéaux de A, il faut démontrer que soit $V(J) = Spec(A)$ soit $V(I) = Spec(A)$. La première relation implique que $IJ \subseteq \mathfrak{p}$ pour tout $\mathfrak{p} \in Spec(A)$ donc, $IJ \subseteq \cap_{\mathfrak{p} \in Spec(A)} \mathfrak{p}$ =l'idéal des éléments nilpotents. La deuxième relation implique que $I + J$ n'est inclus dans aucun idéal premier de A, il est donc égale à A. En conséquence il existe $f \in I$ et $g \in J$ tels que $f + g = 1$, on a aussi $fg \in IJ$ alors fg est nilpotent. Alors, $Spec(A) = D(f) \cup D(1-f)$ et $D(f) \cap D(1-f) = \emptyset$. De même, $D(f) \subseteq V(J)$ et $D(1-f) \subseteq V(I)$. En effet, si $\mathfrak{p} \in D(f)$, i.e., $f \notin \mathfrak{p}$ et si $\mathfrak{p} \notin V(J)$, alors $\mathfrak{p} \in V(I)$, i.e., $I \subseteq \mathfrak{p}$. Mais $f \in I$ et $f \notin \mathfrak{p}$, ce qui est une contradiction. L'autre inclusion est similaire.

Puisque $f(1-f)$ est nilpotent, il existe un $n \in \mathbb{N}$ tel que $f^n(1-f)^n = 0$. On peut écrire $0 = f^n(1-f)^n = f^n(1-fx)$ pour un certain $x \in A$. Donc $f^n = f^{n+1}x$, alors $f^n = f^n(fx) = (f^{n+1}x)(fx) = f^{n+2}x^2$. En itérant ce processus on obtient la relation $f^n = f^{n+k}x^k, k \in \mathbb{N}$. Or $f^n = f^{n+k}x^k$, implique $(fx)^n = f^n x^n = f^{n+k}x^{n+k} = (fx)^{n+k}$, en posant $k = n$ on a $(fx)^n = (fx)^{2n}$, donc $(fx)^n$ est un élément nilpotent, et par hypothèse on a soit $(fx)^n = 1$ soit $(fx)^n = 0$, dans le premier cas on voit que f est une unité et donc $D(f) = Spec(A)$. Mais $D(f) \subseteq V(J)$ donc $V(J) = Spec(A)$ et la démonstration est terminée. On suppose alors $(fx)^n = 0$. On sait que $f^n = f^{n+k}x^k$. En posant de nouveau $k = n$ on trouve $f^n = f^{2n}x^n = f^n(fx)^n = f^n 0 = 0$. Donc $D(f) = \emptyset$ ce qui implique $D(1-f) = Spec(A)$, et comme ci-dessus puisque $D(1-f) \subseteq V(I)$, on a $V(I) = Spec(A)$, et la démonstration est achevée. □

Définition 32. *Un anneau A est dit* semi-local *s'il ne possède qu'un nombre fini d'idéaux maximaux.*

Proposition 33. *Soit A un anneau noetherien tel que tout élément non-diviseur de zéro est inversible, alors A est semi-local.*

PROPOSITION 34. *Soient A un anneau semi-local, et M, N deux A-modules de présentation finie. Si pour tout idéal maximal $\mathfrak{m}$ de A on a $M_\mathfrak{m} \simeq N_\mathfrak{m}$, alors $M \simeq N$.*

PROPOSITION 35. *Si P et Q sont deux sous-modules de M, alors $P = Q$ si et seulement si $P_\mathfrak{m} = Q_\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A.*

PREUVE. On a $(P + Q/Q)_\mathfrak{m} \simeq P_\mathfrak{m} + Q_\mathfrak{m}/Q_\mathfrak{m}$ et $(P + Q/P)_\mathfrak{m} \simeq P_\mathfrak{m} + Q_\mathfrak{m}/P_\mathfrak{m}$. Si $P_\mathfrak{m} = Q_\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$, alors $(P + Q/Q)_\mathfrak{m} = 0 = (P + Q/P)_\mathfrak{m}$. Par conséquent $P + Q/P = P + Q/Q = 0$, ce qui implique que $P = Q$. □

PROPOSITION 36. *Soient A un anneau noetherien et P un A-module projectif de rang 1. Alors P est isomorphe à un idéal projectif de A.*

PREUVE. Soit S l'ensemble des éléments non-diviseurs de zéro dans A. Alors tout élément non-diviseur de zéro dans $A[S^{-1}]$ est inversible et donc par la Proposition 33, il est semi-local. Puisque P est de rang constant 1, on a que $P[S^{-1}]_\mathfrak{m} \simeq A[S^{-1}]_\mathfrak{m}$ pour tout idéal maximal, $\mathfrak{m}$ de A. Donc par la Proposition 34, $P[S^{-1}] \simeq A[S^{-1}]$. On a donc, par la Proposition 17 $P_s \simeq A_s$, pour un $s \in S$. Soit $\phi : P_s \longrightarrow A_s$ un isomorphisme, et soit $\{p_1, \ldots, _k\}$ un système de générateurs de P sur A. On peut supposer que $\phi(\frac{p_i}{1}) = \frac{x_i}{s^l}$ pour tout $i \in \{i, \ldots, k\}$. Alors pour tout $p \in P$ on a $\phi(\frac{p}{1}) = \frac{r}{s^l}$ pour un ceratin $r \in A$. On définit alors une application $f : P \longrightarrow A$ qui envoie p à r. Cette application est bien définie et puisque P_s est libre elle est également injective , on a donc une A-monomorphisme. Par conséquent $P \simeq f(P)$ qui est bien un idéal projectif de A de rang 1. □

PROPOSITION 37. *Soit A un anneau noetherien et local avec l'idéal maximal $\mathfrak{m}$. Soit I un idéal de $R = A[x]$. Si I possède un polynôme unitaire, alors tout élément non-nul $\overline{f}$ dans $(I + \mathfrak{m}R)/\mathfrak{m}R$ est l'image d'un polynôme unitaire de I.*

PREUVE. Soit $k = A/\mathfrak{m}$ et soit $\overline{f}$ un élément non-nul dans $(I+\mathfrak{m}R)/\mathfrak{m}R$. Alors il y a un élément g_1 dans I tel que $\overline{g_1} = \overline{f}$. ("-" veut dire l'image dans $R/\mathfrak{m}R \simeq k[x]$). Soit $r = deg(f)$, puisque f est unitaire on a que $deg(g_1) = n \geq r$. Soit $g_1(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ avec $a_i \in A$. Si $n = r$, alors g_1 est unitaire et la preuve est terminée. En effet puisque $g_1 - f \in \mathfrak{m}R$, on a que $a_r - u \in \mathfrak{m}$ où u est le coefficient du terme x^r dans f. Alors $a_r \notin \mathfrak{m}$, car $u \notin \mathfrak{m}$. Donc a_r est une unité (A est local). On suppose donc que $n > r$. Alors $a_n \in \mathfrak{m}$.

On prétend que I contient un polynôme unitaire de degré $r+1$. En effet, I contient un polynôme unitaire, disons $F'(x)$, si $deg(F') \leq r+1$, en multipliant F' par $x^{r+1-deg(F')}$ on obtient le polynôme cherché. On suppose donc que $deg(F') = d > r+1$. On peut supposer que le coefficient de x^{r+1} est 1. $deg(x^{d-1-r}f(x)) = d-1$ et on a $\overline{x^{d-1-r}g_1(x)} = \overline{x^{d-1-r}f(x)}$. On pose $m = d+n-r-1$ et soit $g_2(x) = x^{d-1-r}g_1(x) - a_n x^{m-d}F'(x)$. Alors $deg(g_2) \leq m-1$ et $g_2 \in I$ et $\overline{g_2} = \overline{x^{d-1-r}}f(x)$ qui est de degré $d-1$. Clairement $deg(g_2) \geq d-1$, et si $deg(g_2) > d-1$ on pose $g_3(x) = g_2(x) - bx^{deg(g_2)-d}F'(x)$, où b est le coefficient du terme de plus grand degré dans g_2, on a de nouveau $\overline{g_3} = \overline{x^{d-1-r}}f$ et $g_3 \in I$ et $d - 1 < deg(g_3) < deg(g_2)$. En répétant ce processus, on obtient un élément g' de I de degré $d-1$ avec $\overline{g'} = \overline{x^{d-1-r}f}$. On sait que $\overline{x^{d-1-r}f}$ est de degré $d-1$, on en déduit que g' est unitaire.

On a alors trouvé un élément unitaire g' de I de degré $d-1$. En répétant cet argument on peut trouver un élément F de I unitaire et de degré $r+1$. De nouveau on peut supposer que le coefficient du terme à plus grand degré est 1. Maintenant $G'(x) = g_1(x) - a_n x^{n-r-1}F(x)$ est de degré $n-1$ et $\overline{G'} = \overline{g_1} = \overline{f}$. Encore une fois, en répétant ce processus, on obtient un polynôme G dans I de degré r tel que $\overline{G} = \overline{f}$. Donc G est aussi unitaire. Ceci termine la démonstration. □

Proposition 38. *Soit A un anneau noetherien. Soit I un idéal projectif de A de rang 1 et soit J un idéal de A contenu dans I. Alors il existe un idéal L de A tel que $LI = J$.*

Preuve. Posons $L := \{f \in A | fI \subseteq J\}$. Vérifions que pour tout idéal maximal $\mathfrak{m}$ de A, on a $(LI)_\mathfrak{m} = J_\mathfrak{m}$. On note que par la définition de L, LI est inclus dans J. Si LI n'est pas inclus dans $\mathfrak{m}$, J n'est pas inclus dans $\mathfrak{m}$ non plus et donc $(LI)_\mathfrak{m} = A_\mathfrak{m} = J_\mathfrak{m}$.

On suppose donc que LI est inclus dans $\mathfrak{m}$. Alors, soit L soit I est inclus dans $\mathfrak{m}$. Puisque J est contenu dans L, dans les deux cas on a $J \subseteq \mathfrak{m}$. Or $L_\mathfrak{m} = \{f \in A_\mathfrak{m} | fI_{\mathfrak{m}\mathfrak{m}}\}$. Si I n'est pas contenu dans $\mathfrak{m}$, alors $J_\mathfrak{m} \subseteq L_\mathfrak{m} = L_\mathfrak{m} I_\mathfrak{m} \subseteq (LI)_\mathfrak{m}$, donc $(LI)_\mathfrak{m} = J_\mathfrak{m}$. Si I est contenu dans $\mathfrak{m}$, alors puisque I est projectif de rang 1, $I_\mathfrak{m} = gA_\mathfrak{m}$, pour un élément non diviseur de zéro g de $A_\mathfrak{m}$ et $L_\mathfrak{m} = \{f \in A_\mathfrak{m} | fg \in J_\mathfrak{m}\}$. En conséquence $J_\mathfrak{m} \supseteq (LI)_\mathfrak{m} = L_\mathfrak{m}(gA_\mathfrak{m})$, mais puisque $J_\mathfrak{m} \subseteq I_\mathfrak{m}$, tout élément de $J_\mathfrak{m}$ s'écrit comme fg pour un $f \in A_\mathfrak{m}$, donc $J_\mathfrak{m} \subseteq L_\mathfrak{m}(gA_\mathfrak{m})$. Il s'en suit que $(LI)_\mathfrak{m} = J_\mathfrak{m}$. Alors par la Proposition 35 on termine la preuve. □

Proposition 39. *Soit A un anneau et soit $\Re$ le radical de A, i.e., $\Re$ est l'intersection de tous les idéaux maximaux de A. Alors pour tout $xinA$ on a, $x \in \Re$ si et seulement si $1 - xy$ est inversible pour tout $y \in A$.*

Preuve. "$\Rightarrow$" : Soit $x \in \Re$ et soit $y \in A$ un élément quelconque. L'élément $1 - xy$ n'appartient à aucun idéal maximal et donc il est inversible. En effet, si $1 - xy \in \mathfrak{m}$, on aura $1 = (1 - xy) + xy \in \mathfrak{m}$, car $x \in \Re \subseteq \mathfrak{m}$, qui est une contraction.

"$\Rightarrow$" : Si l'on que $1 - xy$ est inversible pour tout $y \in A$, et si $\mathfrak{m}$ est un idéal maximal, alors $x \in \mathfrak{m}$. Sinon, l'élément $x + \mathfrak{m} \in A/\mathfrak{m}$ est non-nul et puisque $\mathfrak{m}$ est maximal, $A/\mathfrak{m}$ est un corps, donc il existe une inverse pour $x + \mathfrak{m}$, disons $y + \mathfrak{m}$, on a donc $1 + \mathfrak{m} = (x + \mathfrak{m})(y + \mathfrak{m}) = xy + \mathfrak{m}$, alors $1 - xy \in \mathfrak{m}$, mais ceci est en contradiction avec le fait que $1 - xy$ est inversible. En conséquence $x \in \Re$. □

Proposition 40. *Soit A un anneau, et soit $R = A[x]$ un anneau de polynômes sur A. Soit $T = 1 + \mathfrak{m}R$ l'ensemble des éléments de la forme $1 + y$ avec $y \in \mathfrak{m}R$. Soit encore $f \in R$*

un polynôme unitaire. Alors pour tout idéal maximal M de R, on a soit $M \cap T = \emptyset$, soit $f \notin M$.

Preuve. Si $f \in M$ et $T \cap M \neq \emptyset$, il existe $g \cap M$. On écrit $f = a_n x^n + \cdots + a_0$ avec a_n inversible et on peut supposer $a_n = 1$, on écrit aussi $g = (1 + b_0) + b_1 x + \cdots + b_m x^m$ avec $b_i \in \mathfrak{m}R$. Puisque $b_0 \in \mathfrak{m}$, $1 + b_0 \notin \mathfrak{m}$, donc il est inversible et on peut ainsi supposer que $1 + b_0 = 1$. Donc on est arrivé à la situation où $f, g \in M$, avec $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ et $g = b_m x^m + \cdots + b_1 x + 1$, avec $b_i \in \mathfrak{m}$. Si $m \geq n$ on pose $g' := g - b_m f$, clairement on a $g' = b'_{m'} x^{m'} + \cdots + b'_0 + 1$, avec $b'_i \in \mathfrak{m}$, et $m' < n$, et si l'on fait les modifications que l'on faites sur g on arrive à la situation ci-dessus, et alors on peut supposer $m < n$. On a $f - a_0 g = xh(x)$ pour un polynôme $h \in R$ dont le coefficient du terme à plus grand degré est 1, et puisque $f - a_0 g \in M$ on a soit $x \in M$ soit $h \in M$. Si $x \notin M$ on est dans le deuxième cas, et on constate que degré$(h) = n - 1$, donc en faisant successivement les arguments ci-dessus, et en sachant que $x \notin M$ on trouve des polynômes $f', g' \in M$ où $f' = x + a_0$ et $g' = 1$ qui est une contradiction, par conséquent $x \in M$, mais $1 = 1 + b_1 x + \cdots + b_m x^m - x(b_1 + b_2 x + \cdots + b_m x^{m-1}) = g - x(b_1 + b_2 x + \cdots + b_m x^{m-1}) \in M$, qui est de nouveau une contradiction. □

Proposition 41. *Soit $R = A[x]$ un anneau de polynômes sur un anneau local et noetherien A, et soit I un idéal projectif de R de rang 1 qui contient un polynôme unitaire. Alors I est un idéal principal.*

Preuve. Soit $J = I + \mathfrak{m}R$ et soit $J/\mathfrak{m}R = fk[x]$, pour un polynôme $f \in k[x]$, où $k = A/\mathfrak{m}$ (f existe, car $k[x]$ est principal). Par la Proposition 37, il existe un polynôme $F[x] \in I$ tel que $\overline{F} = f$ (ici "-" veut dire l'image dans $k[x]$). Il s'en suit donc que $J = FR + \mathfrak{m}R$. Par la Proposition 38 $I \cap \mathfrak{m}R = IL$ pour un idéal L de R. Puisque $IL \subseteq \mathfrak{m}R$ et puisque I n'est pas inclus dans $\mathfrak{m}R$, on a $L \subseteq \mathfrak{m}R$. En effet on prétend que $\mathfrak{m}R$ est un idéal premier : Si $p(x)q(x) \in \mathfrak{m}R$, avec $p(x) = \sum_{i=1}^{m} a_i x^i$ et $q(x) = \sum_{j=1}^{n} b_j x^j$, on montre que soit $p \in \mathfrak{m}R$ soit $q \in \mathfrak{m}R$. On suppose par l'absurde que $p, q \notin \mathfrak{m}R$. Soit $t \in \{1, \ldots, m\}$ et $s \in \{1, \ldots, n\}$ les plus petits indices tels que $a_t, b_s \notin \mathfrak{m}$. Le coefficient du terme de degré $t + s$ dans le polynôme pq est $\sum_{i+j=t+s} a_i b_j = a_t b_s + \sum_{i+j=t+s, i<t} a_i b_j + \sum_{i+j=t+s, j<s} a_i b_j$. Ce coefficient est dans $\mathfrak{m}$, car $pq \in \mathfrak{m}R$. Les deux sommes ci-dessus sont aussi dans $\mathfrak{m}$, car $a_i \in \mathfrak{m}$ quand $i < t$ et $b_j \in \mathfrak{m}$ quand $j < s$. Alors $a_t b_s \in \mathfrak{m}$, mais on avait supposé que $a_t, b_s \notin \mathfrak{m}$. Donc on a bien $L \subseteq \mathfrak{m}R$,et alors $IL \subseteq I\mathfrak{m}R = \mathfrak{m}I$. Par conséquent $I \cap \mathfrak{m}R = IL \subseteq \mathfrak{m}I \subseteq I \cap \mathfrak{m}R$, donc $I \cap \mathfrak{m}R = \mathfrak{m}I$.

On a $I + \mathfrak{m}R = J = FR + \mathfrak{m}R$. Alors, $I = FR + I \cap \mathfrak{m}R = FR + \mathfrak{m}I$, où F es un polynôme unitaire. Or $M := I/FR$ est un R/FR-module de type fini et $M = (\mathfrak{m} + FR/FR)M$. Tout idéal maximal de R/FR est de la forme N/FR avec N un idéal maximal de R, qui contient évidemment FR. Soit m un élément de $\mathfrak{m}$ et y un élément de R. Avec la notation de la Proposition 40, $1 - xy \in T$, et puisque N contient un polynôme unitaire par la Proposition 40, $N \cap T = \emptyset$, donc $1 - xy \notin N$ ou de manière équivalente $(1 - xy) + FR \notin N/FR$. On en déduit que pour tout élément y de R, $(1 - xy) + FR$ n'est dans aucun idéal maximal de R/FR, alors il est inversible et par la Proposition 39, $x + FR$ est dans le radical de R/FR. Par conséquent $\mathfrak{m} + FR/FR$ est contenu dans le radial de R/FR. Par Nakayama on en tire que $M = 0$. Donc $I = FR$, et I est principal. $\square$

Proposition 42. *Soit A un anneau principal et soit L un A-module libre de rang r. Soit p un élément non-nul de L. Alors L possède une base $p_1, \ldots, p_r$, telle que $p = ap_1$ pour un $a \in A$.*

Preuve. Soient $q_1, \ldots, q_r$ une base de L et $p = a_1q_1 + \cdots + a_rq_r$, avec $a_i \in A$. Sans perte de généralité, on peut supposer que $a_1 \neq 0$. Puisque A est principal l'idéal engendré par $a_1, \ldots, a_r$ est principal, disons $(a_1, \ldots, a_r) = (a)$. Alors $a_i = ab_i$ pour certains $b_i \in A$. Donc, si $a = c_1a_1 + \cdots + c_ra_r$, alors $c_1b_1 + \cdots + c_rb_r = 1$, car A est intègre. Posons $p_1 = b_1q_1 + \cdots + b_rq_r$. On définit un A-homomorphisme $\phi : L \longrightarrow Ap_1$ qui envoie q_i sur c_ip_1, pour $i \in \{1, \ldots, r\}$. Alors $\phi(p_1) = p_1$, donc ϕ est surjectif, et puisque Ap_1 est un sous-module d'un module libre sur un anneau principal, Ap_1 est aussi libre donc la suite exacte courte suivante est scindée :

$$0 \longrightarrow Ker\phi \longrightarrow L \longrightarrow Ap_1 \longrightarrow 0$$

et donc $L = Ker\phi \oplus Rp_1$.

De nouveau, puisque $Ker\phi$ est un sous-module de L, il est libre. Soit $p_2, \ldots, p_r$ une base pour $Ker\phi$. Alors $p_1, \ldots, p_r$ est une base pour L et $ap_1 = p$. $\square$

Théorème 43 (Horrocks). *Soit A un anneau local noetherien , avec idéal maximal $\mathfrak{m}$. Soit $R = A[x]$ l'anneau de polynômes sur A. Supposons que P soit un R-module projectif de type fini tel que P_f est libre pour un polynôme unitaire $f \in R$. Alors P est libre.*

Preuve. Puisque A est local il ne possède aucun élément idempotent non-trivial, i.e., différent de 0 et 1. En effet si $x^2 = x$ avec $x \in A$, on a $x(x-1) = 0 \in \mathfrak{m}$, donc soit $x \in \mathfrak{m}$ soit $x - 1 \in \mathfrak{m}$. Si $x \in \mathfrak{m}$, alors $x - 1 \notin \mathfrak{m}$, $x - 1$ est donc inversible. Il existe alors $u \in A$ tel que $u(x-1) = 1$. On a

$$0 = ux - ux = ux^2 - ux = xu(x-1) = x.1 = x.$$

Dans le deuxième cas, on obtient pareillement $x - 1 = 0$, donc $x = 1$. Il implique R ne possède aucun élément idempotent non-trivial non plus. En effet si $g(x) \in R$ est idempotent alors $g^2 = g$. Si degré$(g) = l$, alors degré$(g^2) = 2l$, donc $2l = l$, ce qui implique que $l = 0$, alors g est une constante dans A, mais l'on a montré que A ne possède pas d'élément idempotent autre que $0, 1$. Par conséquent $g \in \{0, 1\}$. Alors par la Proposition 31, P est de rang constant, disons n. On prouve le résultat par récurrence sur n.

Si $n = 1$, alors par la Proposition 36, P est isomorphe à un idéal projectif I de R de rang 1. Puisque $P_f \simeq R_f$, on peut supposer $I_f = R_f$. Donc I contient un puissance de f qui est un polynôme unitaire f'. Par la Proposition 41, I est principal, disons $I = (g)$. On veut montrer que I est libre. En effet on a $f' \in I = (g)$, il existe donc $h \in R$ tel que $f' = hg$. Si $r(x)g(x) = 0$ pour un $r \in R$ non-nul, on aura $rf' = 0$. On écrit $r(x) = r_m x^m + \cdots + r_0$ avec $r_m \neq=$. On écrit aussi $f' = u_k x^k + \cdots + u_0$, avec u_k unité. On a $0 = rf' = r_m u_k x^{m+k} + r'_{m+k-1} x^{m+k-1} + \cdots + r'_0$, alors $u_k r_m = 0$, et puisque u_k est inversible on a $r_m = 0$, qui une contradiction. Donc g est une base pour I, il est alors libre, et par conséquent P l'est aussi.

Maintenant on suppose $n \geq 2$. Soit $\frac{p_1}{1}, \ldots, \frac{p_n}{1}$ une base pour P_f avec $p_i \in P$. Notons par "-" l'image modulo $\mathfrak{m}R$. Il existe un $i \in \{1, \ldots, n\}$ tel que $p_i \notin \mathfrak{m}P$, car si tous les p_i sont dans $\mathfrak{m}P$, on aura $\mathfrak{m}P_f = P_f$, donc tout élément de P_f s'écrit comme une combinaison linéaire des p_i avec des coefficients dans $\mathfrak{m}R_f$. En particulier $p_1 = (\sum_{i=1}^{n} \frac{r_i}{f^{k_i}} p_i)$ avec $r_i \in \mathfrak{m}$, et puisque les p_i forment une base on a $\frac{r_1}{f^{k_1}} = 1$ dans R_f, c'est à dire $f^{k_1} \in \mathfrak{m}R$. Mais comme l'on a déjà vu, $\mathfrak{m}R$ est un idéal premier de R, on a alors $f \in \mathfrak{m}R$, mais f est unitaire qui est en contradiction avec le fait que $\mathfrak{m} \neq A$. On peut donc supposer que $p_1 \notin \mathfrak{m}P$, et par conséquent $\overline{p_1} \neq 0$. Par la Proposition 42, on peut trouver $q_1, \ldots, q_n \in P$ tels que $\overline{q_1}, \ldots, \overline{q_n}$ soit une base pour $P/\mathfrak{m}P$ et $\overline{p_1} = a\overline{q_2}$ pour un certain $a \in (A/\mathfrak{m})[x]$.

Or $f^k q_i = a_r p_1 + \cdots + a_n p_n$ pour un $k \geq 1$ et $a_1, \ldots, a_n \in R$. Soit $p = q_1 + x^t p_1$ pour un $t \geq 0$, tel que $f_1 := a_1 + f^k x^t$ soit un polynôme unitaire. Donc

$$f^k p = f^k q_1 + f^k x^t p_1 = (a_1 + f^k x^t) p_1 + a_2 p_2 + \cdots + a_n p_n.$$

Soit $T = 1 + \mathfrak{m}R$ l'ensemble multiplicatif défini dans la Proposition 40. Puisque $\overline{p} = \overline{q_1} + x^t \overline{p_1} = \overline{q_1} + x^t a \overline{q_2}$, on voit que $\overline{p}, \overline{q_2}, \ldots, \overline{q_n}$ engendrent $P/\mathfrak{m}P$, ils engendrent donc $(P/\mathfrak{m}P)_T = P_T/\mathfrak{m}P_T$. $R_T/\mathfrak{m}R_T \simeq (R/\mathfrak{m}R)_T \simeq (A/\mathfrak{m})[x]_T$ et puisque $\mathfrak{m}$ est un idéal maximal $A/\mathfrak{m}$ est un corps, donc $(A/\mathfrak{m})[x]$ et en conséquence $(A/\mathfrak{m})[x]_T$ sont des anneaux principaux. Alors tout $R_T/\mathfrak{m}R_T$-module projectif et en particulier $P_T/\mathfrak{m}P_T$ sont libre et donc $\overline{p}, \overline{q_2}, \ldots, \overline{q_n}$ en est une base. Tout idéal maximal de R_T est de la forme M_T avec M un idéal maximal de R dont l'intersection avec T est vide, donc pour tout $x \in \mathfrak{m}$ et tout $y \in R_T$, $1 - xy \notin M_T$, donc $1 - xy$ est inversible dans R_T, et par la Proposition 39, on voit que x est dans l'intersection des idéaux maximaux de R_T. On en tire alors que $\mathfrak{m}$ est contenu dans cette intersection. On peut donc appliquer Nakayama, et il implique que $p, q_2, \ldots, q_n$ engendrent P_T. On considère l'application $\phi : (R_T)^n \longrightarrow P_T$ qui envoie la base canonique vers ce système de générateurs que l'on vient d'exhiber. Elle est surjective. Soit K son noyau, on a alors une suite exacte courte de R_T-modules :

$$0 \longrightarrow K \longrightarrow (R_T)^n \longrightarrow P_T \longrightarrow 0.$$

Puisque P est projectif, P_T l'est aussi et donc K est de type fini (on a en fait $(R_T)^n \simeq K \oplus P_T$, car P_T projectif implique que la suite est scindée). En tensorisant cette suite exacte par $R_T/\mathfrak{m}R_T$ on obtient la suite exacte courte suivante :

$$0 \longrightarrow K/\mathfrak{m}K \longrightarrow (R_T/\mathfrak{m}R_T)^n \longrightarrow P_T/\mathfrak{m}P_T \longrightarrow 0.$$

Mais, l'application induite $(R_T/\mathfrak{m}R_T)^n \longrightarrow P_T/\mathfrak{m}P_T$ est un isomorphisme, donc $K/\mathfrak{m}K = 0$, de nouveau, en observant que $\mathfrak{m}$ est contenu dans le radical da R_T, et en utilisant Nakayama, on déduit que $K = 0$, et donc $P_T \simeq (R_T)^n$ via ϕ. On en tire alors que $p, q_2, \ldots, q_n$ est une base pour P_T.

Posons $P' = P/Rp$. Alors P'_T est libre de rang $n-1$ avec la base $q_2+(Rp)_T, \ldots, q_n+(Rp)_T$. De même, P_{ff1} a comme base $p, p_2, \ldots, p_n$. Donc P'_{ff1} est libre de rang $n-1$. Si M est un idéal maximal de R, vue que ff_1 est unitaire, on peut appliquer la Proposition 40, et on a soit $ff_1 \in R\backslash M$ soit $T \subseteq R\backslash M$. On a donc soit $P'_M = (P'_{ff1})_M$ soit $P'_M = (P'_T)_M$ respectivement. On a alors en tout cas que P'_M est libre de rang $n-1$. On a montré que P' est localement libre et par la Remarque 28, il est projectif de rang $n-1$. Puisque P'_{ff1} est libre par l'hypothèse d'induction P' est libre. On montre que Rp est également libre. En effet comme on a vue ci-dessus, $f^k p = f_1 p_1 + a_2 p_2 + \cdots + a_n p_n$. Si $rp = 0$ pour un $r \in R$, on aura

$$0 = rf^k p = (rf_1)p_1 + (ra_2)p_2 + \cdots + (ra_n)p_n.$$

Mais $p_1, \ldots, p_n$ est une base pour P_f, donc $rf_1 = 0 \in R_f$. Il existe alors un $l \geq 0$ tel que $f^l r f_1 = 0$, i.e., $(f^l f_1)r = 0$. $f^l f_1$ étant unitaire, on conclu que $r = 0$(par un argument similaire à celui que l'on a fait pour démontrer la liberté de l'idéal I dans le cas $n = 1$). On a donc que $P/Rp, Rp$ sont libres, il s'en suit que P est aussi libre. En effet puisque P/Rp est libre, il est projectif et donc la suite exacte courte

$$0 \longrightarrow Rp \longrightarrow P \longrightarrow P/Rp \longrightarrow 0$$

est scindée, donc $P \simeq Rp \oplus P/Rp$, c'est à dire que P est une somme directe de deux modules libres, par conséquent il est aussi libre. ceci termine la preuve du théorème de Horrocks. $\square$

Le théorème suivant est la généralisation du théorème de Horrocks, qui sera le dernier pas vers le résultat principal de ce traité.

Théorème 44 (Quillen, Suslin). *Soit A un anneau noetherien et soit $R = A[x]$ l'anneau de polynômes sur A. Soit P un R-module projectif de type fini tel que P_f soit libre où f est un polynôme unitaire de R. Alors P est libre.*

Preuve. Pour tout idéal maximal $\mathfrak{m}$ de A le $A_{\mathfrak{m}}[x]$-module $P_{\mathfrak{m}}$ est libre. En effet $A_{\mathfrak{m}}$ est un anneau local, avec l'idéal maximal $\mathfrak{m}$, et f vu comme un élément de $A_{\mathfrak{m}}[x]$ est unitaire et on a $(P_{\mathfrak{m}})_f = (P_f)_{\mathfrak{m}}$ qui est un module libre, on peut donc appliquer le Théorème de Horrocks et voir que $P_{\mathfrak{m}}$ est libre.

Or, tout $A[x]$-module libre est étendu, car $(A[x])^n \simeq A^n \otimes_A A[x]$. Alors pour tout idéal maximal $\mathfrak{m}$ de A, $P_{\mathfrak{m}}$ est étendu. D'après le Théorème de Quillen (Théorème 23), P est aussi étendu. Alors il existe un A-module de type fini N tel que $P \simeq N \otimes_A A[x]$. On va montrer que N est libre et ceci clôt la démonstration.

On a $R_x = A[x]_x = A[x, x^{-1}]$, et on pose $y = x^{-1}$ et $g(y) = x^{-d} f(x) = y^d f(x)$ où d est le degré de f. Puisque f est unitaire le terme constat ed g est inversible. On écrit $g(y) = a_d y^d + a_{d-1} y^{d-1} + \cdots + a_1 y + a_0$ avec a_1 une unité. On a $1 = g(y) - y(a_d y^{d-1} + \cdots + a_0)$, alors $y, g(y)$ sont des éléments comaximaux dans $A[y]$. Donc par la Proposition 5 le diagramme suivant est un pull-back :

$$\begin{tikzcd} A[y] \arrow[r] \arrow[d] & A[y, y^{-1}] = A[x, x^{-1}] \arrow[d] \\ A[y]_g \arrow[r] & A[y]_{yg} = A[x, x^{-1}]_f \end{tikzcd}$$

où les homomorphismes sont les applications de localisations naturelles.

Soit r le rang de P_f et soit F un $A[y]_g$-module libre de rang r, i.e., $F = (A[y]_g)^r$. Puisque P_{xf} est un $A[x, x^{-1}]_f = A[y]_{yg}$-module libre de rang r, l'application naturelle $A[y]_g \longrightarrow A[y]_{yg}$ induit une application naturelle $\phi : F \longrightarrow P_{xf}$ telle que l'homomorphisme induit $F_g \longrightarrow P_{xf}$, par localisation en g soit un isomorphisme. Par la Proposition 15, il existe un $A[y]$-module projectif P' tel que le diagramme suivant soit un pull-back :

$$\begin{tikzcd} P' \arrow[r] \arrow[d] & P_x \arrow[d] \\ F \arrow[r, "\phi"] & P_{xg}. \end{tikzcd}$$

Il s'en suit que $P'_y \simeq P_x$, et donc pour tout idéal maximal $\mathfrak{m}$ de A, on a

$$(P'_{\mathfrak{m}})_y \simeq (P'_y)_{\mathfrak{m}} \simeq (P_x)_{\mathfrak{m}} \simeq (P_{\mathfrak{m}})_x.$$

Mais comme on l'a dit ci-dessus, $P_{\mathfrak{m}}$ est libre donc $(P'_{\mathfrak{m}})_y$ est libre, de nouveau y vu comme un élément de $A_{\mathfrak{m}}[y]$ est unitaire, on applique le Théorème de Horrocks, et on obtient que $P'_{\mathfrak{m}}$ est libre pour tout idéal maximal $\mathfrak{m}$ de A. Il en résulte que $P'_{\mathfrak{m}}$ est étendu, pout tout $\mathfrak{m}$, et alors P' est un $A[y]$-module étendue de A. Il existe alors un A-module de type fini N' tel que $P' \simeq N' \otimes_A A[y]$.

Il existe un morphisme canonique $\psi : A[y]_g/(y)_g \longrightarrow A[y]/(y)$ qui envoie $\frac{h(y)}{g^n} + (y)_g \longmapsto h + (y)$. Puisque le terme constant de g, i.e., $g(0)$ est inversible cette application est un isomorphisme. On a alors les isomorphismes canoniques :

$$P'_g/yP'_g \simeq P'_g \otimes_{A[y]_g} (A[y]_g/(y)_g) \simeq P' \otimes_{A[y]} A[y]_g \otimes_{A[y]_g} (A[y]_g/(y)_g) \simeq$$
$$P' \otimes_{A[y]} (A[y]_g/(y)_g) \simeq P' \otimes_{A[y]} (A[y]/(y)) \simeq P'/yP'.$$

L'application naturelle $P' \longrightarrow F$ induit un isomorphisme $P'_g \simeq F$, en fait ceci est vrai d'après la construction de P'. En mettant toutes ces informations, on obtient des isomorphismes suivants :

$$P'/yP' \simeq P'_g/yP'_g \simeq F/yF.$$

Puisque F est libre, ces isomorphisme impliquent que P'/yP' est aussi libre. Par la Proposition 19, on sait que $N' \simeq P'/yP'$, donc N' est libre.

Soit $a \in A$ un élément quelconque, on a un A-homomorphisme canonique : $N \otimes_A (A[x]/(x-a)) \simeq N$, donné par $n \otimes (h(x) + (x-a)) \longmapsto h(a)n$. Il n'est pas difficile de voir que cette application est en fait un A-isomorphisme. Par ailleurs on sait que $P \simeq N \otimes_A A[x]$, on a donc une série d'isomorphismes canoniques :$P/(x-a)P \simeq$

$$P \otimes_{A[x]} (A[x]/(x-a)) \simeq N \otimes_A A[x] \otimes_{A[x]} (A[x]/(x-a)) \simeq N \otimes_A (A[x]/(x-a)) \simeq N.$$

Donc on a en particulier $N \simeq P/(x-1)P$. De même, on a un isomorphisme $P'/(y-1)P' \simeq N'$.

Or, il existe un $A[x]$-homomorphisme

$$A[x]/(x-1) \otimes_{A[x]} A[x]_x \longrightarrow A[x]/(x-1),\ (h(x) + (x-1)) \otimes (\frac{b(x)}{x^k}) \mapsto b(1)h(x) + (x-1).$$

Il est facile de vérifier que cette application est un $A[x]$-isomorphisme. Ceci implique que

$$P_x/(x-1)P_x \simeq (P/(x-1)P)_x \simeq (P/(x-1)P) \otimes_{A[x]} A[x]_x \simeq$$
$$P \otimes_{A[x]} (A[x]/(x-1)) \otimes_{A[x]} A[x]_x \simeq N \otimes_A A[x] \otimes_{A[x]} (A[x]/(x-1)) \otimes_{A[x]} A[x]_x \simeq$$
$$N \otimes_A A[x] \otimes_{A[x]} (A[x]/(x-1)) \simeq P \otimes_{A[x]} (A[x]/(x-1)) \simeq P/(x-1)P.$$

Le même argument montre que l'on a un isomorphisme $P'/(y-1)P' \simeq P'_y/(y-1)P'_y$.

Puisque x, y sont inversible dans $A[x, x^{-1}]$ et que l'isomorphisme $P'_y \simeq P_x$ est un isomorphisme de $A[x, x^{-1}]$-modules, cet isomorphisme induit un isomorphisme

$$P'_y/(y-1)P'_y \simeq P_x/(x-1)P_x.$$

En résumant tous ceux que l'on a établi jusqu'ici, on obtient :

$$N \simeq P/(x-1)P \simeq P_x/(x-1)P_x \simeq P'_Y/(y-1)P'_y \simeq P'/(y-1)P' \simeq N'$$

N' étant libre, N l'est aussi, et la preuve est achevée. $\square$

On montre maintenant quelques résultats nécessaires pour la suite :

Définition 45. *Soit A un anneau.* La hauteur *d'un idéal premier $\mathfrak{p}$ est le suprêmum des longueurs des chaînes (le nombre des "$\subsetneq$") d'idéaux premier*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}.$$

La dimension de Krull *de A est le suprêmum des hauteurs de tous les idéaux premiers de A.*

Remarque 46. Soit A un anneau, alors la dimension de Krull de A vaut 1 si et seulement si tout idéal premier non-nul de A est maximal.

Proposition 47. *Soit A un anneau factoriel et noetherien. Si la dimension de Krull de A vaut 1, alors il est un anneau principal.*

Preuve. Montrons d'abord que tout idéal premier $\mathfrak{p}$ est principal. Puisque A est noetherien $\mathfrak{p}$ est de finiment engendré, disons $\mathfrak{p} = (p_1, \ldots, p_k)$. On peut supposer les p_i irréductibles, car sinon p_i est un produit des éléments irréductibles et puisque $\mathfrak{p}$ est premier un de ces facteurs appartient à $\mathfrak{p}$ et on peut remplacer p_i par cet élément. Donc en particulier l'idéal engendré par p_1, (p_1) est premier. On a une chaîne $0 \subsetneq (p_1) \subseteq \mathfrak{p}$,et puisque la dimension de A est 1, on a $(p_1) = \mathfrak{p}$ et donc $\mathfrak{p}$ est principal. On montre maintenant que tout idéal de A est principal. Soit donc I un idéal de A, de nouveau I est finiment engendré, donc on peut écrire $I = (a_1, \ldots, a_k)$ pour certains $a_i \in A, i = 1, \ldots, k$. Soit d le plus grand commun diviseur (pgcd) des a_i, et écrivons $a_i = db_i, i = 1, \ldots, k$ pour certains $b_i \in A$. Le pgcd des b_i est alors une unité de A et on pose $J := (b_1, \ldots, b_k)$ l'idéal engendré par les b_i. On a soit $J = A$ soit $J \subsetneq A$, dans le premier cas, il implique que $I = (d)$ et donc l'idéal I est principal. Dans le second cas, il existe un idéal maximal (et en particulier premier) $\mathfrak{m}$ de A tel que $J \subseteq \mathfrak{m}$, puisque $\mathfrak{m}$ est premier, comme l'on a montré ci-dessus, il est principal, disons $\mathfrak{m} = (m)$ pour un certain élément irréductible $m \in A$. $(b_1, \ldots, b_k) = J \subseteq \mathfrak{m}$, alors $m|b_i, i = 1, \ldots, k$, mais ceci est en contradiction avec le fait que pgcd$(b_1, \ldots, b_k)$ est une unité. Par conséquent $J = A$ et comme on a vu, I est principal. □

Proposition 48. *Soient A un anneau principal, $B = A[X]$ et $C = B[S^{-1}]$ où S est l'ensemble des polynômes unitaires de B. Alors la dimension de Krull de C est au plus 1.*

Preuve. Déterminons les idéaux premiers de B. Si P est un idéal premier non nul de B, alors P contient un polynôme non nul f et, comme il est premier, il contient un facteur irréductible g de f. Si g est constant, alors $P/(g) \subset B/(g) = A/(g)[X]$ est soit nul (en ce cas $P = (g)$) soit l'idéal engendré par un polynôme unitaire $\overline{h} \in A/(g)[X]$ que l'on peut relever dans un polynôme unitaire $h \in B$. Si g n'est pas constant, soit $P = (g)$, soit P contient un autre polynôme irréductible h premier à g. Comme g et h sont copremiers dans $K[X]$ (K le corps des fractions de A) on a $1 \in K[X]g + K[X]h$ et donc, en libérant des dénominateurs, on voit que P contient une constante non nulle p, que l'on peut supposer irréductible. On retrouve alors le cas déjà discuté ci-dessus. Les premiers de B sont de la forme (0), (g) pour un g irréductible ou (p, f), où p est une constante irréductible et f un polynôme unitaire (irréductible modulo p) Si on inverse tous les polynômes unitaires, on obtient un C dans lequel les idéaux premiers sont tous principaux. Si on a une inclusion $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ avec $\mathfrak{p}_i, i = 1, 2$ premiers de C, on a $\mathfrak{p}_i = (p_i), i = 1, 2$, pour des éléments irréductibles p_i. Donc $p_i \in (p_2)$, et par conséquent $p_2 | p_1$, mais p_1 est irréductible, donc p_1, p_2 sont associés, et alors $\mathfrak{p}_1 = (p_1) = (p_2) = \mathfrak{p}_2$. On en tire alors que tout idéal premier non-nul est maximal et par la Remarque 46 la dimension de Krull de C vaut 1. □

Voici le théorème principal de cet article :

Théorème 49 (Quillen,Suslin). *Soit $R = A[x_1, \ldots, x_n]$ un anneau de polynômes sur un anneau principal A. Alors tout R-module projectif de type fini est libre.*

Preuve. On démontre ce théorème par induction sur n. Si $n = 0$, alors tout A-module projectif est libre, puisque A est principal.

On suppose donc que $n > 0$. Soit S l'ensemble de tous les polynômes unitaires dans $A[x_1]$, et soit $A' = S^{-1}A[x_1]$. On prétend que A' est un anneau principal. En effet par la Proposition 48, la dimension de Krull de A' est au plus 1. Si elle vaut 0, A' est un corps, donc en particulier un anneau principal. Si cette dimension vaut 1, par la Proposition 47, A' est aussi un anneau principal. $S^{-1}P$ est un $S^{-1}A[x_1, \ldots, x_n] = A'[x_2, \ldots, x_n]$-module projectif de type fini, et A' est principal, donc par l'hypothèse d'induction il s'en suit que $S^{-1}P$ est libre. Par la Proposition 17, il existe un élément $f \in S$, tel que P_f est libre, mais f est unitaire, on peut donc appliquer le Théorème de Quillen, Suslin (Théorème 46) et voir que P est libre. □