Sur les anneaux seminormaux

Une preuve constructive exemplaire

H. Lombardi, Besançon

(d'après Thierry Coquand)

Colloque en l'honneur des 60 ans d'André Galligo.
Nice 2006.

Henri.Lombardi@univ-fcomte.fr

http://hlombardi.free.fr/

plus de détails dans

http://hlombardi.free.fr/publis/NotesDeCoursSeminormal.pdf

Bon Anniversaire

André

Références

[Tra] Traverso C. *Seminormality and the Picard group*. Ann. Scuola Norm. Sup. Pisa, **24** (1970), 585–595.

[Swan] Swan R. G. *On Seminormality.* Journal of Algebra, **67** (1980), 210–229.

[Coq] Coquand T. *On seminormality.* 2006. À paraître au Journal of Algebra.
http://www.cs.chalmers.se/~coquand/min.pdf

[Ric] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc., **103** (1988), 1012–1014.

Une preuve constructive exemplaire

Le théorème de Traverso-Swan affirme qu'un anneau réduit $\mathbf{A}$ est seminormal si et seulement si l'homomorphisme naturel

$$\mathrm{Pic}\,\mathbf{A} \to \mathrm{Pic}\,\mathbf{A}[X]$$

est un isomorphisme ([Tra],[Swan]). Nous exposons ici la preuve constructive élémentaire de ce résultat qui a été donnée par Thierry Coquand dans [Coq].

La méthode utilisée consiste à mettre tout d'abord en place une preuve classique la plus élémentaire possible. Il reste néanmoins, après cette simplification, des arguments hautement non constructifs : preuve par l'absurde basée sur la considération d'un idéal premier minimal.

Cependant, la signification du théorème est **de nature concrète** : si l'anneau est seminormal et si on donne une matrice $P(X)$ qui représente un élément de $\operatorname{Pic}\mathbf{A}[X]$, il faut trouver une similitude entre $P(X)$ et $P(0)$.

La question est alors : est-ce que la preuve par l'absurde basée sur la considération d'un idéal premier minimal est un **miracle** réalisé par les mathématiques classiques ?

Ou bien **est-ce que cette preuve cache un calcul ?**

En fait une méthode générale de décryptage constructif est ici mise en œuvre.

Remplacer les objets abstraits (ici, un *idéal premier minimal générique*) par des *approximations finies* de ces objets, et vérifier que l'argument classique peut fonctionner comme un calcul sur ces approximations finies.

Cette preuve constructive est donc une illustration du fait qu'une sorte de **programme de Hilbert pour l'algèbre abstraite** fonctionne en pratique.

Une citation de Henri Poincaré

Quant à moi je proposerais de s'en tenir aux règles suivantes :

1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots ;
2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini ;
3. Éviter les classifications et les définitions non prédicatives.

Henri Poincaré, in *La logique de l'infini* (Revue de Métaphysique et de Morale 1909). Réédité in *Dernières pensées*, Flammarion.

Qu'est-ce qu'un anneau seminormal ?

Un anneau intègre $\mathbf{A}$ est dit *seminormal* si chaque fois que $b^2 = c^3 \neq 0$, l'élément $a = b/c$ du corps des fractions est en fait dans $\mathbf{A}$. Notons que $a^3 = b$ et $a^2 = c$. Tout anneau intégralement clos est donc seminormal.

Un anneau quelconque $\mathbf{A}$ est dit *seminormal* si chaque fois que $b^2 = c^3$, il existe $a \in \mathbf{A}$ tel que $a^3 = b$ et $a^2 = c$.

Ceci implique que $\mathbf{A}$ est réduit : si $b^2 = 0$ alors $b^2 = 0^3$, d'où un $a \in \mathbf{A}$ avec $a^3 = b$ et $a^2 = 0$, donc $b = 0$.

Dans un anneau si $x^2 = y^2$ et $x^3 = y^3$ alors $(x-y)^3 = 0$. Ainsi :

Fait 1. *Dans un anneau réduit $x^2 = y^2$ et $x^3 = y^3$ impliquent $x = y$.*

En conséquence si un a tel que $a^3 = b$ et $a^2 = c$ existe, il est toujours unique. En outre $\operatorname{Ann} b = \operatorname{Ann} c = \operatorname{Ann} a$.

Le groupe de Picard de l'anneau A

Un **module projectif de type fini** est un module M isomorphe à un facteur direct dans un module libre de rang fini : $M \oplus M' \simeq \mathbf{A}^m$. De manière équivalente, c'est un module isomorphe à l'image d'une matrice de projection.

Une application $\mathbf{A}$-linéaire $\psi : M \to N$ entre modules projectifs de type fini avec $M \oplus M' \simeq \mathbf{A}^m$ et $N \oplus N' \simeq \mathbf{A}^n$ peut être représentée par $\widetilde{\psi} : \mathbf{A}^m \to \mathbf{A}^n$ définie par $\widetilde{\psi}(x \oplus x') = \psi(x)$.

En d'autres termes un module projectif de type fini sur $\mathbf{A}$ **est** une matrice carrée idempotente P à coefficients dans $\mathbf{A}$, et un morphisme de P vers Q **est** une matrice H de format convenable telle que $QH = H = HP$.

Modules projectifs de rang 1

Un module projectif de type fini représenté par une matrice P est **de rang** k lorsque $\det(\mathrm{I} + TP) = (1 + T)^k$.

Un **module projectif de rang constant** 1 est donné par une matrice P telle que $\bigwedge^2 P = 0$ (tous les mineurs d'ordre 2 sont nuls) et $\mathrm{Tr}(P) = 1$ (ceci implique $P^2 = P$).

Les classes d'isomorphisme de modules projectif de rang 1 forment un groupe pour la loi héritée de $\otimes$,
c'est le **GROUPE DE PICARD** $\mathrm{Pic}\,\mathbf{A}$.
L'« inverse » est donné par la transposée de P, qui définit le module dual.

Critère de liberté

Lemme 2. *Soit $P \in \mathbf{A}^{n\times n}$ matrice de projection de rang 1.*
Les propriétés suivantes sont équivalentes :

1. P **a son image libre**
2. *Il existe un vecteur colonne f et un vecteur ligne g tels que* $gf = 1$ **et** $fg = P$**.**
   En outre dans ce cas f et g sont uniques, au produit par une unité près, sous la seule condition que $fg = P$.
3. **Les matrices** $\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P & \\ 0 & & & \end{bmatrix}$ **et** $\mathrm{I}_{n+1,1} := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0_{n,n} & \\ 0 & & & \end{bmatrix}$
   sont semblables.

$$\mathrm{Pic}\,\mathbf{A} \xrightarrow{\mathrm{Pic}\,j} \mathrm{Pic}\,\mathbf{A}[X_1,\ldots,X_\ell] \xrightarrow{\mathrm{Pic}\,Ev_0} \mathrm{Pic}\,\mathbf{A}$$

La composée des deux flèches est l'identité. La première est injective et la deuxième surjective. Donc :

$\mathrm{Pic}\,j$ **est surjective**

(i.e., tout module projectif de rang constant 1 sur $\mathbf{A}[X_1,\ldots,X_\ell] = \mathbf{A}[\underline{X}]$ provient par extension des scalaires d'un module projectif de rang constant 1 sur $\mathbf{A}$)

si et seulement si

$\mathrm{Pic}\,Ev_0$ **est injective**

(i.e. tout module projectif de rang constant 1 sur $\mathbf{A}[\underline{X}]$ qui devient libre sur $\mathbf{A}$ si on évalue les X_i en 0, est déjà libre sur $\mathbf{A}[\underline{X}]$).

Dans ce cas on écrit, par abus, $\mathrm{Pic}\,\mathbf{A} = \mathrm{Pic}\,\mathbf{A}[\underline{X}]$.

Théorème 3. (Traverso-Swan) *Pour un anneau réduit, et* $\ell \geq 1$, $\mathrm{Pic}\,\mathbf{A} = \mathrm{Pic}\,\mathbf{A}[X_1, \ldots, X_\ell]$ *si et seulement si* $\mathbf{A}$ *est seminormal.*

Signification en terme de calculs

Théorème 4. (Traverso-Swan) *Pour un anneau réduit, et* $\ell \geq 1$, *les propriétés suivantes sont équivalentes :*

1. $\mathbf{A}$ *est seminormal.*
2. *Pour toute matrice de projection de rang* 1, $P = (m_{ij}) \in \mathbf{A}[\underline{X}]^{n\times n}$ *qui vérifie*

$$P(0,\ldots,0) = \begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & 0_{n-1,n-1} \end{bmatrix} = \mathrm{I}_{n,1} \ ,$$

il existe $f_1, \ldots, f_n$, $g_1, \ldots, g_n \in \mathbf{A}[\underline{X}]$ *tels que* $f_i g_i = m_{ij}$ *pour tous* i, j.

La condition est nécessaire

I.e., si $\mathbf{A}$ est réduit et $\operatorname{Pic}\mathbf{A} = \operatorname{Pic}\mathbf{A}[X]$ alors $\mathbf{A}$ est seminormal.

Exemple de Schanuel.
Soient $b, c \in \mathbf{A}$ réduit avec $b^2 = c^3$. Soit $\mathbf{B} = \mathbf{A}[a] = \mathbf{A} + a\mathbf{A}$ un anneau réduit contenant $\mathbf{A}$ avec $a^3 = b$, $a^2 = c$. On considère $f_1 = 1 + aX$, $f_2 = cX^2 = g_2$ et $g_1 = (1 - aX)(1 + cX^2)$. On a $f_1 g_1 + f_2 g_2 = 1$.
Donc la matrice $M(X)$ des $f_i g_j$ est idempotente de rang 1.
On vérifie que ses coefficients sont dans $\mathbf{A}$ et que $M(0) = \mathrm{I}_{2,1}$.
Son image est libre sur $\mathbf{B}[X]$. Si elle est libre sur $\mathbf{A}[X]$ il existe des f'_i et g'_j dans $\mathbf{A}[X]$ avec $f'_i g'_j = f_i g_j$. Par unicité $f'_i = u f_i$ avec u inversible dans $\mathbf{A}[X]$ donc dans $\mathbf{A}$. Avec $i = 1$ on obtient $a \in \mathbf{A}$.

NB : On peut prendre $\mathbf{B} = \left(\mathbf{A}[T]\big/\left\langle T^2 - c, T^3 - b\right\rangle\right)_{\mathrm{red}}$.
Si un a est déjà présent dans $\mathbf{A}$, on obtient par unicité $\mathbf{B} = \mathbf{A}$.

Si A est un anneau à pgcd,

$\mathrm{Pic}\,\mathbf{A} = \{1\} = \mathrm{Pic}\,\mathbf{A}[\underline{X}]$

Rappelons que si $\mathbf{A}$ est un anneau à pgcd, il en va de même pour l'anneau des polynomes $\mathbf{A}[\underline{X}]$. Il suffit donc de voir que $\mathrm{Pic}\,\mathbf{A} = \{1\}$.

Démonstration

Soit $P = (m_{i,j})$ une matrice idempotente de rang 1.
On peut supposer que $m_{1,1}$ est régulier.
Soit f le pgcd des éléments de la première ligne. On a $m_{1,j} = fg_j$ avec le pgcd des g_j égal à 1. Puisque f est régulier et $m_{1,1}m_{i,j} = m_{1,j}m_{i,1}$ on obtient $g_1 m_{i,j} = m_{i,1}g_j$.
Ainsi g_1 divise tous les $m_{i,1}g_j$ donc aussi leur pgcd $m_{i,1}$.
On écrit $m_{i,1} = g_1 f_i$. Puisque $g_1 f_1 = m_{1,1} = fg_1$ cela donne $f_1 = f$.
Enfin l'égalité $m_{1,1}m_{i,j} = m_{1,j}m_{i,1}$ donne $f_1 g_1 m_{i,j} = f_1 g_j g_1 f_i$ puis $m_{i,j} = f_i g_j$.

Si $\mathbf{A}$ est intégralement clos,

$\mathrm{Pic}\,\mathbf{A} = \mathrm{Pic}\,\mathbf{A}[\underline{X}]$

Démonstration

Soit $P(\underline{X}) = (m_{i,j}(\underline{X}))_{i,j=1,\ldots,n}$ une matrice idempotente de rang 1 avec $P(0) = \mathrm{I}_{n,1}$.

Soit $\mathbf{K}$ le corps des fractions de $\mathbf{A}$.

Sur $\mathbf{K}[\underline{X}]$ le module $\mathrm{Im}\,P(\underline{X})$ est libre.

Il existe donc $f = (f_1(\underline{X}), \ldots, f_n(\underline{X}))$ et $g = (g_1(\underline{X}), \ldots, g_n(\underline{X}))$ dans $\mathbf{K}[\underline{X}]^n$ tels que $m_{i,j} = f_i g_j$ pour tous i, j.

On peut supposer que $f_1(0) = g_1(0) = 1$.

Alors puisque $f_1 g_j = m_{1,j}$ et vu le **théorème de Kronecker**, les coefficients des g_j sont entiers sur l'anneau engendré par les coefficients des $m_{1,j}$.

Donc les g_j sont dans $\mathbf{A}[\underline{X}]$. Même chose pour les f_i.

Si A est intègre et seminormal,

$\mathrm{Pic}\,\mathbf{A} = \mathrm{Pic}\,\mathbf{A}[\underline{X}]$

Démonstration

Soit $P(\underline{X}) = (m_{i,j}(\underline{X}))_{i,j=1,\ldots,n}$ une matrice idempotente de rang 1 avec $P(0) = \mathrm{I}_{n,1}$.

Il existe $f_1(\underline{X}), \ldots, f_n(\underline{X}), g_1(\underline{X}), \ldots, g_n(\underline{X})$ dans $\mathbf{K}[\underline{X}]^n$ tels que $m_{i,j} = f_i g_j$ pour tous i, j. En outre $f_1(0) = g_1(0) = 1$.

Soit $\mathbf{B}$ le sous anneau de $\mathbf{K}$ engendré par $\mathbf{A}$ et par les coefficients des f_i et des g_j. D'après le théorème de Kronecker, $\mathbf{B}$ est une extension finie de $\mathbf{A}$ (i.e., $\mathbf{B}$ est un $\mathbf{A}$-module de type fini).

Notre but est de montrer que $\mathrm{A} = \mathrm{B}$.

On appelle $\mathfrak{a}$ le conducteur de $\mathbf{A}$ dans $\mathbf{B}$, c'est-à-dire l'ensemble $\{x \in \mathbf{B} \,|\, x\mathbf{B} \subseteq \mathbf{A}\}$. C'est à la fois un idéal de $\mathbf{A}$ et $\mathbf{B}$.

Notre but est maintenant de montrer $\mathfrak{a} = \langle 1 \rangle$.

Si A est intègre et seminormal, alors $\mathrm{Pic}\,\mathrm{A} = \mathrm{Pic}\,\mathrm{A}[X]$. Suite

Lemme 5. *Si* $\mathbf{A} \subseteq \mathbf{B}$, $\mathbf{A}$ *seminormal et* $\mathbf{B}$ *réduit, alors le conducteur* $\mathfrak{a}$ *de* $\mathbf{A}$ *dans* $\mathbf{B}$ *est un idéal radical de* $\mathbf{B}$.

Démonstration

On doit montrer que si $u \in \mathbf{B}$ et $u^2 \in \mathfrak{a}$ alors $u \in \mathfrak{a}$.

Soit donc $c \in \mathbf{B}$, on doit montrer que $uc \in \mathbf{A}$.

On sait que $u^2c^2 \in \mathbf{A}$ et que $u^3c^3 = u^2(uc^3) \in \mathbf{A}$ puisque $u^2 \in \mathfrak{a}$.

Puisque $(u^3c^3)^2 = (u^2c^2)^3$ il existe $a \in \mathbf{A}$ tel que $a^2 = (uc)^2$ et $a^3 = (uc)^3$.

Comme $\mathbf{B}$ est réduit cela implique $a = uc$, et donc $uc \in \mathbf{A}$.

Si A est intègre et seminormal, alors $\mathrm{Pic}\,\mathrm{A} = \mathrm{Pic}\,\mathrm{A}[X]$. Suite

Lemme 6.

Soit $\mathbf{A} \subseteq \mathbf{B}$, $\mathbf{B} = \mathbf{A}[c_1, \ldots, c_q]$ réduit fini sur $\mathbf{A}$.

Soit $\mathfrak{a}$ le conducteur de $\mathbf{A}$ dans $\mathbf{B}$.

On suppose que $\mathfrak{a}$ est un idéal radical, i.e. $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Alors il est égal à $\{x \in \mathbf{A} \,|\, xc_1, \ldots, xc_q \in \mathbf{A}\}$.

Démonstration

En effet si $xc_i \in \mathbf{A}$ alors $x^\ell c_i^\ell \in \mathbf{A}$ pour tout ℓ.

Donc pour un N assez grand $x^N y \in \mathbf{A}$ pour tout $y \in \mathbf{B}$.

Donc x est dans le radical de $\mathfrak{a}$.

(si d majore les degrés des équations de dépendance intégrale des c_i sur $\mathbf{A}$, on pourra prendre $N = (d-1)q$).

Si A est intègre et seminormal, alors $\mathrm{Pic}\,\mathrm{A} = \mathrm{Pic}\,\mathrm{A}[\underline{X}]$. Suite

Fin de la démonstration, en mathématiques classiques.
On a $\mathbf{C} = \mathbf{A}/\mathfrak{a} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$. **Si $\mathfrak{a} \neq \langle 1 \rangle$ soit $\mathfrak{p}$ un idéal premier minimal de $\mathbf{C}$**, $\mathfrak{P}$ l'idéal correspondant de $\mathbf{A}$, $S = \mathbf{C} \setminus \mathfrak{p}$ la partie complémentaire.
Puisque $\mathfrak{p}$ est un idéal premier minimal, et puisque $\mathbf{C}$ est réduit, $S^{-1}\mathbf{C} = \mathbf{L}$ est un corps, contenu dans l'anneau réduit $S^{-1}\mathbf{C}' = \mathbf{L}'$.
Si x est un objet défini sur $\mathbf{A}$ notons $\overline{x}$ ce qu'il devient après le changement de base $\mathbf{A} \to \mathbf{L}'$.
Le module $\overline{M}$ est défini par la matrice $\overline{P}$ dont les coefficients sont dans $\mathbf{L}[\underline{X}]$.
Puisque $\mathbf{L}$ est un corps, $\mathrm{Im}\,\overline{P}$ est libre sur $\mathbf{L}[\underline{X}]$. Cela implique, par unicité (lemme 2) et vu que $f_1(0) = g_1(0) = 1$, que les $\overline{f_i}$ et $\overline{g_j}$ sont dans $\mathbf{L}[\underline{X}]$.
Cela signifie qu'il existe $s \in \mathbf{A} \setminus \mathfrak{P}$ tel que les sf_i et sg_j sont à coefficients dans $\mathbf{A}$. D'après le lemme 6, ceci implique que $s \in \mathfrak{a}$.
Ce qui est absurde.

Rendre la preuve constructive (cas intègre)

Nous discutons maintenant la question de savoir s'il y a eu un miracle, ou si au contraire un calcul est caché dans la preuve précédente.

L'argument par l'absurde dans la preuve classique, peut être interprété comme un argument indirect, qui prouve que l'anneau $\mathrm{A}/\mathfrak{a}$ est trivial en disant, selon toute apparence :
si l'anneau n'était pas trivial, il contiendrait un idéal premier minimal, etc. . . , et finalement il serait trivial.

Mais **une fois remis à l'endroit, l'argument prouve directement que l'anneau $\mathrm{A}/\mathfrak{a}$ est trivial.**

Rendre la preuve constructive (suite)

OK pour l'argument « par l'absurde ».
Et pour le premier minimal ?

Réponse : **faire comme si . . .**
puisque la preuve est finie, elle n'utilise qu'un nombre fini d'informations sur le premier minimal générique,
et **cet idéal premier minimal purement idéal peut être remplacé par une famille finie d'approximations finies qui couvrent tous les cas qui se présentent dans le calcul.**

C'est bien beau votre discours, mais qu'est-ce qu'une approximation finie d'une localisation en un idéal premier minimal ?
C'est une localisation en un élément !
Car rendre inversibles un nombre fini d'éléments c'est rendre inversible leur produit.

Digression

Concernant le renversement d'un raisonnement direct en un raisonnement par l'absurde, on est là face à une sorte de **déformation professionnelle du mathématicien classique**.

Combien de fois n'avons nous pas lu que Euclide prouvait
par l'absurde qu'il existe une infinité de nombres premiers.
Alors que sa preuve donne directement un algorithme qui construit une suite infinie de nombres premiers.

Digression

Même chose pour les objets idéaux qui sont souvent de simples aides heuristiques pour les preuves.

Combien de fois n'avons nous pas lu que Cantor prouvait
par une comparaison des infinis selon leur taille qu'il existe des nombres transcendants.
Alors que sa preuve donne directement un algorithme qui construit une suite infinie de nombres transcendants.

Rendre la preuve constructive (suite)

Il faut d'abord établir un lemme dont l'énoncé est un peu déroutant.

Sa signification intuitive est la suivante :
Soit un anneau C réduit et P un module projectif de rang 1 sur $\mathrm{C}[X]$. Si C n'est pas trivial, il doit y avoir une localisation non triviale $S^{-1}\mathrm{C}$ de C pour laquelle P devient libre.

En mathématiques classiques la réponse est immédiate : la localisation en un idéal premier minimal. C'est l'argument qui a été utilisé dans la preuve précédente, avec l'anneau $\mathbf{C} = \mathbf{A}/\mathfrak{a}$.

Le lemme sous sa forme intuitive **n'est pas vrai** d'un point de vue constructif.
Mais fort heureusement c'est sa contraposée qui nous intéresse, et elle **est vraie** au sens des mathématiques constructives, c'est-à-dire qu'elle nous donne un algorithme !

Rendre la preuve constructive (suite)

La contraposée de

Soit un anneau C réduit et P un module projectif de rang 1 sur $\mathrm{C}[\underline{X}]$. Si C n'est pas trivial, il doit y avoir une localisation non triviale $S^{-1}\mathrm{C}$ de C pour laquelle P devient libre.

c'est

Soit C un anneau réduit et P un module projectif de rang 1 sur $\mathrm{C}[\underline{X}]$. Si toute localisation $S^{-1}\mathrm{C}$ de C pour laquelle P devient libre est triviale, c'est que C lui-même est trivial.

En fait nous utiliserons la version précise suivante dans laquelle seules interviennent les localisations en un élément.

Rendre la preuve constructive (suite)

Voici **LE** lemme

Lemme 7.
Soit C *un anneau réduit et* $P = (m_{i,j}) \in \mathrm{C}[\underline{X}]^{n\times n}$ *une matrice idempotente de rang 1 telle que* $P(0) = \mathrm{I}_{n,1}$.

Supposons que l'implication suivante soit satisfaite :

$$\forall a \in \mathrm{C}, \text{ si } \operatorname{Im} P \text{ est libre sur } \mathrm{C}[1/a][\underline{X}], \text{ alors } a = 0.$$

Alors C **est trivial**, *c'est-à-dire* $1 = 0$ *dans* C.

Utilisation DU lemme,

pour rendre la preuve constructive

La fin de la preuve page 21 devient constructive grâce AU lemme, qui est donc un **lemme d'élimination de l'idéal premier minimal**

On a $\mathbf{C} = \mathbf{A}/\mathfrak{a} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$, deux anneaux réduits. Pour montrer que $\mathbf{C}$ est trivial, il suffit de montrer que $\mathbf{C}$ vérifie, avec la matrice P mod $\mathfrak{a}$, les hypothèses DU lemme.
Considérons donc $a \in \mathbf{A}$ tel que $\operatorname{Im} P$ soit libre sur $\mathbf{C}[1/a][\underline{X}]$.
Notons $\mathbf{C}[1/a] = \mathbf{L} \subseteq \mathbf{C}'[1/a] = \mathbf{L}'$.
Si x est un objet défini sur $\mathbf{A}$ notons $\overline{x}$ ce qu'il devient après le changement de base $\mathbf{A} \to \mathbf{L}'$.
Le module $\overline{M}$ est libre sur $\mathbf{L}[\underline{X}]$ et cela implique, par unicité (lemme 2), vu que $f_1(0) = g_1(0) = 1$ et que $\mathbf{L}$ est réduit, que les $\overline{f_i}$ et $\overline{g_j}$ sont dans $\mathbf{L}[\underline{X}]$.
Cela signifie qu'il existe $N \in \mathbb{N}$ tel que les $a^N f_i$ et $a^N g_j$ sont à coefficients dans $\mathbf{A}$. D'après les lemmes 5 et 6, ceci implique que $a \in \mathfrak{a}$, donc $a = 0$ dans $\mathbf{C}$.

Démonstration DU lemme

Démonstration

Une preuve classique serait la suivante.

Supposons $\mathbf{C}$ non trivial et soit $\mathfrak{p}$ un idéal premier minimal.

Puisque $\mathbf{C}$ est réduit, $\mathbf{C}_{\mathfrak{p}}$ est un corps. Donc $\operatorname{Im} P$ est libre sur $\mathbf{C}_{\mathfrak{p}}[\underline{X}]$.

Cela signifie $m_{i,j} = f_i g_j$ pour tous i, j avec les f_i et $g_j \in \mathbf{C}_{\mathfrak{p}}[\underline{X}]$.

Il existe donc un $a \notin \mathfrak{p}$ tel que les f_i et g_j sont dans $\mathbf{C}[1/a][\underline{X}]$.

Donc $a = 0$ ce qui est une contradiction.

démonstration DU lemme (suite)

Il semble qu'on n'ait pas beaucoup progressé !

On a un lemme d'élimination de l'idéal premier minimal. Mais la preuve du lemme d'élimination utilise un idéal premier minimal !

N'est-ce pas une mauvaise plaisanterie ?

Non, car la preuve du lemme peut être relue en utilisant l'idéal premier minimal de manière purement idéale, de façon dynamique.

démonstration DU lemme (suite)

Imaginons que l'anneau $\mathbf{C}$ soit un corps, c'est-à-dire qu'on ait déjà fait la localisation en un premier minimal.
Alors les f_i et g_j sont calculés selon un algorithme qu'on déduit des preuves constructives données auparavant pour le cas des corps.

Cet algorithme utilise la disjonction a **est nul ou inversible**, pour les éléments a qui sont produits par l'algorithme à partir des coefficients des $m_{i,j}$. Comme $\mathbf{C}$ est seulement un anneau réduit, sans test d'égalité à 0 ni test d'inversibilité, l'algorithme pour les corps, si on l'exécute avec $\mathbf{C}$, doit être remplacé par un arbre dans lequel on ouvre deux branches chaque fois qu'une question a **est-il nul ou inversible ?** est posée par l'algorithme.

démonstration DU lemme (suite)

Nous voici en face d'un arbre, gigantesque, mais fini.

Disons que systématiquement on a mis la branche « a inversible » à gauche, et la branche « $a = 0$ à droite ».

Nous voulons montrer que $\mathbf{C} = 0$.

Regardons José Bové !
Pardon, je voulais dire la branche d'extrême gauche.
On a inversé successivement $a_1, \ldots, a_n$ et le module P est devenu libre sur $\mathbf{C}[1/(a_1 \cdots a_n)][\underline{X}]$.

Conclusion : dans l'anneau C, on a $a_1 \cdots a_n = 0$.

démonstration DU lemme (suite)

Remontons d'un cran.
Dans l'anneau $\mathbf{C}[1/(a_1 \cdots a_{n-1})]$, nous savons que $a_n = 0$.
La branche de gauche n'aurait pas du être ouverte. Regardons le calcul dans la branche $a_n = 0$.
Suivons à partir de là la branche d'extrême gauche.
On a inversé $a_1, \ldots, a_{n-1}$, puis, disons $b_1, \ldots, b_k$ (si $k = 0$ convenons que $b_k = a_{n-1}$).
Et le module P est devenu libre sur $\mathbf{C}[1/(a_1 \cdots b_k)][\underline{X}]$.

Conclusion : dans l'anneau C, on a $a_1 \cdots b_k = 0$.

Et ainsi de suite. Quand on poursuit le processus jusqu'au bout, toutes les branches finissent par mourir et le module P est donc libre sur $\mathbf{C}[\underline{X}] = \mathbf{C}[1/1][\underline{X}]$. Donc $1 = 0$.

Ceci termine la preuve constructive du cas intègre !

Remarque sur le parcours de l'arbre

Notez qu'en fait, le calcul qui sera fait n'aura pas besoin de commencer par écrire l'arbre gigantesque.

Il suffit de suivre la branche d'extrême gauche, remonter d'un cran, aller à droite (une seule fois), puis suivre de nouveau la branche d'extrême-gauche et ainsi de suite.

En pratique on peut espérer que l'espace mémoire ne sera pas saturé, contrairement à ce qui se serait passé si on avait commencé par mettre en place l'arbre tout entier.

Et dans le cas réduit ?

En mathématiques classiques on dirait : tout anneau réduit peut être considéré comme un sous anneau d'un produit de corps. Par exemple le produit des localisés en tous les idéaux premiers minimaux.

Le résultat pour les corps s'étend facilement aux produits de corps.

Alors on recopie la preuve du cas

« $\mathbf{A}$ intègre (sous anneau d'un corps $\mathbf{K}$) »

pour le cas

« $\mathbf{A}$ réduit sous anneau de $\mathbf{K}$, produit de corps ».

Quasi inverses.

En mathématiques constructives, on n'a pas accès l'anneau $\mathbf{K}$ (le produit de corps en question). Mais on a accès au sous anneau $\mathbf{L} \subseteq \mathbf{K}$ engendré par $\mathbf{A}$ et par les **quasi inverses** des éléments de $\mathbf{A}$.

Dans un anneau commutatif $\mathbf{C}$, deux éléments a et b sont dits *quasi inverses* si on a :

$$a^2 b = a, \qquad b^2 a = b$$

On dit aussi que b est *le* quasi inverse de a. On vérifie en effet qu'il est unique.

Un anneau dans lequel tout élément admet un quasi inverse est appelé **Von Neuman régulier**, ou absolument plat, ou zéro-dimensionnel réduit. Ces quasi corps sont les anneaux les plus proches des corps.

Un anneau Von Neuman régulier ressemble tellement à un corps, que la preuve du cas des corps se transfère sans problème.

Alors on recopie la preuve du cas

« $\mathbf{A}$ intègre (sous anneau d'un corps $\mathbf{K}$) »

pour le cas

« $\mathbf{A}$ réduit sous anneau de $\mathbf{L}$, Von Neuman régulier ».

Merci de votre attention