Anneaux seminormaux (d'après Thierry Coquand)

Henri Lombardi (*), Claude Quitté (†)

septembre 2006

Résumé

Le théorème de Traverso-Swan affirme qu'un anneau réduit $\mathbf{A}$ est seminormal si et seulement si l'homomorphisme naturel $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[X]$ est un isomorphisme ([18, 17]). Nous exposons ici la preuve constructive élémentaire de ce résultat qui a été donnée par Thierry Coquand dans [2].

Cet exemple est paradigmatique de la méthode constructive. On obtient au bout du compte une preuve plus simple que la preuve classique initiale. Mais le plus important est que l'argument classique « par l'absurde et au moyen d'un objet idéal » peut être décrypté selon une technique générale qui s'inspire de la philosophie suivante : l'utilisation des objets purement idéaux construits avec l'axiome du choix et le principe du tiers exclu peut être remplacée par celle d'objets concrets qui sont des approximations finies de ces objets idéaux.

Introduction

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 dans *Dernières pensées*, Flammarion.

Le théorème de Traverso-Swan affirme qu'un anneau réduit $\mathbf{A}$ est seminormal si et seulement si l'homomorphisme naturel $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[X]$ est un isomorphisme ([18, 17]).

Nous exposons ici la preuve constructive élémentaire de ce résultat qui a été donnée par Thierry Coquand dans [2].

* Equipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE, email : lombardi@math.univ-fcomte.fr.

† Laboratoire de Mathématiques, SP2MI, Boulevard 3, Teleport 2, BP 179, 86960 FUTUROSCOPE Cedex, FRANCE, email : quitte@mathlabo.univ-poitiers.fr

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

Le décryptage se fait alors avec la « méthode dynamique » qui permet de gérer à la fois le tiers exclu à l'œuvre dans le raisonnement par l'absurde et l'objet idéal que constitue l'idéal premier minimal générique présent dans la preuve classique.

Cet exemple est paradigmatique d'une méthode constructive mise au point récemment, selon une technique générale qui s'inspire de la philosophie suivante : l'utilisation des objets purement idéaux construits avec l'axiome du choix et le principe du tiers exclu peut être remplacée par celle *d'objets concrets qui sont des approximations finies de ces objets idéaux*.

L'histoire commence avec le système de calcul formel D5 [9] dans lequel est mis en évidence qu'on peut calculer dans la cloture algébrique d'un corps, même si on ne sait pas la construire comme un objet mathématique usuel. Ainsi était donnée une signification constructive claire à l'objet idéal « cloture algébrique ».

Dans l'article [8] est expliqué comment on peut interpréter les preuves abstraites des résultats de type Nullstellensatz données via la théorie des modèles. Ici les objets idéaux sont les modèles d'une théorie formelle cohérente (ces modèles existent en vertu d'une version affaiblie de l'axiome du choix). Dans la preuve devenue constructive, chacun de ces objets idéaux est remplacé par « une information finie concernant l'objet idéal ».

Dans [5, 7], les chaînes d'idéaux premiers qui interviennent dans la définition abstraite de la dimension de Krull d'un anneau $\mathbf{A}$ sont remplacées par des suites finies d'éléments de l'anneau. Ainsi est obtenue une définition constructive élémentaire de la dimension de Krull, dans laquelle les idéaux premiers ont été totalement éliminés. Pour les anneaux usuellement utilisés en mathématiques la définition constructive de la dimension de Krull devient un outil algorithmique, même quand ne sont pas disponibles les facilités apportées par les bases de Gröbner. En particulier de grands théorèmes d'algèbre commutative qui utilisent la dimension de Krull ont été complètement décryptés constructivement dans [3, 6]. C'est le cas pour le « splitting-off » de Serre, les théorèmes « stable range » et « de simplification » de Bass, et le théorème de Forster-Swan. En outre la version constructive qui a été mise au point égale ou améliore les meilleures versions classiques de ces théorèmes, obtenues par R. Heitmann dans son remarquable article « non nœthérien » de 1984 [12].

Signalons enfin que dans [19], I. Yengui a montré comment éliminer l'utilisation des idéaux maximaux dans les preuves classiques pour les rendre constructives et a ainsi apporté un raffinement essentiel à la méthode dynamique.

Dans l'exemple qui est traité ici, on obtient au bout du compte une preuve élégante plus simple que la preuve classique initiale. Mais le plus important est que l'argument classique « par l'absurde et au moyen d'un objet idéal » peut être décrypté selon la méthode générale ci-dessus. Considérer la localisation en un idéal premier minimal $\mathfrak{p}$ générique est remplacé par un calcul arborescent où on essaie de rendre inversibles le maximum d'éléments qui se présentent comme obstacles à la preuve. L'arborescence provient du fait que dans la preuve classique, on utilise un argument du type « tout élément x est dans $\mathfrak{p}$ ou hors de $\mathfrak{p}$ ». Comme l'idéal premier est minimal, a priori x doit être hors de $\mathfrak{p}$, et ce n'est que lorsque le calcul montre qu'on a inversé 0 qu'on revient en arrière pour ouvrir une autre branche du calcul.

Nous expliquons la transformation de preuve mise en œuvre dans le cas intègre. Nous donnons en annexe une preuve détaillée du cas d'un anneau seminormal arbitraire.

1 Préliminaires

A, **B**, **C** désignent des anneaux commutatifs.
Si on ne précise pas un homomorphisme est un homomorphisme d'anneaux.

Anneaux seminormaux

Un anneau intègre **A** est dit *seminormal* si lorsque $b^2 = c^3 \neq 0$ alors l'élément $a = b/c$ du corps des fractions est en fait dans **A**. Notons que $a^3 = b$ et $a^2 = c$.

Un anneau quelconque **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 **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 1.1 *Dans un anneau réduit $x^2 = y^2$ et $x^3 = y^3$ impliquent $x = y$.*

En conséquence le a ci-dessus est toujours unique. En outre $\operatorname{Ann} b = \operatorname{Ann} c = \operatorname{Ann} a$.

Catégorie des A-modules projectifs de type fini

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 **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 la catégorie des modules projectifs de type fini sur **A** est équivalente à la catégorie dont les objets sont les matrices carrées idempotentes à coefficients dans **A**, un morphisme de P vers Q étant une matrice H de format convenable telle que $QH = H = HP$. En particulier l'identité de P est représentée par P.

Fait 1.2 *Si M et N sont représentés par les matrices idempotentes $P = (p_{i,j})_{i,j\in I} \in \mathbf{A}^{I\times I}$ et $Q = (q_{k,\ell})_{k,\ell\in J} \in \mathbf{A}^{J\times J}$, alors :*

1. *La somme directe $M \oplus N$ est représentée par* $\operatorname{Diag}(P, Q) = \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}$.
2. *Le produit tensoriel $M \otimes N$ est représenté par le produit de Kronecker $P \otimes Q = (r_{(i,k),(j,\ell)})_{(i,k),(j,\ell)\in I\times J}$, où $r_{(i,k),(j,\ell)} = p_{i,j}q_{k,\ell}$.*
3. *M et N sont isomorphes si et seulement si les matrices* $\operatorname{Diag}(P, 0_n)$ *et* $\operatorname{Diag}(0_m, Q)$ *sont semblables*

Le dernier point se vérifie en remarquant que la projection sur M dans $M \oplus M' \oplus \mathbf{A}^n$ est représentée par la matrice $\operatorname{Diag}(P, 0_n)$ tandis que la projection sur N dans $\mathbf{A}^m \oplus N \oplus N'$ est représentée par la matrice $\operatorname{Diag}(0_m, Q)$, et en décomposant $\mathbf{A}^m \oplus \mathbf{A}^n$ sous la forme $M \oplus M' \oplus N \oplus N'$ on voit que les deux projections sont conjuguées par l'automorphisme qui échange M et N.

Rang d'un module projectif de type fini

Si $\varphi : M \to M$ est un endomorphisme du $\mathbf{A}$-module projectif de type fini M image de la matrice idempotente P et si H représente φ (avec $H = PH = HP$), soit $N = \operatorname{Ker} P$ de sorte que $M \oplus N = \mathbf{A}^n$. Alors on peut définir le déterminant de φ par $\det(\varphi) = \det(\varphi \oplus \mathrm{Id}_n) = \det(H + (\mathrm{I}_n - P))$.

Soit μ_X la multiplication par X dans le $\mathbf{A}[X]$-module $M[X]$ (ce module, étendu de M depuis $\mathbf{A}$, est également représenté par la matrice P), alors $\det(\mu_X) = \mathrm{R}_M(X) = r(X)$ est un polynome qui vérifie $r(XY) = r(X)r(Y)$ et $r(1) = 1$. En d'autres termes ses coefficients forment un système fondamental d'idempotents orthogonaux. Le module est dit de rang k si $r(X) = X^k$.

Un calcul direct montre le fait suivant.

Fait 1.3 *Une matrice $P = (p_{i,j})$ a pour image un module projectif de rang constant 1 si et seulement si les deux propriétés suivantes sont vérifiées*

- $\bigwedge^2 P = 0$, *c'est-à-dire tous les mineurs d'ordre 2 sont nuls,*
- $\operatorname{Tr} P = \sum_i p_{ii} = 1$.

Quand l'image d'une matrice de projection est libre

Si $P \in \mathbf{A}^{n\times n}$ est une matrice de projection dont l'image est libre de rang r, son noyau n'est pas automatiquement libre, et la matrice n'est donc pas à tout coup semblable à la matrice standard $\mathrm{I}_{n,r} = \mathrm{Diag}(\mathrm{I}_r, 0_{n-r}) = \begin{bmatrix} \mathrm{I}_r & 0 \\ 0 & 0_{n-r} \end{bmatrix}$.

Il est intéressant de savoir caractériser simplement le fait que l'image est libre.

Proposition 1.4 *Soit $P \in \mathbf{A}^{n\times n}$. La matrice P est idempotente et d'image libre de rang r si et seulement si il existe deux matrices $X \in \mathbf{A}^{n\times r}$ et $Y \in \mathbf{A}^{r\times n}$ telles que $YX = \mathrm{I}_r$ et $P = XY$. En outre,*

1. $\operatorname{Im} P = \operatorname{Im} X \simeq \operatorname{Im} Y$.
2. *Pour toutes matrices X', Y' de mêmes formats que X et Y et telles que $P = X'Y'$, il existe une unique matrice $U \in \mathsf{GL}_r(\mathbf{A})$ telle $X' = XU$ et $Y = UY'$. En fait $U = YX'$, $U^{-1} = Y'X$, $Y'X' = \mathrm{I}_r$ et les colonnes de X' forment une base de* $\operatorname{Im} P$.

Une autre caractérisation possible est la suivante : la matrice $\mathrm{Diag}(P, 0_r)$ *est semblable à la matrice de projection standard* $\mathrm{I}_{n+r,r}$.

Démonstration.
Supposons que $\operatorname{Im} P$ est libre de rang r. Pour colonnes de X on prend une base de $\operatorname{Im} P$. Alors, il existe une unique matrice Y telle que $P = XY$. Puisque $PX = X$ (car $P^2 = P$) on a $XYX = X$. Puisque les colonnes de X sont indépendantes et que $(\mathrm{I}_r - YX)X = 0$ on a $\mathrm{I}_r = YX$.
Supposons $YX = \mathrm{I}_r$ et $P = XY$. Alors $P^2 = XYXY = X\mathrm{I}_r Y = XY = P$ et $PX = XYX = X$. Donc $\operatorname{Im} P = \operatorname{Im} X$. En outre les colonnes de X sont indépendantes car $XZ = 0$ implique $Z = YXZ = 0$.
1) La suite $\mathbf{A}^n \xrightarrow{\mathrm{I}_n - P} \mathbf{A}^n \xrightarrow{Y} \mathbf{A}^r$ est exacte : en effet $Y(\mathrm{I}_n - P) = 0$ et si $YZ = 0$ alors $PZ = 0$ donc $Z = (\mathrm{I}_n - P)Z$. Ainsi $\operatorname{Im} Y \simeq \mathbf{A}^n/\operatorname{Ker} Y = \mathbf{A}^n/\operatorname{Im}(\mathrm{I}_n - P) \simeq \operatorname{Im} P$.
2) Si maintenant X', Y' sont de mêmes formats que X, Y et $P = X'Y'$, on pose $U = YX'$ et $V = Y'X$. Alors $UV = YX'Y'X = YPX = YX = \mathrm{I}_r$; $X'V = X'Y'X = PX = X$, donc $X' = XU$; $UY' = YX'Y' = YP = Y$, donc $Y' = VY$. Enfin $Y'X' = VYXU = VU = \mathrm{I}_r$.

Concernant la dernière caractérisation il s'agit d'une simple application du point 3 dans le fait 1.2. □

Nous résumons la situation pour les modules projectifs de rang constant 1.

Lemme 1.5 *Une matrice de projection de rang* 1, P, *a son image libre si et seulement si il existe un vecteur colonne* x *et un vecteur ligne* y *tels que* $yx = 1$ *et* $xy = P$. *En outre* x *et* y *sont uniques, au produit par une unité près, sous la seule condition que* $xy = P$.

Le semi anneau de Grothendieck $\mathsf{GK}_0\,\mathbf{A}$ et le groupe de Picard $\mathsf{Pic}\,\mathbf{A}$

$\mathsf{GK}_0\,\mathbf{A}$ est l'ensemble des classes d'isomorphisme de modules projectifs de type fini sur $\mathbf{A}$. C'est un semi anneau pour les lois héritées de $\oplus$ et $\otimes$.

Puisque $\mathbf{A}$ est supposé commutatif, le sous semi anneau de $\mathsf{GK}_0\,\mathbf{A}$ engendré par 1 (la classe du module projectif de type fini $\mathbf{A}$) est isomorphe à $\mathbb{N}$, sauf dans le cas où $\mathbf{A}$ est l'anneau trivial.

Tout élément de $\mathsf{GK}_0\,\mathbf{A}$ peut être représenté par une matrice idempotente à coefficients dans $\mathbf{A}$.

$\mathsf{Pic}\,\mathbf{A}$ est le sous ensemble de $\mathsf{GK}_0\,\mathbf{A}$ formé par les classes d'isomorphisme des modules projectifs de rang constant 1. Il s'agit d'un groupe pour la multiplication. L'« inverse » de M est le dual de M. Si $M \simeq \operatorname{Im} P$, alors $M^\star \simeq \operatorname{Im} {}^tP$. En particulier, si P est une matrice de projection de rang 1, $P \otimes {}^tP$ est une matrice de projection dont l'image est un module libre de rang 1.

On peut d'ailleurs vérifier directement cette propriété en utilisant la caractérisation donnée au lemme 1.5.

Rapport entre $\mathsf{Pic}\,\mathbf{A}$ et les classes d'idéaux inversibles

Un idéal $\mathfrak{a}$ de $\mathbf{A}$ est dit *inversible* s'il existe un idéal $\mathfrak{b}$ tel que $\mathfrak{ab} = a\mathbf{A}$ où a est un élément régulier. Dans ce cas il existe $x_1, \ldots, x_n$ et $y_1, \ldots, y_n$ dans $\mathbf{A}$ tels que $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$, $\mathfrak{b} = \langle y_1, \ldots, y_n\rangle$ et $\sum_i x_i y_i = a$. En outre pour tous i, j il existe un unique $m_{i,j}$ tel que $y_i x_j = a m_{i,j}$ On en tire que la matrice $(m_{i,j})$ est une matrice idempotente de rang 1, et que son image est isomorphe à $\mathfrak{a}$ en tant que $\mathbf{A}$-module.

Deux idéaux inversibles $\mathfrak{a}, \mathfrak{b}$ sont isomorphes en tant que $\mathbf{A}$-modules si et seulement si il existe a, b réguliers tels que $a\mathfrak{a} = b\mathfrak{b}$. Ceci permet de définir le groupe des classes d'idéaux inversibles comme sous-groupe de $\mathsf{Pic}\,\mathbf{A}$. En fait la plupart du temps les deux groupes coïncident.

Par exemple si $\mathbf{A}$ est intègre, toute matrice $(a_{i,j})$ idempotente de rang 1 a un élément régulier sur la diagonale et les coefficients de la ligne correspondante engendrent un idéal inversible isomorphe à l'image de la matrice.

Changement d'anneau de base

Si on a un homomorphisme $\mathbf{A} \xrightarrow{\rho} \mathbf{B}$, l'extension des scalaires de $\mathbf{A}$ à $\mathbf{B}$ transforme un module projectif de type fini M sur $\mathbf{A}$ en un module projectif de type fini $\rho_\star(M)$ sur $\mathbf{B}$. Tout $\mathbf{B}$-module isomorphe à un tel module $\rho_\star(M)$ est dit « étendu » depuis $\mathbf{A}$.

Du point de vue matrices de projection, cela correspond à considérer la matrice transformée par l'homomorphisme ρ.

Cela donne un homomorphisme $\mathsf{GK}_0\,\rho : \mathsf{GK}_0\,\mathbf{A} \to \mathsf{GK}_0\,\mathbf{B}$. D'où le problème qui se pose naturellement : « tout module projectif de type fini sur $\mathbf{B}$ provient-il d'un module projectif de type fini sur $\mathbf{A}$? ». Ou encore : « $\mathsf{GK}_0\,\rho$ est il surjectif ? ».

Par exemple si $\mathbf{Z}$ est le sous anneau de $\mathbf{A}$ engendré par $1_{\mathbf{A}}$, on sait que tous les modules projectifs de rang constant sur $\mathbf{Z}$ sont libres, et la question « les $\mathbf{A}$-modules projectifs de rang constant sont-ils tous étendus depuis $\mathbf{Z}$? » est équivalente à « tous les $\mathbf{A}$-modules projectifs de rang constant sont-ils libres ? ».

Dans le cas $\mathbf{B} = \mathbf{A}[X_1, \ldots, X_m] = \mathbf{A}[\underline{X}]$, on a de plus l'homomorphisme d'évaluation en 0, $\mathbf{B} \xrightarrow{\theta} \mathbf{A}$, avec $\theta \circ \rho = \mathrm{Id}_{\mathbf{A}}$. On en déduit que le $\mathbf{B}$-module projectif de type fini $M = M(\underline{X})$ est étendu si et seulement si il est isomorphe à $M(0) = \theta_\star(M)$.

En ce qui concerne les matrices de projection, une matrice idempotente $P \in \mathbf{B}^{n\times n}$ représente un module étendu depuis $\mathbf{A}$ si et seulement si son image est isomorphe à l'image de $P(0)$.

Si tous les $\mathbf{B}$-modules projectifs de type fini sont étendus depuis $\mathbf{A}$ alors P doit être semblable à $P(0)$, mais ceci peut s'avérer plus difficile à démontrer directement que l'isomorphisme des images.

Concernant les Pic on a les deux homomorphismes de groupe $\mathsf{Pic}\,\mathbf{A} \xrightarrow{\mathsf{Pic}\,\rho} \mathsf{Pic}\,\mathbf{A}[\underline{X}] \xrightarrow{\mathsf{Pic}\,\theta} \mathsf{Pic}\,\mathbf{A}$ qui se composent selon l'identité. Le premier est injectif, le second surjectif, et ce sont des isomorphismes si et seulement si le premier est surjectif, si et seulement si le second est injectif.

Cette dernière propriété signifie : toute matrice $P(\underline{X})$ idempotente de rang 1 sur $\mathbf{A}[\underline{X}]$, vérifiant « $\mathrm{Im}(P(0))$ est libre », vérifie elle-même « $\mathrm{Im}(P(\underline{X}))$ est libre ».

En fait si $\mathrm{Im}(P(0))$ est libre, alors la matrice diagonale par blocs $\mathrm{Diag}(P(0), 0_1)$ est semblable à une matrice de projection standard $\mathrm{I}_{n,1}$. Comme $\mathrm{Im}(\mathrm{Diag}(P(\underline{X}), 0_1))$ est isomorphe à $\mathrm{Im}\, P(\underline{X})$, on obtient le résultat qui suit.

Lemme 1.6 *Les propriétés suivantes sont équivalentes :*

1. *L'homomorphisme naturel* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ *est un isomorphisme,*
2. *Pour toute matrice* $P(\underline{X}) \in \mathbf{A}[\underline{X}]^{n\times n} = (m_{i,j}(\underline{X}))_{i,j\in 1,\ldots,n}$ *idempotente de rang 1 vérifiant* $P(0) = \mathrm{I}_{n,1}$*, il existe* $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{A}[\underline{X}]$ *tels que* $m_{i,j} = f_i g_j$ *pour tous* i, j*.*

Seuls importent les anneaux réduits : $\mathsf{GK}_0\,\mathbf{A}_{\mathrm{red}} = \mathsf{GK}_0\,\mathbf{A}$

Nous notons $\mathbf{A}_{\mathrm{red}}$ l'anneau réduit associé à $\mathbf{A}$, c'est-à-dire $\mathbf{A}/\sqrt{0}$.

Proposition 1.7 *L'application naturelle* $\mathsf{GK}_0(\mathbf{A}) \to \mathsf{GK}_0(\mathbf{A}_{\mathrm{red}})$ *est bijective.*

1. *Injectivité : cela signifie que si deux modules projectifs de type fini* E, F *sur* $\mathbf{A}$ *sont isomorphes sur* $\mathbf{A}_{\mathrm{red}}$*, ils le sont également sur* $\mathbf{A}$*.*
2. *De manière plus précise si deux matrices idempotentes* P, Q *de même format sont conjuguées sur* $\mathbf{A}_{\mathrm{red}}$*, elles le sont également sur* $\mathbf{A}$*, via un isomorphisme qui relève l'isomorphisme de conjugaison résiduel.*
3. *Surjectivité : tout module projectif de type fini sur* $\mathbf{A}_{\mathrm{red}}$ *provient d'un module projectif de type fini sur* $\mathbf{A}$*.*

Démonstration.
2) On note $\overline{x}$ l'objet x vu modulo $\sqrt{0}$. Soit $C \in \mathbf{A}^{n\times n}$ une matrice telle que $\overline{C}$ conjuque $\overline{P}$ à $\overline{Q}$. Puisque $\det C$ est inversible modulo $\sqrt{0}$, $\det C$ est inversible dans $\mathbf{A}$ et $C \in \mathsf{GL}_n(\mathbf{A})$. On a donc $\overline{Q} = \overline{C\,P\,C^{-1}}$. Quitte à remplacer P par $C\,P\,C^{-1}$ on peut supposer $\overline{Q} = \overline{P}$. Alors PQ code une application $\mathbf{A}$-linéaire de $\mathrm{Im}\, P$ vers $\mathrm{Im}\, Q$ qui donne résiduellement l'identité. De même $(\mathrm{I}_n - P)(\mathrm{I}_n - Q)$ code une application $\mathbf{A}$-linéaire de $\mathrm{Ker}\, P$ vers $\mathrm{Ker}\, Q$ qui donne résiduellement l'identité. On considère alors la matrice $A = PQ + (\mathrm{I}_n - P)(\mathrm{I}_n - Q)$ qui réalise $AQ = PQ = PA$ (vérification immédiate) et $\overline{A} = \mathrm{I}_n$: ainsi A est inversible et relève l'isomorphisme de conjugaison résiduel.
1) Pour deux modules projectifs de type fini résiduellement isomorphes $E \simeq \mathrm{Im}\, P$ et $F \simeq \mathrm{Im}\, Q$ on réalise E et F comme images de matrices idempotentes de même format et résiduellement conjuguées : $\mathrm{Diag}(P, 0_m)$ et $\mathrm{Diag}(0_n, Q)$ avec $\mathrm{Diag}(\overline{P}, 0_m)$ semblable à $\mathrm{Diag}(0_n, \overline{Q})$. Puis on applique le point 1.

3) On a la possibilité de relever tout module projectif de type fini grâce à la méthode de Newton. Plus précisément soit $\mathfrak{a}$ l'idéal engendré par les coefficients de $P^2 - P$. Si $\mathfrak{a}$ est contenu dans le nilradical de $\mathbf{A}$, il existe k tel que $\mathfrak{a}^{2^k} = 0$. Par ailleurs si $Q = 3P^2 - 2P^3$, alors $Q \equiv P \bmod \mathfrak{a}$ et $Q^2 - Q$ est multiple de $(P^2 - P)^2$ donc a ses coefficients dans $\mathfrak{a}^2$. Il suffit donc d'itérer k fois l'affectation $P \leftarrow 3P^2 - 2P^3$ pour obtenir le résultat souhaité. □

Corollaire 1.8 *L'homomorphisme canonique* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ *est un isomorphisme si et seulement si l'homomorphisme canonique* $\mathsf{Pic}\,\mathbf{A}_{\mathrm{red}} \to \mathsf{Pic}\,\mathbf{A}_{\mathrm{red}}[\underline{X}]$ *est un isomorphisme.*

Convention 1.9 *Dans la suite nous abrégeons la phrase « l'homomorphisme canonique* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ *est un isomorphisme » en disant (par abus) «* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ *».*

Éléments inversibles de $\mathbf{A}[\underline{X}]$

Lemme 1.10 *Si* $\mathbf{A}$ *est réduit l'homomorphisme de groupes* $\mathbf{A}^\times \to (\mathbf{A}[\underline{X}])^\times$ *est un isomorphisme. Autrement dit si* $f(\underline{X}) \in \mathbf{A}[\underline{X}]$ *est inversible, alors* $f = f(0) \in \mathbf{A}^\times$.

Il suffit de faire la preuve en une variable, et elle résulte d'un calcul direct : si $f(X)g(X) = 1$ avec $\deg(f) \leq m$, $m \geq 1$, on montre que le coefficient de degré m dans f est nilpotent.

Le théorème de Kronecker

Théorème 1.11 *Soient* $f, g \in \mathbf{A}[\underline{X}]$ *et* $h = fg$. *Soit* a *un coefficient de* f *et* b *un coefficient de* g, *alors* ab *est entier sur le sous anneau de* $\mathbf{A}$ *engendré par les coefficients de* h.

En utilisant « l'astuce de Kronecker » (remplacer chaque variable X_k par T^{m^k} pour un m suffisamment grand) il suffit de le montrer pour des polynomes en une variable. Avec deux polynomes de degré 1 en une variable, on voit le résultat à l'œil nu. Avec deux polynomes de degré 2, on voit que ce n'est pas si simple. Néanmoins des preuves constructives existent dans la littérature (cf. [10, 13], et pour un article de synthèse [4]).

2 Théorème de Traverso-Swan. Le cas intègre.

La condition est nécessaire : l'exemple de Schanuel

On montre que si $\mathbf{A}$ est réduit et $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[X]$ alors $\mathbf{A}$ est seminormal. On utilise la caractérisation donnée dans le lemme 1.5.

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

Cas d'un anneau à pgcd

Rappelons qu'un anneau (intègre) à pgcd est un anneau dans lequel deux éléments arbitraires admettent un plus grand commun diviseur, c'est-à-dire une borne supérieure pour la relation de divisibilité. Rappelons aussi que si $\mathbf{A}$ est un anneau à pgcd, il en va de même pour l'anneau des polynomes $\mathbf{A}[\underline{X}]$.

Lemme 2.1 *Si* $\mathbf{A}$ *est un anneau intègre à pgcd,* $\mathsf{Pic}\,\mathbf{A} = \{1\}$.

Remarque. En conséquence $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\underline{X}]$ est un isomorphisme. Notez que le résultat s'applique si $\mathbf{A}$ est un corps discret.

Démonstration.
On utilise la caractérisation donnée dans le lemme 1.5. Soit $P = (m_{i,j})$ une matrice idempotente de rang 1. Puisque $\sum_i m_{i,i} = 1$ 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 $m_{i,j} = f_i g_j$. □

Cas d'un anneau intègre normal

Lemme 2.2 *Si* $\mathbf{A}$ *est intègre et intégralement clos, alors* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.

Démonstration.
On utilise la caractérisation donnée au lemme 1.6. 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 $\operatorname{Im} P(\underline{X})$ est libre et 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. En outre puisque $f_1(0)g_1(0) = 1$ et puisqu'on peut modifier f et g en les multipliant par une unité, 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 $m_{1,j}$. De même les coefficients des f_i sont entiers sur l'anneau engendré par les coefficients des $m_{i,1}$. Mais on suppose $\mathbf{A}$ intégralement clos, donc les f_i et les g_j sont dans $\mathbf{A}[\underline{X}]$. □

Cas d'un anneau intègre seminormal

Traverso [18] avait démontré le théorème dans le cas d'un anneau nœthérien réduit $\mathbf{A}$ (avec une restriction supplémentaire). Pour le cas intègre sans hypothèse nœthérienne on peut consulter [15, 1, 11].

Théorème 2.3 *Si* $\mathbf{A}$ *est intègre et seminormal, alors* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.

Démonstration.
On commence la preuve comme celle du lemme 2.2. 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 $f_1(0) = g_1(0) = 1$. On appelle $\mathbf{B}$ le sous anneau de $\mathbf{K}$ engendré par $\mathbf{A}$ et par les coefficients des f_i et des g_j. Alors, vu 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 $\mathbf{A} = \mathbf{B}$. On appelle $\mathfrak{a}$ le conducteur de $\mathbf{A}$ dans $\mathbf{B}$, c'est-à-dire l'ensemble $\{x \in \mathbf{B} \mid x\mathbf{B} \subseteq \mathbf{A}\}$. C'est à la fois un idéal de $\mathbf{A}$ et $\mathbf{B}$. Notre but est maintenant de montrer $\mathfrak{a} = \langle 1 \rangle$, c'est-à-dire encore que $\mathbf{C} = \mathbf{A}/\mathfrak{a}$ est trivial.

Lemme 2.4 *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 du lemme 2.4.
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 $u^2c^2 \in \mathbf{A}$. Mais aussi $u^3c^3 = u^2(uc^3) \in \mathbf{A}$ 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 $uc \in \mathbf{A}$. □

Remarque. La *cloture seminormale* d'un anneau $\mathbf{A}$ dans un suranneau réduit $\mathbf{B}$ est obtenue en partant de $\mathbf{A}$ et en rajoutant les éléments x de $\mathbf{B}$ tels que x^2 et x^3 sont dans l'anneau préalablement construit. Notez que par le fait 1.1, x est uniquement déterminé par la donnée de x^2 et x^3. La preuve du lemme précédent peut alors être interprétée comme une démonstration de la variante suivante.

Lemme 2.5 *Soient* $\mathbf{A} \subseteq \mathbf{B}$ *réduit,* $\mathbf{A}_1$ *la cloture seminormale de* $\mathbf{A}$ *dans* $\mathbf{B}$, *et* $\mathfrak{a}$ *le conducteur de* $\mathbf{A}_1$ *dans* $\mathbf{B}$. *Alors* $\mathfrak{a}$ *est un idéal radical de* $\mathbf{B}$.

Lemme 2.6 *Soient* $\mathbf{A} \subseteq \mathbf{B}$, $\mathbf{B} = \mathbf{A}[c_1, \ldots, c_q]$ *réduit fini sur* $\mathbf{A}$ *et* $\mathfrak{a}$ *le conducteur de* $\mathbf{A}$ *dans* $\mathbf{B}$. *On suppose que* $\mathfrak{a}$ *est un idéal radical, alors il est égal à* $\{x \in \mathbf{A} \mid xc_1, \ldots, xc_q \in \mathbf{A}\}$.

Démonstration du lemme 2.6.
En effet si $xc_i \in \mathbf{A}$ alors $x^\ell c_i^\ell \in \mathbf{A}$ pour tout ℓ, et 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 $N = (d-1)q$). □

La fin de la démonstration du théorème 2.3 est maintenant donnée en mathématiques classiques. Supposons au contraire que $\mathfrak{a} \neq \langle 1 \rangle$. On a $\mathbf{C} = \mathbf{A}/\mathfrak{a} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$. Soit alors $\mathfrak{p}$ 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, $\operatorname{Im} \overline{P}$ est libre sur $\mathbf{L}[\underline{X}]$. Cela implique, par unicité (lemme 1.5) et vu que $f_1(0) = g_1(0) = 1$, que les $\overline{f_i}$ et $\overline{g_j}$ sont dans $\mathbf{L}[\underline{X}]$ (si $u(X) \in \mathbf{L}[\underline{X}]$ est inversible et $u(0) = 1$, alors $u = 1$). 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 2.6, ceci implique que $s \in \mathfrak{a}$, ce qui est absurde. □

La démonstration donnée ci-dessus pour le théorème 2.3 est une simplification des preuves existantes dans la littérature. Elle n'est cependant pas totalement constructive et elle ne traite que le cas intègre.

Preuve constructive (cas seminormal intègre)

Nous allons donner maintenant une preuve constructive du théorème 2.3.

On commence par remarquer que l'argument par l'absurde dans la preuve classique, peut être interprété comme un argument indirect, qui prouve que l'anneau $\mathbf{A}/\mathfrak{a}$ est trivial en disant, selon toute apparence : si l'anneau n'était pas trivial etc…, il serait trivial. Mais une fois remis à l'endroit, l'argument prouve directement que l'anneau voulu est trivial. On pourra lire à ce sujet le petit article de Richman sur l'anneau trivial ([16]).

Outre cette remarque plutôt anodine (le renversement d'une preuve directe en une preuve par l'absurde est très banal en mathématiques classiques), il nous faut un lemme qui permet d'éliminer l'usage de l'idéal premier premier minimal *purement idéal* qui intervient dans la preuve classique. Dans le processus de décryptage, ceci est le point le plus délicat.

Ce lemme dont l'énoncé est un peu déroutant a la signification intuitive suivante :
Soit $\mathbf{C}$ *un anneau réduit et* P *un module projectif de rang 1 sur* $\mathbf{C}[\underline{X}]$ *; si* $\mathbf{C}$ *n'est pas trivial, il doit y avoir une localisation non triviale* $S^{-1}\mathbf{C}$ *de* $\mathbf{C}$ *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 du cas intègre, 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 :
Soit $\mathbf{C}$ *un anneau réduit et* P *un module projectif de rang 1 sur* $\mathbf{C}[\underline{X}]$ *; si toute localisation* $S^{-1}\mathbf{C}$ *de* $\mathbf{C}$ *pour laquelle* P *devient libre est triviale, c'est que* $\mathbf{C}$ *lui-même est trivial.*
Et elle « est vraie » au sens des mathématiques constructives, c'est-à-dire qu'elle nous donne un algorithme !

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

Voici LE lemme crucial.

Lemme 2.7 (lemme d'élimination de l'idéal premier minimal)
Soit $\mathbf{C}$ *un anneau réduit et* $P = (m_{i,j}) \in \mathbf{C}[\underline{X}]^{n\times n}$ *une matrice idempotente de rang 1 telle que* $P(0) = \mathrm{I}_{n,1}$. *Supposons que l'implication suivante soit satisfaite :*

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

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

Preuve que le lemme 2.7 implique le théorème 2.3.
Nous pouvons reprendre à très peu près la fin de la preuve du théorème 2.3, qui utilisait un idéal premier minimal $\mathfrak{p}$. Le lecteur constatera que grâce AU lemme, on remplace simplement la localisation en $\mathfrak{p}$ par la localisation en un élément a.
On reprend la preuve du théorème à l'endroit où elle devenait non constructive. 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 1.5), 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 $\mathbf{L}[\underline{X}]$ (tenir compte du lemme 1.10).
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 2.4 et 2.6, ceci implique que $a \in \mathfrak{a}$, donc $a = 0$ dans $\mathbf{C}$. □

Preuve du lemme 2.7.
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 $\operatorname{Im} P$ devient libre sur $\mathbf{C}_{\mathfrak{p}}[\underline{X}]$. Cela implique qu'il existe un $a \notin \mathfrak{p}$ tel que $\operatorname{Im} P$ devient libre sur $\mathbf{C}[1/a][\underline{X}]$. Donc $a = 0$ ce qui est une contradiction.
On a un lemme d'élimination de l'idéal premier minimal. Mais la preuve du lemme d'élimination est une preuve par l'absurde qui 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. Voici ce que cela donne.
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 que l'on déduit des preuves constructives données auparavant pour le cas des corps.
Cet algorithme utilise la disjonction « a est nul ou a est 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.
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 ». Regardons ce qui se passe dans la branche d'extrême gauche.
On a inversé successivement a_1, …, a_n et le module P est devenu libre sur $\mathbf{C}[1/(a_1 \cdots a_n)][\underline{X}]$.
Conclusion : dans l'anneau $\mathbf{C}$, *on a* $a_1 \cdots a_n = 0$.
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, …, 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 $\mathbf{C}[1/(a_1 \cdots a_{n-1} b_1 \cdots b_k)][\underline{X}]$.
Conclusion : dans l'anneau $\mathbf{C}$, *on a* $a_1 \cdots a_{n-1} b_1 \cdots b_k = 0$. Remontons d'un cran : $b_k = 0$, la branche de gauche n'aurait pas du être ouverte. Regardons le calcul dans la branche $b_k = 0$…
Et ainsi de suite. Quand on poursuit le processus jusqu'au bout, on se retrouve à la racine de l'arbre avec le module P libre sur $\mathbf{C}[\underline{X}] = \mathbf{C}[1/1][\underline{X}]$. Donc $1 = 0$. □

En utilisant le lemme 2.5 à la place du lemme 2.4 on obtiendra le résultat suivant, plus précis que le théorème 2.3.

Théorème 2.8 *Si* $\mathbf{A}$ *est un anneau intègre et* M *un module projectif de rang* 1 *sur* $\mathbf{A}[\underline{X}]$, *il existe* $c_1, \ldots, c_m$ *dans le corps des fractions de* $\mathbf{A}$ *tels que :*

1. c_i^2 *et* c_i^3 *sont dans* $\mathbf{A}[(c_j)_{j<i}]$ *pour* $i = 1, \ldots, m$,
2. M *est libre sur* $\mathbf{A}[(c_j)_{j\leq m}][X]$.

Annexe : Anneaux zéro-dimensionnels réduits

Dans l'annexe, nous développons un peu la théorie des anneaux dimensionnels réduits, qui sont de bons substituts au corps.

Ceci permet d'obtenir le théorème de Traverso-Swan dans le cas général d'un anneau seminormal non nécessairement intègre.

En outre la preuve du lemme d'élimination de l'idéal premier premier minimal peut être débarrassée de l'arbre gigantesque qui pouvait faire peur. Celui-ci est caché dans les idempotents et la preuve semble plus présentable (mais c'est la même).

Remarque. L'idée de remplacer le corps des fractions de $\mathbf{A}$ par un anneau zéro-dimensionnel réduit contenant $\mathbf{A}$ n'est pas dans [17] : Swan utilise des arguments nettement plus sophitiqués pour ramener le cas général, non pas au cas intègre, mais au cas nœthérien. La preuve dans [2] opère donc des simplifications très nettes par rapport à la preuve classique initiale. En outre le théorème est nouveau dans le sens qu'il donne un algorithme là où auparavant, il y avait une affirmation purement abstraite.

A. Quelques faits de base

On dit qu'un anneau est *zéro-dimensionnel* lorsqu'il vérifie l'axiome suivant :

$$\forall x \in \mathbf{A}\ \exists a \in \mathbf{A}\ \exists d \in \mathbb{N} \qquad x^d = ax^{d+1} \tag{1}$$

Dans le cas réduit $d = 1$ suffit car $x^d(1 - xa) = 0$ implique $x(1 - xa) = 0$.
Dans un anneau commutatif $\mathbf{C}$, deux éléments a et b sont dits *quasi inverses* si on a :

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

On dit aussi que b est *le* quasi inverse de a. On vérifie en effet qu'il est unique : si $a^2b = a = a^2c$, $b^2a = b$ et $c^2a = c$, alors, puisque $ab = a^2b^2$, $ac = a^2c^2$ et $a^2(c - b) = a - a = 0$, on obtient

$$c - b = a(c^2 - b^2) = a(c - b)(c + b) = a^2(c - b)(c^2 + b^2) = 0$$

Par ailleurs si $x^2y = x$, on vérifie que xy^2 est quasi inverse de x. Ainsi :

Fait A.1 *Un anneau est zéro-dimensionnel réduit si et seulement si tout élément admet un quasi inverse.*

De tels anneaux sont aussi qualifiés de *absolument plats* ou encore de *von Neuman réguliers* (cette dernière expression est surtout utilisée dans le cas non commutatif, avec les équations $aba = a$ et $bab = b$).

Les anneaux zéro-dimensionnels réduits peuvent donc être vus comme des anneaux munis qu'une loi unaire supplémentaire $a \mapsto a^\bullet$ qui doit vérifier les axiomes

$$a^2\, a^\bullet = a, \quad a\,(a^\bullet)^2 = a^\bullet. \tag{2}$$

Ceux-ci impliquent notamment, en posant $e_a = aa^\bullet$,

$$\left.\begin{array}{lll} e_a^2 = e_a, & e_a a = a, & e_a a^\bullet = a^\bullet, \\ (a^\bullet)^\bullet = a, & (ab)^\bullet = a^\bullet\, b^\bullet, & 0^\bullet = 0, \\ 1^\bullet = 1, & (x \text{ régulier } \Leftrightarrow\ x\, x^\bullet = 1), & (x \text{ idempotent } \Leftrightarrow\ x = x^\bullet). \end{array}\right\} \tag{3}$$

On en déduit facilement :

Fait A.2 *Un anneau est zéro-dimensionnel réduit si et seulement si tout idéal de type fini est engendré par un idempotent.*

La notion d'anneau zéro-dimensionnel réduit est *la bonne généralisation équationnelle* de la notion de corps. La notion de corps ne peut pas être définie de manière purement équationnelle, mais un corps n'est rien d'autre qu'un anneau zéro-dimensionnel réduit *connexe* (c'est-à-dire avec 0 et 1 comme seuls idempotents).

Lemme A.3 *Soit $\mathbf{A} \subseteq \mathbf{C}$ avec $\mathbf{C}$ zéro-dimensionnel réduit et $a \in \mathbf{C}$. Notons $e_a = aa^\bullet$.*

1. *e_a est l'unique idempotent de $\mathbf{C}$ qui vérifie $\langle a \rangle = \langle e_a \rangle$. En outre $\mathrm{Ann}_{\mathbf{C}}(a) = \mathrm{Ann}_{\mathbf{C}}(e_a) = \langle 1 - e_a \rangle$*
2. *$\mathbf{C} = e_a\mathbf{C} \oplus (1 - e_a)\mathbf{C}$ avec $e_a\mathbf{C} \simeq \mathbf{C}[1/e_a] \simeq \mathbf{C}/\langle 1 - e_a \rangle$ et $(1 - e_a)\mathbf{C} \simeq \mathbf{C}/\langle e_a \rangle$*
   (NB : l'idéal $e_a\mathbf{C}$ n'est pas un sous anneau, mais c'est un anneau avec e_a pour élément neutre multiplicatif).
3. *Dans $e_a\mathbf{C}$, a est inversible et dans $\mathbf{C}/\langle e_a \rangle$, a est nul.*

4. *Si* $a \in \mathbf{A}$, *alors* $e_a\mathbf{A}[a^\bullet] \simeq \mathbf{A}[1/a]$.
5. *Plus généralement, avec* $a, b, c \in \mathbf{A}$ *on a* $(e_ae_be_c)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet] \simeq \mathbf{A}[1/(abc)]$.
6. *Si en outre* $abc = 0$, *alors* $(e_ae_b)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet] \simeq \mathbf{A}[1/(ab)]$.

Démonstration.
Les 3 premiers points sont faciles et classiques. Montrons le point 5. Dans l'anneau $\mathbf{B} = (e_ae_be_c)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet]$, abc est inversible, d'inverse $a^\bullet b^\bullet c^\bullet$. Donc l'homomorphisme composé

$$\psi \,:\, \mathbf{A} \xrightarrow{\ j\ } \mathbf{A}[a^\bullet, b^\bullet, c^\bullet] \xrightarrow{\ x \mapsto e_ae_be_cx\ } \mathbf{B}$$

se factorise avec un unique θ comme suit

$$\mathbf{A} \xrightarrow{\ \pi\ } \mathbf{A}[1/(abc)] \xrightarrow{\ \theta\ } \mathbf{B}.$$

Puisque $\mathbf{A} \subseteq \mathbf{C}$, j est injective et on peut identifier $x \in \mathbf{A}$ et $j(x)$. L'homomorphisme θ est surjectif parce que $\theta(1/abc) = a^\bullet b^\bullet c^\bullet = u$ et dans $\mathbf{B}$, $a^\bullet = bcu$, $b^\bullet = acu$, $c^\bullet = abu$. Par ailleurs $\operatorname{Ker}\pi = \operatorname{Ann}_{\mathbf{A}}(abc) \subseteq \operatorname{Ker}\psi$ et si $x \in \operatorname{Ker}\psi$, alors $e_ae_be_cx = e_{abc}x = 0$, donc $abcx = 0$.
Montrons le point 6. Puisque $abc = 0$, $0 = e_{abc} = e_ae_be_c$ et dans $(e_ae_b)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet] = \mathbf{B}_1$ on a $c^\bullet = e_ae_bc^\bullet = e_ae_b(e_cc^\bullet) = 0$ donc $\mathbf{B}_1 = (e_ae_b)\mathbf{A}[a^\bullet, b^\bullet]$ et on est ramené au point précédent. □

Naturellement les deux derniers points sont plus généraux et s'étendent avec un nombre fini arbitraire d'éléments de $\mathbf{A}$.

Une signification possible du lemme est de considérer qu'il formalise sous une forme un peu plus abstraite ce qui se passe lorsqu'on fait des calculs de manière dynamique dans un anneau réduit en « faisant comme si » c'était un sous anneau d'un corps. Grâce au point 3, ce calcul dynamique est possible (sous réserve de l'existence de $\mathbf{C}$). Grâce aux derniers points, on ramène les calculs dynamiques correspondant à la localisation en un idéal premier minimal à des calculs dans des localisés de $\mathbf{A}$ obtenus en inversant un seul élément.

B. Plongement dans un anneau zéro-dimensionnel réduit

Puisque la notion d'anneau zéro-dimensionnel réduit est purement équationnelle, l'algèbre universelle nous dit que tout anneau commutatif engendre un anneau zéro-dimensionnel réduit (cela fournit le foncteur adjoint au foncteur d'oubli). Nous voulons voir que dans le cas d'un anneau réduit $\mathbf{A}$, l'homomorphisme de $\mathbf{A}$ vers le zéro-dimensionnel réduit qu'il engendre est injectif. Cela nécessite de se fatiguer un petit peu.

Lemme B.1 *Si* $\mathbf{A} \subseteq \mathbf{C}$ *avec* $\mathbf{C}$ *zéro-dimensionnel réduit, et si nous notons* $x^\bullet$ *le quasi inverse de* x, *alors* $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ *est zéro-dimensionnel (c'est donc le sous anneau zéro-dimensionnel de* $\mathbf{C}$ *engendré par* $\mathbf{A}$*).*
Variante : si $\mathbf{A} \subseteq \mathbf{B}$ *réduit, et si chaque* $a \in \mathbf{A}$ *admet un quasi inverse* $a^\bullet$ *dans* $\mathbf{B}$, *l'anneau* $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ *est zéro-dimensionnel.*

Démonstration.
On doit démontrer que tout élément de $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ admet un quasi inverse. Puisque $(ab)^\bullet = a^\bullet b^\bullet$ tout élément de $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ s'écrit sous forme $\sum a_ib_i^\bullet$ avec $a_i, b_i \in \mathbf{A}$. Par ailleurs $a_ib_i^\bullet = a_ib_i^\bullet r_i$ avec $r_i = a_ia_i^\bullet$ idempotent. Par ailleurs étant donnés des idempotents $r_1, \ldots, r_k$ l'algèbre de Boole qu'ils engendrent contient un système fondamental d'idempotents orthogonaux $e_1, \ldots, e_n$ tel que chaque r_i soit la somme des e_j multiples de r_i ($e_jr_i = e_j$). Enfin si $e_1, \ldots, e_n$ est un système fondamental d'idempotents orthogonaux dans $\mathbf{C}$, si $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbf{A}$, si $c = \sum_{i=1}^n a_ib_i^\bullet e_i$ et $c' = \sum_{i=1}^n a_i^\bullet b_i e_i$, alors $c^2c' = c$ et $c'^2c = c'$, donc $c' = c^\bullet$. □

Lemme B.2 *Soit* $\mathbf{A}$ *un anneau réduit et* $a \in \mathbf{A}$. *Soit* $\mathbf{B} = \mathbf{A}[T]/\langle aT^2 - T, a^2T - a\rangle$ *et* $\mathbf{C} = \mathbf{B}_{\mathrm{red}}$. *Soit* $a^\bullet$ *l'image de* T *dans* $\mathbf{C}$. *Alors*

1. $\mathbf{C} \simeq (\mathbf{A}/\langle a\rangle)_{\mathrm{red}} \times \mathbf{A}[1/a]$ *et l'homomorphisme naturel* $\mathbf{A} \to \mathbf{C}$ *est injectif (on identifie* $\mathbf{A}$ *à un sous anneau de* $\mathbf{C}$*).*
2. $a^\bullet$ *est quasi inverse de* a *dans* $\mathbf{C}$.
3. *Pour tout homomorphisme* $\mathbf{A} \xrightarrow{\varphi} \mathbf{A}'$ *tel que* $\varphi(a)$ *admet un quasi inverse dans* $\mathbf{B}$, *il existe un unique homomorphisme* $\mathbf{C} \xrightarrow{\theta} \mathbf{A}'$ *tel que l'homomorphisme composé* $\mathbf{A} \to \mathbf{C} \xrightarrow{\theta} \mathbf{A}'$ *soit égal à* φ.

La démonstration n'offre pas de difficulté et est laissée au lecteur. Le corollaire suivant est une conséquence de la propriété d'unicité forte donnée dans le lemme.

Corollaire B.3 *Notons* $\mathbf{A}_{\{a\}}$ *l'anneau construit au lemme précédent. Soient* $a_1, \ldots, a_n$ *dans* $\mathbf{A}$ *alors l'anneau obtenu en répétant la construction pour chacun des* a_i, *ne dépend pas, à isomorphisme unique près, de l'ordre dans lequel on prend les* a_i *pour faire la construction.*

Par exemple il existe un unique $\mathbf{A}$-homomorphisme de $((\mathbf{A}_{\{a\}})_{\{b\}})_{\{c\}}$ dans $((\mathbf{A}_{\{c\}})_{\{b\}})_{\{a\}}$ et c'est un isomorphisme. Le lemme B.2 et le corollaire B.3 ont pour conséquence immédiate le théorème suivant.

Théorème B.4 *Soit* $\mathbf{A}$ *un anneau réduit. Considérons l'anneau* $\widehat{\mathbf{A}}$ *obtenu comme limite inductive en itérant la construction du lemme B.2. C'est un anneau zéro-dimensionnel réduit et l'homomorphisme naturel* $\mathbf{A} \to \widehat{\mathbf{A}}$ *est injectif. En outre cet anneau est* l'anneau zéro-dimensionnel réduit engendré par $\mathbf{A}$, *au sens suivant : pour tout anneau zéro-dimensionnel réduit* $\mathbf{A}'$, *tout homomorphisme* $\mathbf{A} \xrightarrow{\varphi} \mathbf{A}'$ *se factorise de manière unique via l'homomorphisme naturel* $\mathbf{A} \to \widehat{\mathbf{A}}$.

En bref :

Théorème B.5 *Tout anneau réduit* $\mathbf{A}$ *est contenu dans un anneau zéro-dimensionnel réduit* $\mathbf{C} = \mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$.

C. Anneaux zéro-dimensionnels réduits et corps

Nous avons déjà dit que la notion d'anneau zéro-dimensionnel réduit est *la bonne généralisation équationnelle* de la notion de corps. Cela signifie en particulier que toute conséquence équationnelle de la théorie des corps est en fait une conséquence équationnelle de la théorie des anneaux zéro-dimensionnels réduits.

De manière informelle on peut énoncer un principe local-global élémentaire général qui s'avère en pratique assez efficace.

Machinerie locale-globale élémentaire : des corps discrets aux anneaux zéro-dimensionnels réduits. *La plupart des algorithmes qui fonctionnent avec les corps discrets peuvent être modifiés de manière à fonctionner avec les anneaux zéro-dimensionnels réduits, en cassant l'anneau en deux morceaux chaque fois que l'algorithme écrit pour les corps discrets utilise le test « cet élément est-il nul ou inversible ? ». Dans le premier morceau l'élément en question est nul, dans le second il est inversible.*

Nous avons mis « la plupart » plutôt que « tous » dans la mesure où l'énoncé du résultat de l'algorithme pour les corps discrets doit être écrit sous une forme où n'apparaît pas qu'un corps discret est connexe.

L'application du principe précédent permet d'obtenir le théorème C.1 à partir du lemme 2.1, dès qu'on s'est convaincu que ce dernier donne un algorithme pour les corps discrets.

Théorème C.1 *Si* $\mathbf{C}$ *est un anneau zéro-dimensionnel réduit, tout module projectif de rang constant* 1 *sur* $\mathbf{C}[\underline{X}]$ *est libre.*

Pour le lecteur sceptique, nous donnons quelques détails dans l'annexe E.

D. Théorème de Traverso-Swan. Cas général.

Nouvelle preuve constructive du lemme 2.7
D'après les théorèmes B.5 et C.1 il existe un anneau zéro-dimensionnel réduit $\mathbf{C} = \mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}] \supseteq \mathbf{A}$ avec $\operatorname{Im} P$ libre sur $\mathbf{C}[\underline{X}]$. Cette dernière propriété reste vraie pour un anneau $\mathbf{B} \subseteq \mathbf{C}$ engendré par un nombre fini de quasi inverses $a_1^\bullet, \ldots, a_r^\bullet$ d'éléments de $\mathbf{A}$. Nous écrivons $e_i = a_i a_i^\bullet$ de sorte que e_i est un idempotent tel que $e_i a_i = a_i$ et $e_i a_i^\bullet = a_i^\bullet$. Écrivons aussi $e_i' = 1 - e_i$. Pour simplifier prenons $r = 3$ et il sera clair que l'argument est général. On décompose l'anneau $\mathbf{B}$ en un produit de 2^r anneaux, ou de manière équivalente en une somme directe de 2^r idéaux

$$\mathbf{B} = e_1e_2e_3\mathbf{B} \oplus e_1e_2e_3'\mathbf{B} \oplus e_1e_2'e_3\mathbf{B} \oplus e_1'e_2e_3\mathbf{B} \oplus e_1e_2'e_3'\mathbf{B} \oplus e_1'e_2e_3'\mathbf{B} \oplus e_1'e_2'e_3\mathbf{B} \oplus e_1'e_2'e_3'\mathbf{B} \quad (4)$$

D'après le lemme A.3 point 5

$$e_1e_2e_3\mathbf{B} \simeq e_1e_2e_3\mathbf{A}[a_1^\bullet, a_2^\bullet, a_3^\bullet)] \simeq \mathbf{A}[1/(a_1a_2a_3)]$$

Puisque le module $\operatorname{Im} P$ est libre sur $\mathbf{B}[\underline{X}]$, il l'est sur chacune des 2^r composantes, et donc en particulier sur $e_1e_2e_3\mathbf{B}[\underline{X}] \simeq \mathbf{A}[1/(a_1a_2a_3)][\underline{X}]$. D'après la propriété requise dans le lemme, on obtient $a_1a_2a_3 = 0$, donc $e_1e_2e_3 = 0$, $e_1e_2e_3' = e_1e_2$, etc. . ., et la décomposition (4) devient

$$\mathbf{B} = e_1e_2\mathbf{B} \oplus e_1e_3\mathbf{B} \oplus e_2e_3\mathbf{B} \oplus e_1e_2'e_3'\mathbf{B} \oplus e_1'e_2e_3'\mathbf{B} \oplus e_1'e_2'e_3\mathbf{B} \oplus e_1'e_2'e_3'\mathbf{B} \quad (5)$$

D'après le lemme A.3 point 6 on a $e_1e_2\mathbf{B} \simeq \mathbf{A}[1/(a_1a_2)]$ et on en tire $a_1a_2 = 0$, donc $e_1e_2 = 0$, $e_1e_2' = e_1$, $e_1'e_2 = e_2$. De même $a_1a_3 = 0 = e_1e_3$, $a_2a_3 = 0 = e_2e_3$ et finalement $e_1e_2'e_3' = e_1$, $e_1'e_2e_3' = e_2$, $e_1'e_2'e_3 = e_3$. On obtient une nouvelle décomposition

$$\mathbf{B} = e_1\mathbf{B} \oplus e_2\mathbf{B} \oplus e_3\mathbf{B} \oplus e_1'e_2'e_3'\mathbf{B} \quad (6)$$

Au bout du compte tous les a_i sont nuls et $\mathbf{B} = \mathbf{A} = \mathbf{A}[1/1]$ ce qui permet de conclure que $1 = 0$ dans $\mathbf{A}$. □

Théorème D.1 (Traverso-Swan-Coquand)
Si $\mathbf{A}$ *est un anneau seminormal, alors* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.
Plus précisément pour toute matrice $P \in \mathbf{A}[\underline{X}]^{n\times n}$ *idempotente de rang 1 sur* $\mathbf{A}[\underline{X}]$ *vérifiant* $P(0) = \mathrm{I}_{n,1}$, *on peut construire un vecteur colonne* $f \in \mathbf{A}[\underline{X}]^{n\times 1}$ *et un vecteur ligne* $g \in \mathbf{A}[\underline{X}]^{1\times n}$ *tels que* $P = fg$.

Démonstration.
On reprend mutatis mutandis la preuve donnée dans le cas intègre. Pour le lecteur sceptique voici ce que cela donne.
On utilise la caractérisation donnée au lemme 1.6. 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 $\mathbf{K}$ un anneau zéro-dimensionnel réduit contenant $\mathbf{A}$. Sur $\mathbf{K}[\underline{X}]$ le module $\operatorname{Im} P(\underline{X})$ est libre et 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 $m_{i,j} = f_ig_j$ pour tous i, j. En outre puisque $f_1(0)g_1(0) = 1$ et puisqu'on peut modifier f et g en les multipliant par une unité, on peut supposer que $f_1(0) = g_1(0) = 1$. Alors puisque $f_1g_j = m_{1,j}$ et vu le théorème de Kronecker, les coefficients

des g_j sont entiers sur l'anneau engendré par les coefficients des $m_{1,j}$. De même les coefficients des f_i sont entiers sur l'anneau engendré par les coefficients des $m_{i,1}$.
On appelle $\mathbf{B}$ le sous anneau de $\mathbf{K}$ engendré par $\mathbf{A}$ et par les coefficients des f_i et des g_j. Alors $\mathbf{B}$ 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 $\mathbf{A} = \mathbf{B}$. On appelle $\mathfrak{a}$ le conducteur de $\mathbf{A}$ dans $\mathbf{B}$. Notre but est maintenant de montrer $\mathfrak{a} = \langle 1 \rangle$, c'est-à-dire que $\mathbf{A}/\mathfrak{a}$ est trivial.
D'après le lemme 2.4 $\mathfrak{a}$ est un idéal radical de $\mathbf{B}$. Le lemme 2.6 s'applique avec $\mathbf{A} \subseteq \mathbf{B}$. On a $\mathbf{A}/\mathfrak{a} = \mathbf{C} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$ réduits, et $f_i g_j = m_{i,j}$ au niveau $\mathbf{B}/\mathfrak{a}$. 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 2.7.
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 1.5), 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 $\mathbf{L}[\underline{X}]$ (tenir compte du lemme 1.10).
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 le lemme 2.6, ceci implique que $a \in \mathfrak{a}$, donc $a = 0$ dans $\mathbf{C}$. □

En utilisant le lemme 2.5 à la place du lemme 2.4 on obtiendra le résultat suivant, plus précis que le théorème 2.3.

Théorème D.2 *Si $\mathbf{A}$ est un anneau contenu dans un anneau zéro-dimensionnel réduit $\mathbf{B}$ et M un module projectif de rang 1 sur $\mathbf{A}[\underline{X}]$, il existe $c_1, \ldots, c_m$ dans $\mathbf{B}$ tels que :*

1. *c_i^2 et c_i^3 sont dans $\mathbf{A}[(c_j)_{j<i}]$ pour $i = 1, \ldots, m$,*
2. *M est libre sur $\mathbf{A}[(c_j)_{j\leq m}][X]$.*

E. Anneaux à pgcd

Nous terminons avec une preuve détaillée du théorème C.1, pour le lecteur sceptique quant à la validité de la machinerie locale globale élémentaire page 14.

Définition E.1 *Un anneau $\mathbf{A}$ est dit* quasi intègre *lorsque tout élément admet pour annulateur un (idéal principal engendré par un) idempotent. Pour $a \in \mathbf{A}$, on note alors e_a l'idempotent tel que $\operatorname{Ann}(a) = \langle 1 - e_a \rangle$, de sorte que a est régulier dans $\mathbf{A}[1/e_a]$ et nul dans $\mathbf{A}[1/(1-e_a)]$.*

Un anneau intègre n'est autre qu'un anneau quasi intègre connexe.

Lemme E.2 *On considère $x_1, \ldots, x_n$ des éléments d'un anneau commutatif. Si on a $\operatorname{Ann}(x_i) = \langle r_i \rangle$ où r_i est un idempotent pour $1 \leq i \leq n$, soit s_i tel que $s_i + r_i = 1$, et posons $t_1 = s_1$, $t_2 = r_1 s_2$, $t_3 = r_1 r_2 s_3, \ldots$, $t_{n+1} = r_1 r_2 \cdots r_n$. Alors $t_1, \ldots, t_{n+1}$ est un système fondamental d'idempotents orthogonaux et l'élément $x = x_1 + t_2 x_2 + \cdots + t_n x_n$ vérifie $\operatorname{Ann}(x_1, \ldots, x_n) = \operatorname{Ann}(x) = \langle t_{n+1} \rangle$.*

Corollaire E.3 *Sur un anneau quasi intègre $\mathbf{A}$ soit P une matrice carrée telle que $\operatorname{Tr}(P)$ est régulier. Alors il existe une matrice J de même format telle que $J^2 = J$ et $JPJ = JPJ^{-1}$ admet un coefficient régulier en position $(1,1)$*

Démonstration.
On applique le lemme précédent avec les éléments $x_i = m_{i,i}$ de la diagonale de la matrice. On a $t_{n+1} = 0$ car $t_{n+1}\operatorname{Tr}(P) = 0$. Donc $(t_1, \ldots, t_n)$ est un système fondamental d'idempotents orthogonaux. Notons J_k la matrice de permutation qui échange les vecteurs numéros 1 et k de

la base canonique. On pose $J = t_1\mathrm{I}_n + t_2J_2 + \cdots t_nJ_n$. On a $J^2 = J$ et le coefficient en position $(1,1)$ dans JPJ est égal à $x = t_1x_1 + t_2x_2 + \cdots + t_nx_n = x_1 + t_2x_2 + \cdots + t_nx_n$, donc il est régulier. □

Un anneau zéro-dimensionnel réduit est quasi intègre. Inversement si $\mathbf{A}$ est quasi intègre, l'anneau total des fractions de $\mathbf{A}$, que nous notons $\mathrm{Frac}(\mathbf{A})$, est un anneau zéro-dimensionnel réduit : pour tout a, $\widetilde{a} = (1-e_a)+a$ est régulier et $a/\widetilde{a} = a^\bullet$ est quasi inverse de a dans $\mathrm{Frac}(\mathbf{A})$. En outre, pour tout $a \in \mathbf{A}$, $\mathbf{A}[1/a]$ est un anneau quasi intègre et $\mathrm{Frac}(\mathbf{A}[1/a])$ s'identifie à $e_a\mathrm{Frac}(\mathbf{A}) \simeq \mathrm{Frac}(\mathbf{A})[1/a]$.

Enfin, si $\mathbf{A}$ est quasi intègre, il en va de même pour $\mathbf{A}[X]$, l'annulateur d'un polynome f étant engendré par l'idempotent produit des annulateurs des coefficients.

Dans un anneau quasi intègre si a divise b et b divise a, on a $e_a = e_b$ et $ua = b$ avec un élément u inversible. Ceci permet de développer pour les anneaux quasi intègres une théorie du pgcd tout à fait analogue à celle des anneaux intègres.

Définition E.4 *Un monoïde commutatif régulier est appelé un* monoïde à pgcd *lorsque deux éléments arbitraires admettent toujours un plus grand commun diviseur. Si g est un pgcd pour a et b on écrit $g = \mathrm{pgcd}(a,b)$ (en fait un pgcd n'est défini qu'à un inversible près).*

Lemme E.5 *Soit $\mathbf{A}$ un anneau quasi intègre. Les propriétés suivantes sont équivalentes :*

1. *Le monoïde des éléments réguliers est un monoïde à pgcd.*
2. *Pour chaque idempotent e, les éléments réguliers de $\mathbf{A}[1/e]$ forment un monoïde à pgcd.*
3. *Deux éléments arbitraires admettent toujours un plus grand commun diviseur.*

Dans ce cas on dit que $\mathbf{A}$ est quasi intègre à pgcd, *et le pgcd de deux éléments a et b, bien défini à un inversible près est noté* $\mathrm{pgcd}(a,b)$.

Par exemple, pour 1. implique 2., on considère, pour $a \in e\mathbf{A}$ avec a régulier dans $\mathbf{A}[1/e]$, l'élément $\widetilde{a} = (1-e_a)+a$ régulier dans $\mathbf{A}$. Si g est le pgcd de $\widetilde{a}$ et $\widetilde{c}$ dans $\mathbf{A}$, le même élément g, vu dans $\mathbf{A}[1/e]$, est le pgcd de a et c.

Sur un anneau quasi intègre à pgcd, soit un polynome $f(X) = \sum_{k=0}^n f_kX^k$, on note $\mathrm{G}(f)$ le pgcd (défini à une unité près) des coefficients de f. Si $\mathrm{G}(f) = 1$ on dira que f est primitif[1].

Un anneau quasi intègre à pgcd connexe est un anneau à pgcd usuel.

Il est clair qu'un groupe est un monoïde à pgcd ce qui implique qu'un anneau zéro-dimensionnel réduit est un anneau quasi intègre à pgcd.

Il nous faut vérifier que les arguments dans la preuve du lemme 2.1 s'appliquent aussi bien aux anneaux quasi intègres à pgcd qu'aux anneaux à pgcd usuels. En particulier, si $\mathbf{A}$ est un anneau quasi intègre à pgcd, il en va de même pour $\mathbf{A}[X]$. Ainsi on obtiendra que pour tout anneau zéro-dimensionnel réduit $\mathbf{A}$, l'anneau $\mathbf{A}[\underline{X}]$ est un anneau quasi intègre à pgcd et donc tout module projectif de rang constant 1 sur $\mathbf{A}[\underline{X}]$ est libre.

Regardons tout d'abord ce qui concerne le premier argument dans la preuve :
Soit $P = (m_{i,j})$ une matrice idempotente de rang 1. Puisque $\sum_i m_{i,i} = 1$ on peut supposer que $m_{1,1}$ est régulier.
Il est clair que notre corollaire E.3 fait l'affaire.

Pour le reste nous nous reportons à « la bible » [14], livre dans lequel les démonstrations sont en général réduites à leur forme algorithmique la plus simple.

[1] Ceci entre en conflit avec une autre tradition, qui dit que f est primitif lorsque l'idéal des coefficients de f est égal à $\langle 1\rangle$.

Lemme E.6 (cf. théorème 1.1 page 108 dans [14])
Soient a, b, c dans un anneau quasi intègre à pgcd. Alors

1. $\text{pgcd}(\text{pgcd}(a,b),c) = \text{pgcd}(a,\text{pgcd}(b,c))$.
2. $c \cdot \text{pgcd}(a,b) = \text{pgcd}(ca,cb)$.
3. *Si* $x = \text{pgcd}(a,b)$, *alors* $\text{pgcd}(a,bc) = \text{pgcd}(a,xc)$.
4. *Si* $a|bc$ *et* $\text{pgcd}(a,b) = e_b$ *alors* $a|e_b c$.

Si un des 3 éléments a, b, c est nul, les affirmations sont évidentes. On détermine le système fondamental d'idempotents orthogonaux engendré par e_a, e_b et e_c. Si r_i est un élément de ce système fondamental d'idempotents orthogonaux, dans $\mathbf{A}[1/r_i]$ chacun des 3 éléments a, b, c est nul ou régulier. La preuve donnée dans [14] pour les monoïdes commutatifs réguliers s'applique dans la composante où les trois éléments sont réguliers.

Une conséquence du point 2 dans le lemme ci-dessus est que pour un anneau quasi intègre à pgcd, un polynome primitif est un élément régulier de $\mathbf{A}[X]$.

Lemme E.7 (lemme 4.2 page 123 dans [14]) *Soit* $\mathbf{A}$ *un anneau quasi intègre à pgcd et* $\mathbf{K} = \text{Frac}(\mathbf{A})$. *Si* $f \in \mathbf{K}[X]$ *nous pouvons trouver un polynome primitif* $g \in \mathbf{A}[X]$ *et* $c \in \mathbf{K}$ *tel que* $f = cg$. *Pour une autre décomposition* $f = c'g'$ *du même type, il existe* $u \in \mathbf{A}^\times$ *tel que* $c = uc'$.

Si $f = 0$ on prend $g = 1$ et $c = 0$. Si $\text{G}(f)$ est régulier la preuve dans [14] fonctionne, en remplaçant $\neq 0$ par régulier. Il suffit donc de casser l'anneau en deux morceaux au moyen de l'idempotent $e_{\text{G}(f)}$.

Lemme E.8 (lemme de Gauss, lemme 4.3 page 123 dans [14])
Soit $\mathbf{A}$ *un anneau quasi intègre à pgcd et* $f, g \in \mathbf{A}[X]$ *alors* $\text{G}(f)\text{G}(g) = \text{G}(fg)$.

On considère le système fondamental d'idempotents orthogonaux (r_i) engendré par les e_c pour tous les coefficients c de f et g. Dans chacun des anneaux $\mathbf{A}[1/r_i]$ les polynomes f et g ont un degré bien déterminé[2]. L'élégante preuve par récurrence sur $n + m = \deg(f) + \deg(g)$ donnée dans [14] s'applique :

On raisonne par induction sur $m + n$. Par distributivité (point 2 du lemme E.6) et vu le lemme E.7, on se ramène au cas où $\text{G}(f) = \text{G}(g) = 1$. On pose $c = \text{G}(fg)$ et $d = \text{pgcd}(f_n, c)$. Alors d divise $(f - f_n X^n)\, g$. Si $f = f_n X^n$ le résultat est clair.

Sinon, par hypothèse de récurrence d divise $\text{G}(f - f_n X^n)\, \text{G}(g) = \text{G}(f - f_n X^n)$, donc d divise f et $d = 1$. Ainsi $\text{pgcd}(f_n, c) = 1$. De même $\text{pgcd}(g_m, c) = 1$ et puisque c divise $f_n g_m$, $c = 1$.

Corollaire E.9 (corollaire 4.4 page 123 dans [14])
Soit $\mathbf{A}$ *un anneau quasi intègre à pgcd,* $f, g \in \mathbf{A}[X]$ *et* $\mathbf{K} = \text{Frac}(\mathbf{A})$. *Alors* f *divise* g *dans* $\mathbf{A}[X]$ *si et seulement si* f *divise* g *dans* $\mathbf{K}[X]$ *et* $\text{G}(f)$ *divise* $\text{G}(g)$.

Théorème E.10 (théorème 4.6 page 124 dans [14])
Si $\mathbf{A}$ *est un anneau quasi intègre à pgcd, il en va de même pour* $\mathbf{A}[X]$.

Les preuves dans [14] s'appliquent.

En fait, tout ceci est parfaitement automatique. Les preuves dans [14], qui sont aussi des algorithmes, sont basées sur la disjonction « $x = 0$ ou x régulier » valable pour tout x dans un anneau intègre. Quand on passe aux anneaux quasi intègres, il suffit de réaliser la disjonction en cassant l'anneau en 2 morceaux, au moyen de l'idempotent e_x, chaque fois que la preuve (i.e., l'algorithme) trouve un x qu'il faut traiter.

[2] Précisément un polynome a un degré bien déterminé lorsqu'on connaît un entier $q \geq 0$ tel que le coefficient de degré q est à la fois dominant et régulier, sans avoir à supposer que l'anneau est trivial ou non.

Références

[1] Brewer J.W., Costa D.L. *Seminormality and projective modules over polynomial rings.* J. Algebra **58**, (1979), no. 1, 208–216. 8

[2] Coquand T. *On seminormality* 2006. À paraître au Journal of Algebra. http://www.cs.chalmers.se/~coquand/min.pdf 1, 11

[3] Coquand T. *Sur un théorème de Kronecker concernant les variétés algébriques* C. R. Acad. Sci. Paris, Ser. I **338** (2004), 291–294. 2

[4] Coquand T., Ducos L., Lombardi H., Quitté C. *L'idéal des coefficients du produit de deux polynomes.* Revue des Mathématiques de l'Enseignement Supérieur, **113** (3), (2003), 25–39. 7

[5] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker. (2002) 477–499 . 2

[6] Coquand T., Lombardi H., Quitté C. *Generating non noetherian modules constructively.* Manuscripta mathematica **115**, (2004), 513–520. 2

[7] Coquand T., Lombardi H., Roy M.-F. *Une caractérisation élémentaire de la dimension de Krull.* Preprint 2003. From Sets and Types to Analysis and Topology : Towards Practicable Foundations for Constructive Mathematics (L. Crosilla, P. Schuster, eds.). Oxford University Press. (2005) 239–244. 2

[8] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256. 2

[9] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* EUROCAL '85. Lecture Notes in Computer Science n°204, (Ed. Caviness B.F.) 289–290. Springer 1985. 2

[10] Edwards, H. *Divisor Theory.* Boston, MA : Birkhäuser, 1989 7

[11] Gilmer R., Heitmann R. *On Pic R[X] for R seminormal.* J. Pure Appl. Algebra **16** (1980), 251–257. 8

[12] Heitmann, R. *Generating non-Noetherian modules efficiently.* Michigan Math. **31** 2 (1984) 167–180. 2

[13] Hurwitz, A. *Ueber einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen*, Nachr. kön Ges. Wiss. Göttingen, 1895, 230–240. (*Werke*, vol. 2, 198–207.) 7

[14] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Springer-Verlag (1988). 17, 18

[15] Querré J. *Sur le groupe de classes de diviseurs.* C. R. Acad. Sci. Paris, **284** (1977), 397–399. 8

[16] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc., **103** (1988), 1012–1014. 9

[17] Swan R. G. *On Seminormality.* Journal of Algebra, **67** (1980), 210–229. 1, 11

[18] Traverso C. *Seminormality and the Picard group.* Ann. Scuola Norm. Sup. Pisa, **24** (1970), 585–595. 1, 8

[19] Yengui I., *Making the use of maximal ideals constructive.* (2004) preprint. 2

Table des matières