Available online at www.sciencedirect.com

ScienceDirect

Theoretical Computer Science 392 (2008) 113–127

Theoretical Computer Science

www.elsevier.com/locate/tcs

Seminormal rings (following Thierry Coquand)

Henri Lombardi[a,*], Claude Quitté[b]

[a] *Équipe de Mathématiques, UMR CNRS 6623, 25030 Besançon cedex, France*
[b] *Laboratoire de Mathématiques, SP2MI, Université de Poitiers, Boulevard 3, Teleport 2, BP 179, 86960 Futuroscope Cedex, France*

Abstract

The Traverso–Swan theorem says that a reduced ring $\mathbf{A}$ is seminormal if and only if the natural homomorphism $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[X]$ is an isomorphism [C. Traverso, Seminormality and the Picard group, Ann. Sc. Norm. Sup. Pisa 24 (1970) 585–595; R.G. Swan, On seminormality, J. Algebra 67 (1980) 210–229]. We give here all the details needed to understand the elementary constructive proof for this result given by Coquand in [T. Coquand, On seminormality, J. Algebra 305 (2006) 577–584].

This example is typical of a new constructive method. The final proof is simpler than the initial classical one. More important: the classical argument by absurdum using "an abstract ideal object" is deciphered with a general technique based on the following idea: purely ideal objects constructed using TEM and Choice may be replaced by concrete objects that are "finite approximations" of these ideal objects.

Keywords: Seminormal rings; Traverso's theorem; Constructive algebra; Minimal primes; Dynamical method

1. 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), Reprinted in *Dernières pensées*, Flammarion.

The Traverso–Swan theorem says that a reduced ring $\mathbf{A}$ is seminormal if and only if the natural homomorphism $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[X]$ is an isomorphism [19,18]. We give here all the details needed to understand the elementary constructive proof for this result given by Thierry Coquand in [2].

[*] Corresponding author.
E-mail addresses: henri.lombardi@univ-fcomte.fr (H. Lombardi), quitte@mathlabo.univ-poitiers.fr (C. Quitté).
URL: http://hlombardi.free.fr/ (H. Lombardi).

0304-3975/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2007.10.007

First, we have to give a classical proof (using TEM and Choice) as elementary as possible. After this first simplification we have to remove the remaining nonconstructive arguments. Here it is a proof by absurdum based on the introduction of an abstract ideal object, which is a minimal prime.

The deciphering of this nonconstructive argument is based on the so-called "dynamical method".

This example is paradigmatic of a new general constructive method inspired by the following semantic: purely ideal objects constructed using TEM and Choice may be replaced by *concrete objects that are finite approximations of these ideal objects*.

An important step, where this method was introduced in Computer Algebra from an efficiency point of view, was the computer algebra system D5 [10]: here we see that it is possible to compute inside the algebraic closure of an arbitrary computable field, contrary to the well-known fact that such an algebraic closure cannot exist constructively as a static object. So D5 told us that, from a constructive point of view, the algebraic closure of an arbitrary computable field does exist, not as a static object, but as a dynamical one.

In the paper [9] the dynamical method is explained on the example of abstract proofs, via model theory, of results similar to the Hilbert Nullstellensatz. Here ideal abstract objects are the models of a coherent first order theory. These models have to exist in classical mathematics: this is the compactness theorem in (classical) model theory. When the classical proof is deciphered in a constructive one, each one of these models is replaced by "a finite amount of information concerning it".

In the papers [5,8], chains of prime ideals that are used in classical mathematics in order to define the Krull dimension are replaced by finite sequences of elements of the ring. In this way we obtain an elementary definition of the Krull dimension, without using any prime ideal. The Krull dimension of usual rings matches the elementary definition in a constructive way. So theorems in commutative algebra that have in their hypothesis a bound on the Krull dimension can now be reread in a constructive way, and for several important ones a constructive proof, much more precise than the classical one, has been found. E.g., Serre's "splitting-off", "stable range" and "cancellation" theorems of Bass, and Forster–Swan theorem. Moreover the constructive versions [6,7] are an improvement on the most sophisticated classical versions of these theorems given by R. Heitmann in his remarkable "nonNœtherian" 1984 paper [13].

Finally let us mention that in [20], Yengui has shown how to reread in a dynamical way classical proofs that use maximal ideals.

In the example given in the present paper, we get a proof which is simpler and more elegant than the classical ones. But the most important fact is that the classical argument "by absurdum and using a purely ideal object" is deciphered by following the general method we have sketched. The localisation at a generic minimal prime $\mathfrak{p}$ is replaced by a tree computation where we try to make invertible all elements that appear in the computational proof. The tree comes from the fact that in the classical reasoning one uses an argument saying "any element x of the ring is either inside or outside the generic minimal prime $\mathfrak{p}$ we consider". Since the prime is minimal, a priori x have to be outside of $\mathfrak{p}$. We have to use the branch "x inside $\mathfrak{p}$" only in the case where the computation shows that 0 becomes invertible if x is outside $\mathfrak{p}$.

We shall first explain what happens with an integral ring. We give the proof of the general case in the Annex.

2. Preliminaries

A, **B**, **C** are commutative rings. Used without more precision an "homomorphism" is always a ring homomorphism.

Seminormal rings

An integral ring **A** is said to be *seminormal* if whenever $b^2 = c^3 \neq 0$ the element $a = b/c$ of the fraction field is in **A**. Remark that $a^3 = b$ and $a^2 = c$.

An arbitrary ring **A** is said to be *seminormal* if whenever $b^2 = c^3$, there exists $a \in \mathbf{A}$ such that $a^3 = b$ and $a^2 = c$. This implies that **A** is reduced: if $b^2 = 0$ then $b^2 = 0^3$, so we get an $a \in \mathbf{A}$ with $a^3 = b$ and $a^2 = 0$, thus $b = 0$.

In a ring if $x^2 = y^2$ and $x^3 = y^3$ then $(x - y)^3 = 0$. So:

Fact 2.1. *In a reduced ring $x^2 = y^2$ and $x^3 = y^3$ imply $x = y$.*

Consequently the element a here upon is always unique. Moreover $\operatorname{Ann} b = \operatorname{Ann} c = \operatorname{Ann} a$.

The category of finitely generated projective $\mathbf{A}$*-modules*

A finitely generated projective module is a module M isomorphic to a direct summand of a finite rank free module: $M \oplus M' \simeq \mathbf{A}^m$. Equivalently, it is a module isomorphic to the image of a projection matrix.

An $\mathbf{A}$-linear map $\psi : M \to N$ between finitely generated projective modules with $M \oplus M' \simeq \mathbf{A}^m$ and $N \oplus N' \simeq \mathbf{A}^n$ can be given by the linear map $\widetilde{\psi} : \mathbf{A}^m \to \mathbf{A}^n$ defined by $\widetilde{\psi}(x \oplus x') = \psi(x)$.

In other words the category of finitely generated projective modules over $\mathbf{A}$ is equivalent to the category whose objects are idempotent matrices with coefficients in $\mathbf{A}$, a morphism from P to Q being a matrix H such that $QH = H = HP$. In particular the identity of P is represented by P.

Fact 2.2. *If M and N are represented by idempotent matrices $P = (p_{i,j})_{i,j \in I} \in \mathbf{A}^{I \times I}$ and $Q = (q_{k,\ell})_{k,\ell \in J} \in \mathbf{A}^{J \times J}$, then:*

(1) *The direct sum $M \oplus N$ is represented by* $\mathrm{Diag}(P, Q) = \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}$.

(2) *The tensor product $M \otimes N$ is represented by the Kronecker product*

$$P \otimes Q = (r_{(i,k),(j,\ell)})_{(i,k),(j,\ell) \in I \times J}, \text{ where } r_{(i,k),(j,\ell)} = p_{i,j} q_{k,\ell}.$$

(3) *M and N are isomorphic if and only if matrices* $\mathrm{Diag}(P, 0_n)$ *and* $\mathrm{Diag}(0_m, Q)$ *are similar.*

Proof. *3.* Remark that the projection on M in $M \oplus M' \oplus \mathbf{A}^n$ is represented by the matrix $\mathrm{Diag}(P, 0_n)$ and the projection on N in $\mathbf{A}^m \oplus N \oplus N'$ is represented by the matrix $\mathrm{Diag}(0_m, Q)$. Writing $\mathbf{A}^m \oplus \mathbf{A}^n$ as $M \oplus M' \oplus N \oplus N'$ we see that the two projections are conjugate by the automorphism exchanging M and N. □

Rank of a finitely generated projective module

If $\varphi : M \to M$ is an endomorphism of the finitely generated projective $\mathbf{A}$-module M image of the idempotent matrix P and if H represents φ (with $H = PH = HP$), let $N = \mathrm{Ker}\, P$. So $M \oplus N = \mathbf{A}^n$ and we can define the determinant of φ by $\det(\varphi) = \det(\varphi \oplus \mathrm{Id}_n) = \det(H + (\mathrm{I}_n - P))$.

Let μ_X be the multiplication by X inside the $\mathbf{A}[X]$-module $M[X]$ (this module, an extend of M from $\mathbf{A}$, is also represented by the matrix P), then $\det(\mu_X) = \mathrm{R}_M(X) = r(X)$ is a polynomial satisfying $r(XY) = r(X)r(Y)$ and $r(1) = 1$. In other words its coefficients are a basic system of orthogonal idempotents. The module is said to be *of rank k* if $r(X) = X^k$.
A direct computation shows the following fact.

Fact 2.3. *A matrix $P = (p_{i,j})$ is a projection matrix whose image is a projective module of constant rank 1 if and only if the following properties are satisfied*

- $\bigwedge^2 P = 0$*, i.e., all 2×2 minors are null,*
- $\mathrm{Tr}\, P = \sum_i p_{ii} = 1$.

When the image of a projection matrix is free

If $P \in \mathbf{A}^{n \times n}$ is a projection matrix whose image is free of rank r, its kernel is not always free, so the matrix is not always similar to the standard matrix $\mathrm{I}_{n,r} = \mathrm{Diag}(\mathrm{I}_r, 0_{n-r}) = \begin{bmatrix} \mathrm{I}_r & 0 \\ 0 & 0_{n-r} \end{bmatrix}$.
Let us give a simple characterisation for the fact that the image of an idempotent matrix is free.

Proposition 2.4. *Let $P \in \mathbf{A}^{n \times n}$. The matrix P is idempotent and its image is free of rank r if and only if there exist two matrices $X \in \mathbf{A}^{n \times r}$ and $Y \in \mathbf{A}^{r \times n}$ such that $YX = \mathrm{I}_r$ and $P = XY$. Moreover,*

(1) $\mathrm{Im}\, P = \mathrm{Im}\, X \simeq \mathrm{Im}\, Y$.

(2) *For any matrices X', Y' with same formats as X and Y and such that $P = X'Y'$, there exists a unique matrix $U \in \mathsf{GL}_r(\mathbf{A})$ such that $X' = XU$ and $Y = UY'$. In fact $U = YX'$, $U^{-1} = Y'X$, $Y'X' = \mathrm{I}_r$ and the columns of X' form a basis of* $\mathrm{Im}\, P$.

Another possible characterisation is that the matrix $\mathrm{Diag}(P, 0_r)$ *is similar to the standard projection matrix* $\mathrm{I}_{n+r,r}$.

Proof. Assume that $\mathrm{Im}\, P$ is free of rank r. We take for the columns of X a basis of $\mathrm{Im}\, P$. So, there exists a unique matrix Y such that $P = XY$. Since $PX = X$ (because $P^2 = P$) one has $XYX = X$. Since X is injective and $(\mathrm{I}_r - YX)X = 0$ one has $\mathrm{I}_r = YX$.
Let us assume that $YX = \mathrm{I}_r$ and $P = XY$. Thus $P^2 = XYXY = X\mathrm{I}_rY = XY = P$ and $PX = XYX = X$. Donc $\mathrm{Im}\, P = \mathrm{Im}\, X$. Moreover the columns of X are independent because $XZ = 0$ implies $Z = YXZ = 0$.
(1) The sequence $\mathbf{A}^n \xrightarrow{\mathrm{I}_n - P} \mathbf{A}^n \xrightarrow{Y} \mathbf{A}^r$ is exact: indeed $Y(\mathrm{I}_n - P) = 0$ and if $YZ = 0$ then $PZ = 0$ thus $Z = (\mathrm{I}_n - P)Z$. So $\mathrm{Im}\, Y \simeq \mathbf{A}^n \big/ \mathrm{Ker}\, Y = \mathbf{A}^n \big/ \mathrm{Im}(\mathrm{I}_n - P) \simeq \mathrm{Im}\, P$.
(2) If X', Y' have the same formats as X, Y and $P = X'Y'$, let $U = YX'$ and $V = Y'X$. Thus $UV = YX'Y'X = YPX = YX = \mathrm{I}_r$; $X'V = X'Y'X = PX = X$, so $X' = XU$; $UY' = YX'Y' = YP = Y$, so $Y' = VY$. Finally $Y'X' = VYXU = VU = \mathrm{I}_r$.
Concerning the last characterisation , it is a simple application of point 3 in Fact 2.2. □

For projective modules of constant rank 1 we get the following.

Lemma 2.5. *A projection matrix* P *of rank* 1 *has its image free if and only if there exist a column vector* x *and a row vector* y *such that* $yx = 1$ *and* $xy = P$. *Moreover* x *and* y *are unique up to multiplication by a unit as soon as* $xy = P$.

The Grothendieck semiring $\mathsf{GK}_0\,\mathbf{A}$ *and the Picard group* $\mathsf{Pic}\,\mathbf{A}$

$\mathsf{GK}_0\,\mathbf{A}$ is the set of isomorphism classes of finitely generated projective modules over $\mathbf{A}$. It is a semiring for laws $\oplus$ and $\otimes$.
Since $\mathbf{A}$ is assumed to be commutative, the subsemiring of $\mathsf{GK}_0\,\mathbf{A}$ generated by 1 (the isomorphism class of $\mathbf{A}$) is isomorphic to $\mathbb{N}$, except when $\mathbf{A}$ is the trivial ring.
Any element of $\mathsf{GK}_0\,\mathbf{A}$ can be represented by an idempotent matrix with coefficients in $\mathbf{A}$.
$\mathsf{Pic}\,\mathbf{A}$ is the subset of $\mathsf{GK}_0\,\mathbf{A}$ whose elements are isomorphism classes of projective modules of constant rank 1. It is a group for $\otimes$. The "inverse" of M is its dual. If $M \simeq \mathrm{Im}\, P$ then $M^\star \simeq \mathrm{Im}\, {}^{\mathrm{t}}P$. In particular if P is a projection matrix of rank 1, $P \otimes {}^{\mathrm{t}}P$ is a projection matrix whose image is a free module of rank 1.
This can be verified directly by applying Lemma 2.5.

$\mathsf{Pic}\,\mathbf{A}$ *and classes of invertible ideals*

An ideal $\mathfrak{a}$ of $\mathbf{A}$ is *invertible* if there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab} = a\mathbf{A}$ where a is a regular element. In this case there exist $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ in $\mathbf{A}$ such that $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$, $\mathfrak{b} = \langle y_1, \ldots, y_n \rangle$ and $\sum_i x_i y_i = a$. Moreover for all i, j there exists a unique $m_{i,j}$ such that $y_i x_j = a m_{i,j}$. One deduces that the matrix $(m_{i,j})$ is an idempotent matrix of rank 1, and its image is isomorphic to $\mathfrak{a}$ as $\mathbf{A}$-module.
Two invertible ideals $\mathfrak{a}, \mathfrak{b}$ are isomorphic as $\mathbf{A}$-modules if and only if there exist regular elements a, b such that $a\mathfrak{a} = b\mathfrak{b}$. This allows us to see the class group of $\mathbf{A}$ (i.e., the group of classes of invertible ideals) as a subgroup of $\mathsf{Pic}\,\mathbf{A}$. In most cases the two groups are identical.
For example if $\mathbf{A}$ is integral, any matrix $(a_{i,j})$ which is idempotent of rank 1 has a regular element on its diagonal and the coefficients of the corresponding row generate an invertible ideal isomorphic to the image of the matrix.

Change of ring

Let ρ be an homomorphism $\mathbf{A} \to \mathbf{B}$. The change of ring from $\mathbf{A}$ to $\mathbf{B}$ transforms a finitely generated projective module M over $\mathbf{A}$ in a finitely generated projective module $\rho_\star(M) \simeq M \otimes_{\mathbf{A}} \mathbf{B}$ over $\mathbf{B}$. Any $\mathbf{B}$-module isomorphic to such a module $\rho_\star(M)$ is said "extended" from $\mathbf{A}$. For projection matrices this amounts to consider the matrix after transformation by the homomorphism ρ.
This gives a homomorphism $\mathsf{GK}_0\,\rho : \mathsf{GK}_0\,\mathbf{A} \to \mathsf{GK}_0\,\mathbf{B}$. Whence the natural following problem: "Is each finitely generated projective module over $\mathbf{B}$ extended form a finitely generated projective module over $\mathbf{A}$?". In other words: "Is $\mathsf{GK}_0\,\rho$ onto?".
For example if $\mathbf{Z}$ is the subring of $\mathbf{A}$ generated by $1_{\mathbf{A}}$, we know that $\mathbf{Z}$-projective modules of constant rank are free,

and the question “Are projective modules of constant rank extended from $\mathbf{Z}$?” is equivalent to “Are projective modules of constant rank free?”.

When $\mathbf{B} = \mathbf{A}[X_1, \ldots, X_m] = \mathbf{A}[\,\underline{X}\,]$, one has the evaluation homomorphism in 0, $\mathbf{B} \xrightarrow{\theta} \mathbf{A}$, with $\theta \circ \rho = \mathrm{Id}_{\mathbf{A}}$. This implies that the $\mathbf{B}$-finitely generated projective module $M = M(\,\underline{X}\,)$ is extended from $\mathbf{A}$ if and only if it is isomorphic to $M(0) = \theta_\star(M)$.

Concerning projection matrices, an idempotent matrix $P \in \mathbf{B}^{n\times n}$ represents a module which is extended from $\mathbf{A}$ if and only if its image is isomorphic to the image of $P(0)$.

If all finitely generated projective $\mathbf{B}$-modules are extended from $\mathbf{A}$ then P is similar to $P(0)$, but it may be easier to show only the isomorphism of the images.

Concerning Pic one has two group homomorphisms $\mathsf{Pic}\,\mathbf{A} \xrightarrow{\mathsf{Pic}\,\rho} \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,] \xrightarrow{\mathsf{Pic}\,\theta} \mathsf{Pic}\,\mathbf{A}$ whose composition is the identity. The first one is injective, the second one surjective, and they are isomorphisms if and only if the first one is surjective, if and only if the second one is injective.

The last property means that if a matrix $P(\,\underline{X}\,)$ is idempotent of rank 1 over $\mathbf{A}[\,\underline{X}\,]$ and if $\mathrm{Im}(P(0))$ is free, then $\mathrm{Im}(P(\,\underline{X}\,))$ is free.

In fact if $\mathrm{Im}(P(0))$ is free, then the bloc diagonal matrix $\mathrm{Diag}(P(0), 0_1)$ is similar to a standard projection matrix $\mathrm{I}_{n+1,1}$. As $\mathrm{Im}(\mathrm{Diag}(P(\,\underline{X}\,), 0_1))$ is isomorphic to $\mathrm{Im}\,P(\,\underline{X}\,)$, we get the following result.

Lemma 2.6. *The following are equivalent:*

(1) *The natural homomorphism* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,]$ *is an isomorphism.*

(2) *If a matrix* $P(\,\underline{X}\,) \in \mathbf{A}[\,\underline{X}\,]^{n\times n} = (m_{i,j}(\,\underline{X}\,))_{i,j\in\{1,\ldots,n\}}$ *is idempotent of rank 1 and if* $P(0) = \mathrm{I}_{n,1}$, *then there exist* $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{A}[\,\underline{X}\,]$ *such that* $m_{i,j} = f_i g_j$ *for all* i, j.

Reducing the problems to reduced rings: $\mathsf{GK}_0\,\mathbf{A}_{\mathrm{red}} = \mathsf{GK}_0\,\mathbf{A}$

We note $\mathbf{A}_{\mathrm{red}}$ for $\mathbf{A}\big/\sqrt{0}$.

Proposition 2.7. *The natural map* $\mathsf{GK}_0(\mathbf{A}) \to \mathsf{GK}_0(\mathbf{A}_{\mathrm{red}})$ *is bijective.*

(1) *Injective: this means that if two finitely generated projective modules* E, F *over* $\mathbf{A}$ *are isomorphic over* $\mathbf{A}_{\mathrm{red}}$, *they are also isomorphic over* $\mathbf{A}$.

(2) *If two idempotent matrices* $P, Q \in \mathbf{A}^{n\times n}$ *are conjugate over* $\mathbf{A}_{\mathrm{red}}$, *they are also conjugate over* $\mathbf{A}$.

(3) *Surjective: any finitely generated projective module over* $\mathbf{A}_{\mathrm{red}}$ *comes from a finitely generated projective module over* $\mathbf{A}$.

Proof. (2) Let us note $\overline{x}$ the object x viewed modulo $\sqrt{0}$. Let $C \in \mathbf{A}^{n\times n}$ be a matrix such that $\overline{C}\,\overline{P}\,\overline{C}^{-1} = \overline{Q}$. Since $\det C$ is invertible modulo $\sqrt{0}$, $\det C$ is invertible in $\mathbf{A}$ and C belongs to $\mathsf{GL}_n(\mathbf{A})$. Thus $\overline{Q} = \overline{C\,P\,C^{-1}}$. Replacing P by $C\,P\,C^{-1}$ we may assume that $\overline{Q} = \overline{P}$ and $\overline{C} = \mathrm{I}_n$. Then the matrix $A = QP + (\mathrm{I}_n - Q)(\mathrm{I}_n - P)$ gives $AP = QP = QA$ and $\overline{A} = \mathrm{I}_n$: thus A is invertible, $APA^{-1} = Q$ and $\overline{A} = \overline{C}$.

(1) Two residually isomorphic finitely generated projective modules $E \simeq \mathrm{Im}\,P$ and $F \simeq \mathrm{Im}\,Q$ are images of residually conjugate matrices: $\mathrm{Diag}(P, 0_m)$ and $\mathrm{Diag}(0_n, Q)$ with $\mathrm{Diag}(\overline{P}, 0_m)$ similar to $\mathrm{Diag}(0_n, \overline{Q})$. Thus we can apply (1).

(3) Any finitely generated projective module over $\mathbf{A}_{\mathrm{red}}$ can be seen as the residual module of a finitely generated projective module over $\mathbf{A}$: apply Newton’s method. More precisely let $\mathfrak{a}$ be the ideal generated by the coefficients of $P^2 - P$. If $\mathfrak{a}$ is contained in the nilradical of $\mathbf{A}$, there exists k such that $\mathfrak{a}^{2^k} = 0$. On the other hand if $Q = 3P^2 - 2P^3$, then $Q \equiv P \bmod \mathfrak{a}$ and $Q^2 - Q$ is a multiple of $(P^2 - P)^2$, thus $Q^2 - Q$ has its coefficients in $\mathfrak{a}^2$. Iterating k times the operation $P \leftarrow 3P^2 - 2P^3$ we get the result. □

Corollary 2.8. *The canonical homomorphism* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,]$ *is an isomorphism if and only if the canonical homomorphism* $\mathsf{Pic}\,\mathbf{A}_{\mathrm{red}} \to \mathsf{Pic}\,\mathbf{A}_{\mathrm{red}}[\,\underline{X}\,]$ *is an isomorphism.*

Convention 2.9. *In what follows we abbreviate the sentence “the canonical homomorphism* $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,]$ *is an isomorphism” and we write simply “*$\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,]$*”.*

Invertible elements of $\mathbf{A}[\,\underline{X}\,]$

Lemma 2.10. *If the ring* $\mathbf{A}$ *is reduced, the group homomorphism* $\mathbf{A}^\times \to (\mathbf{A}[\,\underline{X}\,])^\times$ *is an isomorphism. In other words if* $f(\,\underline{X}\,) \in \mathbf{A}[\,\underline{X}\,]$ *is invertible, then* $f = f(0) \in \mathbf{A}^\times$.

It is sufficient to consider $\mathbf{A}[X]$. A direct computation shows that if $f(X)g(X) = 1$ with $\deg(f) \le m$, $m \ge 1$, then the coefficient of degree m of f is nilpotent.

Kronecker's theorem

Theorem 2.11. *Let* $f, g \in \mathbf{A}[\,\underline{X}\,]$ *and* $h = fg$. *Let* a *be a coefficient of* f *and* b *be a coefficient of* g, *then* ab *is integral over the subring of* $\mathbf{A}$ *generated by the coefficients of* h.

Using "the Kronecker trick" (i.e., replace each variable X_k by T^{m^k} for an $m \gg 0$) reduces the problem to univariate polynomials. For univariate polynomials constructive proofs are given in the literature (cf. [11,14], and for a survey [4]).

3. Traverso–Swan theorem, with integral rings

The condition is necessary: Schanuel example

We show that if $\mathbf{A}$ is reduced and $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[X]$ then $\mathbf{A}$ is seminormal. We use the characterisation given in Lemma 2.5.

Let b, c be elements in a reduced ring $\mathbf{A}$ with $b^2 = c^3$. Let $\mathbf{B} = \mathbf{A}[a] = \mathbf{A} + a\mathbf{A}$ be a reduced ring containing $\mathbf{A}$ with $a^3 = b$, $a^2 = c$. Let $f_1 = 1 + aX$, $f_2 = cX^2 = g_2$ and $g_1 = (1 - aX)(1 + cX^2)$. We have $f_1 g_1 + f_2 g_2 = 1$, thus the matrix $M(X) = (f_i g_j)_{1 \le i,j \le 2}$ is idempotent of rank 1. Its coefficients are in $\mathbf{A}$ and $M(0) = \mathrm{I}_{2,1}$. Thus its image is free over $\mathbf{B}[X]$. If it is free over $\mathbf{A}[X]$ then there exist f_i''s and g_j''s in $\mathbf{A}[X]$ with $f_i' g_j' = f_i g_j$. By unicity $f_i' = u f_i$ with u invertible in $\mathbf{A}[X]$. Since $\mathbf{A}$ is reduced u is invertible in $\mathbf{A}$. Since $u f_1 \in \mathbf{A}[X]$ we get $a \in \mathbf{A}$.

NB: we can take $\mathbf{B} = \big(\mathbf{A}[T]/\langle T^2 - c, T^3 - b\rangle\big)_{\mathrm{red}}$, with $a =$ class of T. If some a does exist in $\mathbf{A}$, we get $\mathbf{B} \simeq \mathbf{A}$.

Case of a gcd ring

Let us recall that an (integral) gcd ring is an integral ring where two arbitrary elements have a gcd, i.e., an inferior bound for the divisibility relation. Also if $\mathbf{A}$ is a gcd ring, then $\mathbf{A}[\,\underline{X}\,]$ is a gcd ring.

Lemma 3.1. *If* $\mathbf{A}$ *is an integral gcd ring,* $\mathsf{Pic}\,\mathbf{A} = \{1\}$.

Remark 3.2. Consequently $\mathsf{Pic}\,\mathbf{A} \to \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,]$ is an isomorphism. This works if $\mathbf{A}$ is a discrete field.

Proof. We use the characterisation given in Lemma 2.5. Let $P = (m_{i,j})$ be an idempotent matrix of rank 1. Since $\sum_i m_{i,i} = 1$ we may assume that $m_{1,1}$ is regular. Let f be the gcd of the first row. We have $m_{1,j} = f g_j$ with the gcd of g_j's equal to 1. Since f is regular and $m_{1,1} m_{i,j} = m_{1,j} m_{i,1}$ we have $g_1 m_{i,j} = m_{i,1} g_j$. So g_1 divides all the $m_{i,1} g_j$ and also their gcd $m_{i,1}$. Let us write $m_{i,1} = g_1 f_i$. Since $g_1 f_1 = m_{1,1} = f g_1$ we get $f_1 = f$. Finally the equality $m_{1,1} m_{i,j} = m_{1,j} m_{i,1}$ gives $f_1 g_1 m_{i,j} = f_1 g_j g_1 f_i$ and $m_{i,j} = f_i g_j$. □

Case of an integral normal ring

Lemma 3.3. *If* $\mathbf{A}$ *is integral and integrally closed, then* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\,\underline{X}\,]$.

Proof. We use the characterisation given in Lemma 2.6. Let $(m_{i,j}(\,\underline{X}\,))_{i,j=1,\ldots,n} = P(\,\underline{X}\,)$ be an idempotent matrix of rank 1 with $P(0) = \mathrm{I}_{n,1}$. Let $\mathbf{K}$ be the fraction field of $\mathbf{A}$. On $\mathbf{K}[\,\underline{X}\,]$ the module $\operatorname{Im} P(\,\underline{X}\,)$ is free. Thus there exist $f = (f_1(\,\underline{X}\,), \ldots, f_n(\,\underline{X}\,))$ and $g = (g_1(\,\underline{X}\,), \ldots, g_n(\,\underline{X}\,))$ in $\mathbf{K}[\,\underline{X}\,]^n$ such that $m_{i,j} = f_i g_j$ for all i, j. Moreover since $f_1(0) g_1(0) = 1$ and since we can modify f and g multiplying them by units, we can assume that $f_1(0) = g_1(0) = 1$. Thus since $f_1 g_j = m_{1,j}$ and using Kronecker's theorem, the coefficients of g_j's are integral over the ring generated by the coefficients of $m_{1,j}$'s. In the same way the coefficients of f_i's are integral over the ring generated by the coefficients of $m_{i,1}$'s. As $\mathbf{A}$ is integrally closed the f_i's and g_j's are in $\mathbf{A}[\,\underline{X}\,]$. □

Case of an integral seminormal ring

Traverso [19] has proved the theorem for Nœtherian reduced ring (with some restrictions). For proofs in the case of integral rings without Nœtherian hypothesis see [1,16,12].

Theorem 3.4. *If* $\mathbf{A}$ *is integral and seminormal, then* $\operatorname{Pic}\mathbf{A} = \operatorname{Pic}\mathbf{A}[\,\underline{X}\,]$.

Proof. We start the proof as in Lemma 3.3. There exist

$$f_1(\,\underline{X}\,), \ldots, f_n(\,\underline{X}\,), g_1(\,\underline{X}\,), \ldots, g_n(\,\underline{X}\,) \text{ in } \mathbf{K}[\,\underline{X}\,]^n$$

such that $m_{i,j} = f_i g_j$ for all i, j. Moreover $f_1(0) = g_1(0) = 1$. Let us call $\mathbf{B}$ the subring of $\mathbf{K}$ generated by $\mathbf{A}$ and by the coefficients of f_i's and g_j's. Kronecker's theorem says that $\mathbf{B}$ is a finite extension of $\mathbf{A}$ (i.e., $\mathbf{B}$ is a finitely generated $\mathbf{A}$-module). Our aim is now to show that $\mathbf{A} = \mathbf{B}$. Let us call $\mathfrak{a}$ the conductor of $\mathbf{A}$ in $\mathbf{B}$, i.e., $\{x \in \mathbf{B} \mid x\mathbf{B} \subseteq \mathbf{A}\}$. It is an ideal of $\mathbf{A}$ and of $\mathbf{B}$. Our aim is now to show that $\mathfrak{a} = \langle 1 \rangle$, i.e., that $\mathbf{C} = \mathbf{A}/\mathfrak{a}$ is trivial.

Lemma 3.5. *If* $\mathbf{A} \subseteq \mathbf{B}$, $\mathbf{A}$ *seminormal and* $\mathbf{B}$ *reduced, then the conductor* $\mathfrak{a}$ *of* $\mathbf{A}$ *in* $\mathbf{B}$ *is a radical ideal of* $\mathbf{B}$.

Proof of Lemma 3.5
We have to show that if $u \in \mathbf{B}$ and $u^2 \in \mathfrak{a}$ then $u \in \mathfrak{a}$. Let $c \in \mathbf{B}$, we have to show that $uc \in \mathbf{A}$. We have $u^2c^2 \in \mathbf{A}$, and $u^3c^3 = u^2(uc^3) \in \mathbf{A}$ since $u^2 \in \mathfrak{a}$. Since $(u^3c^3)^2 = (u^2c^2)^3$ there exists $a \in \mathbf{A}$ such that $a^2 = (uc)^2$ and $a^3 = (uc)^3$. Since $\mathbf{B}$ is reduced this implies $a = uc$, and thus $uc \in \mathbf{A}$. □

Remark 3.6. The *seminormal closure* of a ring $\mathbf{A}$ in a reduced overring $\mathbf{B}$ is obtained by starting with $\mathbf{A}$ and adding elements x of $\mathbf{B}$ such that x^2 and x^3 are in the previously constructed ring. Fact 2.1 implies that x is uniquely determined by x^2 and x^3. So the previous proof can be seen as a proof of the following lemma.

Lemma 3.7. *Let* $\mathbf{A} \subseteq \mathbf{B}$ *be reduced rings,* $\mathbf{A}_1$ *the seminormal closure of* $\mathbf{A}$ *in* $\mathbf{B}$, *and* $\mathfrak{a}$ *the conductor of* $\mathbf{A}_1$ *in* $\mathbf{B}$. *Then* $\mathfrak{a}$ *is a radical ideal of* $\mathbf{B}$.

Lemma 3.8. *Let* $\mathbf{A} \subseteq \mathbf{B} = \mathbf{A}[c_1, \ldots, c_q]$ *be reduced rings with* $\mathbf{B}$ *finite over* $\mathbf{A}$. *Let* $\mathfrak{a}$ *be the conductor of* $\mathbf{A}$ *in* $\mathbf{B}$. *Assume that* $\mathfrak{a}$ *is a radical ideal. Then* $\mathfrak{a}$ *is equal to* $\{x \in \mathbf{A} \mid xc_1, \ldots, xc_q \in \mathbf{A}\}$.

Proof of Lemma 3.8.
Indeed if $xc_i \in \mathbf{A}$ then $x^\ell c_i^\ell \in \mathbf{A}$ for all ℓ, and thus for N big enough $x^N y \in \mathbf{A}$ for all $y \in \mathbf{B}$, thus x is in the radical of $\mathfrak{a}$ (if d bounds the degrees of the integral dependence equations of the c_i's over $\mathbf{A}$, one can take $N = (d-1)q$). □

End of the proof of Theorem 3.4, given within classical mathematics.
Let us assume by contradiction that $\mathfrak{a} \neq \langle 1 \rangle$. One has $\mathbf{C} = \mathbf{A}/\mathfrak{a} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$. Let $\mathfrak{p}$ be a minimal prime of $\mathbf{C}$, $\mathfrak{P}$ the corresponding ideal of $\mathbf{A}$, $S = \mathbf{C} \setminus \mathfrak{p}$ the complementary part. Since $\mathfrak{p}$ is a minimal prime and since $\mathbf{C}$ is reduced $S^{-1}\mathbf{C} = \mathbf{L}$ is a field contained in the reduced ring $S^{-1}\mathbf{C}' = \mathbf{L}'$.
If x is an object defined over $\mathbf{A}$ let us call $\overline{x}$ what it becomes after the change of ring $\mathbf{A} \to \mathbf{L}'$. The module $\overline{M}$ is defined by the matrix $\overline{P}$ whose coefficients are in $\mathbf{L}[\,\underline{X}\,]$. Since $\mathbf{L}$ is a field, $\operatorname{Im}\overline{P}$ is free over $\mathbf{L}[\,\underline{X}\,]$. This implies, by unicity (Lemma 2.5) and since $f_1(0) = g_1(0) = 1$, that the polynomials $\overline{f_i}$ and $\overline{g_j}$ are in $\mathbf{L}[\,\underline{X}\,]$ (if $u(X) \in \mathbf{L}[\,\underline{X}\,]$ is invertible and $u(0) = 1$, then $u = 1$). This means that there exists $s \in \mathbf{A} \setminus \mathfrak{P}$ such that the polynomials sf_i and sg_j have their coefficients in $\mathbf{A}$. Thus Lemma 3.8 implies that $s \in \mathfrak{a}$, a contradiction. □

The proof we have given for Theorem 3.4 is a simplification of existing ones in the literature. Nevertheless it is not fully constructive and this gives only the integral case.

Constructive proof (case seminormal and integral)

Remark first that the proof by contradiction shows that the ring $\mathbf{A}/\mathfrak{a}$ is trivial in the following way: if the ring were not trivial &ct..., it should be trivial. In fact the argument proves directly that the ring is trivial after a slight modification. For this kind of things see Richman's paper [17] about the nontrivial use of the trivial ring.
A most difficult task is to eliminate the use of the minimal prime, which is a *purely ideal object* appearing in the classical proof. A lemma is needed for doing this job.

The intuitive meaning of the lemma is the following:
Let $\mathbf{C}$ *be a reduced ring and* P *a projective module of rank* 1 *over* $\mathbf{C}[\,\underline{X}\,]$*; if* $\mathbf{C}$ *is not trivial, some nontrivial localisation* $S^{-1}\mathbf{C}$ *of* $\mathbf{C}$ *have to exist where* P *becomes free.*
In classical mathematics the answer is easy: use the localisation in a minimal prime. This argument appeared in the proof for the ring $\mathbf{C} = \mathbf{A}/\mathfrak{a}$.
The lemma in this intuitive form "is not true" from a constructive point of view (we lack primes). But fortunately it is the contraposed form which is needed:
Let $\mathbf{C}$ *be a reduced ring and* P *a projective module of rank* 1 *over* $\mathbf{C}[\,\underline{X}\,]$*; if each localisation* $S^{-1}\mathbf{C}$ *of* $\mathbf{C}$ *for which* P *becomes free is trivial, then* $\mathbf{C}$ *is itself trivial.*
And this form "is true" from a constructive point of view, i.e., we get an algorithm!
In fact we need the following version where localisations consist only in inverting one element. Here is THE crucial lemma.

Lemma 3.9 (*Elimination of a Minimal Prime*). *Let* $\mathbf{C}$ *be a reduced ring and* $P = (m_{i,j}) \in \mathbf{C}[\,\underline{X}\,]^{n\times n}$ *an idempotent matrix of rank* 1 *such that* $P(0) = \mathrm{I}_{n,1}$*. Let us assume the following implication:*

$$\forall a \in \mathbf{C},\ \textit{if}\ \operatorname{Im} P\ \textit{is free over}\ \mathbf{C}[1/a][\,\underline{X}\,],\ \textit{then}\ a = 0.$$

Then $\mathbf{C}$ *is trivial.*

Proof that Lemma 3.9 *implies Theorem* 3.4.
We can rewrite the end of the proof of Theorem 3.4, merely replacing the localisation at the "purely ideal" minimal prime $\mathfrak{p}$ by the localisation in one element a.
We have two reduced rings $\mathbf{C} = \mathbf{A}/\mathfrak{a} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$. We want to show that $\mathbf{C}$ is trivial. It is sufficient to show that $\mathbf{C}$ satisfies, with the matrix P mod $\mathfrak{a}$, the hypotheses of THE lemma.
So let a be an element of $\mathbf{A}$ such that $\operatorname{Im} P$ is free over $\mathbf{C}[1/a][\,\underline{X}\,]$. Let $\mathbf{C}[1/a] = \mathbf{L} \subseteq \mathbf{C}'[1/a] = \mathbf{L}'$, which is a reduced ring. If x is an object defined over $\mathbf{A}$ let us call $\overline{x}$ what it becomes after the change of ring $\mathbf{A} \to \mathbf{L}'$. The module $\overline{M}$ is free over $\mathbf{L}[\,\underline{X}\,]$ and this implies, by unicity (Lemma 2.5) and since $f_1(0) = g_1(0) = 1$, that the polynomials $\overline{f_i}$ and $\overline{g_j}$ are in $\mathbf{L}[\,\underline{X}\,]$.
This means that there exists $N \in \mathbb{N}$ such that the $a^N f_i$ and $a^N g_j$ have their coefficients in $\mathbf{A}$. Thus Lemmas 3.5 and 3.8 imply $a \in \mathfrak{a}$, i.e., $a = 0$ in $\mathbf{C}$. □

Proof of Lemma 3.9.
A classical proof: let us assume that $\mathbf{C}$ is nontrivial and let $\mathfrak{p}$ be a minimal prime; since $\mathbf{C}$ is reduced, $\mathbf{C}_\mathfrak{p}$ is a field; thus $\operatorname{Im} P$ becomes free over $\mathbf{C}_\mathfrak{p}[\,\underline{X}\,]$; this implies that there exists an $a \notin \mathfrak{p}$ such that $\operatorname{Im} P$ becomes free over $\mathbf{C}[1/a][\,\underline{X}\,]$; thus $a = 0$, a contradiction.
We have a lemma eliminating a minimal prime. But the proof of the elimination lemma is a proof by contradiction using a minimal prime! *This looks like a bad joke.*
No, because this abstract proof can be reread dynamically and becomes constructive. Here is what happens.
Imagine that the ring $\mathbf{C}$ is a discrete field. Then the f_i's and g_j's are calculated with an algorithm corresponding to the case of a discrete field.
This algorithm uses disjunction "a is zero or invertible", for elements a computed by the algorithm from the coefficients of $m_{i,j}$'s. But $\mathbf{C}$ is only a reduced ring, without equality or inversibility test. So the algorithm for discrete fields has to be replaced by a tree where we open two branches each time a question "Is a zero or invertible?" is asked by the algorithm.
We get a tree, huge, but finite. Assume that the branch "a invertible" is put on the left and let us see what happens at the leaf of the leftmost branch. Some elements $a_1, \ldots, a_n$ have been inverted and the module P became free over $\mathbf{C}[1/(a_1 \cdots a_n)][\,\underline{X}\,]$.
Conclusion: in the ring $\mathbf{C}$, *one has* $a_1 \cdots a_n = 0$.
Let us go up one step.
In the ring $\mathbf{C}[1/(a_1 \cdots a_{n-1})]$, we have $a_n = 0$. So there was no need to open the left branch. What happens in the branch $a_n = 0$? We see what is the computation in the leftmost branch after this node. We have inverted $a_1, \ldots, a_{n-1}$, and afterwards we invert $b_1, \ldots, b_k$ (if $k = 0$ let $b_k = a_{n-1}$).
The module P became free on $\mathbf{C}[1/(a_1 \cdots a_{n-1} b_1 \cdots b_k)][\,\underline{X}\,]$.

Conclusion: in the ring $\mathbf{C}$, *one has* $a_1 \cdots a_{n-1} b_1 \cdots b_k = 0$.
Let us go up one step. Since $b_k = 0$ there was no need to open the left branch. What happens in the branch $b_k = 0$? ...
And so on. At the end of the tale we are at the root of the tree and the module P is free on $\mathbf{C}[\,\underline{X}\,] = \mathbf{C}[1/1][\,\underline{X}\,]$. So $1 = 0$. □

If we use Lemma 3.7 instead of Lemma 3.5 we get the following more precise result.

Theorem 3.10. *If* $\mathbf{A}$ *is an integral ring and* M *a projective module of rank* 1 *over* $\mathbf{A}[\,\underline{X}\,]$, *there exist* $c_1, \ldots, c_m$ *in the fraction field of* $\mathbf{A}$ *such that:*

(1) c_i^2 *and* c_i^3 *are in* $\mathbf{A}[(c_j)_{j<i}]$ *for* $i = 1, \ldots, m$,
(2) M *is free over* $\mathbf{A}[(c_j)_{j \le m}][X]$.

This gives a strongly explicit form of the Traverso–Swan theorem for integral rings.

For further reading

[3].

Annex A. Zero-dimensional reduced rings

In this part, we give some important facts in the theory of zero-dimensional reduced rings. These rings are good substitute for fields. As a consequence we get the general form of the Traverso–Swan theorem. Moreover we get a new proof (without computation tree) of Lemma 3.9 (in fact it is essentially the same proof, the tree is only hidden behind idempotents).

Remark A.1. The idea of replacing the fraction field of $\mathbf{A}$ by a zero-dimensional reduced ring containing $\mathbf{A}$ is not in [18]: Swan uses arguments much more sophisticated in order to reduce the general case to the Nœtherian case. The proof of the general case in [2] is thus a striking improvement of Swan's proof. Moreover the theorem is new since it gives an algorithm instead of a purely abstract statement.

A.1. Basic facts

A ring is *zero-dimensional* when we have

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

If the ring is reduced $d = 1$ is sufficient because $x^d(1 - xa) = 0$ implies $x(1 - xa) = 0$.
In a commutative ring $\mathbf{C}$, two elements a and b are *quasi-inverse* if one has

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

We say also that b is *the* quasi-inverse of a. Indeed it is unique: if $a^2 b = a = a^2 c$, $b^2 a = b$ and $c^2 a = c$, then since $ab = a^2 b^2$, $ac = a^2 c^2$ and $a^2(c - b) = a - a = 0$, we get

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

On the other hand if $x^2 y = x$, one sees that xy^2 is the quasi-inverse of x. So:

Fact A.2. *A ring is zero-dimensional reduced if and only if each element has a quasi-inverse.*

Such rings are also called *absolutely flat* or *von Neumann regular* (this is mainly used in the noncommutative case, with the equations $aba = a$ and $bab = b$).
So, zero-dimensional reduced rings can be defined as equational structures, adding a unary law $a \mapsto a^\bullet$ satisfying (2)

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

This implies, with $e_a = aa^\bullet$,

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

As an easy consequence:

Fact A.3. *A ring is zero-dimensional reduced if and only if any finitely generated ideal is generated by an idempotent.*

The notion of zero-dimensional reduced ring is *the good equational generalisation* of the notion of field. A field is nothing but a zero-dimensional reduced ring which is *connected* (i.e., with 0 and 1 as unique idempotents).

Lemma A.4. *Let $\mathbf{A} \subseteq \mathbf{C}$ with $\mathbf{C}$ zero-dimensional reduced and $a \in \mathbf{C}$. We use the notation $e_a = aa^\bullet$.*

(1) *e_a is the unique idempotent of $\mathbf{C}$ such that $\langle a\rangle = \langle e_a\rangle$. Moreover* $\mathrm{Ann}_{\mathbf{C}}(a) = \mathrm{Ann}_{\mathbf{C}}(e_a) = \langle 1 - e_a\rangle$.
(2) *$\mathbf{C} = e_a\mathbf{C} \oplus (1 - e_a)\mathbf{C}$ with $e_a\mathbf{C} \simeq \mathbf{C}[1/e_a] \simeq \mathbf{C}\big/\langle 1 - e_a\rangle$ and $(1 - e_a)\mathbf{C} \simeq \mathbf{C}\big/\langle e_a\rangle$*
(NB: the ideal $e_a\mathbf{C}$ is not a subring, but it is a ring with e_a as 1).
(3) *In $e_a\mathbf{C}$, a is invertible and in $\mathbf{C}\big/\langle e_a\rangle$, a is null.*
(4) *If $a \in \mathbf{A}$, then $e_a\mathbf{A}[a^\bullet] \simeq \mathbf{A}[1/a]$.*
(5) *More generally, with $a, b, c \in \mathbf{A}$ one has $(e_ae_be_c)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet] \simeq \mathbf{A}[1/(abc)]$.*
(6) *If moreover $abc = 0$, then $(e_ae_b)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet] \simeq \mathbf{A}[1/(ab)]$.*

Proof. The first 3 items are easy and well-known. Let us see (5). In the ring $\mathbf{B} = (e_ae_be_c)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet]$, abc is invertible, with inverse $a^\bullet b^\bullet c^\bullet$. Thus the homomorphism

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

factorises with a unique θ in the following way

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

Since $\mathbf{A} \subseteq \mathbf{C}$, j is injective and we can identify $x \in \mathbf{A}$ and $j(x)$. The homomorphism θ is surjective because $\theta(1/abc) = a^\bullet b^\bullet c^\bullet = u$ and in $\mathbf{B}$, $a^\bullet = bcu,\ b^\bullet = acu,\ c^\bullet = abu$. On the other hand $\mathrm{Ker}\,\pi = \mathrm{Ann}_{\mathbf{A}}(abc) \subseteq \mathrm{Ker}\,\psi$ and if $x \in \mathrm{Ker}\,\psi$, then $e_ae_be_cx = e_{abc}x = 0$, thus $abcx = 0$.
Let us see (6). Since $abc = 0$, $0 = e_{abc} = e_ae_be_c$ and in $(e_ae_b)\mathbf{A}[a^\bullet, b^\bullet, c^\bullet] = \mathbf{B}_1$ one has $c^\bullet = e_ae_bc^\bullet = e_ae_b(e_cc^\bullet) = 0$ thus $\mathbf{B}_1 = (e_ae_b)\mathbf{A}[a^\bullet, b^\bullet]$ and we conclude with (5). □

The two last items generalise with an arbitrary finite number of elements of $\mathbf{A}$.

A possible interpretation of Lemma A.4 is that it works as a formalisation of what happens when we do dynamic computations in a reduced ring "as if" it were a subring of a field. Item 3 says that this dynamical computation is possible (at least if we can find $\mathbf{C}$). Last items show that this dynamical computation can mimic efficiently the localisation at a minimal prime.

Annex B. Reduced rings as subrings of a zero-dimensional reduced ring

Since the notion of zero-dimensional reduced ring is purely equational, universal algebra says that any commutative ring generates a zero-dimensional reduced ring (this gives the adjoint functor to the forgetful functor). We have to see that if the ring $\mathbf{A}$ is reduced, the homomorphism from $\mathbf{A}$ to the zero-dimensional reduced ring it generates is injective.

Lemma B.1. *If $\mathbf{A} \subseteq \mathbf{C}$ with $\mathbf{C}$ zero-dimensional reduced, and if $x^\bullet$ denotes the quasi-inverse of x, then the ring $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ is zero-dimensional (thus it is the least zero-dimensional subring of $\mathbf{C}$ containing $\mathbf{A}$).*
Variant: if $\mathbf{A} \subseteq \mathbf{B}$ are reduced rings, and if each $a \in \mathbf{A}$ has a quasi-inverse $a^\bullet$ in $\mathbf{B}$, then the ring $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ is zero-dimensional.

Proof. We have to show that each element of $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ has a quasi-inverse. Since $(ab)^\bullet = a^\bullet b^\bullet$ each element of $\mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$ can be written $\sum a_i b_i^\bullet$ with $a_i, b_i \in \mathbf{A}$. On the other hand $a_i b_i^\bullet = a_i b_i^\bullet r_i$ with $r_i = a_i a_i^\bullet$ idempotent. Moreover if we have idempotents $r_1, \ldots, r_k$ they generate a Boolean algebra containing a basic system of orthogonal idempotents $e_1, \ldots, e_n$ such that $r_i = \sum_{e_j r_i = e_j} e_j$ $(i \in \{1, \ldots, k\})$. Finally if $e_1, \ldots, e_n$ is a basic system of orthogonal idempotents in $\mathbf{C}$, if $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbf{A}$, if $c = \sum_{i=1}^n a_i b_i^\bullet e_i$ and $c' = \sum_{i=1}^n a_i^\bullet b_i e_i$, then $c^2 c' = c$ and $c'^2 c = c'$, thus $c' = c^\bullet$. □

Lemma B.2. *Let* $\mathbf{A}$ *be a reduced ring and* $a \in \mathbf{A}$. *Let* $\mathbf{B} = \mathbf{A}[T]\big/\langle aT^2 - T, a^2T - a\rangle$ *and* $\mathbf{C} = \mathbf{B}_{\mathrm{red}}$. *Let* $a^\bullet$ *be the image of* T *in* $\mathbf{C}$. *Then*

(1) $\mathbf{C} \simeq (\mathbf{A}\big/\langle a\rangle)_{\mathrm{red}} \times \mathbf{A}[1/a]$ *and the natural homomorphism* $\mathbf{A} \to \mathbf{C}$ *is injective (one identifies* $\mathbf{A}$ *to a subring of* $\mathbf{C}$*).*

(2) $a^\bullet$ *is quasi-inverse of* a *in* $\mathbf{C}$.

(3) *For any homomorphism* $\mathbf{A} \xrightarrow{\varphi} \mathbf{A}'$ *such that* $\varphi(a)$ *has a quasi-inverse in* $\mathbf{B}$, *there exists a unique homomorphism* $\mathbf{C} \xrightarrow{\theta} \mathbf{A}'$ *such that the homomorphism* $\mathbf{A} \to \mathbf{C} \xrightarrow{\theta} \mathbf{A}'$ *is equal to* φ.

The proof is left to the reader. The following corollary is a consequence of the strong unicity property given in Lemma B.2.

Corollary B.3. *Let* $a_1, \ldots, a_n \in \mathbf{A}$. *Then the ring we obtain by repeating the construction of* Lemma B.2 *for each* a_i *does not depend, up to unique isomorphism, of the ordering of* a_i*'s.*

Example: let us denote $\mathbf{A}_{\{a\}}$ the ring constructed in Lemma B.2; let $a, b, c \in \mathbf{A}$; then there exists a unique $\mathbf{A}$-homomorphism

$$((\mathbf{A}_{\{a\}})_{\{b\}})_{\{c\}} \longrightarrow ((\mathbf{A}_{\{c\}})_{\{b\}})_{\{a\}}$$

and it is an isomorphism.

Lemma B.2 and Corollary B.3 give the following theorem.

Theorem B.4. *Let* $\mathbf{A}$ *be a reduced ring. We denote by* $\widehat{\mathbf{A}}$ *the ring we obtain as filtered colimit by iterating the construction of* Lemma B.2 *(*Corollary B.3 *says that this works).*
Then $\widehat{\mathbf{A}}$ *is a zero-dimensional reduced ring and the natural homomorphism* $\mathbf{A} \to \widehat{\mathbf{A}}$ *is injective. Moreover this ring is* the zero-dimensional reduced ring generated by $\mathbf{A}$ *with the precise following meaning: for any zero-dimensional reduced ring* $\mathbf{A}'$, *any homomorphism* $\mathbf{A} \xrightarrow{\varphi} \mathbf{A}'$ *factorises in a unique way via the natural homomorphism* $\mathbf{A} \to \widehat{\mathbf{A}}$.

In a shorter form:

Theorem B.5. *Any reduced ring* $\mathbf{A}$ *is contained in a zero-dimensional reduced ring* $\mathbf{C} = \mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}]$.

Annex C. Zero-dimensional reduced rings and fields

We said that the notion of zero-dimensional reduced ring is *the good equational generalisation* of the notion of field. In particular any equational consequence of field theory is an equational consequence of the theory of zero-dimensional reduced rings.

In an informal way we can give the following local–global elementary principle.

Local–global elementary machinery: from discrete fields to zero-dimensional reduced rings. *Most algorithms that work with discrete fields can be modified in order to work with zero-dimensional reduced rings, decomposing the ring in the product of two components each time the algorithm (written for discrete fields) uses the test "Is this element zero or invertible?". In the first component the element is zero, in the second one it is invertible.*

We have written "most" rather than "all" because the result of the algorithm given for discrete fields has to be written in a form where there is no reference to the connectedness of a discrete field.

Applying the previous local–global machinery allows one to get Theorem C.1 from Lemma 3.1, as soon as we have seen that this lemma gives an algorithm for discrete fields.

Theorem C.1. *Let* $\mathbf{C}$ *be a zero-dimensional reduced ring. Then any projective module of constant rank* 1 *over* $\mathbf{C}[\underline{X}]$ *is free.*

For the sceptical reader, we give some details in Annex E.

Annex D. Traverso–Swan's theorem: general case

New constructive proof of Lemma 3.9

Theorems B.5 and C.1 imply there exists a zero-dimensional reduced ring $\mathbf{C} = \mathbf{A}[(a^\bullet)_{a\in\mathbf{A}}] \supseteq \mathbf{A}$ with $\operatorname{Im} P$ free over $\mathbf{C}[\underline{X}]$. This property remains true for a ring $\mathbf{B} \subseteq \mathbf{C}$ generated by a finite number of quasi-inverses $a_1^\bullet, \dots, a_r^\bullet$ of elements of $\mathbf{A}$. We write $e_i = a_i a_i^\bullet$ (e_i is an idempotent such that $e_i a_i = a_i$ and $e_i a_i^\bullet = a_i^\bullet$) and $e_i' = 1 - e_i$. We give the argument for $r = 3$ but it is clear that the argument is general. We decompose the ring $\mathbf{B}$ into a product of 2^r rings. Equivalently we write the ring as a direct sum of 2^r ideals.

$$\mathbf{B} = \left\{ \begin{array}{l} e_1e_2e_3\mathbf{B} \oplus e_1e_2e_3'\mathbf{B} \oplus e_1e_2'e_3\mathbf{B} \oplus e_1'e_2e_3\mathbf{B} \oplus \\ e_1e_2'e_3'\mathbf{B} \oplus e_1'e_2e_3'\mathbf{B} \oplus e_1'e_2'e_3\mathbf{B} \oplus e_1'e_2'e_3'\mathbf{B}. \end{array} \right. \tag{3}$$

Lemma A.4 item (5) shows that

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

Since the module $\operatorname{Im} P$ is free over $\mathbf{B}[\underline{X}]$, it is free over each of the 2^r components. In particular it is free over $e_1e_2e_3\mathbf{B}[\underline{X}] \simeq \mathbf{A}[1/(a_1a_2a_3)][\underline{X}]$. From the hypothesis in Lemma 3.9 we get $a_1a_2a_3 = 0$, thus $e_1e_2e_3 = 0$, $e_1e_2e_3' = e_1e_2$, etc., and the decomposition (3) becomes

$$\mathbf{B} = e_1e_2\mathbf{B} \oplus e_1e_3\mathbf{B} \oplus e_2e_3\mathbf{B} \oplus e_1e_2'e_3'\mathbf{B} \oplus e_1'e_2e_3'\mathbf{B} \oplus e_1'e_2'e_3\mathbf{B} \oplus e_1'e_2'e_3'\mathbf{B}.$$

Lemma A.4 item (6) shows that $e_1e_2\mathbf{B} \simeq \mathbf{A}[1/(a_1a_2)]$. Since P is free over this component we get $a_1a_2 = 0$, thus $e_1e_2 = 0$, $e_1e_2' = e_1$, $e_1'e_2 = e_2$. Similarly $a_1a_3 = 0 = e_1e_3$, $a_2a_3 = 0 = e_2e_3$ and finally $e_1e_2'e_3' = e_1$, $e_1'e_2e_3' = e_2$, $e_1'e_2'e_3 = e_3$. We get a new decomposition

$$\mathbf{B} = e_1\mathbf{B} \oplus e_2\mathbf{B} \oplus e_3\mathbf{B} \oplus e_1'e_2'e_3'\mathbf{B}.$$

At the end each a_i is null and $\mathbf{B} = \mathbf{A} = \mathbf{A}[1/1]$. So $1 = 0$ in $\mathbf{A}$. □

Theorem D.1 (*Traverso–Swan–Coquand*). *If* $\mathbf{A}$ *is a seminormal ring, then* $\mathsf{Pic}\,\mathbf{A} = \mathsf{Pic}\,\mathbf{A}[\underline{X}]$.
More precisely if a matrix $P(\underline{X}) \in \mathbf{A}[\underline{X}]^{n\times n} = (m_{i,j}(\underline{X}))_{i,j\in\{1,\dots,n\}}$ *is idempotent of rank 1 and if* $P(0) = \mathrm{I}_{n,1}$, *then we can construct polynomials*

$$f_1, \dots, f_n, g_1, \dots, g_n \in \mathbf{A}[\underline{X}]$$

such that $m_{i,j} = f_i g_j$ *for all* i, j.

Proof. This proof is only a slight variation of the one given for the integral case.
We use the characterisation given in Lemma 2.6. Let $P(\underline{X}) = (m_{i,j}(\underline{X}))_{i,j=1,\dots,n}$ be an idempotent matrix of rank 1 with $P(0) = \mathrm{I}_{n,1}$. Let $\mathbf{K}$ be a zero-dimensional reduced ring containing $\mathbf{A}$. On $\mathbf{K}[\underline{X}]$ the module $\operatorname{Im} P(\underline{X})$ is free. Thus there exist $f = (f_1(\underline{X}), \dots, f_n(\underline{X}))$ and $g = (g_1(\underline{X}), \dots, g_n(\underline{X}))$ in $\mathbf{K}[\underline{X}]^n$ such that $m_{i,j} = f_i g_j$ for all i, j. Moreover since $f_1(0)g_1(0) = 1$ and since we can modify f and g multiplying them by units, we can assume that $f_1(0) = g_1(0) = 1$. Since $f_1 g_j = m_{1,j}$ and using Kronecker theorem, the coefficients des g_j are integral over the ring generated by the coefficients of $m_{1,j}$'s. In the same way the coefficients of f_i's are integral over the ring generated by the coefficients of $m_{i,1}$'s.
Let $\mathbf{B}$ be the subring of $\mathbf{K}$ generated by $\mathbf{A}$ and by the coefficients of f_i's and g_j's. Thus $\mathbf{B}$ is a finite extension of $\mathbf{A}$ (i.e., $\mathbf{B}$ is a finitely generated $\mathbf{A}$-module). We have to show $\mathbf{A} = \mathbf{B}$. Let us call $\mathfrak{a}$ the conductor of $\mathbf{A}$ in $\mathbf{B}$. Our aim now is to show that $\mathfrak{a} = \langle 1 \rangle$, i.e., $\mathbf{A}/\mathfrak{a}$ is trivial.
Following Lemma 3.5 $\mathfrak{a}$ is a radical ideal of $\mathbf{B}$. Lemma 3.8 applies with $\mathbf{A} \subseteq \mathbf{B}$. We have $\mathbf{A}/\mathfrak{a} = \mathbf{C} \subseteq \mathbf{B}/\mathfrak{a} = \mathbf{C}'$, which is reduced, and $f_i g_j = m_{i,j}$ in $\mathbf{B}/\mathfrak{a}$. To show that $\mathbf{C}$ is trivial, it is sufficient to show that $\mathbf{C}$ satisfies, with the matrix P mod $\mathfrak{a}$, the hypotheses of Lemma 3.9.

So let us consider an $a \in \mathbf{A}$ such that $\operatorname{Im} P$ is free over $\mathbf{C}[1/a][\underline{X}]$ and let $\mathbf{C}[1/a] = \mathbf{L} \subseteq \mathbf{C}'[1/a] = \mathbf{L}'$. If x is an object defined over $\mathbf{A}$ let us call $\overline{x}$ what it becomes after the change of ring $\mathbf{A} \to \mathbf{L}'$. The module $\overline{M}$ is free over $\mathbf{L}[\underline{X}]$. This implies, by unicity (Lemma 2.5) and since $f_1(0) = g_1(0) = 1$, that the polynomials $\overline{f_i}$ and $\overline{g_j}$ are in $\mathbf{L}[\underline{X}]$ (if $u(X) \in \mathbf{L}[\underline{X}]$ is invertible and $u(0) = 1$, then $u = 1$).
This means that there exists $N \in \mathbb{N}$ such that the polynomials $a^N f_i$ and $a^N g_j$ have their coefficients in $\mathbf{A}$. Thus Lemma 3.8 implies that $a \in \mathfrak{a}$, i.e., $a = 0$ in $\mathbf{C}$. □

If we use Lemma 3.7 instead of Lemma 3.5 we get the following more precise result.

Theorem D.2. *If* $\mathbf{A}$ *is a ring contained in a zero-dimensional reduced ring* $\mathbf{B}$ *and* M *a projective module of rank* 1 *over* $\mathbf{A}[\underline{X}]$*, there exist* $c_1, \dots, c_m$ *in* $\mathbf{B}$ *such that:*

(1) c_i^2 *and* c_i^3 *are in* $\mathbf{A}[(c_j)_{j<i}]$ *for* $i = 1, \dots, m$,
(2) M *is free over* $\mathbf{A}[(c_j)_{j \le m}][X]$.

Annex E. Gcd rings

In this section we give a detailed proof of Theorem C.1, without using the local–global elementary machinery (see Annex C).

Definition E.1. A ring $\mathbf{A}$ is called *a pp-ring* if the annihilator of each element is (a principal ideal generated by an) idempotent. For $a \in \mathbf{A}$, we denote e_a the idempotent such that $\operatorname{Ann}(a) = \langle 1 - e_a \rangle$. So a is regular in $\mathbf{A}[1/e_a]$ and null in $\mathbf{A}[1/(1 - e_a)]$.

An integral ring is exactly a connected pp-ring.

Lemma E.2. *Let* $x_1, \dots, x_n$ *be elements of a commutative ring. If one has* $\operatorname{Ann}(x_i) = \langle r_i \rangle$ *where* r_i*'s are idempotent* $(1 \le i \le n)$*, let* $s_i = 1 - r_i$, $t_1 = s_1$, $t_2 = r_1 s_2$, $t_3 = r_1 r_2 s_3, \dots, t_{n+1} = r_1 r_2 \cdots r_n$*. Then* $t_1, \dots, t_{n+1}$ *is a basic system of orthogonal idempotents and the element* $x = x_1 + t_2 x_2 + \cdots + t_n x_n$ *satisfies* $\operatorname{Ann}(x_1, \dots, x_n) = \operatorname{Ann}(x) = \langle t_{n+1} \rangle$.

Corollary E.3. *Let* $\mathbf{A}$ *be a pp-ring and* $P = (m_{ij})_{1 \le i,j \le n}$ *a square matrix such that* $\operatorname{Tr}(P)$ *is regular. Then there exists a matrix* $J \in \mathbf{A}^{n \times n}$ *such that* $J^2 = \mathrm{I}_n$ *and* $JPJ = JPJ^{-1}$ *has a regular coefficient in position* $(1, 1)$.

Proof. We apply Lemma E.2 with the elements $x_i = m_{i,i}$. We have $t_{n+1} = 0$ because $t_{n+1}\operatorname{Tr}(P) = 0$. Thus $(t_1, \dots, t_n)$ is a basic system of orthogonal idempotents. Let J_k be the permutation matrix exchanging vectors 1 and k in the canonical basis. Let $J = t_1 \mathrm{I}_n + t_2 J_2 + \cdots + t_n J_n$. We have $J^2 = \mathrm{I}_n$ and the coefficient in position $(1, 1)$ of JPJ is equal to $x = t_1 x_1 + t_2 x_2 + \cdots + t_n x_n = x_1 + t_2 x_2 + \cdots + t_n x_n$, thus it is regular. □

A zero-dimensional reduced ring is a pp-ring and if $\mathbf{A}$ is a pp-ring, then the total fraction ring of $\mathbf{A}$, denoted by $\operatorname{Frac}(\mathbf{A})$, is a zero-dimensional reduced ring: for all a, $\widetilde{a} = (1 - e_a) + a$ is regular and $a/\widetilde{a} = a^\bullet$ is a quasi-inverse of a in $\operatorname{Frac}(\mathbf{A})$. Moreover, for all $a \in \mathbf{A}$, $\mathbf{A}[1/a]$ is a pp-ring and $\operatorname{Frac}(\mathbf{A}[1/a])$ can be identified with $e_a \operatorname{Frac}(\mathbf{A}) \simeq \operatorname{Frac}(\mathbf{A})[1/a]$.
Finally, if $\mathbf{A}$ is a pp-ring then $\mathbf{A}[X]$ is a pp-ring and the annihilator of a polynomial f is generated by the idempotent equal to the product of annihilators of the coefficients.
In a pp-ring if a divides b and b divides a, one has $e_a = e_b$ and $ua = b$ with an invertible element u. This allows us to develop a theory of gcd pp-rings analogous to the theory of gcd domains.

Definition E.4. A commutative regular monoid is called a *gcd monoid* if any two elements do have a greatest common divisor. If g is a gcd for a and b we write $g = \gcd(a, b)$ (in fact a gcd is defined up to a unit).

Lemma E.5. *Let* $\mathbf{A}$ *be a pp-ring. The following are equivalent:*

(1) *The monoid of regular elements is a gcd monoid.*
(2) *For any idempotent e regular elements of* $\mathbf{A}[1/e]$ *give a gcd monoid.*
(3) *Two arbitrary elements have a gcd.*

In this case we say that $\mathbf{A}$ *is a* gcd pp-ring.

Proof. For example, to show that (1). implies (2), one introduces, for $a \in e\mathbf{A}$ with a regular in $\mathbf{A}[1/e]$, the element $\widetilde{a} = (1 - e_a) + a$ which is regular in $\mathbf{A}$. If g is the gcd of $\widetilde{a}$ and $\widetilde{c}$ in $\mathbf{A}$, the same element g, viewed in $\mathbf{A}[1/e]$, is the gcd of a and c. □

A gcd pp-ring which is connected is a usual gcd ring. A zero-dimensional reduced ring is a gcd pp-ring.
Let $\mathbf{A}$ be a gcd pp-ring and a polynomial $f(X) = \sum_{k=0}^{n} f_k X^k$, we denote by $\mathrm{G}(f)$ the gcd (defined up to a unit) of the coefficients of f. If $\mathrm{G}(f) = 1$ one says that f is primitive.[1]
We have to see that arguments in the proof of Lemma 3.1 work also for gcd pp-rings. In particular, *if* $\mathbf{A}$ *is a gcd pp-ring, so is* $\mathbf{A}[X]$. So for any zero-dimensional reduced ring $\mathbf{A}$, the ring $\mathbf{A}[\,\underline{X}\,]$ is a gcd pp-ring and thus any projective module of constant rank 1 over $\mathbf{A}[\,\underline{X}\,]$ is free.
Let us see the first argument in the proof: *Let* $P = (m_{i,j})$ *be an idempotent matrix of rank 1. Since* $\sum_i m_{i,i} = 1$ *we can assume that* $m_{1,1}$ *is regular.* Corollary E.3 gives the answer.
For the end of the proof we look at the "bible" [15], where all proofs are algorithmic (and often very simple).

Lemma E.6 (*cf. Theorem 1.1 page 108 in [15]*). *Let* a, b, c *be elements of a gcd pp-ring. Then*

(1) $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.
(2) $c \cdot \gcd(a, b) = \gcd(ca, cb)$.
(3) *If* $x = \gcd(a, b)$, *then* $\gcd(a, bc) = \gcd(a, xc)$.
(4) *If* $a|bc$ *and* $\gcd(a, b) = e_b$ *then* $a|e_b c$.

Proof. If one of the 3 elements a, b, c is null, all is clear. In the general case let r_i be an element of the basic system of orthogonal idempotents generated by e_a, e_b and e_c. Each element a, b, c is null or regular in $\mathbf{A}[1/r_i]$. The proof given in [15] for gcd monoids works for the component in which a, b, c are regular. □

A consequence of item (2) in Lemma E.6 is that in a gcd pp-ring, a primitive polynomial is a regular element of $\mathbf{A}[X]$.

Lemma E.7 (*Lemma 4.2 page 123 in [15]*). *Let* $\mathbf{A}$ *be a gcd pp-ring,* $\mathbf{K} = \mathrm{Frac}(\mathbf{A})$ *and* $f \in \mathbf{K}[X]$. *We can find a primitive polynomial* $g \in \mathbf{A}[X]$ *and* $c \in \mathbf{K}$ *such that* $f = cg$. *If we have another decomposition* $f = c'g'$ *then there exists* $u \in \mathbf{A}^\times$ *such that* $c = uc'$.

Proof. If $f = 0$ we take $g = 1$ and $c = 0$. If $\mathrm{G}(f)$ is regular, the proof in [15] works, replacing "$\neq 0$" by "regular". Thus we decompose the ring into two components by using the idempotent $e_{\mathrm{G}(f)}$. □

Lemma E.8 (*Gauss Lemma, Lemma 4.3 page 123 in [15]*). *Let* $\mathbf{A}$ *be a gcd pp-ring and* $f, g \in \mathbf{A}[X]$. *Then* $\mathrm{G}(f)\mathrm{G}(g) = \mathrm{G}(fg)$.

Proof. Let (r_i) be the basic system of orthogonal idempotents generated by e_c's for all coefficients c of f and g. In each ring $\mathbf{A}[1/r_i]$ polynomials f and g have a well-defined degree.[2] Let us see whether the elegant proof by induction on $n + m = \deg(f) + \deg(g)$ given in [15] works.
We reason by induction on $m + n$. By distributivity (item 2 in Lemma E.6) and using Lemma E.7, we are reduced to the case where $\mathrm{G}(f) = \mathrm{G}(g) = 1$. Let $c = \mathrm{G}(fg)$ and $d = \gcd(f_n, c)$. Then d divides $(f - f_n X^n)\, g$. If $f = f_n X^n$ the result is clear. In the other case, by induction hypothesis d divides $\mathrm{G}(f - f_n X^n)\,\mathrm{G}(g) = \mathrm{G}(f - f_n X^n)$, thus d divides f and $d = 1$. So $\gcd(f_n, c) = 1$. Similarly $\gcd(g_m, c) = 1$ and since c divides $f_n g_m$, $c = 1$. □

Finally proofs in [15] for the following two results do work in our new context.

Corollary E.9 (*Corollary 4.4 page 123 in [15]*). *Let* $\mathbf{A}$ *be a gcd pp-ring,* $f, g \in \mathbf{A}[X]$ *and* $\mathbf{K} = \mathrm{Frac}(\mathbf{A})$. *Then* f *divides* g *in* $\mathbf{A}[X]$ *if and only if* f *divides* g *in* $\mathbf{K}[X]$ *and* $\mathrm{G}(f)$ *divides* $\mathrm{G}(g)$.

Theorem E.10 (*Theorem 4.6 page 124 in [15]*). *If* $\mathbf{A}$ *is a gcd pp-ring, then so is* $\mathbf{A}[X]$.

[1] Warning. This conflicts another traditional terminology: f is primitive when the ideal of coefficients of f contains 1.

[2] Precisely we know an integer $q \geq 0$ such that the coefficient of degree q is leading and regular. Note that there is no need to assume that we know whether the ring is trivial or not.

In fact all these verifications are quasi-automatic. Proofs in [15], which are also algorithms, are based on the disjunction "$x = 0$ or x regular" in a gcd integral ring. In the case of gcd pp-rings, it is sufficient to realise the disjunction by decomposing the ring into two components by using the idempotent e_x.

References

[1] J.W. Brewer, D.L. Costa, Seminormality and projective modules over polynomial rings, J. Algebra 58 (1) (1979) 208–216.

[2] T. Coquand, On seminormality, J. Algebra 305 (2006) 577–584.

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

[4] T. Coquand, L. Ducos, H. Lombardi, C. Quitté, L'idéal des coefficients du produit de deux polynomes, Rev. Math. Enseign. Supér. 113 (3) (2003) 25–39.

[5] T. Coquand, H. Lombardi, Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings, in: M. Fontana, S.-E. Kabbaj, S. Wiegand (Eds.), Commutative Ring Theory and Applications, in: Lecture Notes in Pure and Applied Mathematics, vol. 231, M. Dekker, 2002, pp. 477–499.

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

[7] T. Coquand, H. Lombardi, C. Quitté, Dimension de Heitmann des treillis distributifs et des anneaux commutatifs, Publications mathématiques de Besançon. Algèbre et Théorie des Nombres (2006) 57–100.

[8] T. Coquand, H. Lombardi, M.-F. Roy, An elementary characterisation of Krull dimension, in: L. Crosilla, P. Schuster (Eds.), From Sets and Types to Analysis and Topology: Towards Practicable Foundations for Constructive Mathematics, Oxford University Press, 2005, pp. 239–244.

[9] M. Coste, H. Lombardi, M.-F. Roy, Dynamical method in algebra: Effective Nullstellensätze, Ann. Pure Appl. Logic 111 (2001) 203–256.

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

[11] H. Edwards, Divisor Theory, Birkhäuser, Boston, MA, 1989.

[12] R. Gilmer, R. Heitmann, On $\mathsf{Pic}\, R[X]$ for R seminormal, J. Pure Appl. Algebra 16 (1980) 251–257.

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

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

[15] R. Mines, F. Richman, W. Ruitenburg, A Course in Constructive Algebra, Springer-Verlag, 1988.

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

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

[18] R.G. Swan, On seminormality, J. Algebra 67 (1980) 210–229.

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

[20] I. Yengui, Making the use of maximal ideals constructive, Theoret. Comput. Sci. 392 (1–3) (2008) 174–178.