Projective modules over polynomial rings: a constructive approach

Sami Barhoumi ([1]), Henri Lombardi ([2]), Ihsen Yengui ([3])

April 27, 2006

Abstract

We give a constructive proof of the fact that finitely generated projective modules over a polynomial ring with coefficients in a Prüfer domain $\mathbf{R}$ with Krull dimension ≤ 1 are extended from $\mathbf{R}$. In particular, we obtain constructively that finitely generated projective $\mathbf{R}[X_1, \dots, X_n]$-modules, where $\mathbf{R}$ is a Bezout domain with Krull dimension ≤ 1, are free. Our proof is essentially based on a dynamical method for decreasing the Krull dimension and a constructive rereading of the original proof given by Maroscia and Brewer&Costa. Moreover, we obtain a simple constructive proof of a result due to Lequain and Simis stating that finitely generated modules over $\mathbf{R}[X_1, \dots, X_n]$, $n \geq 2$, are extended from $\mathbf{R}$ if and only if this holds for $n = 1$, where $\mathbf{R}$ is an arithmetical ring with finite Krull dimension.

MSC 2000 : 13C10, 19A13, 14Q20, 03F65.

Key words : Quillen-Suslin's Theorem, Finitely generated projective modules, Local-global principles, Arithmetical rings, Constructive Mathematics.

Introduction

In 1955, J.-P. Serre remarked [16] that it was not known whether there exist finitely generated projective modules over $\mathbf{A} = \mathbf{K}[X_1, \dots, X_n]$, $\mathbf{K}$ a field, which are not free. This remark turned into the "Serre conjecture", stating that indeed there were no such modules. Proven independently by D. Quillen [15] and A. A. Suslin [18], it became subsequently known as the Quillen-Suslin theorem. The book of Lam [7] is a nice exposition about Serre's conjecture. The idea of Quillen's proof is to use the fact that if a finitely generated projective $\mathbf{R}[X]$-module is free when tensored by $\mathbf{R}\langle X\rangle$, the localization of $\mathbf{R}[X]$ at monic polynomials, then it is free. Thus, if $\mathcal{P}$ is a class of rings closed under the formation of $\mathbf{R}\langle X\rangle$ and such that, over any $\mathbf{R}$ in $\mathcal{P}$, finitely generated projective module are free, then finitely generated projective modules are free over $\mathbf{R}[X]$, for any $\mathbf{R}$ in $\mathcal{P}$. An easy induction yields that finitely generated projective modules over $\mathbf{R}[X_1, \dots, X_n]$ are free for $\mathbf{R}$ in $\mathcal{P}$. Consequently a lot of mathematicians have been interested in the ring $\mathbf{R}\langle X\rangle$ especially to the question when $\mathbf{R}\langle X\rangle$ is a Prüfer domain. In [1, 13], Maroscia and Brewer&Costa generalized the Quillen-Suslin theorem to Prüfer domains with Krull dimension ≤ 1 as follows:

Theorem *If $\mathbf{R}$ is a Prüfer domain with Krull dimension ≤ 1, then each finitely generated projective module over the ring $\mathbf{R}[X_1, \dots, X_n]$ is extended. In particular, if $\mathbf{R}$ is a Bezout domain with Krull dimension ≤ 1, then each finitely generated projective module over $\mathbf{R}[X_1, \dots, X_n]$ is free.*

[1] Département de Mathématiques, Faculté des Sciences de Sfax, B.P. 802 Sfax, Tunisia

[2] Equipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANÇON cedex, FRANCE, email: henri.lombardi@univ-fcomte.fr.

[3] Département de Mathématiques, Faculté des Sciences de Sfax, B.P. 802 Sfax, Tunisia, Email: ihsen.yengui@fss.rnu.tn

This result was an outstanding generalization of the Quillen-Suslin theorem since it is Noetherian-free. The restriction to Prüfer domains with Krull dimension ≤ 1 is due to the fact that $\mathbf{R}\langle X\rangle$ is a Prüfer domain if and only if $\mathbf{R}$ is a Prüfer domain with Krull dimension ≤ 1.

It is worth pointing out that Lombardi, Quitté and Yengui [12] have obtained a constructive proof of this same result. Our goal is to obtain a simplified proof of the theorem of Maroscia and Brewer&Costa using the same philosophy as in [12] but adding a technical lemma which enables us to decrease dynamically the Krull dimension and thus brings a significant simplification of the proof given in [12].

In [8], Lequain and Simis obtained a stronger theorem with the same conclusion but without the Krull dimension condition. Namely, they proved that for any Prüfer domain $\mathbf{R}$, all finitely generated projective module over the ring $\mathbf{R}[X_1,\dots,X_n]$, $n\geq 2$, are extended from $\mathbf{R}$ if and only if this holds for $n=1$. Coupled with a result by Simis and Vasconcelos [17] asserting that over a valuation ring $\mathbf{V}$, all projective $\mathbf{V}[X]$-modules are free, they obtain that for any Prüfer domain $\mathbf{R}$, all finitely generated projective $\mathbf{R}[X_1,\dots,X_n]$-module are extended from $\mathbf{R}$.

Lequain and Simis put considerable effort for proving this marvellous theorem and they used some quite complicated technical steps. One challenge was to extend this result to arithmetical rings (rings which are locally valuation rings) using only constructive reasoning, that is, to obtain a constructive proof of Lequain-Simis result without supposing that the basic ring $\mathbf{R}$ is integral.

In this paper, we give a simple constructive proof of this result based on one "important" property satisfied by the ring $\mathbf{R}\langle X\rangle$ when $\mathbf{R}$ is an arithmetical ring. Namely, we prove that for any arithmetical ring $\mathbf{R}$ with Krull dimension $\leq d$, the ring $\mathbf{R}\langle X\rangle$ "dynamically behaves like a valuation ring or a localization of a polynomial ring over an arithmetical ring with Krull dimension $\leq d-1$" as will be explained later. The dynamical method is for example explained in [3, 10] and has been used successfully in [19].

In order to obtain a complete constructive proof of Lequain-Simis-Vasconcelos theorem, we should need two more things. First, a constructive argument allowing to drop the finiteness condition on the Krull dimension, as done in [8] (within classical mathematics). Second, a constructive proof of Simis&Vasconcelos theorem [17] asserting that over a valuation ring $\mathbf{V}$, all projective $\mathbf{V}[X]$-modules are free.

In order to avoid repetition, we assume that the reader have a copy of [12] in hands.

The undefined terminology is standard as in [6, 7], and, for constructive algebra in [14].

1 Constructive preliminaries

1.1 Some constructive definitions

If S is a multiplicative subset of a ring $\mathbf{R}$, the localization of $\mathbf{R}$ at S is the ring $S^{-1}\mathbf{R}=\{\frac{x}{s}, x\in\mathbf{R}, s\in S\}$ in which the elements of S are forced into being invertible. For $x_1,\dots,x_r\in\mathbf{R}$, $\mathcal{M}(x_1,\dots,x_r)$ will denote the multiplicative subset of $\mathbf{R}$ generated by $x_1,\dots,x_r$, that is,

$$\mathcal{M}(x_1,\dots,x_r)=\{x_1^{n_1}\cdots x_r^{n_r}, n_i\in\mathbb{N}\}.$$

The localization of $\mathbf{R}$ at $\mathcal{M}(x_1,\dots,x_r)$ is the same one as the localization at $\mathcal{M}(x_1\cdots x_r)$. If $x\in\mathbf{R}$, the localization of $\mathbf{R}$ at the multiplicative subset $\mathcal{M}(x)$ will be denoted by $\mathbf{R}_x$.

Definition 1.1 *(Comaximal multiplicative subsets [5])*
If $S_1,\dots,S_k$ are multiplicative subsets of $\mathbf{R}$, we say that $S_1,\dots,S_k$ are comaximal *if*

$$\forall s_1\in S_1,\dots,s_n\in S_n,\ \exists\, a_1,\dots,a_n\in\mathbf{R}\text{ such that}\sum_{i=1}^{n}a_is_i=1.$$

Definition 1.2 *(Constructive definition of arithmetical rings [5])*
A ring $\mathbf{R}$ *(not necessarily integral) is said to be an* arithmetical ring *if for any* $x_1, x_2 \in \mathbf{R}$ *there exist* $u, v, w \in \mathbf{R}$ *solutions of the following system*

$$\begin{cases} u\,x_2 = v\,x_1 \\ w\,x_2 = (1-u)\,x_1. \end{cases}$$

Thus, x_1 divides x_2 in the ring $\mathbf{R}_u$ and x_2 divides x_1 in the ring $\mathbf{R}_{1-u}$, where the multiplicative subsets $\mathcal{M}(u)$ and $\mathcal{M}(1-u)$ are obviously comaximal. This is not surprising, since we know that if we localize an arithmetical ring at a prime ideal we find a valuation ring (a ring in which all elements are comparable under division).

The following fact is easy;

Fact 1.3 *A ring* $\mathbf{R}$ *is arithmetical if and only for all* $x_1, x_2 \in \mathbf{R}$ *there exist comaximal multiplicative subsets* $S_1, \dots, S_n$ *in* $\mathbf{R}$ *such that in each localization* $\mathbf{R}_{S_i}$*,* x_1 *divides* x_2 *or* x_2 *divides* x_1*.*

An arithmetical integral ring is also called a *Prüfer domain.*

Definition 1.4 *(Constructive definition of Krull dimension [9, 2, 4])*
A ring $\mathbf{R}$ *is said to have Krull dimension less or equal to* d *(in short,* $\dim \mathbf{R} \le d$*) if for every* $x \in \mathbf{R}$*,* $\dim S_x^{-1}\mathbf{R} \le d-1$*, where* $S_x = \{x^k(1+yx), k \in \mathbb{N}, y \in \mathbf{R}\}$ *and with the initialization* $\dim \mathbf{R} \le -1$ *if* $1 = 0$ *in* $\mathbf{R}$ *(*$\mathbf{R}$ *is trivial). A ring* $\mathbf{R}$ *is said to be finite-dimensional if* $\dim \mathbf{R} \le d$ *for some* $d \in \mathbb{N}$*.*

As a particular case, if $\dim \mathbf{R} \le d$, $d \ge 0$ and $x \in \mathrm{Rad}(\mathbf{R})$ then, constructively, $\dim \mathbf{R}[1/x] \le d-1$.

1.2 Dynamical evaluation of an arithmetical ring as a valuation domain

In classical reasonings it is often allowed to derive results for arithmetical rings from the same results obtained for valuation domain, using a so called "local global principle".

Now we explain how to manage this argument in a constructive way. Recall that the Jacobson radical of a ring $\mathbf{R}$ can be defined constructively as $\{\, x \in \mathbf{R} \,|\, 1 + x\mathbf{R} \subseteq \mathbf{R}^\times \,\}$.

The proof given in the case of a valuation domain $\mathbf{V}$ uses the following disjunction principle:

$$\forall a, b \in \mathbf{V}, \qquad ((\exists x \in \mathbf{V}^\times,\ a = xb) \quad \text{or} \quad (\exists y \in \mathrm{Rad}(\mathbf{V}),\ a = yb) \quad \text{or} \quad (\exists z \in \mathrm{Rad}(\mathbf{V}),\ b = za)) \quad (1)$$

When rereading dynamically the proof for the case of an arithmetical ring, we are going to explain that we can open branches with comaximal localizations that mimic the disjunction.

More precisely, in order to well understand what happens we recall the definition of a *finite potential prime ideal* in a ring R (idealistic primes in [2]). This is a pair $\mathfrak{P} = (I; U) = (a_1, \dots, a_n; u_1, \dots u_m)$ of finite sequences of elements in $\mathbf{R}$. To such a potential prime is associated the multiplicative subset

$$\mathcal{S}(\mathfrak{P}) = \{\, u_1^{k_1} \cdots u_m^{k_m} + x_1 a_1 + \cdots + x_n a_n \,|\, k_1, \dots, k_n \in \mathbb{N},\ x_1, \dots, x_n \in \mathbf{R} \,\}.$$

In the ring $\mathcal{S}(\mathfrak{P})^{-1}\mathbf{R}$, denoted as $\mathbf{R}_{\mathfrak{P}}$, $a_1, \dots, a_n$ are in the Jacobson radical, and $u_1, \dots u_m$ are invertible.

Moreover we have the following easy and crucial lemma.

Lemma 1.5 *If* $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ *are finite potential prime ideals defining comaximal localizations of the ring* $\mathbf{R}$*, if moreover* $\mathfrak{P}_1 = (I; U)$ *and* $x \in \mathbf{R}$*, let us define* $\mathfrak{P}_1' = (I, x; U)$ *and* $\mathfrak{P}_1'' = (I; x, U)$*. Then* $\mathfrak{P}_1', \mathfrak{P}_1'', \mathfrak{P}_2, \dots, \mathfrak{P}_m$ *are finite potential prime ideals defining comaximal localizations of the ring* $\mathbf{R}$*.*

Let us now consider two elements a, b in an arithmetical ring $\mathbf{R}$. There exist $u, v, u', v' \in \mathbf{R}$ such that

$$ua = vb,\ u'b = v'a,\ u + u' = 1.$$

The potential primes $(0;u)$ and $(0;u')$ define comaximal localizations. It follows that the potential primes $(v;u)$, $(0;uv)$, $(0;u'v')$ and $(v';u')$ define comaximal localizations. In the first one we get $a = yb$ with y in the Jacobson radical, in the two second ones we get $a = xb$ with x a unit and in the last one we get $b = za$ with z in the Jacobson radical.

A similar thing happens when $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ are finite potential prime ideals defining comaximal localizations of the arithmetical ring $\mathbf{R}$. If $\mathfrak{P}_1 = (I;U)$ then the potential primes

$$(I, v; u, U), (I; uv, U), (I; u'v', U), (I, v'; u', U), \mathfrak{P}_2, \ldots, \mathfrak{P}_m$$

define comaximal localizations of the ring $\mathbf{R}$. In the first one we get $a = yb$ with y in the Jacobson radical, in the two second ones we get $a = xb$ with x a unit and in the 4-th one we get $b = za$ with z in the Jacobson radical.

1.3 The patchings of Quillen and Vaserstein

We give here a detailed constructive proof of the Quillen's patching. This is essentially written up from [6]. The localization at maximal ideals is replaced by localization at comaximal multiplicative subsets.

In [12] the constructive Quillen's patching (Concrete Local-Global Principle 4) is given with only a sketch of proof.

Lemma 1.6 *Let S be a multiplicative subset of a ring $\mathbf{R}$ and consider three matrices A_1, A_2, A_3 with entries in $\mathbf{R}[X]$ such that the product A_1A_2 has the same size as A_3. If $A_1A_2 = A_3$ in $\mathbf{R}_S[X]$ and $A_1(0)A_2(0) = A_3(0)$ in $\mathbf{R}$, then there exists $s \in S$ such that $A_1(sX)A_2(sX) = A_3(sX)$ in $\mathbf{R}[X]$.*

Proof All the coefficients of the matrix $A_1A_2 - A_3$ are multiple of X and become zero after localization at S. Thus, there exists $s \in S$ annihilating all of them. Write $A_1A_2 - A_3 = B(X) = XB_1 + X^2B_2 + \cdots + X^kB_k$. We have $sB_1 = sB_2 = \cdots = sB_k = 0$ and thus $sB_1 = s^2B_2 = \cdots = s^kB_k = 0$, that is, $B(sX) = A_1(sX)A_2(sX) - A_3(sX) = 0$. □

Lemma 1.7 *Let S be a multiplicative subset of a ring $\mathbf{R}$ and consider a matrix $C(X) \in \mathbf{GL}_r(\mathbf{R}_S[X])$. Then there exists $s \in S$ and $U(X,Y) \in \mathbf{GL}_r(\mathbf{R}[X,Y])$ such that $U(X,0) = \mathbf{I}_r$, and, over $\mathbf{R}_S[X,Y]$, $U(X,Y) = C(X+sY)C(X)^{-1}$.*

Proof Set $E(X,Y) = C(X+Y)C(X)^{-1}$ and denote $F(X,Y)$ the inverse of $E(X,Y)$. We have $E(X,0) = \mathbf{I}_r$ and thus $E(X,Y) = \mathbf{I}_r + E_1(X)Y + \cdots + E_k(X)Y^k$. For some $s_1 \in S$, the $s_1^jE_j$ can be written without denominators and thus we obtain a matrix $E'(X,Y) \in \mathbf{R}[X,Y]^{r\times r}$ such that $E'(X,0) = \mathbf{I}_r$, and, over $\mathbf{R}_S[X,Y]$, $E'(X,Y) = E(X, s_1Y)$. We do the same with F (we can choose the same s_1). Hence we obtain $E'(X,Y)F'(X,Y) = \mathbf{I}_r$ in $\mathbf{R}_S[X,Y]^{r\times r}$ and $E'(X,0)F'(X,0) = \mathbf{I}_r$. Applying Lemma 1.6 in which we replace X by Y and $\mathbf{R}$ by $\mathbf{R}[X]$, we obtain $s_2 \in S$ such that $E'(X, s_2Y)F'(X, s_2Y) = \mathbf{I}_r$. Taking $U = E'(X, s_2Y)$ and $s = s_1s_2$, we obtain the desired result. □

Lemma 1.8 *Let S be a multiplicative subset of a ring $\mathbf{R}$ and $M \in \mathbf{R}[X]^{p\times q}$. If $M(X)$ and $M(0)$ are equivalent over $\mathbf{R}_S[X]$ then there exists $s \in S$ such that $M(X+sY)$ and $M(X)$ are equivalent over $\mathbf{R}[X,Y]$.*

Proof Writing $M(X) = C(X)M(0)D(X)$ with $C(X) \in \mathrm{GL}_q(\mathbf{R}_S[X])$ and $D(X) \in \mathbf{GL}_p(\mathbf{R}_S[X])$, we get

$$M(X+Y) = C(X+Y)C(X)^{-1}M(X)D(X)^{-1}D(X+Y).$$

Applying Lemma 1.7, we find $s_1 \in S$, $U(X,Y) \in\in \mathbf{GL}_q(\mathbf{R}[X,Y])$ and $V(X,Y) \in \mathbf{GL}_p(\mathbf{R}[X,Y])$ such that $U(X,0) = \mathbf{I}_q$, $V(X,0) = \mathbf{I}_p$, and, over $\mathbf{R}_S[X,Y]$, $U(X,Y) = C(X+s_1Y)C(X)^{-1}$ and $V(X,Y) = D(X)^{-1}D(X+s_1Y)$. It follows that

$$M(X) = U(X,0)M(X)V(X,0), \text{ and, over } \mathbf{R}_S[X,Y], M(X+s_1Y) = U(X,Y)M(X)V(X,Y).$$

Applying Lemma 1.6 (as in Lemma 1.7), we get $s_2 \in S$ such that $M(X+s_1s_2Y) = U(X,s_2Y)M(X)V(X,s_2Y)$. The desired result is obtained by taking $s = s_1s_2$. □

Theorem 1.9 (Vaserstein) *Let M be a matrix in $\mathbf{R}[X]$ and consider $S_1, \ldots, S_n$ comaximal multiplicative subsets of $\mathbf{R}$. Then $M(X)$ and $M(0)$ are equivalent over $\mathbf{R}[X]$ if and only if, for each $1 \leq i \leq n$, they are equivalent over $\mathbf{R}_{S_i}[X]$.*

Proof It is easy to see that the set of $s \in \mathbf{R}$ such that $M(X + sY)$ is equivalent to $M(X)$ is an ideal of $\mathbf{R}$. Applying lemma 1.8, this ideal meets S_i for each $1 \leq i \leq n$, and thus contains 1. This means that $M(X+Y)$ is equivalent to $M(X)$. To finish, just take $X = 0$. □

Theorem 1.10 (Quillen's patching) *Let P be a finitely presented module over $\mathbf{R}[X]$ and consider $S_1, \ldots, S_n$ comaximal multiplicative subsets of $\mathbf{R}$. Then P is extended from $\mathbf{R}$ if and only if for each $1 \leq i \leq n$, P_{S_i} is extended from $\mathbf{R}_{S_i}$.*

Proof This is a corollary of the previous theorem since the isomorphism between $P(X)$ and $P(0)$ is nothing but the equivalence of two matrices $A(X)$ and $A(0)$ constructed from a relation matrix $M \in \mathbf{R}^{q \times m}$ of $P \simeq \operatorname{Coker} M$ (see [6]):

$$A(X) = \begin{pmatrix} M(X) & 0_{q,q} & 0_{q,q} & 0_{q,m} \\ 0_{q,m} & \mathrm{I}_q & 0_{q,q} & 0_{q,m} \end{pmatrix}.$$

□

1.4 Horrocks' theorem

Local Horrocks' theorem is the following result.

Theorem 1.11 *If $\mathbf{R}$ is a local ring and P a finitely generated projective module over $\mathbf{R}[X]$ which is free over $\mathbf{R}\langle X\rangle$, then it is free over $\mathbf{R}[X]$ (thus extended from $\mathbf{R}$).*

The detailed proof given by Kunz [6] is elementary and constructive, except Lemma 3.13 whose proof is abstract since it uses maximal ideals. In fact this lemma asserts if P is a projective module over $R[X]$ which becomes free of rank k over $\mathbf{R}\langle X\rangle$, then its k-th Fitting ideal equals $\langle 1\rangle$. This result has the following elementary constructive proof. If $P \oplus Q \simeq \mathbf{R}[X]^m$ then $P \oplus Q_1 = P \oplus (Q \oplus \mathbf{R}[X]^k)$ is isomorphic to $\mathbf{R}\langle X\rangle^{m+k}$ over $\mathbf{R}\langle X\rangle$ with Q_1 isomorphic to $\mathbf{R}\langle X\rangle^m$ over $\mathbf{R}\langle X\rangle$. So we may assume $P \simeq \operatorname{Im} F$, where $G = \mathrm{I}_n - F \in \mathbf{R}^{n \times n}$ is an idempotent matrix, similar to a standard projection matrix of rank $n-k$ over $\mathbf{R}\langle X\rangle$. We deduce that $\det(\mathrm{I}_n + TG) = (1+T)^{n-k}$ over $\mathbf{R}\langle X\rangle$. This remains true over $\mathbf{R}[X]$, so the sum of all $n-k$ principal minors of G equal 1. Hence we conclude by noticing that G is a relation matrix for P. For more details see e.g., [11].

The global version is the following one.

Theorem 1.12 *Let S be the multiplicative set of monics in $\mathbf{R}[X]$, $\mathbf{R}$ an arbitrary commutative ring. If P is a finitely generated projective module over $\mathbf{R}[X]$ such that P_S is extended from $\mathbf{R}$, then P is extended from $\mathbf{R}$.*

Sketch of proof. Apply the proof of Theorem 1.11 dynamically in order to mimic the case where $\mathbf{R}$ is a local ring. You get a set of comaximal finite potential primes, $(\mathfrak{P}_i)_{i \in J}$ of $\mathbf{R}$ such that each $P_{\mathfrak{P}_i}$ is extended from $\mathbf{R}_{\mathfrak{P}_i}$. Conclude with the Quillen's patching. □

NB: when we evaluate dynamically a ring as a local ring, we have to mimic the disjunction used in the constructive proof of Theorem 1.11 for a local ring:

$$\forall x \in \mathbf{S}, \qquad (\, x \in \mathbf{S}^{\times} \quad \text{or} \quad x \in \operatorname{Rad}(\mathbf{S})\,) \tag{2}$$

This works by using Lemma 1.5 (as for the disjunction (1) in the arithmetical case). For more details see [10, 12].

1.5 Projective modules over $\mathbf{R}[X_1,\dots,X_n]$, $\mathbf{R}$ a zero-dimensional ring

Let P be a finitely generated projective module of constant rank over $\mathbf{R}[X_1,\dots,X_n]$, where $\mathbf{R}$ is a zero-dimensional ring, given as the image of an idempotent matrix M with entries in $\mathbf{R}[X_1,\dots,X_n]$. We want to prove constructively that P is free. It is easy to see that, since in any ring: nilpotent + unit = unit, we can suppose that $\mathbf{R}$ is reduced.

Finally the constructive Quillen-Suslin theorem for reduced zero-dimensional rings can be easily deduced from the constructive Quillen-Suslin theorem for fields using the "constructive elementary local-global machinery" described by C. Quitté and H. Lombardi in [11] (more precisely, in the section about zero-dimensional rings in Chapter 3).

2 Brewer&Costa-Maroscia Theorem

In this section we give a simplified constructive proof for the following result, which is useful for proving the Brewer&Costa-Maroscia Theorem.

Theorem 2.1 *If* $\mathbf{R}$ *is a reduced arithmetical ring with* $\dim \mathbf{R} \leq 1$ *then* $\mathbf{R}\langle X\rangle$ *is an arithmetical ring.*

Lemma 2.2 *If* $S_1,\dots,S_k$ *are comaximal multiplicative subsets of* $\mathbf{R}$*, then* $\mathbf{R}_{S_1}\langle X\rangle$*, ..., * $\mathbf{R}_{S_k}\langle X\rangle$ *are comaximal localizations of* $\mathbf{R}\langle X\rangle$*.*

Proof We may assume that S_i is saturated (i.e., $xy \in S_i$ implies $x, y \in S_i$). Let $f_i(X)$ be a monic polynomial $\mathbf{R}_{S_i}[X]$. There exists $s_i \in S_i$ such that $s_i f_i(X) \in \mathbf{R}[X]$, with degree d_i and leading coefficient s_i. Let $a_1,\dots,a_k \in \mathbf{R}$ such that $\sum_i a_i s_i = 1$. Let $d = \max(d_1,\dots,d_k)$ and $g_i = a_i X^{d-d_i}$. Then $\sum_i g_i f_i$ is a monic polynomial of degree d in $\mathbf{R}[X]$. □

Lemma 2.3 *If* $\mathbf{V}$ *is a valuation domain with* $\dim \mathbf{V} \leq 1$ *then* $\mathbf{V}\langle X\rangle$ *is an arithmetical ring.*

Proof Let $\mathfrak{m}$ denote the Jacobson radical of $\mathbf{V}$. We use the characterization of arithmetical rings given in Fact 1.3. Let $f, g \in \mathbf{V}[X]$. Using repeatedly the disjunction (1) we can write f and g as follows:
$f = a\,(cF + u)$, $g = b\,(dG + v)$ where a, $b \in \mathbf{V}$, u, v monic polynomials, $c, d \in \mathfrak{m}$, F, $G \in \mathbf{R}[X]$.
Since $\mathbf{V}$ is a valuation ring, we can suppose that a divides b.
Now we open two branches: we localize $\mathbf{V}\langle X\rangle$ at the comaximal multiplicative subsets generated by $cF + u$ and c:

$$\begin{tikzcd} & \mathbf{V}\langle X\rangle \arrow[dl] \arrow[dr] & \\ \mathbf{V}\langle X\rangle_{cF+u} & & \mathbf{V}\langle X\rangle_c \end{tikzcd}$$

On the first hand, in $\mathbf{V}\langle X\rangle_{cF+u}$ everything's great, f divides g (in short, f/g).
On the other hand, the ring $\mathbf{V}\langle X\rangle_c$ is nothing but a localization of $\mathbf{V}_c[X]$. But since $\dim \mathbf{V} \leq 1$ and $c \in \mathfrak{m}$ we infer that $\dim \mathbf{V}_c \leq 0$ and thus $\mathbf{V}_c$ is the field of fractions of $\mathbf{V}$, say $\mathbf{K}$. It follows that $\mathbf{V}\langle X\rangle_c$ is a localization of the polynomial ring $\mathbf{K}[X]$. Now we can finish the proof using the fact that $\mathbf{K}[X]$ is a Bezout ring. In more details: write in $\mathbf{K}[X]$, $f = h\,f'$, $g = h\,g'$ with $h = f \wedge g$, and $\langle f', g'\rangle = 1$. It is clear that f divides g in $\mathbf{K}[X]_{f'}$ and that g divides f in $\mathbf{K}[X]_{g'}$.
To sum up, we obtain the following dynamical tree:

$$\begin{tikzcd} & \mathbf{V}\langle X\rangle \arrow[dl] \arrow[dr] & & \\ \mathbf{V}\langle X\rangle_{cF+u} & & \mathbf{V}\langle X\rangle_c \arrow[dl] \arrow[dr] & \\ f/g & \mathbf{K}[X]_{f'} & & \mathbf{K}[X]_{g'} \\ & f/g & & g/f \end{tikzcd}$$

□

Proof of Thorem 2.1 We give this proof mainly as a concrete explanation of the dynamical method. Let $f, g \in \mathbf{R}[X]$. We use the characterization of arithmetical rings given in Fact 1.3. Using localizations $\mathbf{R}_i$ of $\mathbf{R}$ at comaximal multiplicative sets $\mathcal{S}(\mathfrak{P}_i)$ that mimic the disjunction (1), as explained in Section 1.2, we can write f and g as follows:

$$f = a\,(cF + u),\; g = b\,(dG + v)$$

where a divides b in $\mathbf{R}_i$, u, v monic polynomials in $\mathbf{R}_i[X]$, $c, d \in \mathrm{Rad}(\mathbf{R}_i)$, F, $G \in \mathbf{R}_i[X]$.

Now it is sufficient to finish the proof dropping the index i (this is legitimated by Fact 1.3 and Lemma 2.2).

We open two branches: we localize $\mathbf{R}\langle X\rangle$ at the comaximal multiplicative subsets generated by $cF + u$ and c:

$$\begin{tikzcd}
& \mathbf{R}\langle X\rangle \arrow[dl] \arrow[dr] & \\
\mathbf{R}\langle X\rangle_{cF+u} & & \mathbf{R}\langle X\rangle_c
\end{tikzcd}$$

On the first hand, in $\mathbf{R}\langle X\rangle_{cF+u}$, f divides g.

On the other hand, the ring $\mathbf{R}\langle X\rangle_c$ is nothing but a localization of $\mathbf{R}_c[X]$. But since $\dim \mathbf{R} \leq 1$ and $c \in \mathrm{Rad}(\mathbf{R})$ we infer that $\dim \mathbf{R}_c \leq 0$. It follows that $\mathbf{R}\langle X\rangle_c$ is a localization of the polynomial ring $\mathbf{R}_c[X]$. Now we can finish the proof using the fact that $\mathbf{R}_c[X]$ is a Bezout ring, since $\mathbf{R}_c$ is reduced and zero-dimensional (for details see [11]). So we can write in $\mathbf{R}_c[X]$, $f = h\,f'$, $g = h\,g'$ with $h = f \wedge g$, and $\langle f', g'\rangle = 1$. It is clear that f divides g in $\mathbf{R}_c[X]_{f'}$ and that g divides f in $\mathbf{R}_c[X]_{g'}$.

To sum up, we obtain the following dynamical tree:

$$\begin{tikzcd}
& \mathbf{R}\langle X\rangle \arrow[dl] \arrow[dr] & & \\
\mathbf{R}\langle X\rangle_{cF+u} & & \mathbf{R}\langle X\rangle_c \arrow[ddl] \arrow[ddr] & \\
f/g & & & \\
& \mathbf{R}_c[X]_{f'} & & \mathbf{R}_c[X]_{g'} \\
& f/g & & g/f
\end{tikzcd}$$

□

3 Lequain&Simis Theorem

Theorem 3.1 *Let $d \in \mathbb{N}$ and $\mathbf{R}$ an arithmetical ring with Krull dimension $\leq d$. Let us denote $S_{\mathbf{R},X} = S$ the multiplicative set of monic polynomials inside $\mathbf{R}[X]$. Then for any $f, g \in \mathbf{R}\langle X\rangle$, there exist comaximal subsets $\mathcal{M}_1, \ldots, \mathcal{M}_s$ of $\mathbf{R}\langle X\rangle$ such that for each $1 \leq i \leq s$, either f/g in $\mathbf{R}\langle X\rangle_{\mathcal{M}_i}$ or g/f in $\mathbf{R}\langle X\rangle_{\mathcal{M}_i}$ or $\mathbf{R}\langle X\rangle_{\mathcal{M}_i}$ is a localization of $(\mathbf{R}_{\mathfrak{P}_i}[X])_S$ where $\mathfrak{P}_i$ is a finite potential prime and $\mathbf{R}_{\mathfrak{P}_i}$ has Krull dimension $\leq d - 1$.*

Proof This is done in (the first part of) the proof of Theorem 2.1. This works with Lemma 2.2 and the explanations given in Section 1.2. □

Now we give a constructive proof of our main theorem generalizing the result of Lequain and Simis to arithmetical rings (the proof given by Lequain and Simis for Prüfer domains is not constructive).

Theorem 3.2 (Lequain&Simis)
For any finite-dimensional arithmetical ring $\mathbf{R}$, all finitely generated projective $\mathbf{R}[X_1, \ldots, X_n]$-modules, $n \geq 2$, are extended from $\mathbf{R}$ if and only if all finitely generated projective $\mathbf{R}[X_1]$-modules are extended from $\mathbf{R}$.

Proof "⇒" Straightforward.

"⇐" Since we have a constructive Quillen's patching theorem, we can use the same dynamical trick as for the proof of Theorem 2.1.

We reason by double induction on the number n of variables and the Krull dimension of the basic ring $\mathbf{R}$.
Of course, for the initialization of the induction there is no problem since if $n = 1$ there is nothing to prove and over polynomial rings over zero-dimensional rings (see 1.5) the result is true constructively.
We assume that the construction is given for arithmetical rings of dimension $\leq d$ and for any number of variables. Then we consider an arithmetical ring of dimension $\leq d+1$ and we give the proof by induction on n.
Let P be a finitely generated projective $\mathbf{R}[X_1, \dots, X_n, Y]$-module. It can be seen as the cokernel of a presentation matrix $M = M(X_1, \dots, X_n, Y)$ with entries in $\mathbf{R}[X_1, \dots, X_n, Y]$. Let $A(X_1, \dots, X_n, Y)$ the associated enlarged matrix (as in the proof of Theorem 1.10). Proving that P is extended from $\mathbf{R}[Y]$ is nothing else than constructing invertible matrices Q and R such that $QA = A(0, \dots, 0, Y)R$.
Using the induction hypothesis over n, we try to reduce dynamically M over $\mathbf{R}\langle Y\rangle[X_1, \dots, X_n]$ as if $\mathbf{R}\langle Y\rangle$ was a valuation ring, with the meaning that the disjunction (1) is available.
For doing this job we use repeatedly Theorem 3.1. This will produce a lot of comaximal localizations of type $\mathbf{R}\langle Y\rangle_{\mathcal{M}_i}$. For some of these localizations $\mathbf{R}\langle Y\rangle_{\mathcal{M}_i}$ behaves like a valuation ring, and the construction for the case of n variables works, so we get a convenient reduction (Q_i, R_i) at the corresponding leaves of the tree. The other localizations are localizations of $\mathbf{R}_{\mathfrak{P}_i}[X]$ where $\mathbf{R}_{\mathfrak{P}_i}$ is an arithmetical ring of dimension $\leq d$. The construction for the case of dimension $\leq d$ and $n+1$ variables works, so we get a convenient reduction (Q_i, R_i) at the corresponding leaves of the tree.
By applying the Vaserstein's patching (Theorem 1.9) we get that P_S is extended from $\mathbf{R}\langle Y\rangle$, where $S = S_{\mathbf{R},Y}$ is the multiplicative set of monics in $\mathbf{R}[Y]$.
This means that there exist invertible matrices Q, R in $(\mathbf{R}\langle Y\rangle[X_1, \dots, X_n])$ such that

$$QA = A(0, \dots, 0, Y)R.$$

Since the entries of Q and R are in $\mathbf{R}\langle Y\rangle[X_1, \dots, X_n] \subseteq (\mathbf{R}[X_1, \dots, X_n])\langle Y\rangle$, then by virtue of Horrocks theorem (Theorem 1.12), P is extended from $\mathbf{R}[Y]$. □

This proof will give an algorithm under the following precise hypotheses:

- the ring $\mathbf{R}$ is arithmetic and of Krull dimesion ≤ 1 in an explicite way (Definitions 1.2 and 1.4),
- we have an algorithm for the Simis&Vasconcelos Theorem.

References

[1] Brewer J., Costa D. *Projective modules over some non-Noetherian polynomial rings.* J. Pure Appl. Algebra **13** (1978), no. 2, 157–163.

[2] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*, in: Commutative ring theory and applications. Eds: Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499.

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

[4] Coquand T., Lombardi H., Roy M.-F. *An elementary characterization of Krull dimension.* in 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.

[5] Ducos L., Quitté C., Lombardi H. et Salou M. *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.* Journal of Algebra. **281**, (2004), 604–650

[6] Kunz E. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, 1991.

[7] Lam T. Y. *Serre's conjecture.* Lecture Notes in Mathematics, Vol. 635. Springer-Verlag, Berlin-New York, 1978.

[8] Lequain, Y., Simis, A. *Projective modules over $R[X_1, ..., X_n]$, R a Prüfer domain.* J. Pure Appl. Algebra **18** (2) (1980), 165–171.

[9] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242** (2002), 23–46.

[10] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local-global*, dans: Commutative ring theory and applications. Eds: Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 461–476.

[11] Lombardi H., Quitté C. *Algèbre commutative. Méthodes constructives.* Book in preparation. http://hlombardi.free.fr/publis/A---PTFCours.pdf

[12] Lombardi H., Quitté C., Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* Preprint 2005.

[13] Maroscia P. *Modules projectifs sur certains anneaux de polynomes.* C.R.A.S. Paris **285** série A (1977), 183–185.

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

[15] Quillen D. *Projective modules over polynomial rings.* Invent. Math. **36** (1976), 167–171.

[16] Serre J.-P. Faisceaux algébriques cohérents, Ann. Math. 61 (1955), 191-278.

[17] Simis A., Vasconcelos W. *Projective modules over* $\mathbf{R}[X]$*,* $\mathbf{R}$ *a valuation ring, are free.* Notices. Amer. Math. Soc. **18** (5), 1971.

[18] Suslin A. *Projective modules over polynomial rings are free. (Russian).* Dokl. Akad. Nauk SSSR **229** no. 5 (1976), 1063–1066.

[19] Yengui I., *Making the use of maximal ideals constructive.* Preprint 2004.