Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa

Henri Lombardi ([1]), Claude Quitté ([2]), Ihsen Yengui ([3])

September 13, 2006

Abstract

We give a constructive deciphering for a generalization of the Quillen-Suslin theorem due to Maroscia and Brewer & Costa stating that finitely generated projective modules over $\mathbf{R}[X_1, \ldots, X_n]$, where $\mathbf{R}$ is a Prüfer domain with Krull dimension ≤ 1, are extended from $\mathbf{R}$.

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

Key words : Quillen-Suslin Theorem, Finitely generated projective modules, Local-global principles, Constructive mathematics.

Introduction

In this paper all rings are commutative and unitary.

We follow the philosophy developed in the papers [2, 3, 4, 5, 11, 12, 13, 14, 15, 16, 17, 18, 24, 25]. The main goal is to find the constructive content hidden in abstract proofs of concrete theorems.

The general method consists in replacing some abstract ideal objects whose existence is based on the principle of the excluded middle and the axiom of choice by incomplete specifications of these objects.

This paper is a sequel to [18]. We continue to develop the constructive rereading of abstract methods that use local-global principles. Our explicit proofs are obtained by a deciphering of the arguments contained in the original abstract proofs. We think that this is a first step in the achievement of Hilbert's program for abstract algebra methods.

The following theorem [1, 20] due to Maroscia and Brewer & Costa is an outstanding generalization of the Quillen-Suslin Theorem [22, 23] since it is free of any Noetherian hypothesis.

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

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

[3] Département de Mathématiques, Faculté des Sciences de Sfax, 3018 Sfax, Tunisia, Email: ihsen.yengui@fss.rnu.tn

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

It is worth pointing out that Lequain & Simis [10] have obtained a stronger theorem with the same conclusion but without the Krull dimension condition. The method they used seems to be very different and up to now we did not manage to reread it constructively.

The reader should refer to [18] for further explanations about our strategy concerning concrete local-global principles.

1 A reminder about Quillen's method

This section is based on Kunz [7] and Lam [8].

1.1 Extended Modules

Recall that a module M over $\mathbf{R}[X_1, \ldots, X_n] = \mathbf{R}[\underline{X}]$ is said to be *extended* if it is isomorphic to a module $N \otimes_{\mathbf{R}} \mathbf{R}[X]$ for some $\mathbf{R}$-module N. Necessarily, $N \simeq M/(X_1M + \cdots + X_nM)$. In particular, if M is finitely presented, denoting by $M^0 = M[0, \ldots, 0]$ the $\mathbf{R}$-module obtained by replacing the X_i by 0 in a relation matrix of M, then M is extended if and only if

$$M \simeq M^0 \otimes_{\mathbf{R}} \mathbf{R}[\underline{X}].$$

Notation 1 We use the notation $\mathbf{R}\langle X\rangle$ for the localization $\mathbf{R}[X]_S$ with S the set of monic polynomials.

Let us first recall some constructive notions from [18].

Definition 2 *1) If* S *is a monoid 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* $x_1, \ldots, x_r \in \mathbf{R}$*,* $\mathcal{M}(x_1, \ldots, x_r)$ *will denote the monoid of* $\mathbf{R}$ *generated by* $x_1, \ldots, x_r$*, that is,*

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

The localization of $\mathbf{R}$ *at* $\mathcal{M}(x_1, \ldots, x_r)$ *is the same 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* $\mathbf{R}_x$*.*
2) If $S_1, \ldots, S_k$ *are monoids of* $\mathbf{R}$*, we say that* $S_1, \ldots, S_k$ *are* comaximal *if*

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

3) Let I *and* U *be two subsets of* $\mathbf{R}$*. We denote by* $\mathcal{M}(U)$ *the monoid generated by* U*,* $\mathcal{I}_{\mathbf{R}}(I)$ *or* $\mathcal{I}(I)$ *the ideal generated by* I*, and* $\mathcal{S}(I; U)$ *the monoid* $\mathcal{M}(U) + \mathcal{I}(I)$*. If* $I = \{a_1, \ldots, a_k\}$ *and* $U = \{u_1, \ldots, u_\ell\}$*, we denote* $\mathcal{M}(U)$*,* $\mathcal{I}(I)$ *and* $\mathcal{S}(I; U)$ *respectively by* $\mathcal{M}(u_1, \ldots, u_\ell)$*,* $\mathcal{I}(a_1, \ldots, a_k)$ *and* $\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell)$*. It is easy to see that for any* $a \in \mathbf{R}$*, the monoids* $\mathcal{S}(I; U, a)$ *and* $\mathcal{S}(I, a; U)$ *are comaximal in* $\mathbf{R}_{\mathcal{S}(I;U)}$*.*

The following theorem can be found in [7] (see Vaserstein Theorem, IV.1.18 page 100 and Quillen Theorem, IV.1.20 page 101).

Theorem 3 (Quillen) *If a finitely presented* $\mathbf{R}[X]$*-module is extended after localization at any maximal ideal of* $\mathbf{R}$*, then it is extended.*

This theorem cannot be directly used from a constructive point of view. However, its proof is based on a *propagation lemma* which is implicit, with a constructive proof, in [7] (look at the ideal I in the proof of Vaserstein Theorem IV.1.8, whose corollary is the Quillen patching).

Lemma 4 (propagation lemma) *Let* M *a finitely presented* $\mathbf{R}[X]$*-module. Then the following set is an ideal of* $\mathbf{R}$*:*

$$I = \{ \ s \in \mathbf{R} \ : M_s \text{ is extended } \}.$$

This lemma is easily equivalent to the following concrete local-global principle.

Concrete local-global principle 5 *Let* M *be a finitely presented* $\mathbf{R}[X]$*-module, and* $S_1, \ldots, S_n$ *comaximal monoids of* $\mathbf{R}$*. If all the* M_{S_i}*'s are extended, then so is* M*.*

Proof First assume Lemma 4 and let $S_1, \ldots, S_n$ be comaximal monoids of $\mathbf{R}$ such that all the M_{S_i} are extended. For each i there is an $s_i \in S_i$ such that $M_{s_i} = M[1/s_i]$ is extended. Since the S_i's are comaximal, the ideal generated by the s_i's contains 1, so Lemma 4 says that $M = M[1/1]$ is extended.
In the other way, assume Concrete local global principle 5, and let s, t s.t. M_s and M_t are extended. Consider an element u of the ideal generated by s and t. In the ring $\mathbf{R}_u$, the monoids $s^{\mathbb{N}}$ and $t^{\mathbb{N}}$ generated by s and t are comaximal. Applying Concrete local global principle 5 to the ring $\mathbf{R}_u$, the monoids $s^{\mathbb{N}}$ and $t^{\mathbb{N}}$ and the module M_u, we get that M_u is extended. □

Consequently, we just need a sufficiently simple proof in the local case in order to run constructively Theorem 3 above as explained in [18].

Another important theorem used by Kunz is Horrocks Theorem IV.3.11 page 114 in [7]:

Theorem 6 (Horrocks) *If* $\mathbf{R}$ *is a local ring and* M *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).*

Note that the hypothesis $M \otimes_{\mathbf{R}[X]} \mathbf{R}\langle X\rangle$ is a free $\mathbf{R}\langle X\rangle$-module is equivalent to the fact that M_f is a free $\mathbf{R}[X]_f$-module for some monic polynomial $f \in \mathbf{R}[X]$ (see e.g., Corollary 2.7 p. 18 in [9]).

The detailed proof given by Kunz [7] 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 $\mathbf{R}[X]$ 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 $P \oplus Q_1 = P \oplus (Q \oplus \mathbf{R}[X]^k)$ becomes 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 $P \simeq \mathrm{Im}F$, where $G = \mathrm{I}_n - F \in \mathbf{R}[X]^{n\times n}$ is an idempotent matrix, conjugate 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 $\mathbf{R}\langle X\rangle$. Since $\mathbf{R}[X]$ is a subring of $\mathbf{R}\langle X\rangle$ this remains true over $\mathbf{R}[X]$. So the sum of all $n-k$ principal minors of G is equal to 1 (i.e. the coefficient of T^{n-k} in $\det(\mathrm{I}_n + TG)$). Hence we conclude by noticing that G is a relation matrix for P. For more details see e.g., [19].

The global version of Theorem 6 above is the following one.

Theorem 7 *Let S be the multiplicative set of monics in $\mathbf{R}[X]$, $\mathbf{R}$ an arbitrary ring. If M is a finitely generated projective module over $\mathbf{R}[X]$ such that M_S is extended from $\mathbf{R}$, then M is extended from $\mathbf{R}$.*

Sketch of proof. Apply the proof of Theorem 6 dynamically in order to mimic the case where $\mathbf{R}$ is a local ring. You get a set of comaximal monoids S_i of $\mathbf{R}$ such that each P_{S_i} is extended from $\mathbf{R}_{S_i}$. Conclude with the Concrete local-global Principle 5 above. □

1.2 Quillen Induction

Constructively, the *radical* $\mathrm{Rad}(\mathbf{R})$ of a ring $\mathbf{R}$ is the set of all the $x \in \mathbf{R}$ such that $1+x\mathbf{R} \subset \mathbf{R}^\times$, where $\mathbf{R}^\times$ is the group of units of $\mathbf{R}$. A ring $\mathbf{R}$ is *local* if it satisfies:

$$\forall x \in \mathbf{R} \quad x \in \mathbf{R}^\times \ \vee \ 1+x \in \mathbf{R}^\times. \tag{1}$$

It is *residually discrete local* if it satisfies:

$$\forall x \in \mathbf{R} \quad x \in \mathbf{R}^\times \ \vee \ x \in \mathrm{Rad}(\mathbf{R}) \tag{2}$$

From a classical point of view, we have (1) $\Leftrightarrow$ (2), but the constructive meaning of (2) is stronger than that of (1).

Recall Lam's exposition [8] about *Quillen Induction* for passing from the local to the global case.

Quillen Induction *Suppose that a class of rings $\mathcal{F}$ satisfies the following properties:*

Q1 *If $\mathbf{R} \in \mathcal{F}$ then $\mathbf{R}\langle X\rangle \in \mathcal{F}$.*

Q2 *If $\mathbf{R} \in \mathcal{F}$ then $\mathbf{R}_\mathfrak{m} \in \mathcal{F}$ for any maximal ideal $\mathfrak{m}$ of $\mathbf{R}$.*

Q3 *If $\mathbf{R} \in \mathcal{F}$ and $\mathbf{R}$ is local, and if M is a finitely generated projective $\mathbf{R}[X]$-module, then M is extended from $\mathbf{R}$ (that is, free).*

Then, for each $\mathbf{R} \in \mathcal{F}$, if M is a finitely generated projective $\mathbf{R}[X_1,\ldots,X_n]$-module, then M is extended from $\mathbf{R}$.

Lam's proof of Quillen Induction is based on "Affine Horrocks" Theorem V.2.2 page 130 of [8], which is Horrocks Theorem 6 above, and Corollary V.1.7 page 128, used with one variable, which is Quillen Theorem 3 above.

In order to obtain a constructive formulation of the Quillen Induction, we have to replace condition Q2 by

Q2a *If $\mathbf{R} \in \mathcal{F}$ then $\mathbf{R}_a \in \mathcal{F}$ for any $a \in \mathbf{R}$.*

Moreover, notice that it is a folklore that every finitely generated projective module over a local ring is free. In more details (extracted from [19]), let $F = (f_{i,j})_{1\le i,j\le m}$ be an idempotent matrix with coefficients in a local ring $\mathbf{A}$. We want to prove that F is conjugate to a standard projection matrix. Two cases may arise:

– If $f_{1,1}$ is invertible, then one can find $G \in \mathrm{GL}_m(\mathbf{A})$ such that

$$GFG^{-1} = \begin{pmatrix} 1 & 0_{1,m-1} \\ 0_{m-1,1} & F_1 \end{pmatrix},$$

where F_1 is an idempotent matrix of size $(m-1) \times (m-1)$, and an induction on m applies.

– If $1 - f_{1,1}$ is invertible, then one can find $H \in \mathrm{GL}_m(\mathbf{A})$ such that

$$HFH^{-1} = \begin{pmatrix} 0 & 0_{1,m-1} \\ 0_{m-1,1} & F_2 \end{pmatrix},$$

where F_2 is an idempotent matrix of size $(m-1) \times (m-1)$, and again an induction on m applies.

Our constructive rereading method of the Quillen Induction above starts from the proof of Q3 which treats the local case. This proof (which depends on the class $\mathcal{F}$) is already written in the literature. Moreover, the classical proof we find in the literature is often simple enough to be read as a constructive proof with the hypothesis that $\mathbf{R}$ is residually discrete local. In our case, this will follow from Horroks Theorem 6 above, Theorem 16 below, and the fact that every finitely generated projective module over a Bezout domain is free.

Let us now recall a General Constructive Rereading Principle which enables to automatically obtain a quasi-global version of a theorem from its local version.

General Principle 5 of [18] *When rereading an explicit proof given in case* $\mathbf{R}$ *is local, with an arbitrary ring* $\mathbf{R}$*, start with* $\mathbf{R} = \mathbf{R}_{\mathcal{S}(0;1)}$*. Then, at each disjunction (for an element* a *produced when computing in the local case)*

$$a \in \mathbf{R}^{\times} \ \vee \ a \in \mathrm{Rad}(\mathbf{R}),$$

replace the "current" ring $\mathbf{R}_{\mathcal{S}(I;U)}$ *by both* $\mathbf{R}_{\mathcal{S}(I;U,a)}$ *and* $\mathbf{R}_{\mathcal{S}(I,a;U)}$ *in which the computations can be pursued. At the end of this rereading, one obtains a finite family of rings* $\mathbf{R}_{\mathcal{S}(I_j;U_j)}$ *with comaximal monoids* $\mathcal{S}(I_j;U_j)$ *and finite sets* I_j, U_j.

With this Principle in hands, the "dynamical" rereading of the local proof of Q3 shows the following more precise result Q3a.

Q3a *If* $\mathbf{R} \in \mathcal{F}$*, and if* M *is a finitely generated projective* $\mathbf{R}[X]$*-module, then one can construct a family* (S_i) *of comaximal monoids of* $\mathbf{R}$ *such that each finitely generated projective* $\mathbf{R}_{S_i}[X]$*-module* M_{S_i} *is extended from* $\mathbf{R}_{S_i}$.

Thus, in the global case, the rereading of the local proof allows the construction of a finite family of comaximal monoids (S_i) such that the Concrete local global principle 5 above (which is a particular case of General Principle 5 in [18]) applies[1]. By the rereading Q3a of the proof of Q3, and applying the Concrete local global principle 5, we finally obtain:

Q3b *If* $\mathbf{R} \in \mathcal{F}$*, and if* M *is a finitely generated projective* $\mathbf{R}[X]$*-module, then* M *is extended from* $\mathbf{R}$.

[1] In this way one treats constructively the classical argument which is a priori "without a constructive content", except if one has an exceptional command of the production of maximal ideals. This argument works as follows: if the theorem was not true in the global case, the ideal I of Lemma 4 would be strict, thus contained in a maximal ideal P, but the localization at this maximal ideal P and the proof of the local case provide an element s which is at the same time in I and not in P, a contradiction.

This result Q3b is nothing else that the case $n = 1$ in Quillen Theorem 3 above. So, when the constructive rereading of the proof of Q3 works for the class $\mathcal{F}$, we get constructively the case $n = 1$.

Now we note that following Lam [8] p. 137-138, Quillen Induction works from Q1, from the case $n = 1$ and from global Horrocks Theorem 7 above. Moreover the argument of Lam for this implication is simple and constructive.

So if we give for the class $\mathcal{F}$ constructive proofs of Q1, Q2a and Q3 (under the hypothesis that the ring is residually discrete local), we get first Q3b (the case $n = 1$) and next the full result, with an algorithm (since the proof is constructive). More precisely we get at the end an explicit construction of the isomorphism between the module $M = M[X_1, \dots, X_n]$ and the module $M^0 = M[0, \dots, 0]$.

Summary of our constructive rereading of Quillen Induction. Q3b can be seen as a concrete substitute to Q2 and Q3 in Quillen Induction. And Quillen Induction has two distinct components. The first one is that Q2 and Q3 imply Q3b, i.e., the case $n = 1$. The second one is that Q1 and Q3b imply the general case (n arbitrary). The first component is not fully constructive, but in each concrete case (for a given class $\mathcal{F}$) we hope to be able to reread the proof in a constructive way: for this we replace Q2 by Q2a and Q3 by a careful examination of a simple proof that local rings in the class $\mathcal{F}$ satisfy the case $n = 1$. The second component is elementary and constructive, using global Horrocks Theorem 7.

2 The theorem of Maroscia and Brewer & Costa

2.1 Krull Dimension

In order to use constructively the hypothesis that $\mathbf{R}$ has Krull dimension ≤ 1, we recall the following result [2, 13]:

A ring $\mathbf{R}$ has Krull dimension ≤ 1 if and only if

$$\forall a, b \in \mathbf{R},\ \ \exists n \in \mathbb{N},\ \ \exists x, y \in \mathbf{R}, \quad a^n(b^n(1 + xb) + ya) = 0 \tag{3}$$

or equivalently

$$\forall a, b \in \mathbf{R},\ \ \exists n \in \mathbb{N}, \quad a^n b^n \in a^n b^{n+1}\mathbf{R} + a^{n+1}\mathbf{R}. \tag{4}$$

In the sequel, we will consider the family of identities in (3) as the constructive meaning of the hypothesis that $\mathbf{R}$ has Krull dimension ≤ 1. An identity of type (3) is sometimes called a *collapse*.

To simplify the computation of collapses related to Krull dimension ≤ 1, we introduce the following ideal $I_{\mathbf{R}}(a, b)$.

Notation 8 *If a, b are two elements of a ring $\mathbf{R}$, we denote by $I_{\mathbf{R}}(a, b)$ the set of all $z \in \mathbf{R}$ such that there exist $x, y \in \mathbf{R}$ and $n \in \mathbb{N}$ satisfying $a^n(b^n(z + xb) + ya) = 0$. In other words,*

$$I_{\mathbf{R}}(a, b) = \cup_{n \in \mathbb{N}}(a^n b^{n+1}\mathbf{R} + a^{n+1}\mathbf{R} : a^n b^n \mathbf{R}).$$

We then obtain:

Lemma 9

- *$I_{\mathbf{R}}(a, b)$ is an ideal of $\mathbf{R}$,*

- *$z \in I_{\mathbf{R}}(a,b) \;\Rightarrow\; uvz \in I_{\mathbf{R}}(ua,vb)$,*
- *if $\varphi : \mathbf{R} \to \mathbf{T}$ is an homomorphism, then $\varphi(I_{\mathbf{R}}(a,b)) \subset I_{\mathbf{T}}(\varphi(a),\varphi(b))$,*
- *the Krull dimension of $\mathbf{R}$ is $\leq 1 \iff \forall\, a,b \in \mathbf{R},\ I_{\mathbf{R}}(a,b) = \langle 1 \rangle$.*

2.2 A crucial result

Recall that a ring $\mathbf{R}$ is *Bezout* if each finitely generated ideal is principal, *arithmetical* if each finitely generated ideal is locally principal.

A constructive characterization of arithmetical rings is the following:

$$\forall x,y \in \mathbf{R} \quad \exists s,t,a,b \in \mathbf{R} \left\{ \begin{array}{rcl} s\,x & = & a\,y \\ b\,x & = & t\,y \\ s+t & = & 1 \end{array} \right. \tag{5}$$

See [5] or [14] for detailed explanations about this. In fact Property (5) amounts to say that each finitely generated ideal becomes principal after localization at a finite family of comaximal monoids.

An integral domain is called a *Prüfer domain* if it is arithmetical.

More generally a reduced arithmetical ring is called a *Prüfer ring* in [5, 14] following the terminology proposed in [6]. It is characterized by the fact that finitely generated ideals are flat.

A *coherent ring* is a ring in which finitely generated ideals are finitely presented. A *pp-ring* is a ring in which principal ideals are projective, which means that the annihilator of each element is idempotent.

A coherent Prüfer ring is often called a *semi-hereditary ring*. Since a finitely presented module is flat if and only if it is projective, coherent Prüfer ring are characterized by the fact that finitely generated ideals are projective. And an arithmetical ring is a coherent Prüfer ring if and only if it is a *pp-ring*.

Finally let us recall some well known results concerning Bezout rings. A Bezout ring is reduced and coherent if and only if it is a pp-ring. Over a Bezout pp-ring, each constant rank projective module is free. Over a Bezout domain each finitely generated projective module is free.

For a constructive approach of all previously cited facts see [5, 14].

The following result of Brewer & Costa is an important intermediate result for Quillen Induction.

Theorem 10 *If $\mathbf{R}$ is a Prüfer domain with Krull dimension ≤ 1 then so is $\mathbf{R}\langle X \rangle$.*

Next, we will give a constructive proof of a slightly more general version of the result above.

Theorem 11 *If $\mathbf{R}$ is a coherent Prüfer ring with Krull dimension ≤ 1 then so is $\mathbf{R}\langle X \rangle$.*

2.3 A local theorem

In the sequel, the letters a,b,c will denote elements of $\mathbf{R}$ and f,g,h elements of $\mathbf{R}[X]$.

In this section, we will prove a local version of Theorem 11 above.

A local Prüfer ring is nothing but a valuation ring. From a constructive point of view, we require the ring to be a residually discrete local coherent Prüfer ring. More precisely, the ring must satisfy constructively the following hypotheses:

$$\left\{\begin{array}{rrcl} \forall x \in \mathbf{R} & x^2=0 & \Rightarrow & x=0 \\ \forall x,y \in \mathbf{R} & \exists z\ x=zy & \text{or} & \exists z\ y=zx \\ \forall x \in \mathbf{R} & x \in \mathbf{R}^\times & \text{or} & x \in \mathrm{Rad}(\mathbf{R}) \\ \forall x \in \mathbf{R} & \mathrm{Ann}(x)=0 & \text{or} & \mathrm{Ann}(x)=1 \end{array}\right. \tag{6}$$

E.g., the constructive meaning of the third item is that for each element $x \in \mathbf{R}$, we are able either to find an y such that $xy = 1$ or to find for each z an y such that $(1 + xz)y = 1$.

The first two properties imply that the ring has no zero-divisors ($xy = 0$, $x = zy \Rightarrow zy^2 = 0 \Rightarrow (zy)^2 = 0 \Rightarrow zy = 0 \Rightarrow x = 0$), thus in classical mathematics the last two properties are automatically satisfied[2].

We easily infer that (with $\mathcal{R} = \mathrm{Rad}(\mathbf{R})$)

$$\left\{\begin{array}{lrcccl} \forall x,y \in \mathbf{R} & \exists z \in \mathcal{R}\ \ x=zy & \text{or} & \exists z \in \mathcal{R}\ \ y=zx & \text{or} & \exists u \in \mathbf{R}^\times\ \ y=ux \\ \forall x,y \in \mathbf{R} & xy=0 & \Rightarrow & (x=0 & \text{or} & y=0) \end{array}\right. \tag{7}$$

The following easy lemmas are useful for the proof of our Theorem 16.

Lemma 12 *If the ring* $\mathbf{R}$ *satisfies* (7)*, then each* $F \in \mathbf{R}[X]$ *can be written as* $F = a\,f$ *with* $f = b\,f_1 + f_2$ *where* $b \in \mathrm{Rad}(\mathbf{R})$ *and* f_2 *is monic.*

Proof By the first property in (7), there is one coefficient of F, say a, dividing all the others. Thus, we can write $F = a\,f$ for some $f \in \mathbf{R}[X]$ with at least one coefficient equal to 1. Now, write $f = f_2 + f_3$ with f_2 monic and all the coefficients of f_3 are in $\mathrm{Rad}(\mathbf{R})$. Again, there is one coefficient in f_3, say b, dividing all the others. Thus, $f_3 = b\,f_1$ for some $f_1 \in \mathbf{R}[X]$. □

Lemma 13 *If* $\mathbf{R}$ *has Krull dimension* ≤ 1*,* $c \in \mathbf{R}$ *is regular and* $b \in \mathrm{Rad}(\mathbf{R})$*, then* c *divides a power of* b*.*

Proof Just use the equality (3) and the fact that $1 + b\,\mathbf{R} \subset \mathbf{R}^\times$.

□

Corollary 14 *If* $\mathbf{R}$ *has Krull dimension* ≤ 1 *and* $f = b\,f_1 + f_2 \in \mathbf{R}[X]$ *with* $b \in \mathrm{Rad}(\mathbf{R})$ *and* f_2 *monic, then for every regular* $c \in \mathbf{R}$*,* $\langle f, c\rangle$ *contains a monic.*

Proof Using Lemma 13, we know that there exists $n \in \mathbb{N}$ such that c divides b^n. Thus, the monic polynomial $f_2^n \in \langle f, b^n\rangle \subseteq \langle f, c\rangle$.

□

Remark 15 *In any ring* $\mathbf{R}$*, if the gcd of two elements* x *and* y *exists, and* $\langle x, y\rangle$ *is principal, then* $\langle x, y\rangle = \langle \gcd(x, y)\rangle$*.*

A local version of Theorem 11 above is Theorem 16 below.

[2] The last property means that "$x = 0$ or x regular". If the ring is not trivial, since it has no zero-divisors, this can be rewritten as "$x = 0$ or $x \neq 0$". Shortly, in the case of a non trivial ring, we require our valuation ring to be discrete and residually discrete local, but we don't demand to know whether the ring is trivial or not.

Theorem 16 *If* $\mathbf{R}$ *is a residually discrete local coherent Prüfer ring (that is satisfies* (6)*) and has Krull dimension* ≤ 1*, then* $\mathbf{R}\langle X\rangle$ *is a Bezout domain with Krull dimension* ≤ 1.

Proof We first prove that $\mathbf{R}\langle X\rangle$ is a Bezout domain. It is a domain (each element is zero or regular) since $\mathbf{R}$ is a domain. Since $\mathbf{R}$ is a discrete gcd-domain (that is, each pair of nonzero elements has a greatest common divisor), we know that so is $\mathbf{R}[X]$ (see for example Theorem IV.4.7 of [21]), as well as the ring $\mathbf{R}\langle X\rangle$. Recall that a gcd-ring $\mathbf{B}$ is Bezout if and only if

$$\forall x, y \in \mathbf{B}, \quad (\operatorname{gcd}(x,y) = 1 \quad \Longrightarrow \quad \langle x, y\rangle = \langle 1\rangle\,).$$

For the purpose to prove that $\mathbf{R}\langle X\rangle$ is Bezout, consider $F, G \in \mathbf{R}\langle X\rangle$ such that $\operatorname{gcd}(F,G) = 1$ and show that $1 \in \langle F, G\rangle$; we can suppose $F \neq 0$ and $G \neq 0$. Since monic polynomials are invertible in $\mathbf{R}\langle X\rangle$, we can suppose that $F, G \in \mathbf{R}[X]$. We must show that $\langle F, G\rangle_{\mathbf{R}[X]}$ contains a monic polynomial. Let $H = \operatorname{gcd}(F,G)_{\mathbf{R}[X]}$; in $\mathbf{R}\langle X\rangle$, we have $H \mid \operatorname{gcd}(F,G)_{\mathbf{R}\langle X\rangle} = 1$ so the leading coefficient of H is invertible in $\mathbf{R}$. Using $\langle F, G\rangle_{\mathbf{R}[X]} = H\langle F/H, G/H\rangle_{\mathbf{R}[X]}$, we see that we may suppose $H = 1$. Following Lemma 12, we have $F = a\,f = a\,(b\,f_1 + f_2)$, $G = a'\,g = a'\,(b'\,g_1 + g_2)$, with b, $b' \in \operatorname{Rad}(\mathbf{R})$ and f_2, g_2 monic. In $\mathbf{R}\langle X\rangle$ we have:

$$\operatorname{gcd}(F,G) = \operatorname{gcd}(a\,f, a'\,g) = 1 \;\Rightarrow\; \operatorname{gcd}(a, a') = 1$$

Thus $\operatorname{gcd}(F,G) = 1$ in $\mathbf{R}\langle X\rangle$ implies that a or a' is invertible in $\mathbf{R}$. Suppose for example that $a = 1$. The fact that $\operatorname{gcd}(F,G)_{\mathbf{R}[X]} = 1$ yields that the gcd in $\mathbf{K}[X]$ (where $\mathbf{K}$ is the quotient field of $\mathbf{R}$) is equal to 1, that is, there is a regular element c in $\mathbf{R} \cap \langle F, G\rangle_{\mathbf{R}[X]}$. By Corollary 14, we get a monic polynomial in $\langle c, F\rangle_{\mathbf{R}[X]} \subseteq \langle F, G\rangle_{\mathbf{R}[X]}$, as desired.

Now, let us check that the Krull dimension of $\mathbf{R}\langle X\rangle$ is ≤ 1. The Krull dimension of $\mathbf{K}[X]$ is ≤ 1, and more precisely, for all $F, G \in \mathbf{R}[X]$ (keeping the same notations as above), we have an explicit collapse in $\mathbf{K}[X]$ ([2, 13]) which can be rewritten in $\mathbf{R}[X]$ (by clearing the denominators) as follows:

$$\exists n \in \mathbb{N}, \;\; \exists\, h_1, h_2 \in \mathbf{R}[X], \;\; \exists\, w \in \mathbf{R} \setminus \{0\} \quad F^n(G^n(w + h_1 G) + h_2 F) = 0.$$

This means that $\exists\, w \in \mathbf{R} \setminus \{0\}$, such that $w \in I_{\mathbf{R}\langle X\rangle}(F,G)$. Moreover, we have $1 \in I_{\mathbf{R}}(a, a')$ and a fortiori $1 \in I_{\mathbf{R}\langle X\rangle}(a, a')$, implying that $fg \in I_{\mathbf{R}\langle X\rangle}(af, a'g) = I_{\mathbf{R}\langle X\rangle}(F,G)$. Finally, since the gcd in $\mathbf{R}\langle X\rangle$ of w and fg is equal to 1 (this is due to the fact that fg is primitive), the ideal $I_{\mathbf{R}\langle X\rangle}(F,G)$, which contains w and fg, must contain 1.

Finally the fact that $\mathbf{R}\langle X\rangle$ is a pp-ring can be easly checked under the only hypothesis that $\mathbf{R}$ is a pp-ring. □

2.4 A quasi-global version

The constructive rereading method for the use of abstract local-global principles, explained in [18], and applied to the proof of Theorem 16 above, provides an algorithmic proof for the following quasi-global proposition.

Proposition 17 *Let* $\mathbf{R}$ *be a coherent Prüfer ring with Krull dimension* ≤ 1. *Considering* $F, G \in \mathbf{R}[X]$:

- *There exists a family* (S_i) *of comaximal monoids of* $\mathbf{R}$ *such that in each* $\mathbf{R}_{S_i}\langle X\rangle$ *the ideal* $\langle F, G\rangle$ *is finitely generated and projective.*

- *There exists a family (S_i) of comaximal monoids of* $\mathbf{R}$ *such that in each* $\mathbf{B}_i = \mathbf{R}_{S_i}\langle X\rangle$ *we have a collapse* $I_{\mathbf{B}_i}(F,G) = 1$*.*

An immediate corollary of Proposition 17 is Theorem 11 above, because the properties that a finitely generated ideal is projective and that two elements produce a collapse are local properties: it suffices to check them after localizations at a family of comaximal monoids ([2, 5, 14]).

2.5 Conclusion

Let $\mathcal{F}$ the class of coherent Prüfer rings with Krull dimension ≤ 1. This class satisfies clearly the localization property Q2a. It satisfies Q1 by Theorem 11.

Theorem 16 above asserts that if $\mathbf{R} \in \mathcal{F}$ is residually discrete local, then $\mathbf{R}\langle X\rangle$ is a Bezout domain. In particular, every projective module over $\mathbf{R}\langle X\rangle$ is free. Combined with Horrocks Theorem 6 above, we then obtain condition Q3 in Quillen Induction.

As our proof of Q3 is elementary and constructive, the dynamical rereading we have explained in section 1.2 works and gives versions Q3a and Q3b. We finally get constructively:

Theorem 18 *If* $\mathbf{R}$ *is a coherent Prüfer ring with Krull dimension* ≤ 1*, then every finitely generated projective module over* $\mathbf{R}[X_1,\dots,X_n]$ *is extended. In particular, if* $\mathbf{R}$ *is a Bezout pp-ring with Krull dimension* ≤ 1*, then every constant rank projective module over* $\mathbf{R}[X_1,\dots,X_n]$ *is free.*

References

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

[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. 1, 6, 9, 10

[3] Coquand T., Lombardi H., Quitté C. *Generating non-noetherian modules constructively.* Manuscripta mathematica **115** (2004), 513–520. 1

[4] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze.* Annals of Pure and Applied Logic **111** (2001), 203–256. 1

[5] Ducos L., Quitté C., Lombardi H., Salou M. *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.* Journal of Algebra **281** (2004), 604–650 1, 7, 10

[6] Hermida J., Sánchez-Giralda T. *Linear Equations over Commutative Rings and Determinantal Ideals.* Journal of Algebra **99**, (1986) 72–79. 7

[7] Kunz E. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, 1991. 2, 3

[8] Lam T. Y. *Serre's conjecture.* Lecture Notes in Mathematics, Vol. 635. Springer-Verlag, Berlin-New York, 1978. 2, 4, 6

[9] Lam T. Y. *Serre's Problem on Projective Modules.* Springer Monographs in Mathematics, 2006. 3

[10] 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. 2

[11] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini.* Publications Mathématiques de Besançon. Théorie des nombres. 1997. 1

[12] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic **91** (1998), 59–92. 1

[13] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242** (2002), 23–46. 1, 6, 9

[14] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive.* Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 1, 7, 10

[15] Lombardi H. *Hidden constructions in abstract algebra (1) Integral dependance relations.* Journal of Pure and Applied Algebra **167** (2002), 259–267. 1

[16] Lombardi H. *Constructions cachées en algèbre abstraite (4) La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier.* Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 1

[17] Lombardi H. *Constructions cachées en algèbre abstraite (5) Principe local-global de Pfister et variantes.* International Journal of Commutative Rings **2** (4) (2003), 157–176. 1

[18] 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. 1, 2, 3, 5, 9

[19] Lombardi H., Quitté C. *Théorie constructive élémentaire des modules projectifs de type fini.* (2003), Preprint). 3, 4

[20] Maroscia P. *Modules projectifs sur certains anneaux de polynomes.* C.R.A.S. Paris **285** série A (1977), 183–185. 1

[21] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, 1988. 9

[22] Quillen D. *Projective modules over polynomial rings.* Invent. Math. **36** (1976), 167–171. 1

[23] Suslin A. *Projective modules over polynomial rings are free. (Russian).* Dokl. Akad. Nauk SSSR **229** no. 5 (1976), 1063–1066. 1

[24] Yengui I. *Making the use of maximal ideals constructive.* (2004), Preprint. 1

[25] Yengui I. *Dynamical Gröbner bases.* Journal of Algebra **301** (2006), 447–458. 1