The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

1958-9

Summer School and Conference Mathematics, Algorithms and Proofs

11 - 29 August 2008

Projective modules over polynomial rings and dynamical Gröbner bases

Ihsen Yengui
Department of Mathematics, Faculty of Sciences of Sfax,
Sfax, Tunisia

Lectures on Constructive Algebra

ICTP, Trieste, Italy, 11-24 August, 2008

Title: Projective modules over polynomial rings and dynamical Gröbner bases

By

Ihsen Yengui

Departement of Mathematics, Faculty of Sciences of Sfax, 3000 Sfax, Tunisia

Email: ihsen.yengui@fss.rnu.tn

Contents

1 Introduction

In these lecture notes, we will follow the philosophy developed in the papers [8, 20, 21, 22, 26, 33, 42, 43, 44, 45, 46, 47, 48, 49, 52, 53, 56, 72, 73]. The main goal is to find the constructive content hidden in abstract proofs of concrete theorems in Commutative Algebra and especially well-known theorems concerning projective modules over polynomial rings.

The general method consists in replacing some abstract ideal objects whose existence is based on the third excluded middle principle and the axiom of choice by incomplete specifications of these objects. We think that this is a first step in the achievement of Hilbert's program for abstract algebra methods:

Hilbert's program. If we prove using ideal methods a concrete statement, one can always eliminate the use of these elements and obtain a purely elementary proof.

Constructive Algebra can be seen as an abstract version of Computer Algebra. In Computer Algebra, one tries to get efficient algorithms for solving "concrete problems given in an algebraic formulation". A problem is "concrete" if its hypotheses and conclusion do have a computational content.

Constructive Algebra can be understood as a first "preprocessing" for Computer Algebra: finding general algorithms, even if they are not efficient. Moreover, in Constructive Algebra one tries to give general algorithms for solving virtually "any" theorem of Abstract Algebra. So a first task is often to understand what is the computational content hidden in hypotheses that are formulated in a very abstract way. E.g., what is a good constructive definition for a local ring, a valuation ring, an arithmetical ring, a ring of Krull dimension ≤ 2 and so on? A good constructive definition must be equivalent to the usual definition in classical mathematics, it has to have a computational content, and it has to be satisfied by usual objects (of usual mathematics) satisfying the abstract definition.

Let us consider the classical theorem saying "any polynomial P in $\mathbf{K}[X]$ is a product of irreducible polynomials ($\mathbf{K}$ a field)". This leads to an interesting problem. Surely no general algorithm can give the solution of this theorem. So what is the constructive content of this theorem? A possible answer is the following one: when doing computations with P, you can always do as if you knew its decomposition in irreducibles. At the beginning, start as if P were irreducible. If some strange thing appears (the gcd of P and another polynomial Q is a strict divisor of P), use this fact in order to improve the decomposition of P.

This trick was invented in Computer Algebra as the D5-philosophy [25, 27, 57]. Following this computational trick you are able to compute inside the algebraic closure $\widetilde{\mathbf{K}}$ of $\mathbf{K}$ even if it not possible to "construct" $\widetilde{\mathbf{K}}$.

This was called the "dynamical evaluation" (of the algebraic closure). And since our general method is directly inspired by this trick, we call it "constructive dynamical rereading of abstract proofs".

From a logical point of view, the "dynamical evaluation" gives a constructive substitute for two highly nonconstructive tools of Abstract Algebra: the Third Excluded Middle and Zorn's Lemma. These tools are needed to "construct" the algebraic closure $\widetilde{\mathbf{K}}$: the dynamical evaluation allows to find the fully computational content of this "construction". The paper [22] is an excellent reference about the foundations of dynamical methods in algebra.

In these lectures, the dynamical evaluation is used in order to find constructive substitutes to very elegant abstract theorems such as Quillen's patching, Quillen Induction and Lequain-Simis Induction.

Very important is the constructive rewriting of "abstract local-global principles". In classical proofs using this kind of principle, the argument is "let us see what happens after localization at an arbitray prime ideal of $\mathbf{R}$". Prime ideals are too abstract objects from a computational point of view, particularly if you want to deal with a general commutative ring. In the constructive rereading, the argument is "let us see what happens when the ring is a residually discrete local ring", i.e., if $\forall x$, $(x \in \mathbf{R}^\times$ or $\forall y\,(1+xy) \in \mathbf{R}^\times)$. If you get a constructive proof in this particular case, you are done by "dynamically evaluating an arbitrary ring $\mathbf{R}$ as a residually discrete local ring".

I will try to approach constructively the problem of projective modules over polynomial rings originally raised by J.-P. Serre [68] in 1955. Serre remarked that it was not known whether there exist finitely generated projective modules over multivariate polynomial rings with coefficients in a field, which are not free. This remark turned into the "Serre's conjecture" or "Serre's problem", stating that indeed there were no such modules. Proven independently by D. Quillen [63] and A. A. Suslin [70] in 1976, it became subsequently known as the Quillen-Suslin theorem. I will give constructive proofs of Quillen and Suslin proofs of Serre's problem, simple and constructive proofs of some subsequent developments in the theory of projective modules over polynomial rings, and also I will cast light on a new progress very recently obtained concerning the Hermite ring Conjecture.

Another important example of dynamical computation is the notion of "dynamical Gröbner basis" which will be the subject of the fifth section. I will also explain how to compute dynamically a generating set for the syzygy module of multivariate polynomials over a Dedekind ring with zero divisors. These techniques will be useful for the computation of free-bases of the examples of projective modules studied in the previous sections.

The present notes are based on five lectures on Constructive Algebra that I gave in the occasion of the Summer School (Mathematics, Algorithms and Proofs) held at the ICTP (Trieste, Italy) from 11 to 24 August 2008.

Lecture 1: Projective modules, Concrete local-global principles, Quillen's proof of Serre's problem, notably Quillen's patching theorem, Horrocks' theorem, Quillen's induction theorem.

Lecture 2: Suslin's proof of Serre's problem, a general method for making the use of maximal ideals constructive.

Lecture 3: Constructive comparison between the rings $R(X)$ and $R\langle X\rangle$ and application to the Lequain-Simis induction theorem, a constructive proof of the Lequain-Simis-Vasconcelos theorem asserting that for any arithmetical ring R, all finitely generated projective $R[X_1,\ldots,X_n]$-modules are extended from R.

Lecture 4: A new progress concerning the long-standing Hermite ring Conjecture (1972) asserting that if R is an Hermite ring (that is, all finitely generated stably free R-modules are free) then so is $R[X]$. Of course, a positive solution to this conjecture will imply a positive solution to the famous Bass-Quillen Conjecture (1976) saying that for any local regular ring R, all finitely generated projective $R[X]$-modules are free. We will prove (constructively) that for any ring R with Krull dimension ≤ 1, $R[X]$ is an Hermite ring. Moreover, the corresponding completion of unimodular rows can be done using elementary matrices (instead of invertible matrices). In other words, we will prove that for any ring R with Krull dimension ≤ 1 and $n \geq 3$, any unimodular vector $\in R[X]^n$ can be completed into an elementary matrice $\in R[X]^{n\times n}$. We will also give a generalization of this result in all dimensions and we will discuss some new open questions and conjectures that it raises.

Lecture 5: A dynamical method for computing a Gröbner basis and a generating set for the syzygy module of multivariate polynomials with coefficients in a Dedekind ring with zero divisors.

The undefined terminology is standard as in [24, 37, 39], and, for constructive algebra in [51, 55]. For a rigorous constructive study of finitely generated projective modules, I warmly recommend the excellent forthcoming book [51]. An english translation of this book is coming soon.

2 Quillen's proof of Serre's problem

2.1 Finitely generated projective modules

Definition 1. *Let P be a module over a ring $\mathbf{R}$. We say that P is a projective $\mathbf{R}$-module if any surjective $\mathbf{R}$-module homomorphism $\alpha : M \to P$ has a right inverse $\beta : P \to M$; or equivalently, if it is isomorphic to a direct summand in a free $\mathbf{R}$-module. It is finitely generated and projective if and only if it is isomorphic to a direct summand in $\mathbf{R}^n$ for some n.*

Definition 2. *Let $\mathbf{R}$ be a ring. The isomorphism classes of finitely generated projective modules over $\mathbf{R}$ form an abelian semigroup* $\mathrm{Proj}\,\mathbf{R}$ *with $\oplus$ as the addition operation and with the 0-module as the identity element. As* $\mathrm{Proj}\,\mathbf{R}$ *need not be a group, it is therefore convenient to force it into being a group by considering its Groethendieck group (or group completion)* $\mathrm{K}_0(\mathbf{R})$.

Example 3.

(i) Every free module is projective.

(ii) Suppose that m and n are coprime natural numbers. Then as abelian groups (and also as $(\mathbb{Z}/mn\mathbb{Z})$-modules), we have $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$. Thus, $\mathbb{Z}/m\mathbb{Z}$ is a projective $(\mathbb{Z}/mn\mathbb{Z})$-module which is not free as it contains fewer than mn elements.

(iii) An ideal I of an interal domain $\mathbf{R}$ is projective if and only if it is invertible. Integral domains in which every ideal is invertible are known as Dedekind domains, and they are important in number theory. For example, the ring of integers in any algebraic number field is a Dedekind domain. So, by considering a Dedekind domain which is not a PID, one can find an example of a projective module (an invertible ideal) which is not free (not principal).

Remark 4.

(i) **Projective modules via idempotent matrices [67]:** There is another approach to finitely generated projective modules which is more concrete and therefore more convenient for our constructive approach. If P is a finitely generated projective $\mathbf{R}$-module, we may assume (replacing P by an isomorphic module) that $P \oplus Q = \mathbf{R}^n$ for some n, and we consider the idempotent matrix M of the $\mathbf{R}$-module homomorphism p from $\mathbf{R}^n$ to itself which is the identity on P and 0 on Q written in the standard basis. So, P can be

seen (up to isomorphism) as the image of an idempotent matrix M. Conversely, different idempotent matrices can give rise to the same isomorphism class of projective modules. As a matter of fact, if M and N are idempotent matrices over a ring $\mathbf{R}$ (of possibly different size), the corresponding finitely generated projective modules are isomorphic if and only if it is possible to enlarge the sizes of M and N (by adding zeros in the lower right-hand corner) so that they have the same size $s \times s$ and conjugate under the group $\mathrm{GL}_s(\mathbf{R})$. We will embed $\mathrm{M}_n(\mathbf{R})$ in $\mathrm{M}_{n+1}(\mathbf{R})$ by $M \mapsto \begin{pmatrix} M & 0 \\ 0 & 0 \end{pmatrix}$, $\mathrm{GL}_n(\mathbf{R})$ in $\mathrm{GL}_{n+1}(\mathbf{R})$ by the group homomorphism $M \mapsto \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$, so that we can define by $\mathrm{M}(\mathbf{R})$ (resp., $\mathrm{GL}(\mathbf{R})$) as the infinite union of the $\mathrm{M}_n(\mathbf{R})$ (resp., $\mathrm{GL}_n(\mathbf{R})$). Denoting by $\mathrm{Idem}(\mathbf{R})$ the set of idempotent matrices in $\mathrm{M}(\mathbf{R})$, $\operatorname{Proj}\mathbf{R}$ may be identified with the set of conjugaison orbits of $\mathrm{GL}(\mathbf{R})$ on $\mathrm{Idem}(\mathbf{R})$. The semigroup operation is induced by $(M, N) \mapsto \begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$ and $\mathrm{K}_0(\mathbf{R})$ is the Groethendieck group of this semigroup. Denoting by $M = (m_{i,j})_{i,j\in I}$ and $N = (n_{k,\ell})_{k,\ell\in J}$, the Kronecker product $M \otimes N := (r_{(i,k),(j,\ell)})_{(i,k),(j,\ell)\in I\times J}$, where $r_{(i,k),(j,\ell)} = m_{i,j}n_{k,\ell}$, corresponds to the tensor product $\operatorname{Im} M \otimes \operatorname{Im} N$.

(*ii*) **Projective modules via Fitting ideals [51]:** The theory of Fitting ideals of finitely presented modules is an extremely efficient computing machinery from a theoretical constructive point of view. Recall that if G is a presentation matrix of a module T given by q generators related by m relations, the Fitting ideals of T are the ideals

$$\mathcal{F}_n(T) := \mathcal{D}_{q-n}(G),$$

where for any integer k, $\mathcal{D}_k(G)$ denotes the determinantial ideal of G of order k, that is the ideal generated by all the minors of G of size k, with the convention that for $k \leq 0$, $\mathcal{D}_k(G) = \langle 1\rangle$, and for $k > \min(m, n)$, $\mathcal{D}_k(G) = \langle 0\rangle$. It is worth pointing out that the Fitting ideals of a finitely presented module T don't depend on the choosen presentation matrix G and that one has

$$\langle 0\rangle = \mathcal{F}_{-1}(T) \subseteq \mathcal{F}_0(T) \subseteq \mathcal{F}_q(T) = \langle 1\rangle.$$

Projectivity can be tested via the Fitting ideals as follows: *A finitely presented* $\mathbf{R}$*-module is projective if and only if its Fitting ideals are projective (or equivalenty, principal generated by idempotent elements)* (see [51]).

(*iii*) **Projective modules of rank one:** To any ring $\mathbf{R}$ we can associate its *Picard group* $\operatorname{Pic}\mathbf{R}$, i.e., the group of projective $\mathbf{R}$-modules of rank one equipped with tensor product as group operation. The inverse of P is its dual $P^\star$. If $P \simeq \operatorname{Im} M$ then $P^\star \simeq \operatorname{Im} {}^{\mathrm{t}}M$. In particular, if M is a rank one idempotent matrix, then $M \otimes {}^{\mathrm{t}}M$ is an idempotent matrix whose image is a rank one free module.

In case $\mathbf{R}$ is an integral domain or a Noetherian ring, $\operatorname{Pic}\mathbf{R}$ is isomorphic to the *class group* of $\mathbf{R}$, group of invertible ideals in the field of fractions of $\mathbf{R}$, modulo the principal ideals. So, this generalizes to an arbitrary ring the class group introduced originally by Kummer.

Recall that a ring $\mathbf{R}$ is *local* if it satisfies:

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

Theorem 5. *If* $\mathbf{R}$ *is a local ring, then every finitely generated projective* $\mathbf{R}$*-module is free. In particular,* $\mathrm{K}_0(\mathbf{R}) \cong \mathbb{Z}$ *(since* $\operatorname{Proj}\mathbf{R} \cong \mathbb{N}$*) with generator the isomorphism class of a free module of rank* 1 *(*$\cong \mathbf{R}$*).*

Proof. Let $F = (f_{i,j})_{1\leq i,j\leq m}$ be an idempotent matrix with coefficients in a local ring $\mathbf{R}$. Let us prove that F is conjugate to a standard projection matrix. Two cases may arise:

– If $f_{1,1}$ is invertible, then one can find $G \in \mathrm{GL}_m(\mathbf{R})$ 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 $H \in \mathrm{GL}_m(\mathbf{R})$ 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.

□

The following theorem gives a local characterization of projective modules.

Theorem 6. *An $\mathbf{R}$-module P is projective if and only if there exist comaximal elements $s_1, \dots, s_k \in \mathbf{R}$ (i.e., $\langle s_1, \dots, s_k \rangle = \mathbf{R}$) such that for each $1 \leq i \leq k$, $P_{s_i} := P \otimes \mathbf{R}[\frac{1}{s_i}]$ is a free $\mathbf{R}[\frac{1}{s_i}]$-module.*

Definition 7. *A module M over $\mathbf{R}[X_1, \dots, X_n] = \mathbf{R}[\underline{X}]$ is said to be* extended from $\mathbf{R}$ *(or simply,* extended*) if it is isomorphic to a module $N \otimes_{\mathbf{R}} \mathbf{R}[\underline{X}]$ for some $\mathbf{R}$-module N. Necessarily*

$$N \simeq \mathbf{R} \otimes_{\mathbf{R}[\underline{X}]} M \text{ through } \rho : \mathbf{R}[\underline{X}] \to \mathbf{R},\ f \mapsto f(0),$$

i.e., $N \simeq M/(X_1 M + \cdots + X_n M)$. In particular, if M is finitely presented, denoting by $M^0 = M[0, \dots, 0]$ 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

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

or equivalently, if the matrices M and M^0 are equivalent using invertible matrices with entries in $\mathbf{R}[\underline{X}]$.

If M is given as the image of an idempotent matrix $F = F(X_1, \dots, X_n)$, then M is extended if and only if F is conjugate to $F(0, \dots, 0)$.

Definition 8. (Finitely generated projective modules of constant rank)

(*i*) **Classical approach [38]:** *The rank of a nonzero free module $\mathbf{R}^m$ is defined by $\mathrm{rk}_{\mathbf{R}}(\mathbf{R}^m) = m$. If P is a finitely generated projective module, as it is locally free (i.e., $P_{\mathfrak{p}} := P \otimes_{\mathbf{R}} R_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module for any $\mathfrak{p} \in \mathrm{Spec}(\mathbf{R})$, where $\mathrm{Spec}(\mathbf{R})$ denotes the set of prime ideals of $\mathbf{R}$), we define the (rank) map $\mathrm{rk}(P) : \mathrm{Spec}(\mathbf{R}) \to \mathbb{N}$ by $\mathrm{rk}(P)(\mathfrak{p}) = \mathrm{rk}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}})$. The map $\mathrm{rk}(P)$ is locally constant. Especially if $\mathrm{Spec}(\mathbf{R})$ is connected, i.e., if $\mathbf{R}$ is not a direct product of nontrivial rings (or equivalently, if $\mathbf{R}$ has no nontrivial idempotents), then $\mathrm{rk}(P)$ is constant.*

(*ii*) **Constructive approach [51]:** *Roughly speaking, if $\varphi : P \to P$ is an endomorphism of a finitely generated projective $\mathbf{R}$-module P, then supposing that $P \oplus Q$ is isomorphic to a free module, then the determinant of $\varphi_1 := \varphi \oplus \mathrm{Id}_Q$ depends only on φ; it is called the determinant of φ. Now, let us consider the $\mathbf{R}[X]$-module $P[X] := P \otimes_{\mathbf{R}} \mathbf{R}[X]$. The polynomial $R_P(X) := \det(X\mathrm{Id}_P)$ is called the rank polynomial of the module P. If P is free of rank k, then clearly $R_P(X) = X^k$. Moreover, $R_{P \oplus Q}(X) = R_P(X) R_Q(X)$, $R_P(X) R_P(Y) = R_P(XY)$, and $R_P(1) = 1$, in such a way the coefficients of $R_P(X)$ form a fundamental system of orthogonal idempotents ($\sum e_i = 1$ and $e_i e_j = 0$ for $i \neq j$).*

Now, this terminology being established, a finitely generated projective $\mathbf{R}$-module P is said to have rank equal to h if $R_P(X) = X^h$. If we don't specify h, we say that P has a constant rank.

For any finitely generated projective $\mathbf{R}$-module P, denoting by $R_P(X) = \sum_{h=0}^{n} r_h X^h$ (as said above, the r_h's form a fundamental system of orthogonal idempotents), we have $P = \bigoplus_{h=0}^{n} r_h P$ as $\mathbf{R}$-modules, and each module $r_h P$ is a constant rank projective $\mathbf{R}/\langle 1 - r_h \rangle$-module of rank h (recall that $\mathbf{R}/\langle 1 - r_h \rangle \cong \mathbf{R}[\frac{1}{r_h}]$).

2.2 Finitely generated stably free modules

Definition 9. *An $\mathbf{R}$-module P is said to be finitely generated stably free (of rank $n - m$) if $P \oplus \mathbf{R}^m \cong \mathbf{R}^n$ for some m, n. This amounts to say that P is isomorphic to the kernel of an epimorhism $f : \mathbf{R}^n \to \mathbf{R}^m$. If M is the $m \times n$ matrix associated with f, then M is right invertible, i.e., there exists an $n \times m$ matrix N such that $MN = \mathrm{I}_m$. Conversely, the kernel of any right invertible matrix defines a finitely generated stably free module. So, the study of finitely generated stably free $\mathbf{R}$-modules becomes equivalent to the study of right invertible rectangular matrices over $\mathbf{R}$.*

Example 10.

(*i*) Every free module is stably free.

(*ii*) Every stably free module is projective. The converse does not hold. To see this, it suffices to consider a non principal ideal in a Dedekind domain (for example, the ideal $\langle 3, 2 + \sqrt{-5} \rangle$ in the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$). It is a rank one projective module (as it is an invertible ideal) but not a stably free module since as will be seen in Theorem 18, stably free modules of rank one are free.

The following gives a criterion for the freeness of finitely generated stably free modules in matrix terms.

Proposition 11. *For any right invertible $m \times n$ matrix M, the (stably free) solution space of M is free if and only if M can be completed to an invertible matrix by adding a suitable number of new rows.*

Definition 12. *We say that $(b_1,\dots,b_n)$ is a unimodular row (or that ${}^{\mathrm{t}}(b_1,\dots,b_n)$ is a unimodular vector) if the row matrix $(b_1,\dots,b_n)$ is right invertible, i.e., if $\langle b_1,\dots,b_n\rangle = \mathbf{R}$. The set of such unimodular rows will be denoted by $\mathrm{Um}_n(\mathbf{R})$ (in order to lighten the notation, we use the same notation for unimodular vectors).*

The following gives a criterion for the freeness of all finitely generated stably free modules over a ring $\mathbf{R}$ in terms of unimodular rows.

Proposition 13. *For any ring $\mathbf{R}$, the following are equivalent:*

(*i*) *Any finitely generated stably free module is free.*

(*ii*) *Any unimodular row over $\mathbf{R}$ can be completed to an invertible matrix.*

Definition 14. *Rings satisfying the above equivalent properties will be called Hermite rings.*

The following proposition gives a more precise formulation of Proposition 13.

Proposition 15. *For any ring $\mathbf{R}$ and integer $d \geq 0$, the following are equivalent:*

(*i*) *Any finitely generated stably free module of rank $> d$ is free.*

(*ii*) *Any unimodular row over $\mathbf{R}$ of length $\geq d+2$ can be completed to an invertible matrix over $\mathbf{R}$.*

(*iii*) *For $n \geq d+2$, $\mathrm{GL}_n(\mathbf{R})$ acts transitively on $\mathrm{Um}_n(\mathbf{R})$.*

In fact, when studying finitely generated stably free modules, one has only to care about stably free modules of rank ≥ 2, since as will be seen in Theorem 18, stably free of rank 1 are free.

Notation 16. *Let $\mathbf{R}$ be ring and $A \in \mathbf{R}^{n\times m}$ an $n \times m$ matrix with entries in $\mathbf{R}$. Denote by $A_1,\dots,A_m$ the columns of A, so that we can write $A = [A_1,\dots,A_m]$. If $I = (i_1,\dots,i_r)$ is a sequence of natural numbers with $1 \leq i_1 < \cdots < i_r \leq m$, we denote by A_I the matrix $[A_{i_1},\dots,A_{i_r}]$.*

Binet-Cauchy Formula 17. *Let $\mathbf{R}$ be ring and consider two matrices $M \in \mathbf{R}^{s\times r}$ and $N \in \mathbf{R}^{r\times s}$, $r \leq s$. Then*

$$\det(MN) = \sum_I \det(M_I)\,\det(N_I),$$

where I runs through all sequences of natural numbers $(i_1,\dots,i_r)$ with $1 \leq i_1 < \cdots < i_r \leq s$.

Theorem 18. *For any ring $\mathbf{R}$, any stably free $\mathbf{R}$-module of rank 1 is free ($\cong \mathbf{R}$).*

Proof. Let P be a stably free $\mathbf{R}$-module of rank 1 (i.e., $P \oplus \mathbf{R}^{n-1} \cong \mathbf{R}^n$ for some $n \geq 2$) represented as the solution space of a right invertible $(n-1)\times n$ matrix M. That is, $P = \mathrm{Ker}\, M$ and $\exists\, N \in \mathbf{R}^{n\times(n-1)}$ such that $MN = \mathrm{I}_{n-1}$. Proving that P is free is nothing else than proving that M can be completed to an invertible matrix (see Proposition 11). This clearly amounts to prove that the maximal minors $b_1,\dots,b_n$ are comaximal, i.e., $1 \in \langle b_1,\dots,b_n\rangle$. As a matter of fact, if $a_1b_1 + \cdots + a_nb_n = 1$ then M can be completed to a matrix of determinant 1 by adding a last row $[a_1,\dots,a_n]$ with appropriate signs. Thus, our task is reduced to prove that $1 \in \langle b_1,\dots,b_n\rangle$.

Classical approach: Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{R}$. Then, modulo $\mathfrak{m}$, we have $\bar{M}\bar{N} = \mathrm{I}_{n-1}$. Since $\bar{M}$ is right invertible, it has rank $n-1$ and can be completed by linear algebra to an invertible matrix $M_{\mathfrak{m}} \in \mathrm{GL}_n(\mathbf{R}/\mathfrak{m})$. Thus, $\det M_{\mathfrak{m}} \neq \bar{0}$ and a fortiori $\langle b_1,\dots,b_n\rangle \not\subseteq \mathfrak{m}$.

Constructive aproach: Reasoning modulo $\langle b_1,\dots,b_n\rangle$, the fact that $\bar{M}\bar{N} = \mathrm{I}_{n-1}$ together with the Binet-Cauchy Formula 17 give that $\bar{1} = \bar{0}$. Thus, $1 \in \langle b_1,\dots,b_n\rangle$. □

Remark 19. It is worth pointing out that there is no analogue to Theorem 18 for projective modules. As a matter of fact, for any ring $\mathbf{R}$ all finitely generated projective $\mathbf{R}[X]$-modules of rank one are extended from $\mathbf{R}$ if and only if $\mathbf{R}$ is seminormal, that is, each time $b^2 = c^3$ in $\mathbf{R}$, there exists $a \in \mathbf{R}$ such that $a^3 = b$ and $a^2 = c$ (this is the Traverso-Swan theorem which has been treated recently constructively by T. Coquand [18] followed by H. Lombardi and C. Quitté [50] and also by S. Barhoumi and H. Lombardi [7]; see Problem 146). If $\mathbf{R}$ is a ring which is not seminormal then one can explicitly construct a rank one projective $\mathbf{R}$-module which is not free (see Schanuel's example which will be given in Question 4.b) of Problem 146).

2.3 Concrete local-global principle

We explain here how the constructive deciphering of classical proofs in commutative algebra using a local-global principle works. This section is essentially written up from [49].

2.3.1 From local to quasi-global

The classical reasoning by localization works as follows. When the ring is local a property P is satisfied by virtue of a quite concrete proof. When the ring is not local, the same property remains true (from a classical nonconstructive point of view) as it suffices to check it locally.

When carefully examining the first proof, some computations come into view. These computations are feasible thanks to the following principle:

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

This principle is in fact applied to elements coming from the proof itself. In case of a non necessarily local ring, we repeat the same proof, replacing at each disjunction "x is a unit or x is in the radical" in the passage of the proof we are considering, by the consideration of two rings $\mathbf{T}_x$ and $\mathbf{T}_{1+x\mathbf{T}}$, where $\mathbf{T}$ is the "current" localization of the ring $\mathbf{R}$ we start with. When the initial proof is completely unrolled, we obtain a finite number (since the proof is finite) of localizations $\mathbf{R}_{S_i}$, for each of them the property is true. Moreover, the corresponding Zariski open subsets U_{S_i} cover $\mathrm{Spec}(\mathbf{R})$ implying that the property P is true for $\mathbf{A}$, and this time in an entirely explicit way.

Definition 20. *(Constructive definition of the radical)*
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). Constructively a *discrete field* is defined as a ring in which each element is zero or invertible, with an explicit test for the "or". An *Heyting field* (or a field) is defined as a local ring whose Jacobson radical is 0. So $\mathbf{R}$ is residually discrete local exactly when it is local and the residue field $\mathbf{R}/\mathrm{Rad}(\mathbf{R})$ is a discrete field.

Definition 21. *(Monoids and saturations)*

(*i*) *We say that* S *is a* multiplicative subset *(or a* monoid*) of a ring* $\mathbf{R}$ *if*

$$\begin{cases} 1 \in S \\ \forall\, s,t \in S, \ \ s\,t \in S. \end{cases}$$

(*ii*) *A monid* S *of a ring* $\mathbf{R}$ *is sait to be* saturated *if we have the implication*

$$\forall\, s,t \in \mathbf{R}, \ \ (s\,t \in S \ \Rightarrow \ s \in S).$$

(*iii*) *The localization of* $\mathbf{R}$ *at* S *will be denoted by* $S^{-1}\mathbf{R}$ *or* $\mathbf{R}_S$*. If* S *is generated by* $s \in \mathbf{R}$*, we denote* $\mathbf{R}_S$ *by* $\mathbf{R}_s$ *or* $\mathbf{R}[1/s]$*. Note here that* $\mathbf{R}_s$ *is isomorphic to the ring* $\mathbf{R}[T]/(sT-1)$*. Saturating a monoid* S *(that is, replacing* S *by its saturation* $\bar{S} := \{s \in \mathbf{R} \ \ \exists\, t \in \mathbf{R} \quad s\,t \in S\}$*) does not change the localization* $\mathbf{R}_S$*. Two monoids are said to be* equivalent *if they have the same saturation.*

Definition 22. *(Comaximal monoids) Let* $S, S_1, \ldots, S_n$ *be monids of a ring* $\mathbf{R}$*.*

(1) *We say that the monoids* $S_1, \ldots, S_n$ *are* comaximal *if any ideal of* $\mathbf{R}$ *meeting all the* S_i *must contain* 1*. In other words, if we have:*

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

(2) *We say that the monoids* $S_1, \ldots, S_n$ *cover the monoid* S *if* S *is contained in the* S_i *and any ideal of* $\mathbf{R}$ *meeting all the* S_i *must meet* S*. In other words, if we have:*

$$\forall s_1 \in S_1 \ \cdots \ \forall s_n \in S_n \ \ \exists a_1, \ldots, a_n \in \mathbf{R} \quad | \quad \sum_{i=1}^{n} a_i s_i \in S.$$

Remark that comaximal multiplicative sets remain comaximal when you replace the ring by a bigger one or the multiplicative subsets by smaller ones.

In classical algebra (with the axiom of the prime ideal) this amounts to say, in the first case, that the Zariski open subsets U_{S_i} cover $\mathrm{Spec}(\mathbf{R})$ and, in the second case, that the Zariski open subsets U_{S_i} cover the open subset U_S. From a constructive point of view, $\mathrm{Spec}(\mathbf{R})$ is a topological space via its open subsets U_S but whose points are often hardly accessible.

We have the following immediate result.

Lemma 23. (Associativity and transitivity of coverings)

(1) *(Associativity) If monoids $S_1, \ldots, S_n$ of a ring $\mathbf{R}$ cover a monid S and each S_ℓ is covered by some monoids $S_{\ell,1}, \ldots, S_{\ell,m_\ell}$, then the $S_{\ell,j}$ cover S.*

(2) *(Transitivity) Let S be a monoid of a ring $\mathbf{R}$ and $S_1, \ldots, S_n$ monoids of the ring $\mathbf{R}_S$. For $\ell = 1, \ldots, n$, let V_ℓ be he monoid of $\mathbf{R}$ formed by the denominators of the elements of S_ℓ. Then the monoids $V_1, \ldots, V_n$ cover S*

Definition and notation 24. *Let I and U two subsets of a ring $\mathbf{R}$. 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 $\mathcal{S}(I;U)$ by $\mathcal{M}(u_1, \ldots, u_\ell)$, $\mathcal{I}(a_1, \ldots, a_k)$ and $\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell)$, respectively.*

Remark 25. (1) *It is clear that if u is equal to a product $u_1 \cdots u_\ell$, then the monoids $\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell)$ and $\mathcal{S}(a_1, \ldots, a_k; u)$ are equivalent.*

(2) *When we localize at $S = \mathcal{S}(I;U)$, the elements of U are forced into being invertible and those of I end up on the radical of $\mathbf{R}_S$.*

Our feeling is that the "good category" would be that whose objects are couples $(\mathbf{R}, I)$ where $\mathbf{R}$ is a commutative ring and I is an ideal contained in the radical of $\mathbf{R}$. Arrows from $(\mathbf{R}, I)$ onto $(\mathbf{R}', I')$ are rings homomorphisms $f : \mathbf{R} \to \mathbf{R}'$ such that $f(I) \subset I'$. Thus, we can retrieve usual rings by taking $I = 0$ and local rings (equipped with the notion of local homomorphism) by taking I equal to the maximal ideal. In order to "localize" an object $(\mathbf{A}, I)$ in this category, we use a monoid U and an ideal J in such a way we form the new object $(\mathbf{R}_{\mathcal{S}(J_1;U)}, J_1\mathbf{R}_{\mathcal{S}(J_1;U)})$, where $J_1 = I + J$.

The following lemma will play a crucial role when we want to reread constructively with an arbitrary ring a proof given in the local case.

Lemma 26. *Let U and I be two subsets of a ring $\mathbf{R}$ and consider $a \in \mathbf{R}$. Then the monoids $\mathcal{S}(I;U,a)$ and $\mathcal{S}(I,a;U)$ cover the monoid $\mathcal{S}(I;U)$.*

Proof. Preuve For $x \in \mathcal{S}(I;U,a)$ and $y \in \mathcal{S}(I,a;U)$, we have to find a linear combination of the form $x_1x+y_1y \in \mathcal{S}(I;U)$ $(x_1, y_1 \in \mathbf{R})$. Write $x = u_1a^k + j_1$, $y = (u_2 + j_2) - (az)$ with $u_1, u_2 \in \mathcal{M}(U)$, $j_1, j_2 \in \mathcal{I}(I)$, $z \in \mathbf{R}$. The classical identity $c^k - d^k = (c-d) \times \cdots$ gives a $y_2 \in \mathbf{A}$ such that $y_2y = (u_2 + j_2)^k - (az)^k = (u_2^k + j_3) - (az)^k$. Just write $z^kx + u_1y_2y = u_1u_2^k + u_1j_3 + j_1z^k = u_4 + j_4$. □

It is worth pointing out that in the lemma above, we have

$$a \in (\mathbf{R}_{\mathcal{S}(I;U,a)})^\times \text{ and } a \in \mathrm{Rad}(\mathbf{R}_{\mathcal{S}(I,a;U)}).$$

Having this lemma in hands, we can state the following general deciphering principle allowing to automatically get a quasi-global version of a theorem from its local version.

General local-global Principle 27. *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.

The following examples are frequent and ensue immediately from Lemmas 23 and 26, except the first one which is an easy exercise.

Examples 28. Let $\mathbf{R}$ be a ring, U and I subsets of $\mathbf{R}$, and $S = \mathcal{S}(I;U)$.

(1) Let $s_1, \ldots, s_n \in \mathbf{R}$ be comaximal elements (i.e., such that $\mathcal{I}(s_1, \ldots, s_n) = \mathbf{R}$). Then the monoids $S_i = \mathcal{M}(s_i)$ are comaximal.
More generally, if $t_1, \ldots, t_n \in \mathbf{R}$ are comaximal elements in $\mathbf{R}_S$, then the monoids $\mathcal{S}(I;U,t_i)$ cover the monoid S.

(2) Let $s_1, \ldots, s_n \in \mathbf{R}$. The monoids $S_1 = \mathcal{S}(0;s_1)$, $S_2 = \mathcal{S}(s_1;s_2)$, $S_3 = \mathcal{S}(s_1,s_2;s_3)$, ..., $S_n = \mathcal{S}(s_1,\ldots,s_{n-1};s_n)$ and $S_{n+1} = \mathcal{S}(s_1,\ldots,s_n;1)$ are comaximal.
More generally, the monoids $V_1 = \mathcal{S}(I;U,s_1)$, $V_2 = \mathcal{S}(I,s_1;U,s_2)$, $V_3 = \mathcal{S}(I,s_1,s_2;U,s_3)$, ..., $V_n = \mathcal{S}(I,s_1,\ldots,s_{n-1};U,s_n)$ and $V_{n+1} = \mathcal{S}(I,s_1,\ldots,s_n;U)$ cover the monoid S.

(3) If $S, S_1, \ldots, S_n \subset \mathbf{R}$ are comaximal monoids and if $b = a/(u+i) \in \mathbf{R}_S$ then $\mathcal{S}(I;U,a), \mathcal{S}(I,a;U), S_1, \ldots, S_n \in \mathbf{R}$ are comaximal.

2.3.2 From quasi-global to global

Different variant versions of the abstract local-global principle in commutative algebra can be reread constructively: the localization at each prime ideal is replaced by the localization at a finite family of comaximal monoids.

In other words, in these "concrete" versions, we affirm that some properties pass from the quasi-global to the global.

As an illustration, we cite the following results which often permit to finish our constructive rereading.

Concrete local-global Principle 29. *Let $S_1, \ldots, S_n$ be comaximal monoids in a ring $\mathbf{R}$ and let $a, b \in \mathbf{R}$. Then we have the following equivalences:*

(1) *Concrete gluing of equalities:*
$$a = b \quad \text{in} \quad \mathbf{R} \qquad \Longleftrightarrow \qquad \forall i \in \{1,\ldots,n\} \;\; a/1 = b/1 \quad \text{in} \quad \mathbf{R}_{S_i}$$

(2) *Concrete gluing of nonzero divisors:*
$$\begin{array}{c} a \text{ is not a zero divisor in } \mathbf{R} \qquad \Longleftrightarrow \\ \forall i \in \{1,\ldots,n\} \;\; a/1 \text{ is not a zero divisor in } \mathbf{R}_{S_i} \end{array}$$

(3) *Concrete gluing of units:*
$$\begin{array}{c} a \text{ is a unit in } \mathbf{R} \quad \Longleftrightarrow \\ \forall i \in \{1,\ldots,n\} \;\; a/1 \text{ is a unit in } \mathbf{R}_{S_i} \end{array}$$

(4) *Concrete gluing of solutions of linear systems: let B be a matrix $\in \mathbf{R}^{m\times p}$ and C a column vector $\in \mathbf{R}^{m\times 1}$.*
$$\begin{array}{c} \text{The linear system } BX = C \text{ has a solution in } \mathbf{R}^{p\times 1} \quad \Longleftrightarrow \\ \forall i \in \{1,\ldots,n\} \text{ the linear system } BX = C \text{ has a solution in } \mathbf{R}_{S_i}^{p\times 1} \end{array}$$

(5) *Concrete gluing of direct summands: let M be a finitely generated submodule of a finitely presented module N.*
$$\begin{array}{c} M \text{ is a direct summand of } N \quad \Longleftrightarrow \\ \forall i \in \{1,\ldots,n\} \; M_{S_i} \text{ is a direct summand of } N_{S_i} \end{array}$$

Concrete local-global Principle 30. (Concrete gluing of module finiteness properties) *Let $S_1, \ldots S_n$ be comaximal monoids of a ring $\mathbf{R}$ and let M be an $\mathbf{R}$-module. Then we have the following equivalences:*

(1) *M is finitely generated if and only if each of the M_{S_i} is a finitely generated $\mathbf{R}_{S_i}$-module.*

(2) *M is finitely presented if and only if each of the M_{S_i} is a finitely presented $\mathbf{R}_{S_i}$-module.*

(3) *M is flat if and only if each of the M_{S_i} is a flat $\mathbf{R}_{S_i}$-module.*

(4) *M is a finitely generated projective module if and only if each of the M_{S_i} is a finitely generated projective $\mathbf{R}_{S_i}$-module.*

(5) *M is projective of rank k if and only if each of the M_{S_i} is a projective $\mathbf{R}_{S_i}$-module of rank k.*

(6) *M is coherent if and only if each of the M_{S_i} is a coherent $\mathbf{R}_{S_i}$-module.*

(7) *M is Noetherian if and only if each of the M_{S_i} is a Noetherian $\mathbf{R}_{S_i}$-module.*

One can rarely find such stated principles in the classical literature. In Quillen's style, the corresponding general principle is in general stated using localizations at all prime ideals, but the proof often brings in a crucial lemma which has exactly the same signification as the corresponding concrete local-global principle. For example, we can state the concrete local-global principle 30 "à la Quillen" under the following form.

Lemma 31. (Propagation lemma for some module finiteness properties)
Let M be an $\mathbf{R}$-module. The following subsets I_k of $\mathbf{R}$ are ideals.

(1) $I_1 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a finitely generated* $\mathbf{R}_s$*-module*$\}$.

(2) $I_2 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a finitely presented* $\mathbf{R}_s$*-module*$\}$.

(3) $I_3 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a flat* $\mathbf{R}_s$*-module*$\}$.

(4) $I_4 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a finitely generated projective* $\mathbf{R}_s$*-module*$\}$.

(5) $I_5 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a rank k projective* $\mathbf{R}_s$*-module*$\}$.

(6) $I_6 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a coherent* $\mathbf{R}_s$*-module*$\}$.

(7) $I_7 = \{\ s \in \mathbf{R}\ :\ M_s$ *is a Noetherian* $\mathbf{R}_s$*-module*$\}$.

Remark 32. In general, let P be a property which is stable under localization. Then the following version of the concrete local-global principle:

- for each ring $\mathbf{R}$, if P is true after localizations at comaximal elements of $\mathbf{R}$, then it is true in $\mathbf{R}$,

and its *propagation lemma* version:

- the set $I_P = \{\ s \in \mathbf{R}\ :\ P$ is true in $\mathbf{R}_s\ \}$, is an ideal of $\mathbf{R}$,

are equivalent. On the one hand, the propagation lemma version clearly implies the first one. On the other hand, for the converse, if $s, s' \in I_P$ and $t = s + s'$ then $s/1$ and $s'/1$ are comaximal elements of $\mathbf{A}_t$ and P is true in both $(\mathbf{R}_t)_s \simeq (\mathbf{R}_s)_t \simeq \mathbf{R}_{st}$ and $(\mathbf{R}_t)_{s'} \simeq (\mathbf{R}_{s'})_t \simeq \mathbf{R}_{s't}$. Thus, P is true in $\mathbf{A}_t$ by the concrete local-global principle.
It is worth pointing out that, in general, for any monoid S, we have the following implication

- P is true in $\mathbf{R}_S \Rightarrow P$ is true in $\mathbf{R}_s$ for some $s \in S$,

establishing the equivalence between the *concrete local-global principle for comaximal elements* and the *concrete local-global principle for comaximal monoids*. This is in general indispensable since the explained rereading system (General principle 27) naturally produces a local-global version with comaximal elements rather than with comaximal monoids.

2.4 The patchings of Quillen and Vaserstein

We give here a detailed constructive proof of the Quillen's patching. This is essentially written up from [37]. The localization at maximal ideals is replaced by localization at comaximal multiplicative subsets.

In [52] the constructive Quillen's patching (Concrete local-global Principle 4) is given with only a sketch of proof.

Lemma 33. *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 34. *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 $s_1^j E_j$ 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 33 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 35. *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 34, 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 $M(X) = U(X,0)M(X)V(X,0)$, and over $\mathbf{R}_S[X,Y]$, $M(X+s_1Y) = U(X,Y)M(X)V(X,Y)$.

Applying Lemma 33 (as in Lemma 34), 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 36. (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 $1 \le i \le n$, 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 35, this ideal meets S_i for each $1 \le i \le n$, and thus contains 1. This means that $M(X+Y)$ is equivalent to $M(X)$. To finish, just take $X = 0$. □

Theorem 37. (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 $1 \le i \le n$, 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 $P \simeq \mathrm{Coker}\, M$:

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

□

2.5 Horrocks' theorem

Local Horrocks' theorem is the following result.

Theorem 38. (Local Horrocks extension theorem)
If $\mathbf{R}$ is a residually discrete 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 $\mathbf{R}[X]$ (i.e., extended from $\mathbf{R}$).

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 [39]). The detailed proof given by Kunz [37] 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 $P \simeq \mathbf{Im}F$, 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., [51].

A global version is obtained from a constructive proof of the local one by the Quillen's patching and applying the General local-global Principle 27.

Theorem 39. (Global Horrocks extension theorem)
Let S be the multiplicative set of monic polynomials 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 $\mathbf{R}$.

Proof. Sketch of proof. Apply the General local-global principle 27 and conclude with the Concrete Quillen's patching Theorem 37. □

2.6 Quillen induction theorem

Let $\mathbf{R}$ be a commutative unitary ring. We denote by S the multiplicative subset of $\mathbf{R}[X]$ formed by monic polynomials . Let

$$\mathbf{R}\langle X\rangle := S^{-1}\mathbf{R}[X].$$

The interest in the properties of $\mathbf{R}\langle X\rangle$ branched in many directions and is attested by the abundance of articles on $\mathbf{R}\langle X\rangle$ appearing in the literature (see [31] for a comprehensive list of papers dealing with the ring $\mathbf{R}\langle X\rangle$). The ring $\mathbf{R}\langle X\rangle$ played an important role in Quillen's solution to Serre's problem [63] and its succeeding generalizations to non-Noetherian rings [13, 40, 54] as can be seen in these notes.

Classical Quillen induction is the following one.

Theorem 40. (Quillen Induction)
Suppose that a class of rings $\mathcal{P}$ satisfies the following properties:

(i) *If $\mathbf{R} \in \mathcal{P}$ then $\mathbf{R}\langle X\rangle \in \mathcal{P}$.*

(ii) *If $\mathbf{R} \in \mathcal{P}$ then $\mathbf{R}_{\mathfrak{m}} \in \mathcal{P}$ for any maximal ideal $\mathfrak{m}$ of $\mathbf{R}$.*

(iii) *If $\mathbf{R} \in \mathcal{P}$ 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 $\mathbf{R} \in \mathcal{P}$, if M is a finitely generated projective $\mathbf{R}[X_1, \ldots, X_n]$-module, then M is extended from $\mathbf{R}$.

Quillen induction needs maximal ideals, it works in classical mathematics but it cannot be fully constructive. The fact that (ii) and (iii) imply the case $n = 1$ in the conclusion needs a priori a constructive rereading, where one replaces Quillen's patching with maximal ideals by the constructive form (Theorem 37) with comaximal multiplicative subsets.

On the contrary, the "inductive step" in the proof is elementary (see e.g., [39]) and is based only on the following hypotheses.

(i) If $\mathbf{R} \in \mathcal{P}$ then $\mathbf{R}\langle X\rangle \in \mathcal{P}$.

(iii') If $\mathbf{R} \in \mathcal{P}$ and M is a finitely generated projective $\mathbf{R}[X]$-module, then M is extended from $\mathbf{R}$.

In the case of Serre'problem, $\mathbf{R}$ is a discrete field. So (i) and (iii') are well-known. Remark that (iii') is also given by Horrocks' global Theorem 39. So Quillen's proof is deciphered in a fully constructive way. Moreover, since a zero-dimensional reduced local ring is a discrete field we obtain the following well-known generalization (see [13]).

Theorem 41. (Quillen-Suslin, non-Noetherian version)

1. *If $\mathbf{R}$ is a zero-dimensional reduced ring then any finitely generated projective module P over $\mathbf{R}[X_1, \ldots, X_n]$ is extended from $\mathbf{R}$ (i.e., isomorphic to a direct sum of modules $e_i\mathbf{R}[\underline{X}]$ where the e_i's are idempotent elements of $\mathbf{R}$).*
2. *As a particular case, any finitely generated projective module of constant rank over $\mathbf{R}[X_1, \ldots, X_n]$ is free.*
3. *More generally the results work for any zero-dimensional ring.*

Proof. The first point can be obtained from the local case by the constructive Quillen's patching Theorem 37. It can also be viewed as a concrete application of the General local-global Principle 27.
Let us denote by $\mathbf{R}_{\mathrm{red}}$ the reduced ring associated to a ring $\mathbf{R}$. Recall that $\mathrm{K}_0(\mathbf{R})$ is the set isomorphism classes of finitely generated projective $\mathbf{R}$-modules.
The third point follows from the fact that the canonical map $M \mapsto M_{\mathrm{red}}$, $\mathrm{K}_0(\mathbf{R}) \to \mathrm{K}_0(\mathbf{R}_{\mathrm{red}})$ is a bijection. Moreover $\mathbf{R}_{\mathrm{red}}[X_1, \ldots, X_n] = \mathbf{R}[X_1, \ldots, X_n]_{\mathrm{red}}$. □

3 Suslin's proof of Serre's problem

3.1 Making the use of maximal ideals constructive

This subsection is extracted from [72]. The purpose is to decipher constructively a lemma of Suslin [70] which played a central role in his second solution of Serre's problem. This lemma says that for a commutative ring $\mathbf{R}$ if $\langle v_1(X),\dots,v_n(X)\rangle = \mathbf{R}[X]$ where v_1 is monic and $n \geq 3$, then there exist $\gamma_1,\dots,\gamma_\ell \in \mathrm{E}_{n-1}(\mathbf{R}[X])$ (the subgroup of $\mathrm{SL}_{n-1}(\mathbf{R}[X])$ generated by elementary matrices) such that $\langle \mathrm{Res}(v_1, e_1.\gamma_1\,{}^{\mathrm{t}}(v_2,\dots,v_n)),\dots,\mathrm{Res}(v_1, e_1.\gamma_\ell\,{}^{\mathrm{t}}(v_2,\dots,v_n))\rangle = \mathbf{R}$. By the constructive proof we give, Suslin's proof of Serre 's problem becomes fully constructive. As a matter of fact, the lemma cited above is the only nonconstructive step in Suslin's elementary proof of Serre's problem [70]. Moreover, the new method with which we treat this academic example may be a model for miming constructively abstract proofs in which one works modulo each maximal ideal to prove that a given ideal contains 1. The Concrete local-global principle developed in Subsection 2.3 cannot be used here since the proof we want to decipher constructively, instead of passing to the localizations at each maximal ideal, passes to the residue fields modulo each maximal ideal.

In the literature, in order to surmount the obstacle of this lemma which is true for any ring $\mathbf{A}$, constructive mathematicians interested in Suslin's techniques for Suslin's stability theorem and Quillen-Suslin theorem are restricted to a few rings satisfying additional conditions and in which one knows effectively the form of all the maximal ideals. For instance, in [29, 31, 41, 62], the authors utilize the facts that for a discrete field $\mathbf{K}$, the ring $\mathbf{K}[X_1,\dots,X_k]$ is Noetherian and has an effective Nullstellensatz (see the proof of Theorem 4.3 of [62]). For all these reasons, we think that a constructive proof of Suslin's lemma without any restriction on the ring $\mathbf{A}$ will enable the extension of the known algorithms for the Suslin's stability and Quillen-Suslin theorems for a wider class of rings. Another feature of our method is that it may be a model for miming constructively abstract proofs passing to all the residue fields (that is, quotients by maximal ideals) in order to prove that an ideal contains 1. Note that we have already treated constructively the other main aspect of utilization of maximal ideals which is the localization at all maximal ideals (see Section 2.3). It is also worth pointing out that we will also give another constructive proof of the lemma of Suslin in the particular case $\mathbf{R}$ contains an infinite field using efficient elementary operations.

3.2 A remainder about the resultant

In this subsection, we content ourselves with a brief outline of *resultant*: an important idea in constructive algebra whose development owes considerably to famous pioneers such as Bezout, Cayley, Euler, Herman, Hurwitz, Kronecker, Macaulay, Noether, and Sylvester, among others.

This subsection will be focused on the few properties of the resultant that we need in our constructive view toward projective modules over polynomial rings.

Definition 42. *Let* $\mathbf{R}$ *be a ring,*

$$f = a_0X^\ell + a_1X^{\ell-1} + \cdots + a_\ell \in \mathbf{R}[X],\ a_0 \neq 0,\ a_i \in R,$$

and

$$g = b_0X^m + b_1X^{m-1} + \cdots + b_m \in \mathbf{R}[X],\ b_0 \neq 0,\ b_i \in R.$$

The resultant of f *and* g*, denoted by* $\mathrm{Res}_X(f,g)$ *or simply* $\mathrm{Res}(f,g)$ *if there is no risk of ambiguity, is the determinant of the* $(m+\ell)\times(m+\ell)$ *matrix below (called the Sylvester matrix of* f *and* g *with respect to* X*):*

$$\mathrm{Syl}(f,\ g,\ X) = \begin{pmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\
 & \vdots & & a_1 & & \vdots & & b_1 \\
a_\ell & & & & b_m & & & \\
 & a_\ell & & \vdots & & b_m & & \vdots \\
 & & \ddots & & & & \ddots & \\
 & & & a_\ell & & & & b_m
\end{pmatrix}$$

$$\underbrace{\qquad\qquad\qquad}_{m \text{ columns}} \quad \underbrace{\qquad\qquad\qquad}_{\ell \text{ columns}}$$

The resultant is an efficient tool for eliminating variables as can be seen in the following proposition. Applying this proposition in the particular case $R[X] = \mathbf{K}[X_1, \ldots, X_n]$, $\mathbf{K}$ a field, $\mathrm{Res}_{X_n}(f, g)$ is in the first elimination ideal $\langle f, g\rangle \cap \mathbf{K}[X_1, \ldots, X_{n-1}]$.

Proposition 43. *Let $\mathbf{R}$ be a ring. Then, for any f, $g \in \mathbf{R}[X]$, there exist h_1, $h_2 \in R[X]$ such that*

$$h_1 f + h_2 g = \mathrm{Res}_X(f, g) \in \mathbf{R}$$

with $\deg(h_1) \leq m - 1$ *and* $\deg(h_2) \leq \ell - 1$.

Proof. First notice that

$$(X^{\ell+m-1}, \ldots, X, 1)\ \mathrm{Syl}(f,\ g,\ X) = (X^{m-1}f, \ldots, f, X^{\ell-1}g, \ldots, g).$$

Thus, by Cramer's rule, considering 1 as the $(\ell + m - 1)^{\text{th}}$ unknown of the linear system whose matrix is $\mathrm{Syl}(f, g,\ X)$, $\mathrm{Res}_X(f, g)$ is the determinant of the Sylvester matrix of f and g in which the last row is replaced by $(X^{m-1}f, \ldots, f, X^{\ell-1}g, \ldots, g)$.

□

Corollary 44. *Let $\mathbf{K}$ be a field and f, $g \in \mathbf{K}[X] \setminus \{0\}$. Then*

(i) $1 \in \langle f, g\rangle \Leftrightarrow \gcd(f, g)$ *is constant* $\Leftrightarrow \mathrm{Res}(f, g) \neq 0$.

(ii) f and g have a common factor $\Leftrightarrow \gcd(f, g)$ *is nonconstant* $\Leftrightarrow \mathrm{Res}(f, g) = 0$.

Since in these notes we are concerned with the general setting of multivariate polynomials over a ring, we are tempted to say that Corollary 44 remains valid for any ring $\mathbf{R}$, where the condition "$\mathrm{Res}(f, g) \neq 0$" is replaced by "$\mathrm{Res}(f, g) \in \mathbf{R}^\times$". Of course the implication "$\mathrm{Res}(f, g) \in \mathbf{R}^\times \Rightarrow 1 \in \langle f, g\rangle$ " is always true thanks to Proposition 43. Unfortunately, the converse does not hold as will be shown by the following example. This is essentially due to the fact that if I is an ideal of a ring $\mathbf{R}$, then modulo I, we have not that $\overline{\mathrm{Res}(f, g)} = \mathrm{Res}(\bar{f}, \bar{g})$ for any f, $g \in \mathbf{R}[X]$.

Example 45. Let $\mathbf{R} = \mathbb{Z}$, $I = 3\mathbb{Z}$, $f = 6X^2 + X$, $g = 3X + 1$.
In $\mathbb{Z}[X]$, we have $1 \in \langle f_1, f_2\rangle$ as attested by the identity $3f + (1 - 6X)g = 1$ (this can be found by computing a dynamical Gröbner basis for $\langle f, g\rangle$ as in Section 7. In more details $S(f, g) = f - 2Xg = -X =: h$, $S(g, h) = g + 3h = 1$). However

$$\mathrm{Res}(f, g) = \begin{vmatrix} 6 & 3 & 1 \\ 1 & 1 & 3 \\ 0 & 0 & 1 \end{vmatrix} = 3 \notin \mathbb{Z}^\times,\ \mathrm{Res}(\bar{f}, \bar{g}) = \bar{1} \neq \overline{\mathrm{Res}(f, g)} = \bar{0}.$$

As can bee seen in this example, whether $\overline{\mathrm{Res}(f, g)} = \mathrm{Res}(\bar{f}, \bar{g})$ modulo I or not depends mainly on whether the leading coefficients of f and g belong to I or not. We will discuss this fact in the following immediate lemma. The leading coefficient of a polynomial $h \in \mathbf{R}[X]$ will be denoted by $\mathrm{LC}(h)$.

Lemma 46. *Let I be an ideal of a ring $\mathbf{R}$, and consider two polynomials $f = a_0X^\ell + a_1X^{\ell-1} + \cdots + a_\ell$, $g = b_0X^m + b_1X^{m-1} + \cdots + b_m \in \mathbf{R}[X]$ with $a_0 \neq 0$ and $b_0 \neq 0$ and such that modulo I, $\bar{f} \neq \bar{0}$ and $\bar{g} \neq \bar{0}$. Then*

(1) *If* $\overline{\mathrm{LC}(f)} \neq \bar{0}$ *and* $\overline{\mathrm{LC}(g)} \neq \bar{0}$ *then* $\overline{\mathrm{Res}(f, g)} = \mathrm{Res}(\bar{f}, \bar{g})$.

(2) *If* $\overline{\mathrm{LC}(f)} = \bar{0}$ *and* $\overline{\mathrm{LC}(g)} = \bar{0}$ *then* $\overline{\mathrm{Res}(f, g)} = 0$ *(and may be* $\neq \mathrm{Res}(\bar{f}, \bar{g})$*).*

(3) *If* $\overline{\mathrm{LC}(f)} \neq \bar{0}$ *and* $\overline{\mathrm{LC}(g)} = \bar{0}$ *then* $\overline{\mathrm{Res}(f, g)} = \bar{a}_0^{(\deg g - \deg \bar{g})}\mathrm{Res}(\bar{f}, \bar{g})$.

(4) *If* $\overline{\mathrm{LC}(f)} = \bar{0}$ *and* $\overline{\mathrm{LC}(g)} \neq \bar{0}$ *then* $\overline{\mathrm{Res}(f, g)} = \pm\bar{b}_0^{(\deg f - \deg \bar{f})}\mathrm{Res}(\bar{f}, \bar{g})$.

In fact, for the purpose of generalizing Corollary 44 to rings, we have to suppose that f or g is monic.

Proposition 47.
Let $\mathbf{R}$ be a ring and $f, g \in \mathbf{R}[X] \setminus \{0\}$ with f monic. Then

$$1 \in \langle f, g\rangle \text{ in } \mathbf{R}[X] \quad \Longleftrightarrow \quad \mathrm{Res}(f, g) \in \mathbf{R}^\times$$

Proof. A classical nonconstructive proof: we have only to prove the implication "$\Rightarrow$", the implication "$\Leftarrow$" being immediate by virtue of Proposition 43. For this, let $\mathfrak{m}$ be a maximal ideal of $\mathbf{R}$. Applying Lemma 46, we have $\overline{\mathrm{Res}(f,g)} = \mathrm{Res}(\bar{f},\bar{g})$ modulo $\mathfrak{m}$. Moreover, since $\mathbf{R}/\mathfrak{m}$ is a field, then using Corollary 44, we infer that $\overline{\mathrm{Res}(f,g)} \neq \bar{0}$, that is, $\mathrm{Res}(f,g) \notin \mathfrak{m}$. Since this is true for any maximal ideal of $\mathbf{R}$, then necessarily $\mathrm{Res}(f,g) \in \mathbf{R}^\times$. □

Proof. A constructive proof: let h_1, $h_2 \in \mathbf{R}[X]$ such that $h_1 f + h_2 g = 1$. Since f is monic, we have $\mathrm{Res}(f, h_2 g) = \mathrm{Res}(f,h_2)\,\mathrm{Res}(f,g)$ and $\mathrm{Res}(f,h_2g) = \mathrm{Res}(f, h_1f + h_2g) = \mathrm{Res}(f,1) = 1$. □

3.3 A lemma of Suslin

If $a_1,\dots,a_k$ are elements in a ring $\mathbf{B}$, we will denote by $\langle a_1,\dots,a_k\rangle$ the ideal of $\mathbf{B}$ generated by these elements.

Recall that for any ring $\mathbf{B}$ and $n \geq 1$, an $n \times n$ elementary matrix $E_{i,j}(a)$ over $\mathbf{B}$, where $i \neq j$ and $a \in \mathbf{B}$, is the matrix with 1s on the diagonal, a on position (i,j) and 0s elsewhere, that is, $E_{i,j}(a)$ is the matrix corresponding to the elementary operation $L_i \to L_i + aL_j$. $\mathrm{E}_n(\mathbf{B})$ will denote the subgroup of $\mathrm{SL}_n(\mathbf{B})$ generated by elementary matrices.

Theorem 48. (Suslin's lemma)
Let $\mathbf{A}$ be a commutative ring. If $\langle v_1(X),\dots,v_n(X)\rangle = \mathbf{A}[X]$ where v_1 is monic and $n \geq 2$, then there exist $\gamma_1,\dots,\gamma_\ell \in \mathrm{E}_{n-1}(\mathbf{A}[X])$ such that, denoting by w_i the first coordinate of $\gamma_i\,{}^{\mathrm{t}}(v_2,\dots,v_n)$, we have

$$\langle \mathrm{Res}(v_1,w_1),\dots,\mathrm{Res}(v_1,w_\ell)\rangle = \mathbf{A}.$$

Proof. For $n = 2$, we have $\mathrm{Res}(f,g) \in \mathbf{A}^\times$ by Proposition 47.

Suppose $n \geq 3$. We can without loss of generality suppose that all the v_i for $i \geq 2$ have degrees $< d = \deg v_1$. For the sake of simplicity, we write v_i instead of $\overline{v_i}$. We will use the notation $e_1.x$, where x is a column vector, to denote the first coordinate of x.

Suslin's proof: It consists in solving the problem modulo an arbitrary maximal ideal $\mathfrak{M}$ using a unique matrix $\gamma^{\mathfrak{M}} \in \mathrm{E}_{n-1}(\mathbf{A}/\mathfrak{M})[X]$ which transforms ${}^{\mathrm{t}}(v_2,\dots,v_n)$ into ${}^{\mathrm{t}}(g,0\dots,0)$ where g is the gcd of $v_2,\dots,v_n$ in $(\mathbf{A}/\mathfrak{M})[X]$. This matrix is given by a classical algorithm using elementary operations on ${}^{\mathrm{t}}(v_2,\dots,v_n)$. One starts by choosing a minimum degree component, say v_2, then the v_i, $3 \leq i \leq n$, are replaced by their remainders modulo v_2. By iterations, we obtain a column whose all components are zero except the first one. The matrix $\gamma^{\mathfrak{M}}$ lifts as a matrix $\gamma_{\mathfrak{M}} \in \mathrm{E}_{n-1}(\mathbf{A}[X])$. It follows that the first component $w_{\mathfrak{M}}$ of $\gamma_{\mathfrak{M}}\,{}^{\mathrm{t}}(v_2,\dots,v_n)$ is equal to the gcd of $v_2,\dots,v_n$ in $(\mathbf{A}/\mathfrak{M})[X]$. Thus, $\mathrm{Res}(v_1,w_{\mathfrak{M}}) \notin \mathfrak{M}$.

Constructive rereading of Suslin's proof: Let $u_1(X),\dots,u_n(X) \in \mathbf{A}[X]$ such that $v_1u_1 + \cdots + v_nu_n = 1$. Set $w = v_3u_3 + \cdots + v_nu_n$ and $V = {}^{\mathrm{t}}(v_2,\dots,v_n)$. We suppose that v_1 has degree d and for $2 \leq i \leq n$, the formal degree of v_i is $d_i < d$. This means that v_i has no coefficient of degree $> d_i$ but one does not guarantee that $\deg v_i = d_i$ (it is not necessary to have a zero test inside $\mathbf{A}$).

We proceed by induction on $\min_{2\leq i\leq n}\{d_i\}$. To simplify, we always suppose that $d_2 = \min_{2\leq i\leq n}\{d_i\}$.

For $d_2 = -1$, $v_2 = 0$ and by one elementary operation, we put w in the second coordinate. We have $\mathrm{Res}(v_1,w) = \mathrm{Res}(v_1, v_1u_1 + w) = \mathrm{Res}(v_1,1) = 1$ and we are done.
Now, suppose that we can find the desired elementary matrices for $d_2 = m-1$ and let show that we can do the job for $d_2 = m$.
Let a be the coefficient of degree m of v_2 and consider the ring $\mathbf{B} = \mathbf{A}/\langle a\rangle$. In $\mathbf{B}$, all the induction hypotheses are satisfied without changing the v_i nor the u_i. Thus, we can obtain $\Gamma_1,\dots,\Gamma_k \in \mathrm{E}_{n-1}(\mathbf{B}[X])$ such that

$$\langle \mathrm{Res}(v_1, e_1.\Gamma_1V),\dots,\mathrm{Res}(v_1,e_1.\Gamma_kV)\rangle = \mathbf{B}.$$

It follows that, denoting by $\Upsilon_1,\dots,\Upsilon_k$ the matrices in $\mathrm{E}_{n-1}(\mathbf{A}[X])$ lifting respectively $\Gamma_1,\dots,\Gamma_k$, we have

$$\langle \mathrm{Res}(v_1, e_1.\Upsilon_1V),\dots,\mathrm{Res}(v_1,e_1.\Upsilon_kV), a\rangle = \mathbf{A}.$$

Let $b \in \mathbf{A}$ such that

$$ab \equiv 1 \mod \langle \mathrm{Res}(v_1, e_1.\Upsilon_1V),\dots,\mathrm{Res}(v_1,e_1.\Upsilon_kV)\rangle = J$$

and consider the ring $\mathbf{C} = \mathbf{A}/J$. Note that in $\mathbf{C}$, we have $ab = 1$.
By an elementary operation, we replace v_3 by its remainder modulo v_2, say v_3', and then we exchange v_2 and $-v_3'$. The new column V' obtained has as first coordinate a polynomial with formal degree $m-1$. The induction hypothesis applies and we obtain $\Delta_1,\dots,\Delta_r \in \mathrm{E}_{n-1}(\mathbf{C}[X])$ such that

$$\langle \mathrm{Res}(v_1, e_1.\Delta_1V'),\dots,\mathrm{Res}(v_1,e_1.\Delta_rV')\rangle = \mathbf{C}.$$

Since V' is the image of V by a matrix in $\mathrm{E}_{n-1}(\mathbf{C}[X])$, we obtain matrices $\Lambda_1,\dots,\Lambda_r \in \mathrm{E}_{n-1}(\mathbf{C}[X])$ such that

$$\langle \mathrm{Res}(v_1, e_1.\Lambda_1V),\dots,\mathrm{Res}(v_1,e_1.\Lambda_rV)\rangle = \mathbf{C}.$$

The matrices Λ_j lift in $\mathrm{E}_{n-1}(\mathbf{A}[X])$ as, say $\Psi_1,\dots,\Psi_r$.

Finally, we obtain

$$\langle \mathrm{Res}(v_1, e_1.\Psi_1 V), \ldots, \mathrm{Res}(v_1, e_1.\Psi_r V)\rangle + J = \mathbf{A},$$

the desired conclusion.

□

Example 49. Take $\mathbf{A} = \mathbb{Z}$ and

$$V = {}^{\mathrm{t}}(v_1, v_2, v_3) = {}^{\mathrm{t}}(x^2 + 2x + 2,\ 3,\ 2x^2 + 11x - 3) \in \mathrm{Um}_3(\mathbb{Z}[x]),$$

(taking $u_1 = -2x + 2$, $u_2 = -3x^2 + x - 1$, $u_3 = x$, we have $u_1v_1 + u_2v_2 + u_3v_3 = 1$). It is worth pointing out that the u_i's can be found by constructing a dynamical Gröbner basis for $\langle v_1, v_2, v_3\rangle$ as in Section 7. Following the algorithm given in the proof of Theorem 48 and keeping the same notations, one has to perform a euclidean division of v_3 by v_1, so that ${}^{\mathrm{t}}(v_1, v_2, v_3) \overset{E_{3,1}(-2)}{\longrightarrow} {}^{\mathrm{t}}(v_1, v_2, \tilde{v}_3 = 7x - 7)$, and then passes to the ring $(\mathbb{Z}/3\mathbb{Z})[x]$. This yields to $\ell = 2$, $\gamma_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\gamma_2 = \mathrm{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and finally

$$\langle \mathrm{Res}(v_1, e_1.\gamma_1\, {}^{\mathrm{t}}(v_2, v_3)),\ \mathrm{Res}(v_1, e_1.\gamma_2\, {}^{\mathrm{t}}(v_2, v_3))\rangle = \langle 170,\ 9\rangle = \mathbb{Z}.$$

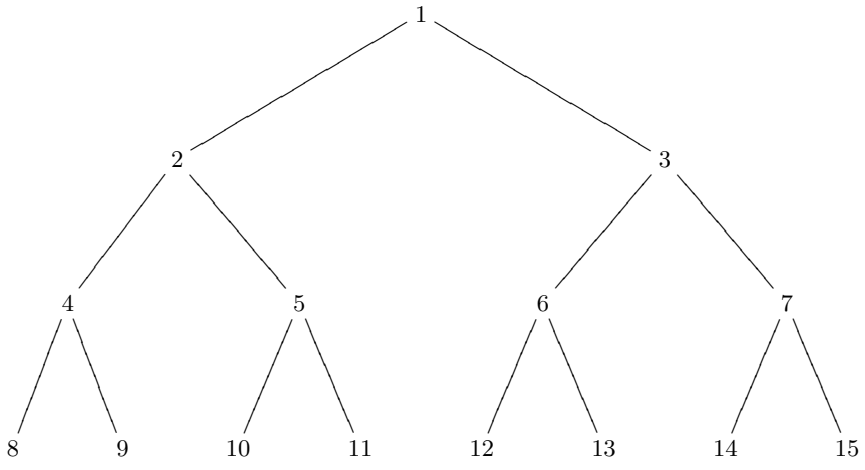
This example will be pursued in Section 3.6 where as a fruit of the computations above we will obtain a free basis for the syzygy module $\mathrm{Syz}(v_1, v_2, v_3)$.

Remark 50. It is easy to see that in Theorem 48, with the hypothesis $\deg v_i \leq d$ for $1 \leq i \leq n$, the number ℓ of matrices γ_j in the group $\mathrm{E}_{n-1}(\mathbf{A}[X])$ is bounded by 2^d. Moreover, each γ_j is the product of at most $2d$ elementary matrices. It is worth pointing out that there is an alternative constructive proof of Suslin's lemma (see Theorem 52) using only $(n-2)d+1$ matrices γ_j, each of them is the product of $n-2$ elementary matrices. This is substantially better than the general constructive proof we give above but requires the additional condition that $\mathbf{A}$ has at least $(n-2)d+1$ elements $y_0, \ldots, y_{(n-2)d}$ such that $y_i - y_j \in \mathbf{A}^\times$ for all $i \neq j$ (for example, if $\mathbf{A}$ contains an infinite field).

3.4 A more general strategy (by "backtracking")

As already mentioned above, contrary to the local-global principles explained in Section 2.3, we do not reread a proof in which one localizes at a generic prime ideal $\mathfrak{P}$ or at a generic maximal ideal $\mathfrak{M}$ but a proof in which one passes modulo a generic maximal ideal $\mathfrak{M}$ in order to prove that an ideal $\mathfrak{a}$ of a ring $\mathbf{A}$ contains 1. The classical proof is very often by contradiction: for a generic maximal ideal $\mathfrak{M}$, if $\mathfrak{a} \subseteq \mathfrak{M}$ then $1 \in \mathfrak{M}$. But, in fact, this reasoning hides a concrete fact: $1 = 0$ in the residue field $\mathbf{A}/\mathfrak{M}$ (see [65]). Consequently, this reasoning by contradiction can be converted dynamically into a constructive proof as follows. One has to do the necessary computations as if $\mathbf{A}/\mathfrak{a}$ was a field. Every time one needs to know if an element x_i is null or a unit modulo $\mathfrak{a}$, he has just to force it into being null by adding it to $\mathfrak{a}$. Suppose for example that we have established that $1 \in \mathfrak{a} + \langle x_1, x_2, x_3\rangle$ (this corresponds in the classical proof to the fact that: $x_1, x_2, x_3 \in \mathfrak{M} \ \Rightarrow\ 1 \in \mathfrak{M}$). This means that x_3 is a unit modulo $\mathfrak{a} + \langle x_1, x_2\rangle$ and thus one has to follow the classical proof in case $x_1, x_2 \in \mathfrak{M}$ and x_3 is a unit modulo $\mathfrak{M}$. It is worth pointing out that there is no need of $\mathfrak{M}$ since one has already computed an inverse of x_3 modulo $\mathfrak{a} + \langle x_1, x_2\rangle$.

For the purpose of illustrating this strategy, let us consider an example of a binary tree corresponding to the computations produced by a "local-global" rereading:



In the tree above, the disjunctions correspond to a test:

$$x \in \mathbf{A}_i^{\times} \quad \vee \quad 1-x \ \in \mathbf{A}_i^{\times},$$

and each node corresponds to a localization $\mathbf{A}_i$ of the initial ring $\mathbf{A}$. In order to glue the local solutions (at the terminal nodes, that is, at the leaves), one has to go back from the leaves to the root in a "parallel" way. Now imagine that these disjunctions correspond to a test:

$$x \in \mathbf{A}_i^{\times} \quad \vee \quad x = 0 \text{ in } \mathbf{A}_i,$$

and each node i corresponds to a quotient $\mathbf{A}_i$ of the initial ring $\mathbf{A}$. Following the classical proof which proves that an ideal $\mathfrak{a}$ of $\mathbf{A}$ contains 1, one has to start with the leaf which is completely on the right (leaf 15), that is, to follow the path $1 \to 3 \to 7 \to 15$ by considering the successive corresponding quotients $\mathbf{A} = \mathbf{A}/\langle 0\rangle$, $\mathbf{A}/\langle a_1\rangle$, $\mathbf{A}/\langle a_1, a_3\rangle$, and $\mathbf{A}/\langle a_1, a_3, a_7\rangle$. Using just the information at the leaf 15 where the considered ring is $\mathbf{A}/\langle a_1, a_3, a_7\rangle$ (this information corresponds in the classical proof to the fact that: $a_1, a_3, a_7 \in \mathfrak{M} \ \Rightarrow \ 1 \in \mathfrak{M}$), one obtains an element $b_{15} \in \mathbf{A}$ such that $1 \in \langle a_1, a_3, a_7, b_{15}\rangle$, or equivalently, a_7 is a unit modulo $\langle a_1, a_3, b_{15}\rangle$. Now, we go back to the node 7 but with a new quotient $\mathbf{A}/\langle a_1, a_3, b_{15}\rangle$ (note that at the first passage through 7 the considered quotient ring was $\mathbf{A}/\langle a_1, a_3\rangle$) and we can follow the branch $7 \to 14$ (this corresponds in the classical proof to the fact that: $a_1, a_3 \in \mathfrak{M}$ and a_7 is a unit modulo $\mathfrak{M} \ \Rightarrow \ 1 \in \mathfrak{M}$). This will produce an element b_{14} such that $1 \in \langle a_1, a_3, b_{14}, b_{15}\rangle$, or equivalently, a_3 is a unit modulo $\langle a_1, b_{14}, b_{15}\rangle$. Thus, we can go back to the node 3 through the branch $14 \to 7 \to 3$, and so on. In the end, the entire path followed is

$$\begin{array}{c} 1 \to 3 \to 7 \to 15 \to 7 \to 14 \to 7 \to 3 \to 6 \to 13 \to 6 \to 12 \to 6 \to 3 \to 1 \to \\ 2 \to 5 \to 11 \to 5 \to 10 \to 5 \to 2 \to 4 \to 9 \to 4 \to 8 \to 4 \to 2 \to 1. \end{array}$$

Finally, at the root of the tree (node 1), we get that $1 \in \langle b_8, \ldots, b_{15}\rangle$ in the ring $\mathbf{A}/\langle 0\rangle = \mathbf{A}$. It is worth pointing out that, as can be seen above, another major difference between a "local-global tree" and the tree produced by our method is that the quotient ring changes at each new passage through the considered node. For example, in the first passage through 7, the ring was $\mathbf{A}/\langle a_1, a_3\rangle$, in the second passage it becomes $\mathbf{A}/\langle a_1, a_3, b_{15}\rangle$, and in the last one the ring is $\mathbf{A}/\langle a_1, a_3, b_{14}, b_{15}\rangle$.

We can sum up this new method as follows:

Elimination of maximal ideals by backtracking 51. When rereading dynamically the original proof, follow systematically the branch $x_i \in \mathfrak{M}$ any time you find a disjunction "$x_i \in \mathfrak{M} \ \vee \ x_i \notin \mathfrak{M}$" in the proof until getting $1 = 0$ in the quotient. That is, in the corresponding leaf of the tree, you get $1 \in \langle x_1, \ldots, x_k\rangle$ for some $x_1, \ldots, x_k \in \mathbf{A}$. This means that at the node $\langle x_1, \ldots, x_{k-1}\rangle \subseteq \mathfrak{M}$, you know a concrete $a \in \mathbf{A}$ such that $1 - ax_k \in \langle x_1, \ldots, x_{k-1}\rangle$. So you can follow the proof.

If the proof given for a generic maximal ideal is sufficiently "uniform", you know a bound for the depth of the (infinite branching) tree. For example in Suslin's lemma, the depth is $\deg(v_1)$. So your "finite branching dynamical evaluation" is finite: you get an algorithm.

3.5 Suslin's lemma for rings containing an infinite field

By the following theorem, we give an elimination process close to that given in Proposition 4.72 of [11]. The proof given in [11] was'nt constructive as it made use of roots in algebraic closures.

Theorem 52. (Suslin's lemma, particular case, new formulation)
Let $\mathbf{A}$ be a commutative ring containing an infinite field $\mathbf{K}$ and let us fix a sequence $(y_i)_{i\in\mathbb{N}}$ of pairwise distinct elements in $\mathbf{K}$. Let $v_1, \ldots, v_n \in \mathbf{A}[X]$ such that v_1 is monic and $n \geq 2$. Then
$1 \in \langle v_1, \ldots, v_n\rangle \ \Leftrightarrow \ 1 \in \langle \mathrm{Res}_X(v_1, v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n),\ 0 \leq i \leq (n-2)\, d\rangle$.

Proof. The implication "$\Leftarrow$" is straightforward.
Let us denote by $w_i := v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n$, $r_i := \mathrm{Res}_X(v_1, w_i)$, $0 \leq i \leq s = (n-2)\, d$, $\ell := d + 1$, where $d = \deg v_1$, and suppose that $1 \in \langle v_1, \ldots, v_n\rangle$.

Let $Z_0 = \cdots = Z_{n-3} = z_0$,
$Z_{n-2} = \cdots = Z_{2n-5} = z_1$,
$\vdots$
$Z_{(n-2)k} = \cdots = Z_{(n-2)(k+1)-1} = z_k$,
$\vdots$

$Z_{(n-2)(d-1)} = \cdots = Z_{(n-2)d-1} = z_{d-1}$,
$Z_{(n-2)d} = z_d$,
be an enumeration of ℓ indeterminates over $\mathbf{A}$ with $n-2$ repetitions except the last one which is repeated once. Let us denote by

$$I = \langle v_1(Z_i),\, w_i(Z_i) \mid 0 \le i \le s\rangle, \quad \mathbf{A}_\ell = \mathbf{A}[Z_0, \ldots, Z_s]/I\,.$$

First we prove that $1 = 0$ in $\mathbf{A}_\ell$.
Letting $0 \le i_1 < \cdots < i_{n-1} \le s$, we have:

$$\begin{pmatrix} 1 & y_{i_1} & \ldots & y_{i_1}^{n-2} \\ 1 & y_{i_2} & \ldots & y_{i_2}^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{i_{n-1}} & \ldots & y_{i_{n-1}}^{n-2} \end{pmatrix} \begin{pmatrix} v_2 \\ v_3 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} w_{i_1} \\ w_{i_2} \\ \vdots \\ w_{i_{n-1}} \end{pmatrix}.$$

As the matrix above is a Vandermonde matrix, its determinant is equal to

$$\prod_{1 \le \ell < k \le n-1} (y_{i_k} - y_{i_\ell}),$$

which is invertible in $\mathbf{A}$. Thus, $v_2, \ldots, v_n \in \langle w_{i_1}, \ldots, w_{i_{n-1}}\rangle$ and a fortiori

$$v_2(Z_{i_1}), \ldots, v_n(Z_{i_1}) \in I + \langle w_{i_2}(Z_{i_1}), \ldots, w_{i_{n-1}}(Z_{i_1})\rangle \subseteq I + \langle Z_{i_1} - Z_{i_2}, \ldots, Z_{i_1} - Z_{i_{n-1}}\rangle,$$

and hence, using the fact that $1 \in \langle v_1, \ldots, v_n\rangle$, we obtain that

$$1 \in I + \langle Z_{i_1} - Z_{i_2}, \ldots, Z_{i_1} - Z_{i_{n-1}}\rangle.$$

Thus, for $0 \le i < j \le d$,

$$1 \in I + \langle Z_{(n-2)i} - Z_{(n-2)i+1}, \ldots, Z_{(n-2)i} - Z_{(n-2)(i+1)-1}, Z_{(n-2)i} - Z_{(n-2)j}\rangle$$

$$= I + \langle z_i - z_j\rangle,$$

that is $z_i - z_j$ is invertible in $\mathbf{A}_\ell$.
On the other hand, by clearing the denominators in the Lagrange interpolation formula, we obtain

$$v_1(X)\ \left(\textstyle\prod_{i\neq j}(z_i - z_j)\right) \in \langle v_1(z_1), \ldots, v_1(z_\ell)\rangle\ \subseteq\ \mathbf{A}[z_1, \ldots, z_\ell][X]$$

(here we need the hypothesis $\ell = \deg v_1 + 1$).
In $\mathbf{A}_\ell$, $\prod_{i\neq j}(z_i - z_j)$ is invertible, $v_1(z_1) = \cdots = v_1(z_\ell) = 0$, thus $v_1(X) = 0$ in $\mathbf{A}_\ell[X]$. Since v_1 is monic, we obtain $1 = 0$ in $\mathbf{A}_\ell$, that is $1 \in I$.

For $0 \le k \le s$, denote $I_k = \langle v_1(Z_i), w_i(Z_i) \mid 0 \le i \le k\rangle$, $J_k = I_k + \langle r_i \mid k < i \le s\rangle$ and $\mathbf{A}_k = \mathbf{A}[Z_1, \ldots, Z_k]/I_k$. Note that $I_s = I$, so $1 \in I_s = J_s$. Using Proposition 47 we get by induction on k from s to 0 that $1 \in J_k$: in order to go from $k+1$ to k consider the ring $\mathbf{B}_k = \mathbf{A}[Z_1, \ldots, Z_k]/\langle r_{k+2}, \ldots, r_s\rangle$ and apply Proposition 47 with $X = Z_{k+1}$, $a = v_1(Z_{k+1})$, $b = w_{k+1}(Z_{k+1})$. So $1 \in J_0 = \langle r_s, \ldots, r_0\rangle$.

□

Remark 53. Of course, in Theorem 52, it would suffice to suppose that $\mathbf{A}$ contains $(n-2)d + 1$ elements $y_0, \ldots, y_{(n-2)d}$ such that $y_i - y_j \in \mathbf{A}^\times$ for all $i \neq j$.

3.6 Suslin's algorithm for reduction of polynomial unimodular rows

For any ring $\mathbf{B}$, when we say that a matrix $N \in \mathrm{M}_n(\mathbf{B})$ $(n \ge 3)$ is in $\mathrm{SL}_2(\mathbf{B})$ we mean that it is of the form

$$\begin{pmatrix} N' & 0 & \ldots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

with $N' \in \mathrm{SL}_2(\mathbf{B})$.

Lemma 54. (Translation by the resultant, [70] Lemma 2.1)
Let $\mathbf{R}$ *be a commutative ring. Let* $f_1, f_2 \in \mathbf{R}[X]$, $b, d \in \mathbf{R}$, *and let* $r = \mathrm{Res}(f_1, f_2) \in \mathbf{R}$. *Then there exists* $B \in \mathrm{SL}_2(\mathbf{R}[X])$ *such that*

$$B \begin{pmatrix} f_1(b) \\ f_2(b) \end{pmatrix} = \begin{pmatrix} f_1(b+rd) \\ f_2(b+rd) \end{pmatrix}.$$

Proof. Take $g_1, g_2 \in \mathbf{R}[X]$ such that $f_1\, g_1 + f_2\, g_2 = r$, denote by s_1, s_2, t_1, t_2 the polynomials in $\mathbf{R}[X, Y, Z]$ such that

$f_1(X + YZ) = f_1(X) + Y s_1(X, Y, Z)$,
$f_2(X + YZ) = f_2(X) + Y s_2(X, Y, Z)$,
$g_1(X + YZ) = g_1(X) + Y t_1(X, Y, Z)$,
$g_2(X + YZ) = g_2(X) + Y t_2(X, Y, Z)$,

and set

$B_{1,1} = 1 + s_1(b, r, d)\, g_1(b) + t_2(b, r, d)\, f_2(b)$,
$B_{1,2} = s_1(b, r, d)\, g_2(b) - t_2(b, r, d)\, f_1(b)$,
$B_{2,1} = s_2(b, r, d)\, g_1(b) - t_1(b, r, d)\, f_2(b)$,
$B_{2,2} = 1 + s_2(b, r, d)\, g_2(b) + t_1(b, r, d)\, f_1(b)$.

Then, one can take $B = \begin{pmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix}$.

□

Algorithm 55. (An algorithm for eliminating variables from unimodular polynomial vectors with coefficients in a ring containing an infinite field)

Input: *A column* $\mathcal{V} = \mathcal{V}(X) = {}^{\mathrm{t}}(v_1(X), \ldots, v_n(X)) \in \mathrm{Um}_n(\mathbf{A}[X])$ *such that* v_1 *is monic.*
Output: *A matrix* $\mathcal{B} \in \mathrm{SL}_n(\mathbf{A}[X])$ *such that* $\mathcal{B}\,\mathcal{V} = \mathcal{V}(0)$.

Step 1: *For* $0 \leq i \leq s = (n-2)d$, *where* $d = \deg_X v_1$, *set* $w_i = v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n$, *compute* $r_i := \mathrm{Res}_X(v_1, w_i)$ *and find* $\alpha_0, \ldots, \alpha_s \in \mathbf{A}$ *such that* $\alpha_0 r_0 + \cdots + \alpha_s r_s = 1$ *(here we use Theorem 52).*
For $0 \leq i \leq s$, *compute* $f_i, g_i \in \mathbf{A}[X]$ *such that* $f_i v_1 + g_i w_i = r_i$ *(use Proposition 43).*

Step 2: *Set*
$b_{s+1} := 0$,
$b_s := \alpha_s\, r_s X$,
$b_{s-1} := b_s + \alpha_{s-1} r_{s-1} X$,
$\vdots$
$b_0 := b_1 + \alpha_0 r_0 X = X$ *(this follows from the fact that* $X = \sum_{i=0}^{s} \alpha_i r_i X$*).*

Step 3: *For* $1 \leq i \leq s+1$, *find* $\mathcal{B}_i \in \mathrm{SL}_n(\mathbf{A}[X])$ *such that* $\mathcal{B}_i \mathcal{V}(b_{i-1}) = \mathcal{V}(b_i)$.
In more details, let γ_i *be the matrix corresponding to the elementary operation* $L_2 \to L_2 + \sum_{j=3}^{n} y_i^{j-2} L_j$, *that is,*

$$\gamma_i := E_{2,n}(y_i^{n-2}) \cdots E_{2,3}(y_i).$$

For $3 \leq j \leq n$, *set* $F_{i,j} := \frac{v_j(b_{i-1}) - v_j(b_i)}{b_{i-1} - b_i} = \frac{v_j(b_{i-1}) - v_j(b_i)}{\alpha_i r_i X} \in \mathbf{A}[X]$, *so that one obtains*

$$v_j(b_{i-1}) - v_j(b_i) = \alpha_i r_i X F_{i,j} = \alpha_i X F_{i,j}\, f_i(b_{i-1}) v_1(b_{i-1}) + \alpha_i X F_{i,j}\, g_i(b_{i-1}) w_i(b_{i-1})$$

$$= \sigma_{i,j}\, v_1(b_{i-1}) + \tau_{i,j}\, w_i(b_{i-1}),$$

with

$$\sigma_{i,j} := \alpha_i X F_{i,j}\, f_i(b_{i-1}), \tau_{i,j} := \alpha_i X F_{i,j}\, g_i(b_{i-1}) \in \mathbf{A}[X].$$

Let $\Gamma_i \in \mathrm{E}_n(\mathbf{A}[X])$ *be the matrix corresponding to the elementary operations:*
$L_j \to L_j - \sigma_{i,j} L_1 - \tau_{i,j} L_2$, $3 \leq j \leq n$, *that is*

$$\Gamma_i := \prod_{j=3}^{n} E_{j,1}(-\sigma_{i,j})\, E_{j,2}(-\tau_{i,j}).$$

Set

$$B_{i,2} := \Gamma_i\,\gamma_i \in \mathrm{E}_n(\mathbf{A}[X]),$$

so that we have

$$B_{i,2}\mathcal{V}(b_{i-1}) = \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \\ v_3(b_i) \\ \vdots \\ v_n(b_i) \end{pmatrix}.$$

Following Lemma 54, set

$s_{i,1}(X,Y,Z) := \frac{v_1(X+YZ)-v_1(X)}{Y} \in \mathbf{A}[X,Y,Z]$,
$s_{i,2}(X,Y,Z) := \frac{w_i(X+YZ)-w_i(X)}{Y} \in \mathbf{A}[X,Y,Z]$,
$t_{i,1}(X,Y,Z) := \frac{f_i(X+YZ)-f_i(X)}{Y} \in \mathbf{A}[X,Y,Z]$,
$t_{i,2}(X,Y,Z) := \frac{g_i(X+YZ)-g_i(X)}{Y} \in \mathbf{A}[X,Y,Z]$,
$C_{i,1,1} := 1 + s_{i,1}(b_{i-1}, r_i, -\alpha_i X)\, f_i(b_{i-1}) + t_{i,2}(b_{i-1}, r_i, -\alpha_i X)\, w_i(b_{i-1}) \in \mathbf{A}[X]$,
$C_{i,1,2} = s_{i,1}(b_{i-1}, r_i, -\alpha_i X)\, g_i(b_{i-1}) - t_{i,2}(b_{i-1}, r_i, -\alpha_i X)\, v_1(b_{i-1}) \in \mathbf{A}[X]$,
$C_{i,2,1} = s_{i,2}(b_{i-1}, r_i, -\alpha_i X)\, f_i(b_{i-1}) - t_{i,1}(b_{i-1}, r_i, -\alpha_i X)\, w_i(b_{i-1}) \in \mathbf{A}[X]$,
$C_{i,2,2} = 1 + s_{i,2}(b_{i-1}, r_i, -\alpha_i X)\, g_i(b_{i-1}) + t_{i,1}(b_{i-1}, r_i, -\alpha_i X)\, v_1(b_{i-1}) \in \mathbf{A}[X]$,

$$C_i := \begin{pmatrix} C_{i,1,1} & C_{i,1,2} \\ C_{i,2,1} & C_{i,2,2} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{A}[X]).$$

Note that

$$C_i \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ w_i(b_i) \end{pmatrix}.$$

Set

$$B_{i,1} := \gamma_i^{-1} \begin{pmatrix} C_i & 0 \\ 0 & I_{n-2} \end{pmatrix},$$

with

$$\gamma_i^{-1} = E_{2,3}(-y_i) \cdots E_{2,n}(-y_i^{n-2}).$$

Set

$$\mathcal{B}_i := B_{i,1}\, B_{i,2} \in \mathrm{SL}_n(\mathbf{A}[X]),$$

so that $\mathcal{B}_i\mathcal{V}(b_{i-1}) = \mathcal{V}(b_i)$.

Step 4: $\mathcal{B} := \mathcal{B}_{s+1} \cdots \mathcal{B}_1$.

Example 56. Now, let $\mathcal{V} = \begin{pmatrix} x + y^2 - 1 \\ -x + y^2 - 2xy \\ x - y^3 + 2 \end{pmatrix} \in \mathrm{Um}_3(\mathbb{Q}[x,y])$.

Algorithm 55 has been implemented using the Computer Algebra System **Maple**. The code of our algorithm (**UnimodElimination**) gives a matrix $B \in \mathrm{SL}_3(\mathbb{Q}[x,y])$ eliminating one variable. In this example, $B\,\mathcal{V} = \mathcal{V}(0,y)$.

```
>  V:=matrix([[x+y^2-1], [-x+y^2-2*x*y], [x-y^3+2]]);

 > B:=UnimodElimination(V,x);

  B := matrix([[1+27/151*x-56/151*x*y-24/151*x*y^2-8/151*y^3*x,
  -35/151*x-4/151*x*y^2-14/151*x*y, -62/151*x-8/151*x*y^2-28/151*x*y],
   [2/151*x*y+56/151*y^3*x+16/151*y^4*x+136/151*x*y^2-27/151*x,
   1+84/151*x*y+8/151*y^3*x+32/151*x*y^2+35/151*x,
   152/151*x*y+16/151*y^3*x+64/151*x*y^2+62/151*x],
    [-56/151*x*y-8/151*y^3*x-24/151*x*y^2+27/151*x, -35/151*x-4/151*x*y^2-14/151*x*y,
     1-62/151*x-8/151*x*y^2-28/151*x*y]])

 > VV:=expandvector(multiply(B,V));

 VV := matrix([[-1+y^2], [y^2], [2-y^3]])
```

Let us fix an infinite sequence of pairwise distinct elements (y_i) in $\mathbf{K}$ and use the notation $\underline{X} = (X_1, \ldots, X_k)$.

Algorithm 57. (An algorithm for the Quillen-Suslin theorem: case of $\mathbf{K}[X_1, \ldots, X_k]$ where $\mathbf{K}$ is an infinite field

Input: *One column* $\mathcal{V} = \mathcal{V}(\underline{X}) = {}^{\mathrm{t}}(v_1(\underline{X}), \ldots, v_n(\underline{X})) \in \mathrm{Um}_n(\mathbf{K}[\underline{X}])$ *such* $\max_{1 \leq i \leq n}\{\deg v_i\} = d$ *(here by degree we mean total degree), where* $d \geq 2$.

Output: *A matrix* G *in* $\mathrm{SL}_n(\mathbf{K}[\underline{X}])$ *such that* $G\mathcal{V} = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

For j *from* k *to* 1 *perform steps 1 and 2:*

Step 1: *Make a linear change of variables so that* v_1 *becomes monic at* X_j.

Step 2 *Perform Algorithm 1 with* $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_{j-1}]$ *and* $X = X_j$. *Output the new* $\mathcal{V}$.

Example 58. (Example 56 continued)

Let $\mathcal{V} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} x + y^2 - 1 \\ -x + y^2 - 2xy \\ x - y^3 + 2 \end{pmatrix} \in \mathrm{Um}_3(\mathbb{Q}[x, y])$.

Recall that the syzygy module of (v_1, v_2, v_3) is

$$\mathrm{Syz}(v_1, v_2, v_3) := \{ {}^{\mathrm{t}}(w_1, w_2, w_3) \in \mathbb{Q}[x, y]^{3 \times 1} \text{ such that } w_1 v_1 + w_2 v_2 + w_3 v_3 = 0\}.$$

Recall also that since ${}^{\mathrm{t}}(v_1, v_2, v_3) \in \mathrm{Um}_3(\mathbb{Q}[x, y])$, $\mathrm{Syz}(v_1, v_2, v_3)$ is a projective $\mathbb{Q}[x, y]$-module which is free of rank 2 by the Quillen-Suslin Theorem 41. A generating set for $\mathrm{Syz}(v_1, v_2, v_3)$ can be obtained using Gröbner bases techniques (see for example [24, 32]). For this, let us open a **Singular** Session (for more details see [32]):

```
> ring B=0,(x,y),dp;
> ideal I=x+y2-1,-x+y2-2xy,x-y3+2;
> module N=syz(I);
> N;

N[1]=2y3*gen(1)+2xy*gen(1)+2y2*gen(3)+y2*gen(2)-y2*gen(1)+2x*gen(3)
+x*gen(2)-x*gen(1)-2*gen(3)-gen(2)-4*gen(1)

N[2]=4xy2*gen(1)-14y3*gen(1)+4xy*gen(3)+2xy*gen(2)-12xy*gen(1)
-14y2*gen(3)-7y2*gen(2)+7y2*gen(1)-10x*gen(3)-5x*gen(2)+5x*gen(1)
-2y*gen(2)+12*gen(3)+11*gen(2)+24*gen(1)

N[3]=8x2y*gen(1)-98y3*gen(1)+8x2*gen(3)+4x2*gen(2)-4x2*gen(1)
-98xy*gen(1)-98y2*gen(3)-49y2*gen(2)+53y2*gen(1)-98x*gen(3)-53x*gen(2)
+25x*gen(1)+4y*gen(3)-12y*gen(2)+8y*gen(1)+94*gen(3)+61*gen(2)+188*gen(1)
```

One can read that $\mathrm{Syz}(v_1, v_2, v_3) = \langle \mathfrak{u}_1, \mathfrak{u}_2, \mathfrak{u}_3 \rangle$ with
$\mathfrak{u}_1 = {}^{\mathrm{t}}(2y^3 + 2xy - y^2 - x - 4,\ y^2 + x - 1,\ 2y^2 + 2x - 2)$,
$\mathfrak{u}_2 = {}^{\mathrm{t}}(4xy^2 - 14y^3 - 12xy + 7y^2 + 5x + 24,\ 2xy - 7y^2 - 5x - 2y + 11,\ 4xy - 14y^2 - 10x + 12)$,
$\mathfrak{u}_3 = {}^{\mathrm{t}}(8x^2y - 98y^3 - 4x^2 - 98xy + 53y^3 + 25x + 8y + 188,\ 4x^2 - 49y^2 - 53x - 12y + 61,$
$8x^2 - 98y^2 + 4y + 94)$.

But this is not a **minimal** set of generators for $\mathrm{Syz}(v_1, v_2, v_3)$!
In order to obtain such a minimal generating set one has to compute a free basis for $\mathrm{Syz}(v_1, v_2, v_3)$. We have implemented Algorithm 57 using the Computer Algebra System **Maple**. It computes a matrix $G \in \mathrm{SL}_3(\mathbb{Q}[x, y])$ such that $G\,\mathcal{V} = {}^{\mathrm{t}}(1, 0, 0)$.

```
G := matrix([[-1+60/151*x*y^3+540/151*x*y^2+62/151*x*y-108/151*x+2*y^2-128/151*x*y^5
-272/151*x*y^4-32/151*x*y^6,
-40/151*x*y^2+266/151*x*y+140/151*x-72/151*x*y^4-172/151*x*y^3+3-2*y^2-16/151*x*y^5,
 248/151*x-48/151*x*y^2+484/151*x*y-144/151*x*y^4-312/151*x*y^3-32/151*x*y^5],
 [-y^2+64/151*x*y^5+144/151*x*y^4+2/151*x*y^3-190/151*x*y^2+27/151*x-2/151*x*y
 +16/151*x*y^6,
 36/151*x*y^4+90/151*x*y^3+38/151*x*y^2-1-35/151*x-84/151*x*y+y^2+8/151*x*y^5,
 60/151*x*y^2+72/151*x*y^4+164/151*x*y^3-152/151*x*y-62/151*x+16/151*x*y^5],
```

```
[2-190/151*x*y^3-344/151*x*y^2-172/151*x*y+135/151*x-y^3+64/151*x*y^6+160/151*x*y^5
+26/151*x*y^4+16/151*x*y^7,
 -76/151*x*y^2-210/151*x*y-175/151*x+36/151*x*y^5+98/151*x*y^4+54/151*x*y^3-2+y^3
 +8/151*x*y^6,
 -310/151*x-152/151*x*y^2-388/151*x*y+92/151*x*y^3+72/151*x*y^5+180/151*x*y^4
 +16/151*x*y^6+1]])
```

Thus, denoting by

$$\epsilon_1 = \begin{pmatrix} -151y^2 + 64xy^5 + 144xy^4 + 2xy^3 - 190xy^2 + 27x - 2xy + 16xy^6 \\ 36xy^4 + 90xy^3 + 38xy^2 - 151 - 35x - 84xy + 151y^2 + 8xy^5 \\ 60xy^2 + 72xy^4 + 164xy^3 - 152xy - 62x + 16xy^5 \end{pmatrix},$$

and

$$\epsilon_2 = \begin{pmatrix} 302 - 190xy^3 - 344xy^2 - 172xy + 135x - 151y^3 + 64xy^6 + 160xy^5 + 26xy^4 + 16xy^7 \\ -76xy^2 - 210xy - 175x + 36xy^5 + 98xy^4 + 54xy^3 - 302 + 151y^3 + 8xy^6 \\ -310x - 152xy^2 - 388xy + 92xy^3 + 72xy^5 + 180xy^4 + 16xy^6 + 151 \end{pmatrix},$$

(ϵ_1, ϵ_2) is a free basis for $\mathrm{Syz}(v_1, v_2, v_3)$. A minimal parametrization of the set $\mathcal{E}$ of all inverses of $\mathcal{V}$ is

$$\mathcal{E} := \{\mathcal{U} = (u_1, u_2, u_3) \in \mathbb{Q}[x, y]^{1\times 3} \text{ such that } \mathcal{U}\,\mathcal{V} = 1\} = \{\epsilon_0 + \alpha\epsilon_1 + \beta\epsilon_2,\ \alpha,\ \beta \in \mathbb{Q}[x, y]\},$$

where $\epsilon_0 = \frac{1}{151}\begin{pmatrix} -151 + 60xy^3 + 540xy^2 + 62xy - 108x + 302y^2 - 128xy^5 - 272xy^4 - 32xy^6 \\ -40xy^2 + 266xy + 140x - 72xy^4 - 172xy^3 + 453 - 302y^2 - 16xy^5 \\ 248x - 48xy^2 + 484xy - 144xy^4 - 312xy^3 - 32xy^5 \end{pmatrix}$.

Algorithm 59. (An algorithm for eliminating variables from unimodular polynomial vectors with coefficients in a ring, general case
Input: *A column* $\mathcal{V} = \mathcal{V}(X) = {}^{\mathrm{t}}(v_1(X), \ldots, v_n(X)) \in \mathrm{Um}_n(\mathbf{A}[X])$ *such that* v_1 *is monic.*

Output: *A matrix* $\mathcal{B} \in \mathrm{SL}_n(\mathbf{A}[X])$ *such that* $\mathcal{B}\,\mathcal{V} = \mathcal{V}(0)$.

Step 1: *Find* $\gamma_0, \ldots, \gamma_s \in \mathrm{E}_{n-1}(\mathbf{A}[X])$ *such that denoting* $w_i = e_1.\gamma_i\,{}^{\mathrm{t}}(v_2, \ldots, v_n)$ *and* $r_i = \mathrm{Res}(v_1, w_i)$*, we can find* $\alpha_0, \ldots, \alpha_s \in \mathbf{A}$ *such that* $\alpha_0 r_0 + \cdots + \alpha_s r_s = 1$ *(here we use the algorithm given in the proof of Theorem 48). For* $0 \leq i \leq s$*, compute* $f_i, g_i \in \mathbf{A}[X]$ *such that* $f_i v_1 + g_i w_i = r_i$ *(use Proposition 43).*

Step 2: *Perform steps 2-4 of Algorithm 1 doing the necessary small changes.*

Example 60. (Example 49 continued)
Take $\mathbf{A} = \mathbb{Z}$ and $V = {}^{\mathrm{t}}(x^2 + 2x + 2,\ 3,\ 2x^2 + 11x - 3) \in \mathrm{Um}_3(\mathbb{Z}[x])$.

A generating set for $\mathrm{Syz}(v_1, v_2, v_3)$ can be obtained by computing a dynamical Gröbner basis for the ideal $\langle v_1, v_2, v_3\rangle$ (see Section 7). A dynamical computation gives

$$\mathrm{Syz}(v_1, v_2, v_3) = \langle \begin{pmatrix} 3 \\ -X^2 - 2X - 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -2X^2 - 11X + 3 \\ 3 \end{pmatrix}, \begin{pmatrix} -2X^3 - 11X^2 - 18X \\ 7X^3 + 14X^2 + 14X \\ X^3 + 2X^2 + 2X \end{pmatrix},$$
$$\begin{pmatrix} -21 - 6X \\ 14 + 21X \\ 3X \end{pmatrix}, \begin{pmatrix} -4X^3 - 36X^2 - 71X + 21 \\ 14X^3 + 77X^2 - 21X \\ 2X^3 + 11X^2 - 3X + 14 \end{pmatrix}\rangle.$$

But of course as mentioned above this is not a minimal generating set for $\mathrm{Syz}(v_1, v_2, v_3)$ as it is a rank 2 free $\mathbb{Z}[x]$-module (by the Lequain-Simis-Vasconcelos Theorem 91). Following Algorithm 59 and doing the computations by hands (assisted by the computer algebra system **Maple**) we get a matrix $G \in \mathrm{SL}_3(\mathbb{Z}[x])$ such that

$$G\,V = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

```
> V:=matrix(3,1,[x^2+2*x+2,3,2*x^2+11*x-3]);
```

```
> G :=matrix([[2+29142*x^2+340*x+4788*x^3, -25686*x^2-2394*x^3-272*x-1,
 -6192*x^2-2394*x^3-44*x],
 [-3-43713*x^2-510*x-7182*x^3, 38529*x^2+3591*x^3+408*x+2,
 9288*x^2+3591*x^3+66*x], [12+204092*x^2+2975*x+33516*x^3,
```

```
 -179851*x^2-16758*x^3-2429*x-7, -43393*x^2-16758*x^3-434*x+1]])
```

```
> det(G);
```

$$1$$

```
> F:=expandvector(multiply(G,V));
```

```
                        F := matrix([[1], [0], [0]])
```

Thus,

$$\left(\begin{pmatrix} -3-43713x^2-510x-7182x^3 \\ 38529x^2+3591x^3+408x+2 \\ 9288x^2+3591x^3+66x \end{pmatrix}, \begin{pmatrix} 12+204092x^2+2975x+33516x^3 \\ -179851x^2-16758x^3-2429x-7 \\ -43393x^2-16758x^3-434x+1 \end{pmatrix}\right)$$

is a free basis for $\mathrm{Syz}(v_1, v_2, v_3)$.

```
> inverse(G);
```

```
      matrix([[x^2+2*x+2, 5586*x^3+14465*x^2+146*x+1, 1197*x^3+3096*x^2+22*x],
       [3, 2, 0],
        [2*x^2+11*x-3, 11172*x^3+68032*x^2+999*x+2, 2394*x^3+14571*x^2+170*x+1]])
```

The matrix G^{-1} is a completion of V into an invertible matrix as V is the first column of G^{-1}.

3.7 Suslin's solution to Serre's problem

Theorem 61. (Unimodular completion theorem) *Let* $\mathbf{K}$ *be a field,* $\mathbf{R} = \mathbf{K}[X_1, \ldots, X_r]$ *and consider a unimodular vector*

$$f = {}^{\mathrm{t}}(f_1(X_1, \ldots, X_r), \ldots, f_n(X_1, \ldots, X_r)),$$

in $\mathbf{R}^{n\times 1}$. *Then, there exists a matrix* $H \in \mathrm{SL}_n(\mathbf{R})$ *such that* $Hf = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.
In other words, f *is the first column of a matrix* $\in \mathrm{SL}_n(\mathbf{R})$.

Proof. If $n = 1$ or 2, the result is straightforward. If $n > 2$ and $r = 1$, the result comes from the fact that $\mathbf{R}$ is a principal domain. It is explicitly given by a Smith reduction of the column matrix f. For $r \geq 2$, we make an induction on r. If the field $\mathbf{K}$ has enough elements (for example, if it is infinite), we can make a linear change of variables so that one of the f_i becomes monic. Else, we make a change of variables " à la Nagata": $Y_r = X_r$, and for $1 \leq j < r$, $Y_j = X_j + X_r^{d^j}$, with a sufficiently large integer d. It suffices now to use Algorithm 59. □

Theorem 62. (Suslin's solution to Serre's problem) *Let* $\mathbf{K}$ *be a field,* $\mathbf{R} = \mathbf{K}[X_1, \ldots, X_r]$ *and* M *a finitely generated stably free* $\mathbf{R}$*-module. Then* M *is free.*

Proof. We have by hypothesis an isomorphism

$$\varphi : \mathbf{R}^k \oplus M \longrightarrow \mathbf{R}^{\ell+k}$$

for some integers k and ℓ. If $k = 0$, there is nothing to prove. Suppose that $k > 0$. The vector $f = \varphi((e_{k,1}, 0_M))$ (where $e_{k,1}$ is the first vector in the canonical basis of $\mathbf{R}^k$) is unimodular. To see this, just consider the linear form λ over $\mathbf{R}^{\ell+k}$ mapping y ($y \in \mathbf{R}^{\ell+k}$) to the first coordinate of $\varphi^{-1}(y)$. We have $\lambda(y_1, \ldots, y_{k+\ell}) = u_1y_1 + \cdots + u_{k+\ell}y_{k+\ell}$ and $\lambda(f) = 1$.
Consider f as a column vector. Taking the composition of φ with the isomorphism given in Theorem 61, we obtain an isomorphism ψ mapping $(e_{k,1}, 0_M)$ to $e_{k+\ell,1}$. By passing modulo $\mathbf{A}(e_{k,1}, 0_M)$ and modulo $\mathbf{A}e_{k+\ell,1}$, we get an isomorphism

$$\theta : \mathbf{R}^{k-1} \oplus M \longrightarrow \mathbf{R}^{\ell+k-1}.$$

□

4 Constructive definitions of Krull dimension

This section is taken from the papers [20, 22, 23, 44].

4.1 Ideals and filters

Let S be a monoid (a multiplicative subset) of a ring $\mathbf{R}$. If M is an $\mathbf{R}$-module, then the $\mathbf{R}_S$-module M_S is obtained by extension of the scalars from $\mathbf{R}$ to $\mathbf{R}_S$. In particular, if M is finitely generated, finitely presented or projective, then so is M_S.

Recall that S is said to be *saturated* if

$$\forall\, s, t \in \mathbf{R},\ st \in S \ \Rightarrow\ s \in S.$$

A saturated monoid is also called a *filter*. Note that denoting

$$\overline{S} = \{s \in \mathbf{R}, \exists\, t \in \mathbf{R} \text{ such that } st \in S\},$$

$\overline{S}$ is a saturated monoid of $\mathbf{R}$ called the *saturation* of S, and we have

$$\mathbf{R}_{\overline{S}} = \mathbf{R}_S.$$

Note that there is a duality between ideals and filters. On the one hand, ideals are used to pass to the quotient, that is, to force the elements of the considered ideal $\mathfrak{a}$ of $\mathbf{R}$ into being zero in $\mathbf{R}/\mathfrak{a}$. On the other hand, filters are used to localize, that is, to force the elements of the considered monoid into being invertible.

An ideal is prime if and only if its complementary if a filter. A filter whose complementary is an ideal is called a *prime filter*.

The duality between ideals and filters is also a duality between addition and multiplication as can be seen by the axioms defining ideals (resp., prime ideals) and filters (resp., prime filters):

Ideal $\mathcal{I}$	*Filter* $\mathcal{F}$
$\vdash\ 0 \in \mathcal{I}$	$\vdash\ 1 \in \mathcal{F}$
$x \in \mathcal{I},\ y \in \mathcal{I}\ \vdash\ x+y \in \mathcal{I}$	$x \in \mathcal{F},\ y \in \mathcal{F}\ \vdash\ xy \in \mathcal{F}$
$x \in \mathcal{I}\ \vdash\ xy \in \mathcal{I}$	$xy \in \mathcal{F}\ \vdash\ x \in \mathcal{F}$
prime	*prime*
$xy \in \mathcal{I}\ \vdash\ x \in \mathcal{I} \vee y \in \mathcal{I}$	$x+y \in \mathcal{F}\ \vdash\ x \in \mathcal{F} \vee y \in \mathcal{F}$
$1 \in \mathcal{I}\ \vdash\ \mathit{False}$	$0 \in \mathcal{F}\ \vdash\ \mathit{False}$

4.2 Zariski lattice

Notation 63. *If $\mathfrak{a}$ be an ideal of $\mathbf{R}$, we denote $\mathrm{D}_{\mathbf{R}}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ the radical of $\mathfrak{a}$, that is, the set of all $x \in \mathbf{R}$ such that $x^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$.*
If $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$, we often denote $\mathrm{D}_{\mathbf{R}}(x_1, \ldots, x_n)$ instead of $\mathrm{D}_{\mathbf{R}}(\mathfrak{a})$.

Definition 64. *We denote $\operatorname{Zar}\mathbf{R}$ the set of all the $\mathrm{D}_{\mathbf{R}}(x_1, \ldots, x_n)$, where $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in \mathbf{R}$. This set is ordered by inclusion.*

Fact 65. $\operatorname{Zar}\mathbf{R}$ *is a distributive lattice equipped with*

$$\mathrm{D}_{\mathbf{R}}(\mathfrak{a}_1) \vee \mathrm{D}_{\mathbf{R}}(\mathfrak{a}_2) = \mathrm{D}_{\mathbf{R}}(\mathfrak{a}_1 + \mathfrak{a}_2) \qquad \mathrm{D}_{\mathbf{R}}(\mathfrak{a}_1) \wedge \mathrm{D}_{\mathbf{R}}(\mathfrak{a}_2) = \mathrm{D}_{\mathbf{R}}(\mathfrak{a}_1\, \mathfrak{a}_2).$$

$\operatorname{Zar}\mathbf{R}$ *is called the Zariski lattice of the ring $\mathbf{R}$.*

4.3 Krull boundary

Let us recall the classical definition of the Krull dimension of a ring $\mathbf{R}$. A finite chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of $n+1$ proper prime ideals of $\mathbf{R}$ is said to have length n. If $\mathbf{R}$ has no proper prime ideal (that is, $\mathbf{R}$ is trivial), we say that $\mathbf{R}$ has Krull dimension -1. If there is a nonnegative integer d such that $\mathbf{R}$ contains a chain of proper prime ideals of length d, but no such chain of length $d+1$, we say that $\mathbf{R}$ has Krull dimension d, and we write $\mathrm{Kdim}\mathbf{R} = d$ or simply $\dim \mathbf{R} = d$. Otherwise, we say that $\mathbf{R}$ is infinite dimensional. For example, a field or a finite product of fields has Krull dimension 0; $\mathbb{Z}$ or more generally a principal domain which is not a field has Krull dimension 1.

Definition 66. *Let $\mathbf{R}$ be a ring and $x \in \mathbf{R}$.*

(1) *The upper Krull boundary of x in $\mathbf{R}$ is the quotient ring $\mathbf{R}^{\{x\}} := \mathbf{R}/\mathrm{K}_{\mathbf{R}}(x)$, where $\mathrm{K}_{\mathbf{R}}(x) := \langle x\rangle + (\mathrm{D}_{\mathbf{R}}(0) : x) = \langle x\rangle + \{b \in \mathbf{R},\ bx \text{ is nilpotent}\}$.*

We will say that $\mathrm{K}_{\mathbf{R}}(x)$ is the Krull boundary ideal of x.

(2) *The lower Krull boundary of x in $\mathbf{R}$ is the localized ring $\mathbf{R}_{\{x\}} := \mathbf{R}_{S_{\{x\}}}$, where $S_{\{x\}} := x^{\mathbb{N}}(1 + x\mathbf{R}) = \{x^k(1+xy),\ k \in \mathbb{N},\ y \in \mathbf{R}\}$.*

We will say that $S_{\{x\}}$ is the Krull boundary monoid of x.

The terminology above is legitimated by the following geometric case: if $\mathbf{R} = \mathbf{K}[V]$ is the ring of rational functions over an affine variety V, an element $f \in \mathbf{R}$ represents a function over V whose zeroes form an affine subvariety W. Hence, $\mathbf{R}/\mathrm{D}_{\mathbf{R}}(\mathrm{K}_{\mathbf{R}}(f))$, which is the reduced ring associated to $\mathbf{R}^{\{f\}}$, is the ring $\mathbf{K}[W']$, where W' is the boundary of W in V.

The following theorem gives an inductive elementary characterization of the Krull dimension starting from dimension -1 which means that the ring is trivial ($1 = 0$). This inductive characterization corresponds to the geometrical intuition that a variety is of dimension $\leq k$ if and only if any subvariety has a boundary of dimension $< k$.

Theorem 67. *For any ring $\mathbf{R}$ and $\ell \in \mathbb{N}$, the following assertions are equivalent:*

(i) $\mathrm{Kdim}\mathbf{R} \leq \ell$.

(ii) *For any $x \in \mathbf{R}$,* $\mathrm{Kdim}\mathbf{R}^{\{x\}} \leq \ell - 1$.

(iii) *For any $x \in \mathbf{R}$,* $\mathrm{Kdim}\mathbf{R}_{\{x\}} \leq \ell - 1$.

(iv) *For any $x_0, \ldots, x_\ell \in \mathbf{R}$, there exist $a_0, \ldots, a_\ell \in \mathbf{R}$ and $m_0, \ldots, m_\ell \in \mathbb{N}$ such that*

$$x_0^{m_0}(x_1^{m_1} \cdots (x_\ell^{m_\ell}(1 + a_\ell\, x_\ell) + \cdots + a_1 x_1) + a_0 x_0) = 0.$$

Proof. Let us first prove the equivalence between assertions (i) and (ii). Recall that for any monoid S of $\mathbf{R}$, the prime ideals of R_S are of the form $S^{-1}\mathfrak{p} := \{\frac{t}{s},\ t \in \mathfrak{p},\ s \in S\}$, where $\mathfrak{p}$ is a prime ideal of $\mathbf{R}$ not meeting S. The desired equivalence results from the following two immediate affirmations:
(a) For any $x \in \mathbf{R}$ and any maximal ideal $\mathfrak{m}$ of $\mathbf{R}$, $S_{\{x\}} \cap \mathfrak{m} \neq \emptyset$.
(b) If $\mathfrak{m}$ is a maximal ideal of $\mathbf{R}$, and if $x \in \mathfrak{m} \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal contained in $\mathfrak{m}$, then $S_{\{x\}} \cap \mathfrak{p} = \emptyset$.
Thus, if $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$ is a chain of proper prime ideals of $\mathbf{R}$ with $\mathfrak{p}_\ell$ maximal, then for any $x \in \mathbf{R}$, when localizing at $S_{\{x\}}$, it will be shortened to at least $S_{\{x\}}^{-1}\mathfrak{p}_0 \subsetneq S_{\{x\}}^{-1}\mathfrak{p}_1 \subsetneq \cdots \subsetneq S_{\{x\}}^{-1}\mathfrak{p}_{\ell-1}$, and to exactly $S_{\{x\}}^{-1}\mathfrak{p}_0 \subsetneq S_{\{x\}}^{-1}\mathfrak{p}_1 \subsetneq \cdots \subsetneq S_{\{x\}}^{-1}\mathfrak{p}_{\ell-1}$ if $x \in \mathfrak{p}_\ell \setminus \mathfrak{p}_{\ell-1}$.
The equivalence between assertions (i) and (iii) can be proven in a dual way, just replace prime ideals by prime filters. Recall that for any ideal $\mathfrak{J}$ of $\mathbf{R}$, the prime filters of $\mathbf{R}/\mathfrak{J}$ are of the form $(S + \mathfrak{J})/\mathfrak{J}$, where S is a prime filter of $\mathbf{R}$ not meeting $\mathfrak{J}$. Affirmations (a) and (b) are thus replaced by the following dual affirmations (a') and (b'):
(a') For any $x \in \mathbf{R}$ and any maximal filter S of $\mathbf{R}$, $S \cap \mathrm{K}_{\mathbf{R}}(x) \neq \emptyset$.
(b') If S is a maximal filter of $\mathbf{R}$, and if $x \in S \setminus S'$, where $S' \subset S$ is a prime filter, then $S' \cap \mathrm{K}_{\mathbf{R}}(x) = \emptyset$.

Let us prove by induction on ℓ that the assertions (iii) and (iv) (for example) are equivalent. If $\ell = 0$ this is trivial. Suppose that the result is true for ℓ. If S is a monoid of $\mathbf{R}$, then $\mathrm{Kdim}\mathbf{R}_S \leq \ell$ if and only if for any $x_0, \ldots, x_\ell \in \mathbf{R}$, there exist $a_0, \ldots, a_\ell \in \mathbf{R}$, $m_0, \ldots, m_\ell \in \mathbb{N}$, and $s \in S$ such that $x_0^{m_0}(x_1^{m_1} \cdots (x_\ell^{m_\ell}(s + a_\ell\, x_\ell) + \cdots + a_1 x_1) + a_0 x_0) = 0$. Just replace s by an arbitrary element of the form $x_{\ell+1}^{m_{\ell+1}}(1 + a_{\ell+1}\, x_{\ell+1})$.

□

4.4 Pseudo regular sequences and Krull dimension

Definition 68. *Let $(x_1, \ldots, x_\ell)$ be a sequence of length ℓ in a ring $\mathbf{R}$.*

- *We say that the sequence $(x_1, \ldots, x_\ell)$ is pseudo singular (or collapses) if there exist $a_1, \ldots, a_\ell \in \mathbf{R}$ and $m_1, \ldots, m_\ell \in \mathbb{N}$ such that*

$$x_1^{m_1}(x_2^{m_2} \cdots (x_\ell^{m_\ell}(1 + a_\ell\, x_\ell) + \cdots + a_2 x_2) + a_1 x_1) = 0.$$

- *We say that the sequence $(x_1, \ldots, x_\ell)$ is pseudo regular if it does not collapse.*

The connection with regular sequences is given by the following straightforward proposition.

Proposition 69. *A regular sequence is pseudo regular.*

Using Theorem 68 and the notion of pseudo regular sequence we can now formulate a constructive definition of Krull dimension.

Definition 70. (Constructive definition of Krull dimension)
- *We say that a ring $\mathbf{R}$ has dimension -1 if it is trivial ($1 = 0$). Otherwise, we say that $\mathbf{R}$ has dimension ≥ 0.*
- *We say that a ring $\mathbf{R}$ has dimension $\leq \ell - 1$ if each sequence of length ℓ collapses.*
- *We say that a ring $\mathbf{R}$ has dimension $\geq \ell$ if there exists a pseudo regular sequence of length ℓ.*
- *We say that a ring $\mathbf{R}$ has dimension ℓ if its dimension is $\geq \ell$ and $\leq \ell$ at the same time.*

Examples 71. *1) A ring $\mathbf{R}$ has dimension ≤ 0 if and only if*

$$\forall x \in \mathbf{R},\ \exists n \in \mathbb{N},\ \exists\, a \in \mathbf{R} \ \mid\ x^n = a x^{n+1}. \tag{3}$$

2) A local ring $\mathbf{R}$ has dimension 0 if and only if

$$\forall x \in \mathbf{R},\ x \text{ is invertible or nilpotent.} \tag{4}$$

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

$$\forall a, b \in \mathbf{R},\ \exists n \in \mathbb{N},\ \exists\, x, y \in \mathbf{R} \ \mid\ a^n(b^n(1 + xb) + ya) = 0. \tag{5}$$

4.5 Krull dimension of a polynomial ring over a discrete field

We first need the following intermediary result.

Proposition 72. *Let $\mathbf{K}$ be a discrete field, $\mathbf{R}$ a commutative $\mathbf{K}$-algebra, and $x_1, \ldots, x_\ell \in \mathbf{R}$ algebraically independent over $\mathbf{K}$. Then the sequence $(x_1, \ldots, x_\ell)$ is pseudo singular.*

Proof. Let $Q(x_1, \ldots, x_\ell) = 0$ be an algebraic relation over $\mathbf{K}$ testifying the dependence between the x_i. Let us order the monomial of Q with nonzero coefficients by the lexicographic order. We can without loss of generality suppose that the first nonzero coefficient of Q is 1. Denoting this monomial by $x_1^{m_1} \cdots x_\ell^{m_\ell}$, it is clear that Q can be written in the form
$Q = x_1^{m_1} \cdots x_\ell^{m_\ell} + x_1^{m_1} \cdots x_\ell^{1+m_\ell} R_\ell + x_1^{m_1} \cdots x_{\ell-1}^{1+m_{\ell-1}} R_{\ell-1} + \cdots + x_1^{m_1} x_2^{1+m_2} R_2 + x_1^{1+m_1} R_1$, the desired collapse. □

Theorem 73. *If $\mathbf{K}$ is a discrete field, then the Krull dimension of $\mathbf{K}[X_1, \ldots, X_\ell]$ is equal to ℓ.*

Proof. Just use Proposition 72 and the fact that the sequence $(X_1, \ldots, X_\ell)$ is pseudo regular since it is regular (see Proposition 69). □

Note that we have painlessly obtained this fundamental result quashing the common opinion that constructive proofs are necessarily more complicated than classical proofs.

4.6 Application to the stable range theorem

This subsection is extracted from [21]. It proposes a simple and elegant constructive proof of the stable range theorem.

Lemma 74. $\sqrt{\langle y, b\rangle} = \sqrt{\langle y+b, by\rangle}$.

Proof. It is clear that $\sqrt{\langle y+b, by\rangle} \subseteq \sqrt{\langle y, b\rangle}$. The converse follows from the identity $y^2 = (y+b)y - yb$. □

Lemma 75. *If by is nilpotent then* $1 \in \sqrt{\langle y, b\rangle} \Leftrightarrow 1 \in \sqrt{\langle y+b\rangle}$.

Proof. By virtue of Lemma 74, $1 \in \sqrt{\langle y, b\rangle} \Leftrightarrow 1 \in \sqrt{\langle y+b, by\rangle} \Leftrightarrow 1 \in \sqrt{\langle y+b\rangle}$ (*by* being nilpotent). □

Theorem 76. *If the Krull dimension of a ring $\mathbf{R}$ is $< s$ then for any $a, b_1, \ldots, b_s \in \mathbf{R}$ such that $1 \in \langle a, b_1, \ldots, b_s\rangle$, there exist $x_1, \ldots, x_s \in \mathbf{R}$ such that $1 \in \langle b_1 + ax_1, \ldots, b_s + ax_s\rangle$.*

Proof. We proceed by induction on s. If $s = 0$ the result is clear as the ring $\mathbf{R}$ is trivial. If $s > 0$, let I be the ideal boundary of b_s. We have $b_s \in I$ and the dimension of $\mathbf{R}/I < s-1$. By induction, we can find $x_1, \ldots, x_{s-1}$ such that

$$1 \in \langle b_1 + ax_1, \ldots, b_{s-1} + ax_{s-1}\rangle$$

in $\mathbf{R}/I$. This means that there exists $x_s \in \mathbf{R}$ such that $b_s x_s$ is nilpotent and

$$1 \in \langle b_1 + ax_1, \ldots, b_{s-1} + ax_{s-1}, b_s, x_s\rangle.$$

Now to obtain the desired result, one has only to reason modulo $\langle b_1 + ax_1, \ldots, b_{s-1} + ax_{s-1}\rangle$ and to use Lemmas 74 and 75. □

As an immediate consequence, we get the following so-called stable range theorem.

Theorem 77. (Stable range theorem) *Let $\mathbf{R}$ be a ring of dimension $\leq d$, $n \geq d+1$, and let $v = (v_0, \ldots, v_n) \in \mathrm{Um}_{n+1}(\mathbf{R})$. Then there exists $E \in \mathrm{E}_{n+1}(R)$ such that $E\,v = (1, 0, \ldots, 0)$.*

Corollary 78. (Stable range theorem, bis) *For any ring $\mathbf{R}$ with Krull dimension $\leq d$, all finitely generated stably free $\mathbf{R}$-modules of rank $> d$ are free.*

Proof. Use Proposition 15. □

5 Projective modules over $\mathbf{R}[X_1, \ldots, X_n]$, $\mathbf{R}$ an arithmetical ring

5.1 A constructive proof of Brewer-Costa-Maroscia Theorem

This subsection is extracted from [52]. The aim is to prove constructively the following theorem [13, 54] due to Maroscia and Brewer & Costa which is a remarkable generalization of the Quillen-Suslin Theorem since it is free of any Noetherian hypothesis.

Theorem 79. *If $\mathbf{R}$ is a Prüfer domain of 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 of Krull dimension ≤ 1, then each finitely generated projective module over $\mathbf{R}[X_1, \ldots, X_n]$ is free.*

We will also propose in this Chapter 5 an alternative simpler constructive proof of Theorem 79 (see Remark 93).

5.1.1 Krull Dimension ≤ 1

In order to use constructively the hypothesis that $\mathbf{R}$ has Krull dimension ≤ 1, we recall the following constructive meaning of Krull dimension ≤ 1:

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

$$\forall a, b \in \mathbf{R},\ \ \exists\, n \in \mathbb{N},\ \ \exists\, x, y \in \mathbf{R} \ \ \mid \ \ a^n(b^n(1+xb) + ya) = 0 \tag{6}$$

or equivalently

$$\forall a, b \in \mathbf{R},\ \ \exists\, n \in \mathbb{N} \ \ \mid \ \ a^n b^n \in a^n b^{n+1}\mathbf{R} + a^{n+1}\mathbf{R}. \tag{7}$$

In the sequel, we will consider the family of identities in (6) as the constructive meaning of the hypothesis that $\mathbf{R}$ has Krull dimension ≤ 1.

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

Notation 80. *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,*

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

Lemma 81.

- *$I_{\mathbf{R}}(a, b)$ 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 $\leq 1 \iff \forall\ a, b \in \mathbf{R}$, $I_{\mathbf{R}}(a, b) = \langle 1\rangle$.*

5.1.2 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:

$$\forall x, y \in \mathbf{R} \quad \exists s, t, a, b \in \mathbf{R} \ \left\{ \begin{array}{rcl} s\,x & = & a\,y \\ b\,x & = & t\,y \\ s+t & = & 1 \end{array} \right. \tag{8}$$

See [26] or [45] for detailed explanations about this characterization. In fact Property (8) 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 [26, 45] following the terminology proposed in [34]. 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 [26, 45].

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

Theorem 82. *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 83. *If $\mathbf{R}$ is a coherent Prüfer ring with Krull dimension ≤ 1 then so is $\mathbf{R}\langle X\rangle$.*

5.1.3 A local theorem

In the sequel, the letters a, b, c will denote elements of $\mathbf{R}$ and f, g, h elements of $\mathbf{R}[X]$. We will prove a local version of Theorem 83 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:

$$\left\{ \begin{array}{rrcl} \forall x \in \mathbf{R} & x^2 = 0 & \Rightarrow & x = 0 \\ \forall x, y \in \mathbf{R} & \exists z\ x = zy & \text{or} & \exists z\ y = zx \\ \forall x \in \mathbf{R} & x \in \mathbf{R}^\times & \text{or} & x \in \mathrm{Rad}(\mathbf{R}) \\ \forall x \in \mathbf{R} & \mathrm{Ann}(x) = 0 & \text{or} & \mathrm{Ann}(x) = 1 \end{array} \right. \tag{9}$$

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[1].

[1] 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.

Denoting $\mathrm{Rad}(\mathbf{R})$ by $\mathcal{R}$ we easily infer that

$$\left\{\begin{array}{llllll} \forall x,y\in\mathbf{R} & \exists z\in\mathcal{R}\ x=zy & \text{or} & \exists z\in\mathcal{R}\ y=zx & \text{or} & \exists u\in\mathbf{R}^\times\ y=ux \\ \forall x,y\in\mathbf{R} & xy=0 & \Rightarrow & (x=0 & \text{or} & y=0) \end{array}\right. \tag{10}$$

The following easy lemmas are useful for the proof of our Theorem 88.

Lemma 84. *If the ring $\mathbf{R}$ satisfies* (10)*, 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 (10), 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 85. *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 (6) and the fact that $1+b\,\mathbf{R}\subset\mathbf{R}^\times$.

□

Corollary 86. *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 85, 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 87. *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 83 is Theorem 88.

Theorem 88. *If $\mathbf{R}$ is a residually discrete local coherent Prüfer ring (that is, it satisfies* (9)*) 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) so is $\mathbf{R}[X]$ (see for example Theorem IV.4.7 of [55]) and $\mathbf{R}\langle X\rangle$ as well. Recall that a gcd-ring $\mathbf{B}$ is Bezout if and only if

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

To prove that $\mathbf{R}\langle X\rangle$ is Bezout, consider $F,G\in\mathbf{R}\langle X\rangle$ such that $\gcd(F,G)=1$ and let us show that $1\in\langle F,G\rangle$. We may assume w.l.o.g. that $F\neq 0$ and $G\neq 0$. Since monic polynomials are invertible in $\mathbf{R}\langle X\rangle$, we may also assume that $F,G\in\mathbf{R}[X]$. We need to show that $\langle F,G\rangle_{\mathbf{R}[X]}$ contains a monic polynomial. Letting $H=\gcd(F,G)_{\mathbf{R}[X]}$, H divides $\gcd(F,G)_{\mathbf{R}\langle X\rangle}=1$ (in $\mathbf{R}\langle X\rangle$) and so the leading coefficient of H is invertible in $\mathbf{R}$. Using the equality $\langle F,G\rangle_{\mathbf{R}[X]}=H\langle F/H,G/H\rangle_{\mathbf{R}[X]}$, we see that we may suppose $H=1$. Following Lemma 84, we have $F=a\,f=a\,(b\,f_1+f_2)$, $G=a'\,g=a'\,(b'\,g_1+g_2)$, with b, $b'\in\mathrm{Rad}(\mathbf{R})$ and f_2, g_2 monic. In $\mathbf{R}\langle X\rangle$ we have:

$$\gcd(F,G)=\gcd(a\,f,a'\,g)=1\ \Rightarrow\ \gcd(a,a')=1.$$

Thus, $\gcd(F,G)=1$ in $\mathbf{R}\langle X\rangle$ implies that either a or a' is invertible in $\mathbf{R}$. Suppose for example that $a=1$. The fact that $\gcd(F,G)_{\mathbf{R}[X]}=1$ 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 86, 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 $\mathbf{K}[X]$ ([20, 44]) which can be rewritten in $\mathbf{R}[X]$ (by clearing the denominators) as follows:

$$\exists n\in\mathbb{N},\ \ \exists\,h_1,h_2\in\mathbf{R}[X],\ \ \exists\,w\in\mathbf{R}\setminus\{0\}\quad F^n(G^n(w+h_1G)+h_2F)=0.$$

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, contains 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. □

5.1.4 A quasi-global version

Applying the General local-global Principle 27 to the proof of Theorem 88 above, we get an algorithmic proof for the following quasi-global proposition.

Proposition 89. *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 89 is Theorem 83. This is due to the fact that finitely generated ideals are projective and that two elements producing a collapse are local properties, i.e., it suffices to check them after localizations at a family of comaximal monoids ([20, 26, 45]).

Let $\mathcal{F}$ be the class of coherent Prüfer rings of Krull dimension ≤ 1. This class clearly satisfies the localization property Q2a. It satisfies Q1 by Theorem 83.

Theorem 88 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 39, we obtain condition Q3.

As our proof of Q3 is elementary and constructive, the General local-global principle 27 works and gives versions Q3a and Q3b. Finally we constructively get:

Theorem 90. *If* $\mathbf{R}$ *is a coherent Prüfer ring with Krull dimension* ≤ 1*, then every finitely generated projective module over* $\mathbf{R}[X_1, \ldots, X_n]$ *is extended. In particular, if* $\mathbf{R}$ *is a Bezout pp-ring with Krull dimension* ≤ 1*, then every constant rank projective module over* $\mathbf{R}[X_1, \ldots, X_n]$ *is free.*

5.2 The theorem of Lequain, Simis and Vasconcelos

This subsection is extracted from [28]. Let $\mathbf{R}$ be a commutative unitary ring. We denote by $\mathbf{R}(X)$ the localization of $\mathbf{R}[X]$ at primitive polynomials, i.e., polynomials whose coefficients generate the whole ring $\mathbf{R}$. Of course, the ring $\mathbf{R}(X)$ is also a localization of $\mathbf{R}\langle X\rangle$ and we have $\mathbf{R}[X] \subseteq \mathbf{R}\langle X\rangle \subseteq \mathbf{R}(X)$. The containment $\mathbf{R}\langle X\rangle \subseteq \mathbf{R}(X)$ becomes an equality if and only if $\mathbf{R}$ has Krull dimension 0 (in short, $\operatorname{Kdim}\mathbf{R} = 0$) [35].

The construction $\mathbf{R}(X)$ turned out to be an efficient tool for proving results on $\mathbf{R}$ via passage to $\mathbf{R}(X)$.

As seen in the previous subsection, the restriction in Brewer-Costa-Maroscia theorem 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. Subsequently, in order to generalize the Quillen-Suslin theorem to Prüfer domains and seeing that the class of Prüfer domains is not stable under the formation $\mathbf{R}\langle X\rangle$, Lequain and Simis [40] found a clever way to bypass this difficulty by proving the following new induction theorem.

Lequain-Simis Induction Theorem *Suppose that a class of rings* $\mathcal{F}$ *satisfies the following properties:*

(i) *If* $\mathbf{R} \in \mathcal{F}$*, then every nonmaximal prime ideal of* $\mathbf{R}$ *has finite height.*

(ii) $\mathbf{R} \in \mathcal{F} \Rightarrow \mathbf{R}[X]_{\mathfrak{p}[X]} \in \mathcal{F}$ *for any prime ideal* $\mathfrak{p}$ *of* $\mathbf{R}$*.*

(iii) $\mathbf{R} \in \mathcal{F} \Rightarrow \mathbf{R}_{\mathfrak{p}} \in \mathcal{F}$ *for any prime ideal* $\mathfrak{p}$ *of* $\mathbf{R}$*.*

(iv) $\mathbf{R} \in \mathcal{F}$ *and* $\mathbf{R}$ *local* $\Rightarrow$ *any finitely generated projective module over* $\mathbf{R}[X]$ *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* $\mathbf{R}$*.*

It is worth pointing out that when coupled with a result by Simis and Vasconcelos [69] asserting that over a valuation ring $\mathbf{V}$, all projective $\mathbf{V}[X]$-modules are free, the Lequain-Simis Induction Theorem yields to the following elegant theorem.

Theorem 91. (Lequain-Simis-Vasconcelos) *For any Prüfer domain* $\mathbf{R}$*, all finitely generated projective* $\mathbf{R}[X_1, \ldots, X_n]$*-modules are extended from* $\mathbf{R}$*.*

In this subsection, we will prove that for any ring $\mathbf{R}$ with Krull dimension $\leq d$, the ring $\mathbf{R}\langle X\rangle$ "dynamically behaves like the ring $\mathbf{R}(X)$ or a localization of a polynomial ring of type $(S^{-1}\mathbf{R})[X]$ with S a multiplicative subset of $\mathbf{R}$ and the Krull dimension of $S^{-1}\mathbf{R}$ is $\leq d-1$".

As application of our dynamical comparison between the rings $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$, we give a constructive variation of Lequain-Simis Induction Theorem - using a simple proof. Note that Lequain and Simis put considerable effort for proving this marvellous theorem and they used some quite complicated technical steps.

Constructive Induction Theorem *Let $\mathcal{F}$ be a class of commutative rings with finite Krull dimensions satisfying the properties below:*

(ii') *If $\mathbf{R}\in\mathcal{F}$ then $\mathbf{R}(X)\in\mathcal{F}$.*

(iii) *$\mathbf{R}\in\mathcal{F}\Rightarrow\mathbf{R}_S\in\mathcal{F}$ for each multiplicative subset S in $\mathbf{R}$.*

(iv') *If $\mathbf{R}\in\mathcal{F}$ then any finitely generated projective module over $\mathbf{R}[X]$ is extended from $\mathbf{R}$.*

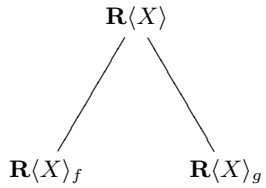
Then, for each $\mathbf{R}\in\mathcal{F}$, if M is a finitely generated projective $\mathbf{R}[X_1,\ldots,X_n]$-module, then M is extended from $\mathbf{R}$.

5.2.1 A dynamical comparison between the rings $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$

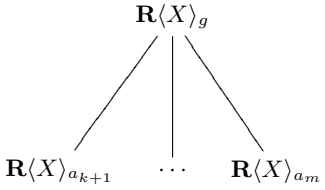
By the following theorem, we prove that for any ring $\mathbf{R}$ with Krull dimension $\leq d$, the ring $\mathbf{R}\langle X\rangle$ "dynamically behaves like the ring $\mathbf{R}(X)$ or a localization of a polynomial ring of type $(S^{-1}\mathbf{R})[X]$ with S a multiplicative subset of $\mathbf{R}$ and the Krull dimension of $S^{-1}\mathbf{R}$ is $\leq d-1$".

Theorem 92. *Let $d\in\mathbb{N}$ and $\mathbf{R}$ a ring with Krull dimension $\leq d$. Then for any primitive polynomial $f\in\mathbf{R}[X]$, there exist comaximal subsets $V_1,\ldots,V_s$ of $\mathbf{R}\langle X\rangle$ such that for each $1\leq i\leq s$, either f is invertible in $\mathbf{R}\langle X\rangle_{V_i}$ or $\mathbf{R}\langle X\rangle_{V_i}$ is a localization of $(S^{-1}_{\mathbf{R},a_i}\mathbf{R})[X]$, where $S_{\mathbf{R},a_i}=a_i^{\mathbb{N}}(1+a_i\mathbf{R})$, for some coefficient a_i of f (note that* $\operatorname{Kdim} S^{-1}_{\mathbf{R},a_i}\mathbf{R}\leq d-1$*).*

Proof.
First case: $\mathbf{R}$ is residually discrete local. Observe that any primitive polynomial $f\in\mathbf{R}[X]$ can be written in the form $f=g+u$ where $g,u\in\mathbf{R}[X]$, all the coefficients of g are in the Jacobson radical $\operatorname{Rad}(\mathbf{R})$ of $\mathbf{R}$ and u is quasi monic (that is, the leading coefficient of u is invertible). If the degree of u is k, then $g=\sum_{j>k}a_jX^j$. Now we open two branches: we localize $\mathbf{R}\langle X\rangle$ at the comaximal multiplicative subsets generated by f and g.



In $\mathbf{R}\langle X\rangle_f$, f is clearly invertible.
In $\mathbf{R}\langle X\rangle_g$, write $g=\sum_{j=k+1}^m a_jX^j$, where the $a_j\in\operatorname{Rad}(\mathbf{R})$. It follows that the multiplicative subsets $\mathcal{M}(a_{k+1}),\ldots,\mathcal{M}(a_s)$ are comaximal in $\mathbf{R}\langle X\rangle_g$. Note that for any $k+1\leq i\leq m$, $\mathcal{M}(a_i)^{-1}(\mathbf{R}\langle X\rangle_g)$ is a localization of the polynomial ring $\mathbf{R}_{a_i}[X]$ and $\dim\mathbf{R}_{a_i}<\dim\mathbf{R}$.



General case: $\mathbf{R}$ arbitrary. Apply the General local-global Principle 27. Precisely this gives the following computation. First we remark that since f is primitive, say $f=\sum_{j=0}^m a_jX^j$, the multiplicative subsets $U_m=\mathcal{M}(a_m)$, $U_{m-1}=\mathcal{S}_{\mathbf{R}}(a_m;a_{m-1})$, $\ldots$, $U_k=\mathcal{S}_{\mathbf{R}}(a_m,\ldots,a_{k+1};a_k)$, $\ldots$, $U_0=\mathcal{S}_{\mathbf{R}}(a_m,\ldots,a_1;a_0)$ are comaximal in $\mathbf{R}$. It is now sufficient to prove the conclusion for each ring $\mathbf{R}_{U_i}$. And this conclusion is obtained from the proof given for the first case. □

Remark 93. If $\mathbf{R}$ is a valuation domain then any $f \in \mathbf{R}[X]$ is easily written as $f = ag$ where $a \in \mathbf{R}$ and $g \in \mathbf{R}[X]$ is primitive, invertible in $\mathbf{R}(X)$. From this fact, it follows easily that $\mathbf{R}(X)$ is again a valuation domain, and if $\operatorname{Kdim} \mathbf{R} \leq d$ then $\operatorname{Kdim} \mathbf{R}(X) \leq d$. So by Theorem 92, we painlessly get constructively that:

(i) If $\mathbf{R}$ is a valuation domain with $\operatorname{Kdim} \mathbf{R} \leq 1$ then $\mathbf{R}\langle X\rangle$ is a Prüfer domain with $\operatorname{Kdim} \mathbf{R} \leq 1$ (we retrieve a very simple constructive proof of the Brewer-Costa-Maroscia Theorem 90). As a matter of fact, it is clear that in this case, in one of the $\mathbf{R}\langle X\rangle_{U_i}$, the computations are done like in $\mathbf{R}(X)$, while the other $\mathbf{R}\langle X\rangle_{U_i}$ are localizations of the polynomial ring $\mathbf{K}[X]$ where $\mathbf{K}$ is the quotient field of $\mathbf{R}$.

(ii) If $\mathbf{R}$ is a Prüfer domain with $\operatorname{Kdim} \mathbf{R} \leq 1$ then so is $\mathbf{R}\langle X\rangle$.
This is obtained from (i) by application of the General Constructive Rereading Principle.

Remark 94. If $\operatorname{Kdim} \mathbf{R} = 0$ then clearly $\mathbf{R}\langle X\rangle = \mathbf{R}(X)$ (the rings $S_{a_i}^{-1}\mathbf{R}$ in Theorem 92 being trivial). This constructive proof is more simpler than that given in [35].

5.2.2 The Lequain-Simis Induction Theorem

In order to generalize the Quillen-Suslin theorem to Prüfer domains and seeing that the class of Prüfer domains is not stable under the formation $\mathbf{R}\langle X\rangle$, Lequain and Simis [40] found a clever way to bypass this difficulty by proving the following new induction theorem.

Theorem 95. (Lequain-Simis Induction) *Suppose that a class of rings $\mathcal{F}$ satisfies the following properties:*

(i) *If $\mathbf{R} \in \mathcal{F}$, then every nonmaximal prime ideal of $\mathbf{R}$ has finite height.*

(ii) $\mathbf{R} \in \mathcal{F} \Rightarrow \mathbf{R}[X]_{\mathfrak{p}[X]} \in \mathcal{F}$ *for any prime ideal $\mathfrak{p}$ of $\mathbf{R}$.*

(iii) $\mathbf{R} \in \mathcal{F} \Rightarrow \mathbf{R}_{\mathfrak{p}} \in \mathcal{F}$ *for any prime ideal $\mathfrak{p}$ of $\mathbf{R}$.*

(iv) $\mathbf{R} \in \mathcal{F}$ *and* $\mathbf{R}$ *local* $\Rightarrow$ *any finitely generated projective module over $\mathbf{R}[X]$ 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 $\mathbf{R}$.

Note here that if $\mathbf{R}$ is local with maximal ideal $\mathfrak{m}$, then $\mathbf{R}(X) = \mathbf{R}[X]_{\mathfrak{m}[X]}$.
We propose here a constructive variation of Lequain-Simis Induction Theorem using a simple proof. This is one important application of our dynamical comparison between the rings $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$.

Theorem 96. (Constructive Induction Theorem) *Let $\mathcal{F}$ be a class of commutative rings with finite Krull dimensions satisfying the properties below:*

(ii') *If $\mathbf{R} \in \mathcal{F}$ then $\mathbf{R}(X) \in \mathcal{F}$.*

(iii) $\mathbf{R} \in \mathcal{F} \Rightarrow \mathbf{R}_S \in \mathcal{F}$ *for each multiplicative subset S in $\mathbf{R}$.*

(iv') *If $\mathbf{R} \in \mathcal{F}$ then any finitely generated projective module over $\mathbf{R}[X]$ is extended from $\mathbf{R}$.*

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 $\mathbf{R}$.

Proof. We reason by double induction on the number n of variables and the Krull dimension of the basic ring $\mathbf{R}$. For the initialization of the induction there is no problem since if $n = 1$ there is nothing to prove and for polynomial rings over zero-dimensional rings (see Theorem 41) the result is true constructively.
We assume that the construction is given with n variables for rings in $\mathcal{F}$. Then we consider the case of $n+1$ variables and we give the proof by induction on the dimension of the ring $\mathbf{R} \in \mathcal{F}$. We assume that the dimension is $\leq d+1$ with $d \geq 0$ and the construction has been done for rings of dimension $\leq d$.
Let P be a finitely generated projective $\mathbf{R}[X_1, \ldots, X_n, Y]$-module. Let us denote X for $X_1, \ldots, X_n$. The module P can be seen as the cokernel of a presentation matrix $M = M(X, Y)$ with entries in $\mathbf{R}[X, Y]$. Let $A(X, Y)$ be the associated enlarged matrix (as in the proof of Theorem 37).
Using the induction hypothesis over n and (ii') we know that $A(X, Y)$ and $A(0, Y)$ are equivalent over the ring $\mathbf{R}(Y)[X]$. This means that there exist matrices Q_1, R_1 with entries in $\mathbf{R}[X, Y]$ such that

$$Q_1 A(X, Y) = A(0, Y) R_1 \tag{11}$$

$$\text{where} \quad \det(Q_1) \quad \text{and} \quad \det(R_1) \quad \text{are primitive polynomials in } \mathbf{R}[Y]. \tag{12}$$

We first want to show that $A(X,Y)$ and $A(0,Y)$ are equivalent over $\mathbf{R}\langle Y\rangle[X]$. Using the Vaserstein's patching, for doing this job it is sufficient to show that A and $A(0,Y)$ are equivalent over $\mathbf{R}\langle Y\rangle[X]_{\mathcal{M}_i}$ for comaximal multiplicative subsets $\mathcal{M}_i$.
We consider the primitive polynomial $f = \det(Q_1)\det(R_1) \in \mathbf{R}[Y]$ and we apply Theorem 92. We get comaximal subsets $V_1, \ldots, V_s$ of $\mathbf{R}\langle Y\rangle$ such that for each $1 \leq i \leq s$, either f is invertible in $\mathbf{R}\langle Y\rangle_{V_i}$ or $\mathbf{R}\langle Y\rangle_{V_i}$ is a localization of $\mathbf{R}_{a_i}[Y]$ for some $a_i \in \mathbf{R}$ such that $\mathbf{R}_{a_i}$ has Krull dimension $\leq d$.
In the first case $\det(Q_1)$ and $\det(R_1)$ are invertible in $\mathbf{R}\langle Y\rangle_{V_i}$. This implies that $A(X,Y)$ and $A(0,Y)$ are equivalent over $\mathbf{R}\langle Y\rangle[X]_{Vi}$.
In the second case, by induction hypothesis on the dimension, $A(X,Y)$ and $A(0,0)$ are equivalent over $\mathbf{R}_{a_i}[Y][X]$. An immediate consequence is that $A(X,Y)$ and $A(0,Y)$ are equivalent over $\mathbf{R}_{a_i}[Y][X]$. Finally they are also equivalent over $\mathbf{R}\langle Y\rangle[X]_{V_i}$ which is a localization of the previous ring.
Now we know that there exist invertible matrices Q, R over the ring $\mathbf{R}\langle Y\rangle[X] \subseteq (\mathbf{R}[X])\langle Y\rangle$ such that

$$Q\,A(X,Y) = A(0,Y)\,R.$$

We know also that $A(0,0)$ and $A(0,Y)$ are equivalent over $\mathbf{R}[Y] \subseteq (\mathbf{R}[X])\langle Y\rangle$ (case $n=1$) and $A(0,0)$ and $A(X,0)$ are equivalent over $\mathbf{R}[X] \subseteq (\mathbf{R}[X])\langle Y\rangle$. So $A(X,0)$ and $A(X,Y)$ are equivalent over $(\mathbf{R}[X])\langle Y\rangle$, and by virtue of Horrocks Theorem 39, P is extended from $\mathbf{R}[X]$, i.e., $A(X,0)$ and $A(X,Y)$ are equivalent over $\mathbf{R}[X,Y]$. By induction hypothesis, P is extended from $\mathbf{R}$. □

Remark 97. In fact, the proof does'nt use "any" multiplicative subset of rings $\mathbf{R}$ in $\mathcal{F}$, but only multiplicative subsets obtained by iterating localizations at some $\mathcal{S}(a_1, \ldots, a_k; u)$.

Recall that a ring is called a pp-ring if the annihilator ideal of any element is generated by an idempotent.

Corollary 98. (Lequain-Simis Theorem) *For any finite-dimensional arithmetical pp-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. We prove that the class $\mathcal{F}$ of finite-dimensional arithmetical pp-rings such that all finitely generated projective $\mathbf{R}[X_1]$-modules are extended from $\mathbf{R}$ satisfies the hypothesis in our induction theorem. Only the first point (ii') is problematic. We assume to have a constructive proof in the local case, i.e., the case of valuation domains. So, starting with an arithmetical pp-ring, the General local-global Principle 27 gives comaximal multiplicative sets where the needed computations are done successfully. This allows to give the desired global conclusion in an explicit way. □

Remark 99. Thierry Coquand announced recently a constructive proof of the Bass-Simis-Vasconcelos theorem (projective modules over $\mathbf{V}[X]$, $\mathbf{V}$ a valuation domain, are free) [19].

As always constructive proofs work in classical mathematics and Theorem 96 applies. Moreover, in classical mathematics, we get the following variation:

Theorem 100. (New classical induction theorem) *Let* $\mathcal{F}$ *be a class of commutative rings with finite Krull dimensions satisfying the properties below:*

(ii) *If* $\mathbf{R} \in \mathcal{F}$ *and* $\mathbf{R}$ *is local then* $\mathbf{R}(X) \in \mathcal{F}$*.*

(iii') $\mathbf{R} \in \mathcal{F} \Rightarrow \mathbf{R}_S \in \mathcal{F}$ *for each multiplicative set* S *in* $\mathbf{R}$*.*

(iv) *If* $\mathbf{R} \in \mathcal{F}$ *and* $\mathbf{R}$ *is local then any finitely generated projective module over* $\mathbf{R}[X]$ *is extended from* $\mathbf{R}$*.*

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* $\mathbf{R}$*.*

Proof. From (ii) and (iv) we deduce (ii') and (iv') in Theorem 96 by using the abstract Quillen's patching that uses maximal ideals. □

6 The Hermite ring conjecture

6.1 The Hermite ring conjecture in dimension one

This subsection is extracted from [74]. Quillen's and Suslin's proofs of Serre's problem on projective modules had a big effect on the subsequent development of the study of projective modules. Nevertheless, many old conjectures and open questions about projective modules over polynomial rings still wait for solutions. Our concern here is the following equivalent two conjectures.

Conjecture 101. (Hermite ring conjecture (1972) [38, 39]) *If* $\mathbf{R}$ *is an Hermite ring, then* $\mathbf{R}[X]$ *is also Hermite.*

Conjecture 102. *If* $\mathbf{R}$ *is a ring and* $v = (v_0(X), \ldots, v_n(X))$ *is a unimodular row over* $\mathbf{R}[X]$ *such that* $v(0) = (1, 0, \ldots, 0)$*, then* v *can be completed to a matrix in* $\mathrm{GL}_{n+1}(\mathbf{R}[X])$*.*

Recall that a ring $\mathbf{A}$ is said to be Hermite if any finitely generated stably free $\mathbf{A}$-module is free (see Definition 14). Examples of Hermite rings are local rings (see Theorem 5), rings of Krull dimension ≤ 1 (see Corollary 78), polynomial rings over Bezout domains (see Subsection 5.2), and polynomial rings over zero-dimensional rings (see Theorem 41).

In this section we will prove constructively that for any ring $\mathbf{R}$ of Krull dimension ≤ 1 and $n \geq 3$, the group $\mathrm{E}_n(\mathbf{R}[X])$ acts transitively on $\mathrm{Um}_n(\mathbf{R}[X])$. In particular, we obtain that for any ring $\mathbf{R}$ with Krull dimension ≤ 1, all finitely generated stably free modules over $\mathbf{R}[X]$ are free. This settles the long-standing Hermite ring conjecture for rings of Krull dimension ≤ 1. The proof we give relies heavily on the very nice paper [66] of Roitman.

Let us begin by giving a constructive and elementary proof of a lemma which was used by Roitman [66] in the proof of his Theorem 5. The proof of this lemma given by Lam in [38, 39] (Chapter III, Lemma 1.1) is not constructive and relies on the "going-up" property of integral extensions.

Lemma 103. *Let* $\mathbf{R}$ *be a ring, and* I *an ideal in* $\mathbf{R}[X]$ *that contains a monic polynomial. Let* J *be an ideal in* $\mathbf{R}$ *such that* $I + J[X] = \mathbf{R}[X]$*. Then* $(I \cap \mathbf{R}) + J = \mathbf{R}$*.*

Proof. Let us denote by f a monic polynomial in I. Since $I + J[X] = \mathbf{R}[X]$, there exist $g \in I$ and $h \in J[X]$ such that $g + h = 1$. It follows that $\langle \bar{f}, \bar{g} \rangle = (\mathbf{R}/J)[X]$ where the classes are taken modulo $J[X]$. By virtue of Proposition 47, we obtain that $\mathrm{Res}(\bar{f}, \bar{g}) \in (\mathbf{R}/J)^\times$. As f is a monic polynomial, $\mathrm{Res}(\bar{f}, \bar{g}) = \overline{\mathrm{Res}(f, g)}$, and thus $\langle \mathrm{Res}(f, g) \rangle + J = \mathbf{R}$. The desired conclusion follows from the fact that $\mathrm{Res}(f, g) \in I \cap \mathbf{R}$. □

The following three lemmas were already proven constructively by their authors.

Lemma 104. (Roitman's Lemma [66]) *Let* $\mathbf{R}$ *be a ring, and* $f(X) \in \mathbf{R}[X]$ *of degree* $n > 0$*, such that* $f(0) \in \mathbf{R}^\times$*. Then for any* $g(X) \in \mathbf{R}[X]$ *and* $k \geq \deg g(X) - \deg f(X) + 1$ *there exists* $h_k(X) \in \mathbf{R}[X]$ *of degree* $< n$ *such that* $g(X) \equiv X^k h_k(X) \mod \langle f(X) \rangle$*.*

Proof. Let $f(X) = a_0 + \cdots + a_n X^n$, $g(X) = c_0 + \cdots + c_m X^m$. Let $g(X) - c_0 a_0^{-1} f(X) = X h_1(X)$. Then $g(X) \equiv X h_1(X) \mod \langle f(X) \rangle$ and $\deg h_1(X) < \max(m, n)$. Similarly we obtain $h_2(X)$ such that $h_1(X) \equiv X h_2(X) \mod \langle f(X) \rangle$, $g(X) \equiv X^2 h_2(X) \mod \langle f(X) \rangle$, $\deg h_2(X) < \max(m-1, n)$, and so on. □

Lemma 105. (Vaserstein's Lemma [39]) *Let* $\mathbf{R}$ *be a ring, and* ${}^{\mathrm{t}}(x_0, \ldots, x_r) \in \mathrm{Um}_{r+1}(\mathbf{R})$*,* $r \geq 2$*, and let* t *be an element of* $\mathbf{R}$ *which is invertible* $\mod \langle x_0, \ldots, x_{r-2} \rangle$*. Then there exists* $E \in \mathrm{E}_{r+1}(\mathbf{R})$ *such that* $E\,(x_0, \ldots, x_r) = {}^{\mathrm{t}}(x_0, \ldots, x_{r-1}, t^2 x_r)$*.*

Proof. This is also Proposition III.6.1.(b) of Lam [39] (page 125). The proofs given by Lam and Roitman are constructive and free of any Noetherian hypothesis. □

Lemma 106. (Bass' Lemma [17]) *Let* $k \in \mathbb{N}$*,* $\mathbf{R}$ *a ring,* $f_1, \ldots, f_r \in \mathbf{R}[X]$ *with degrees* $\leq k-1$*, and* $f_{r+1} \in \mathbf{R}[X]$ *monic with degree* k*. If the coefficients of* $f_1, \ldots, f_r$ *generate the ideal* $\mathbf{R}$ *of* $\mathbf{R}$*, then* $\langle f_1, \ldots, f_r, f_{r+1} \rangle$ *contains a monic with degree* $k - 1$*.*

Proof. Let us denote by $\mathfrak{a} = \langle f_1, \ldots, f_r, f_{r+1} \rangle$ and $\mathfrak{b}$ the ideal formed by the coefficients of X^{k-1} of the elements of $\mathfrak{a}$ having degree $\leq k-1$. It suffices to prove that $\mathfrak{b} = \mathbf{R}$. In fact we will prove that $\mathfrak{b}$ contains all the coefficients of $f_1, \ldots, f_r$. For $1 \leq i \leq r$, denoting by $f_i = b_0 + b_1 X + \cdots + b_{k-1} X^{k-1}$ and $f_{r+1} = a_0 + \cdots + a_{k-1} X^{k-1} + X^k$, we have $b_{k-1} \in \mathfrak{b}$ and $f_i' = X f_i - b_{k-1} f = b_0' + b_1' X + \cdots + b_{k-1}' X^{k-1} \in \mathfrak{a}$ with $b_j' \equiv b_{j-1} \mod \langle b_{k-1} \rangle$. Thus, $b_{k-1}' = b_{k-2} - a_{k-1} b_{k-1} \in \mathfrak{b}$, $b_{k-2} \in \mathfrak{b}$, and so on until getting that all the b_i's are in $\mathfrak{b}$. □

Now we're reaching a crucial stage in our objective to prove the Hermite ring conjecture for rings of Krull dimension ≤ 1.

Lemma 107. *Let* $\mathbf{R}$ *be a reduced local ring of dimension* ≤ 1*,* $n \geq 2$*, and let* $v(X) = {}^{\mathrm{t}}(v_0(X), \ldots, v_n(X)) \in \mathrm{Um}_{n+1}(\mathbf{R}[X])$*. Then there exists* $E \in \mathrm{E}_{n+1}(R[X])$ *such that* $E\,v(X) = {}^{\mathrm{t}}(v_0(X), v_1(X), c_2, \ldots, c_n)$*, where* $c_i \in \mathbf{R}$*.*

Proof. As stated by Rao in his proof of Proposition 1.4.4 of [64], this is implicit in [66] (Theorem 5). It is worth pointing out, that the hypothesis that for each non-zero-divisor π of $\mathbf{R}$ there exists $E_\pi \in \mathrm{E}_{n+1}(R[X])$ such that $E_\pi\, v(X) \equiv v(0) \mod (\pi\mathbf{R}[X])^{n+1}$ is guaranteed by the fact that $\dim(\mathbf{R}/\pi\mathbf{R}) \leq 0$. Moreover, there is no need of the Noetherian hypothesis and we can obtain a fully constructive proof of the desired result. To see this, let us reread carefully Roitman's proof of his Theorem 5 in [66] and let us list the intermediary results he used and which we need for our lemma:

- If v_0 is a monic polynomial then there exists $E \in \mathrm{E}_{n+1}(R[X])$ such that $E\,v(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$. This is Theorem 48.
- Roitman's Lemma 104.
- Vaserstein's Lemma 105.
- In case $\deg(v_0) = 1$ we immediately get that for $i \geq 2$, $\deg(v_i) < 1$, and thus v_i is constant. In more details, by Lemma 104, we can suppose that, for $1 \leq i \leq n$, $v_i = X^{2k} w_i$ with $\deg(w_i) < \deg(v_0) = 1$, that is, $w_i \in \mathbf{R}$. Now by Vaserstein's Lemma 105 (taking $t = X$), we can suppose that $v_i \in \mathbf{R}$ for $1 \leq i \leq n$.
- Lemma 2 of [66]. This is the stable range theorem and there is no need of the Noetherian hypothesis. See Theorem 77.
- Lemma III.1.1 of [38, 39]. This is Lemma 103 above.
- Lemma 106.

□

Theorem 108. *Let* $\mathbf{R}$ *be a ring of dimension* ≤ 1*,* $n \geq 2$*, and let* $v(X) = {}^{\mathrm{t}}(v_0(X), \ldots, v_n(X)) \in \mathrm{Um}_{n+1}(\mathbf{R}[X])$*. Then there exists* $E \in \mathrm{E}_{n+1}(R[X])$ *such that* $E\,v(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$*.*

Proof. By virtue of the Stable range theorem (see Theorem 77), it suffices to prove that there exists $E \in \mathrm{E}_{n+1}(R[X])$ such that $E\,v(X) = v(0)$. By the local-global principle for elementary matrices [39] (see [49] for a constructive proof), we can suppose that $\mathbf{R}$ is local. Moreover, it is clear that we can suppose that $\mathbf{R}$ is reduced. By virtue of Lemma 107, there exists $E \in \mathrm{E}_{n+1}(R[X])$ such that $E\,v(X) = {}^{\mathrm{t}}(v_0(X), v_1(X), c_2, \ldots, c_n)$, where $c_i \in \mathbf{R}$. So we can without loss of generality suppose that $v_0 = a$ is constant.
Now, let us consider the ring $\mathbf{T} := \mathbf{R}/\mathcal{I}(a)$. Since $\dim \mathbf{T} \leq 0$ (see Theorem 68), we have that $\mathbf{T}\langle X\rangle = \mathbf{T}(X)$ (see Remark 94) and thus $\mathbf{T}\langle X\rangle$ is a local ring. It follows that one among $v_1, \ldots, v_n$, say v_1, divides a monic polynomial in $\mathbf{T}[X]$. This means that there exist a monic polynomial $u \in \mathbf{R}[X]$, $w, h_1, h_2 \in \mathbf{R}[X]$ with $ah_2 = 0$, such that

$$wv_1 = u + ah_1 + h_2.$$

This means that $1 \in \langle v_1, a, h_2\rangle$ in the ring $\mathbf{R}\langle X\rangle$ and thus $1 \in \langle v_1, a + h_2\rangle$ by Lemma 75. That is, $\exists\, w_1,\, w_2 \in \mathbf{R}[X] \mid v_1 w_1 + (a + h_2)w_2 =: \tilde{u}$ is a monic polynomial.
Let $d \in \mathbb{N}$ and denote by $u_0, \ldots, u_n$ polynomials in $\mathbf{R}[X]$ such that $u_0 v_0 + \cdots + u_n v_n = 1$. Denoting by

$$\gamma_1 := E_{1,2}(h_2 u_1) \cdots E_{1,n+1}(h_2 u_n),$$

$$\gamma_2 := E_{3,2}(X^d w_1)\, E_{3,1}(X^d w_2),$$

$$\gamma := \gamma_2\, \gamma_1,$$

we have

$$\gamma_1 v = {}^{\mathrm{t}}(a + h_2, v_1, \ldots, v_n),$$

and

$$\gamma\, v = {}^{\mathrm{t}}(a + h_2, v_1, v_2 + X^d \tilde{u}, v_3, \ldots, v_n).$$

So, for sufficiently large d, the third entry of $\gamma\, v$ becomes a monic polynomial. Thus, as already seen in Theorem 52, we have an algorithm transforming $\gamma\, v$ into ${}^{\mathrm{t}}(1, 0, \ldots, 0)$ using elementary operations.

□

Corollary 109. *For any ring* $\mathbf{R}$ *of Krull dimension* ≤ 1*, all finitely generated stably free modules over* $\mathbf{R}[X]$ *are free.*

Proof. We know that if $\mathbf{R}$ has Krull dimension ≤ 1 then all finitely generated stably free modules over $\mathbf{R}$ are free (see Corollary 78 and Theorem 77). So, we have only to prove that all finitely generated stably free modules over $\mathbf{R}[X]$ are extended from $\mathbf{R}$. For this, let $v = {}^{\mathrm{t}}(v_0(X), \ldots, v_n(X)) \in \mathbf{R}[X]^{n+1}$ $(n \geq 2)$ be a unimodular vector. Our task amounts to prove that there exists $\Gamma \in \mathrm{GL}_{n+1}(\mathbf{R}[X])$ such that $\Gamma V = {}^{\mathrm{t}}(1, 0, \ldots, 0)$. This follows from Theorem 115.

□

Corollary 110. *The Hermite ring conjecture is true for rings of Krull dimension* ≤ 1*.*

Corollary 109 encourages us to set the Conjecture 111. It is worth pointing out, that one cannot use the Quillen Induction Theorem 40 nor the constructive version of the Lequain-Simis Induction Theorem (Theorem 96) in order to settle affirmatively this conjecture because the class of rings with Krull dimension ≤ 1 is not stable by passage to none of the formations $\mathbf{R}\langle X\rangle$ and $\mathbf{R}(X)$. As a matter of fact, we have $\dim \mathbf{R}\langle X\rangle = \dim \mathbf{R}(X) = \dim \mathbf{R}[X] - 1$ [16], and thus to see this it suffices to consider a ring $\mathbf{R}$ such $\dim \mathbf{R} = 1 < \dim_{\mathrm{v}} \mathbf{R} = \dim \mathbf{R}\langle X\rangle = \dim \mathbf{R}(X) = 2$ (for example $\mathbf{R} = \mathbb{Q} + y\,\mathbb{Q}(x)[y] = \{f(y) \in \mathbb{Q}(x)[y] \mid f(0) \in \mathbb{Q}\}$ where x, y are two independent indeterminates over the field of rationals $\mathbb{Q}$ [15]).

Conjecture 111. *For any ring* $\mathbf{R}$ *of Krull dimension* ≤ 1*, and* $k \in \mathbb{N}$*, all finitely generated stably free modules over* $\mathbf{R}[X_1, \ldots, X_k]$ *are free.*

Also, Corollary 109 raises the $\mathbf{K}_1$-analogue question. I will state it as a conjecture.

Conjecture 112. *Let* $\mathbf{R}$ *be a ring of Krull dimension* ≤ 1 *and* $n \geq 3$*. Then every matrix* $M \in \mathrm{SL}_n(\mathbf{R}[X])$ *is congruent to* $M(0)$ *modulo* $\mathrm{E}_n(\mathbf{R}[X])$*.*

In fact, by virtue of Theorem 115 and the local-global principle for elementary matrices (see [49] for a constructive proof), Conjecture 112 is equivalent to the following conjecture.

Conjecture 113. *Suppose* $\mathbf{R}$ *is a local ring of Krull dimension* ≤ 1*, and*

$$M = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbf{R}[X]).$$

Then $M \in \mathrm{E}_3(\mathbf{R}[X])$*.*

We will end this subsection by the following question about the analogue of Corollary 109 for Laurent polynomial rings.

Question 114. *Is it true that for any ring* $\mathbf{R}$ *of Krull dimension* ≤ 1*, all finitely generated stably free modules over* $\mathbf{R}[X, X^{-1}]$ *are free ?*

6.2 Stably free modules over $\mathbf{R}[X]$ of rank $> \dim \mathbf{R}$ are free

The purpose of this subsection is to extend the results obtained in the one-dimensional case to the general case and of course always without supposing that the base ring is Noetherian. This subsection is extracted from [75].

Theorem 115. *Let* $\mathbf{R}$ *be a ring of dimension* $\leq d$*,* $n \geq d + 1$*, and let* $v(X) = {}^{\mathrm{t}}(v_0(X), \ldots, v_n(X)) \in \mathrm{Um}_{n+1}(\mathbf{R}[X])$*. Then there exists* $E \in \mathrm{E}_{n+1}(R[X])$ *such that* $E\,v(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$*.*

Proof. By the Stable range Theorem 77, for any $w \in \mathrm{Um}_{n+1}(\mathbf{R})$, there exists $M \in \mathrm{E}_{n+1}(R)$ such that $M\,w = {}^{\mathrm{t}}(1, 0, \ldots, 0)$. So, it suffices to prove that there exists $E \in \mathrm{E}_{n+1}(R[X])$ such that $E\,v(X) = v(0)$. For this aim, by the local-global principle for elementary matrices [39] (see [51] for a constructive proof), we can suppose that $\mathbf{R}$ is local. Moreover, it is clear that we can suppose that $\mathbf{R}$ is reduced.
We prove the claim by double induction on the number N of nonzero coefficients of $v_0(X), \ldots, v_n(X)$ and d, starting with $N = 1$ (in that case the result is immediate) and $d = 0$ (in that case the result is well-known).

We will first prove a first claim: $v(X)$ can be transformed by elementary operations into a vector with one constant entry.
Let $N > 1$ and $d > 0$. We may assume that $v_0(0) \in \mathbf{R}^{\times}$. Let us denote by a the leading coefficient of v_0 and $m_0 := \deg v_0$. If $a \in \mathbf{R}^{\times}$ then the result follows from Suslin's lemma (Theorem 48). So we may

assume $a \in \mathrm{Rad}(\mathbf{R})$. By the induction hypothesis applied to the ring $\mathbf{R}/\langle a\rangle$, we can assume that $v(X) \equiv {}^{\mathrm{t}}(1,0,\dots,0) \mod (a\mathbf{R}[X])^{n+1}$.
By Lemma 104, we assume now $v_i = X^{2k}w_i$, where $\deg w_i < m_0$ for $1 \leq i \leq n$. By Lemma 105, we assume $\deg v_i < m_0$.
If $m_0 \leq 1$, our first claim is established. Assume now that $m_0 \geq 2$. Let $(c_1,\dots,c_{m_0(n-1)})$ be the coefficients of $1, X, \dots, X^{m_0-1}$ in the polynomials $v_2(X),\dots,v_n(X)$. By Lemma 103, the ideal generated in $\mathbf{R}_a$ by $\mathbf{R}_a \cap (v_0\mathbf{R}_a[X] + v_1\mathbf{R}_a[X])$ and the c_i's is $\mathbf{R}_a$. As $m_0(n-1) \geq 2d > \dim \mathbf{R}_a$, by the Stable range Theorem 77 there exists

$$(c'_1,\dots,c'_{m_0(n-1)}) \equiv (c_1,\dots,c_{m_0(n-1)}) \mod (v_0\mathbf{R}[X] + v_1\mathbf{R}[X]) \cap \mathbf{R}$$

such that $c'_1\mathbf{R}_a + \cdots + c'_{m_0(n-1)}\mathbf{R}_a = \mathbf{R}_a$. Assume that we have already $c_1\mathbf{R}_a + \cdots + c_{m_0(n-1)}\mathbf{R}_a = \mathbf{R}_a$. By Lemma 106, the ideal $\langle v_0, v_2, \dots, v_n\rangle$ of $\mathbf{R}[X]$ contains a polynomial $w(X)$ of degree $m_0 - 1$ which is unitary in $\mathbf{R}_a$. Let us denote the leading coefficient of w by ua^k where $u \in \mathbf{R}^\times$ and that of v_1 by b. Using Lemma 105, we achieve by elementary operations

$${}^{\mathrm{t}}(v_0, v_1, \dots, v_n) \;\to\; {}^{\mathrm{t}}(v_0, a^{2k}v_1, \dots, v_n) \;\to\; {}^{\mathrm{t}}(v_0, a^{2k}v_1 + (1 - a^k u^{-1}b)w, v_2, \dots, v_n).$$

Now, $a^{2k}v_1 + (1 - a^k u^{-1}b)w$ is unitary in $\mathbf{R}_a$, so assume v_1 unitary in $\mathbf{R}_a$, $\deg(v_1) := m_1 < m_0$. By Lemma 105, as a is invertible modulo $\langle v_0, v_1\rangle$, by elementary operations, ${}^{\mathrm{t}}(v_0, v_1, v_2, \dots, v_n)$ can be transformed into ${}^{\mathrm{t}}(v_0, v_1, a^\ell v_2, \dots, a^\ell v_n)$ for a suitable $\ell \in \mathbb{N}$ so that we can divide (like in Euclidean division) all $a^\ell v_2, \dots, a^\ell v_n$ by v_1, and thus we can assume that $\deg v_i < m_1$ for $2 \leq i \leq n$.
Repeating the argument above we lower the degree of v_1 until reaching the desired form of our first claim.

Assume now that $v_0 = a \in \mathbf{R}$. Let us consider the ring $\mathbf{T} := \mathbf{R}/\mathcal{I}(a)$. Since $\dim \mathbf{T} \leq d-1$ (see Theorem 68) and $(\overline{v}_1,\dots,\overline{v}_n) \in \mathrm{Um}_n(\mathbf{T}[X])$, there exists $E_1 \in \mathrm{E}_n(\mathbf{R}[X])$ such that

$$E_1\,{}^{\mathrm{t}}(v_1,\dots,v_n) = {}^{\mathrm{t}}(1 + ah_1 + y_1\tilde{h}_1, ah_2 + y_2\tilde{h}_2, \dots, ah_n + y_n\tilde{h}_n),$$

where $h_i, \tilde{h}_i \in \mathbf{R}[X]$, $y_i \in \mathbf{R}$ with $ay_i = 0$.
Denoting by $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & E_1 \end{pmatrix} \in \mathrm{E}_{n+1}(\mathbf{R}[X])$, we have

$$E_2\, v = {}^{\mathrm{t}}(a, 1 + ah_1 + y_1\tilde{h}_1, ah_2 + y_2\tilde{h}_2, \dots, ah_n + y_n\tilde{h}_n).$$

Thus,

$$E_{1,2}(-a)E_{2,1}(-h_1)\cdots E_{n+1,1}(-h_n)\,E_2\, v = {}^{\mathrm{t}}(0, 1 + y_1\tilde{h}_1, y_2\tilde{h}_2, \dots, y_n\tilde{h}_n) =: \tilde{v},$$

and we can easily find $E_3 \in \mathrm{E}_{n+1}(\mathbf{R}[X])$ such that $E_3\,\tilde{v} = {}^{\mathrm{t}}(1,0,\dots,0)$.

□

Corollary 116. *For any ring $\mathbf{R}$ with Krull dimension $\leq d$, all finitely generated stably free modules over $\mathbf{R}[X]$ of rank $> d$ are free.*

Proof. By the Stable range theorem (Corollary 78), all finitely generated stably free modules over $\mathbf{R}$ of rank $> d$ are free. So, we have only to prove that all finitely generated stably free modules over $\mathbf{R}[X]$ are extended from $\mathbf{R}$. For this, let $v = {}^{\mathrm{t}}(v_0(X),\dots,v_n(X)) \in \mathbf{R}[X]^{n+1}$ $(n \geq d+1)$ be a unimodular vector. Our task amounts to prove that there exists $\Gamma \in \mathrm{GL}_{n+1}(\mathbf{R}[X])$ such that $\Gamma\, V = {}^{\mathrm{t}}(1,0,\dots,0)$. This follows from Theorem 115.

□

Corollary 116 encourages us to set the following conjecture.

Conjecture 117. *For any ring $\mathbf{R}$ with Krull dimension $\leq d$, all finitely generated stably free modules over $\mathbf{R}[X_1,\dots,X_k]$ of rank $> d$ are free.*

As in the one-dimensional case, Corollary 116 raises the analogue question for Laurent polynomial rings.

Question 118. *Is it true that for any ring $\mathbf{R}$ of Krull dimension $\leq d$, all finitely generated stably free modules over $\mathbf{R}[X, X^{-1}]$ of rank $> d$ are free ?*

7 Dynamical Gröbner bases over arithmetical rings

The concept of Gröbner basis was originally introduced by Buchberger in his Ph.D. thesis (1965) in order to solve the ideal membership problem for polynomial rings over a field [17]. The ideal membership problem has received considerable attention from the constructive algebra community resulting in algorithms that generalize the work of Buchberger [1, 2, 3, 30, 36]. A dynamical approach to Gröbner bases over principal rings was first introduced in [73]. Our goal in this section is to extend the notion of dynamical Gröbner basis to Dedekind rings and to show how to compute dynamically the syzygy module.

First note that for a Dedekind domain $\mathbf{R}$ with field of fractions $\mathbf{F}$, a necessary condition so that $f \in \langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s\rangle$ in $\mathbf{F}[X_1, \ldots, X_n]$.
Suppose that this condition is fulfilled, that is there exists $d \in \mathbf{R} \setminus \{0\}$ such that

$$d\, f \in \langle f_1, \ldots, f_s\rangle \text{ in } \mathbf{R}[X_1, \ldots, X_n] \quad (0).$$

If the basic ring $\mathbf{R}$ is a Dedekind domain in which complete prime factorization is feasible, we can write

$$\langle d\rangle = \prod_{i=1}^{\ell} \mathfrak{p}_i^{n_i},$$

where the $\mathfrak{p}_i$ are nonzero distinct prime ideals of $\mathbf{R}$.
Other necessary conditions so that $f \in \langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}_{p_i\mathbf{R}}[X_1, \ldots, X_n]$ for each $1 \leq i \leq \ell$. Here the polynomial ring is over the discrete valuation domain $\mathbf{R}_{\mathfrak{p}_i}$. Write:

$$d_i\, f \in \langle f_1, \ldots, f_s\rangle \text{ in } \mathbf{R}[X_1, \ldots, X_n] \text{ for some } d_i \in \mathbf{R} \setminus \mathfrak{p}_i. \quad (i)$$

Since no prime of $\mathbf{R}$ contains the ideal $\langle d, d_1, \ldots, d_\ell\rangle$, we obtain that $1 \in \langle d, d_1, \ldots, d_\ell\rangle$, that is we can find an equality $\alpha d + \alpha_1 d_1 + \cdots + \alpha_\ell d_\ell = 1$, $\alpha, \alpha_i \in \mathbf{R}$. Using this Bezout identity, we can find an equality asserting that $f \in \langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$. Thus, the necessary conditions are sufficient and it suffices to treat the problem in case the basic ring is a discrete valuation domain.

This method raises the following question:

How to avoid the obstacle of complete prime factorization if it is expensive or infeasible in the considered Dedekind ring?

The fact that the method explained above is based on gluing "local realizability" appeals to the use of dynamical methods and more precisely, as in [73], the use of the notion of "dynamical Gröbner basis". Our goal is to mimic dynamically as much as we can the method explained above using a constructive theory of Dedekind rings. As will be seen later in this course, we will use "partial factorizations" like in [26] by proceeding as if the considered ring was a valuation ring.

This section is extracted from [4, 33, 73].

7.1 Gröbner bases over a valuation ring

Definition 119. *Let $\mathbf{R}$ be a ring, $f = \sum_\alpha a_\alpha X^\alpha$ a nonzero polynomial in $\mathbf{R}[X_1, \ldots, X_n]$, E a non empty subset of $\mathbf{R}[X_1, \ldots, X_n]$, and $>$ a monomial order.*

1) The X^α (resp. the $a_\alpha X^\alpha$) are called the monomials (resp. the terms) of f.
2) The multidegree of f is $\mathrm{mdeg}(f) := \max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$.
3) The leading coefficient of f is $\mathrm{LC}(f) := a_{\mathrm{mdeg}(f)} \in \mathbf{R}$.
4) The leading monomial of f is $\mathrm{LM}(f) := X^{\mathrm{mdeg}(f)}$.
5) The leading term of f is $\mathrm{LT}(f) := \mathrm{LC}(f)\,\mathrm{LM}(f)$.
6) $\mathrm{LT}(E) := \{\mathrm{LT}(g), g \in E\}$.
7) $\langle \mathrm{LT}(E)\rangle := \langle \mathrm{LT}(g), g \in E\rangle$ *(ideal of $\mathbf{R}[X_1, \ldots, X_n]$).*
8) For $g, h \in \mathbf{R}[X_1, \ldots, X_n] \setminus \{0\}$, we say that $\mathrm{LT}(g)$ *divides* $\mathrm{LT}(h)$ *if* $\mathrm{LM}(g)$ *divides* $\mathrm{LM}(h)$ *and* $\mathrm{LC}(g)$ *divides* $\mathrm{LC}(h)$.

Definition 120. *Let $\mathbf{R}$ be a ring, $f, g \in \mathbf{R}[X_1, \ldots, X_n] \setminus \{0\}$, $I = \langle f_1, \ldots, f_s\rangle$ a nonzero finitely generated ideal of $\mathbf{R}[X_1, \ldots, X_n]$, and $>$ a monomial order.*

1) If $\mathrm{mdeg}(f) = \alpha$ *and* $\mathrm{mdeg}(g) = \beta$ *then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i.*
If $\mathrm{LC}(g)$ *divides* $\mathrm{LC}(f)$ *or* $\mathrm{LC}(f)$ *divides* $\mathrm{LC}(g)$*, the S-polynomial of f and g is the combination:*

$S(f,g) = \frac{X^\gamma}{\mathrm{LM}(f)} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \frac{X^\gamma}{\mathrm{LM}(g)} g$ *if* $\mathrm{LC}(g)$ *divides* $\mathrm{LC}(f)$.

$S(f,g) = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \frac{X^\gamma}{\mathrm{LM}(f)} f - \frac{X^\gamma}{\mathrm{LM}(g)} g$ *if* $\mathrm{LC}(f)$ *divides* $\mathrm{LC}(g)$ *and* $\mathrm{LC}(g)$ *does not divide* $\mathrm{LC}(f)$.

2) As in the classical division algorithm in $\mathbf{F}[X_1, \ldots, X_n]$ *(*$\mathbf{F}$ *field) (see [24], page 61), for each polynomials* $h, h_1, \ldots, h_m \in \mathbf{R}[X_1, \ldots, X_n]$*, there exist* $q_1, \ldots, q_m, r \in \mathbf{R}[X_1, \ldots, X_n]$ *such that*

$$h = q_1 h_1 + \cdots + q_m h_m + r,$$

where either $r = 0$ *or* r *is a sum of terms none of which is divisible by any of* $\mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_m)$*. The polynomial* r *is called a remainder of* h *on division by* $H = \{h_1, \ldots, h_m\}$ *and denoted* $r = \overline{h}^H$*.*

3) $G = \{f_1, \ldots, f_s\}$ *is said to be a Gröbner basis for* I *if* $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$.

Lemma 121. *Let* $\mathbf{R}$ *be a valuation ring and* $I = \langle a_\alpha X^\alpha, \alpha \in A \rangle$ *an ideal of* $\mathbf{R}[X_1, \ldots, X_n]$ *generated by a collection of terms. Then a term* bX^β *lies in* I *if and only if* X^β *is divisible by* X^α *and* b *is divisible by* a_α *for some* $\alpha \in A$*.*

Proof. It is obvious that the condition is sufficient. For proving the necessity, write $bX^\beta = \sum_{i=1}^s c_i a_{\alpha_i} X^{\gamma_i} X^{\alpha_i}$ for some $\alpha_1, \ldots, \alpha_s \in A$, $c_i, a_{\alpha_i} \in \mathbf{R} \setminus \{0\}$, and $\gamma_i \in \mathbb{N}^n$. Ignoring the superfluous terms, for each $1 \leq i \leq s$, $\gamma_i + \alpha_i = \beta$, and $b = \sum_{i=1}^s c_i a_{\alpha_i}$. It is clear that for each $1 \leq i \leq s$, X^β is divisible by X^{α_i}. Since all the coefficients are comparable under division, we can suppose that a_{α_1} divides all the a_{α_i} and thus divides b.

□

The following lemma will be of big utility since it is the missing key for the characterization of Gröbner bases by means of S-polynomials (see [24], page 82).

Lemma 122. *Let* $\mathbf{R}$ *be a valuation ring,* $>$ *a monomial order, and* $f_1, \ldots, f_s \in \mathbf{R}[X_1, \ldots, X_n]$ *such that* $\mathrm{mdeg}(f_i) = \gamma$ *for each* $1 \leq i \leq s$*. If* $\mathrm{mdeg}(\sum_{i=1}^s a_i f_i) < \gamma$ *for some* $a_1, \ldots, a_s \in \mathbf{R}$*, then* $\sum_{i=1}^s a_i f_i$ *is a linear combination with coefficients in* $\mathbf{R}$ *of the S-polynomials* $S(f_i, f_j)$ *for* $1 \leq i, j \leq s$*. Furthermore, each* $S(f_i, f_j)$ *has multidegree* $< \gamma$

Proof. Since $\mathbf{R}$ is a valuation ring, we can suppose that $\mathrm{LC}(f_s)/\mathrm{LC}(f_{s-1})/\cdots/\mathrm{LC}(f_1)$. Thus for $i < j$, $S(f_i, f_j) = f_i - \frac{\mathrm{LC}(f_i)}{\mathrm{LC}(f_j)} f_j$.

$\sum_{i=1}^s a_i f_i = a_1(f_1 - \frac{\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)} f_2) + (a_2 + \frac{\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)} a_1)(f_2 - \frac{\mathrm{LC}(f_2)}{\mathrm{LC}(f_3)} f_3)$
$+ \cdots + (a_{s-1} + \frac{\mathrm{LC}(f_{s-2})}{\mathrm{LC}(f_{s-1})} a_{s-2} + \cdots + \frac{\mathrm{LC}(f_1)}{\mathrm{LC}(f_{s-1})} a_1)(f_{s-1} - \frac{\mathrm{LC}(f_{s-1})}{\mathrm{LC}(f_s)} f_s)$
$+ (a_s + \frac{\mathrm{LC}(f_{s-1})}{\mathrm{LC}(f_s)} a_{s-1} + \cdots + \frac{\mathrm{LC}(f_1)}{\mathrm{LC}(f_s)} a_1) f_s.$

But $a_s + \frac{\mathrm{LC}(f_{s-1})}{\mathrm{LC}(f_s)} a_{s-1} + \cdots + \frac{\mathrm{LC}(f_1)}{\mathrm{LC}(f_s)} a_1 = 0$ since $\mathrm{mdeg}(\sum_{i=1}^s a_i f_i) < \gamma$.

□

Using Lemma 121 and Lemma 122, we generalize some classical results about the existence and characterization of Gröbner basis for ideals in polynomial rings over Noetherian valuations rings.

Theorem 123. *Let* $\mathbf{R}$ *be a valuation ring ,* $I = \langle g_1, \ldots, g_s \rangle$ *an ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order* $>$*. Then,* $G = \{g_1, \ldots, g_s\}$ *is a Gröbner basis for* I *if and only if for all pairs* $i \neq j$*, the remainder on division of* $S(g_i, g_j)$ *by* G *is zero.*

Buchberger's Algorithm for Noetherian valuation rings. *Let* $\mathbf{R}$ *be a Noetherian valuation ring,* $I = \langle g_1, \ldots, g_s \rangle$ *a nonzero ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order* $>$*. Then, a Gröbner basis for* I *can be computed in a finite number of steps by the following algorithm:*

Input: $g_1, \ldots, g_s$
Output: a Gröbner basis G for $\langle g_1, \ldots, g_s \rangle$ with $\{g_1, \ldots, g_s\} \subseteq G$

$G := \{g_1, \ldots, g_s\}$
REPEAT
$G' := G$
For each pair $f \neq g$ in G' DO
  $S := \overline{S(f,g)}^{G'}$
  If $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

Proof. It is exactly the same algorithm as in the case the basic ring is a field. The only modifications are in the definition of S-polynomials and in the divisions of terms. Just, note that this algorithm must terminate after a finite number of iterations since the basic ring is Noetherian.

□

Of course, many results originally established for Gröbner bases over fields (see [24]) can fairly be extended to Noetherian valuation rings using our approach. For instance, the notions of minimal and reduced Gröbner bases (uniqueness up to an invertible element in the basic ring).

Example of applications: the structure of codes over a finite-chain ring

Cyclic codes correspond to ideals of $\mathbf{R}[X]/\langle X^n - 1\rangle$, $\mathbf{R}$ a finite chain ring, that is, a ring with finitely many ideals and whose ideals are linearly ordered by inclusion (these are Noetherian valuation rings). Examples of finite-chain rings are:
(i) $\mathbb{Z}/p^k\mathbb{Z}$,
(ii) Galois rings $GR(p^k, n) = (\mathbb{Z}/p^k\mathbb{Z})[t]/\langle f\rangle$ where f is a monic irreducible polynomial in $(\mathbb{Z}/p^k\mathbb{Z})[t]$ of degree n whose image modulo p is irreducible,
(iii) $\mathbf{D}/\langle a^k\rangle$ with $\mathbf{D}$ a principal domain, a an irreducible element.

Let $q : \mathbf{R}[X] \to \mathbf{R}[X]/\langle X^n - 1\rangle$ be the quotient map. One advantage of having a Gröbner basis as a set of generators is that $q(c)$ is a codeword if and only if c reduces to zero with respect to G. Thus reduction with respect to G (which replaces division by the generator polynomial over a field) can be used for error detection [14, 58, 59, 60, 61].

Example 124. *([14], Example 2.4.6)* Let $\mathbf{V}[X, Y] = (\mathbb{Z}/27\mathbb{Z})[X, Y]$ and consider $\mathcal{G} = \{g_i\}_{i=1}^4$, where $g_1 = 9, g_2 = X + 1, g_3 = 3Y^2, g_4 = Y^3 + 13Y^2 - 12$. Let us fix the lexicographic order as monomial order with $X > Y$.

$S(g_1, g_2) = Xg_1 - 9g_2 = -9 \xrightarrow{g_1} 0,$
$S(g_1, g_3) = Y^2g_1 - 3g_3 = 0,$
$S(g_1, g_4) = -9Y^2 \xrightarrow{g_1} 0,$
$S(g_2, g_3) = 3Y^2g_2 - Xg_3 = 3Y^2 \xrightarrow{g_3} 0,$
$S(g_2, g_4) = Y^3g_2 - Xg_4 = -13XY^2 + 12X + Y^3 \xrightarrow{g_2} 12X + Y^3 + 13Y^2 \xrightarrow{g_2} Y^3 + 13Y^2 - 12 \xrightarrow{g_3} 0,$
$S(g_3, g_4) = Yg_3 - 3g_4 = -12Y^3 + 9 \xrightarrow{g_3} 9 \xrightarrow{g_1} 0.$

Thus, $\mathcal{G}$ is a Gröbner basis for $\langle g_1, g_2, g_3, g_4\rangle$ in $\mathbf{V}[X, Y]$.

Example 125. Let $\mathbf{V}[X, Y] = (\mathbb{Z}/4\mathbb{Z})[X, Y]$ and consider the ideal $I = \langle f_1, f_2, f_3\rangle$, where $f_1 = X^4 - X, f_2 = Y^3 - 1, f_3 = 2XY$. Let us fix the lexicographic order as monomial order with $X > Y$.

$S(f_1, f_2) = Y^3f_1 - X^4f_2 = X^4 - XY^3 \xrightarrow{f_1} X - XY^3 \xrightarrow{f_2} 0,$
$S(f_1, f_3) = 2Yf_1 - X^3f_3 = -2XY \xrightarrow{f_3} 0,$
$S(f_2, f_3) = 2Xf_2 - Y^2f_3 = -2X =: f_4,$
$S(f_2, f_4) = 2Xf_2 + Y^3f_4 = -2X \xrightarrow{f_4} 0,$
$S(f_1, f_4) = 2f_1 + X^3f_4 = -2X \xrightarrow{f_4} 0,$
$f_3 \xrightarrow{f_4} 0.$

Thus, $\mathcal{G} = \{f_1, f_2, f_4\}$ is a Gröbner basis for I in $\mathbf{V}[X, Y]$.

A natural question arising is :

For a valuation ring $\mathbf{R}$*, is it always possible to compute a Gröbner basis for each finitely generated nonzero ideal of* $\mathbf{R}[X_1, \ldots, X_n]$ *by Buchberger's Algorithm (without supposing that* $\mathbf{R}$ *is Noetherian) in a finite number of steps ?*

In fact, in the integral case, if the totally ordered group corresponding to the valuation is not archimedian, Buchberger's Algorithm does not always work in a finite number of steps as can be seen by the following example.

Example 126. Let $\mathbf{V}$ be a valuation domain with a corresponding valuation v and group G. Suppose that G is not archimedian, that is there exist $a, b \in \mathbf{V}$ such that:

$$v(a) > 0, \text{ and } \forall\, n \in \mathbb{N}^*,\ v(b) > n\, v(a).$$

Denote by I the ideal of $\mathbf{V}[X]$ generated by $g_1 = aX + 1$ and $g_2 = b$.
Since $S(g_1, g_2) = (\frac{b}{a})g_1 - Xg_2 = \frac{b}{a}$ and $\frac{b}{a}$ is not divisible by b, then one must add $g_3 = \frac{b}{a}$ when executing Buchberger's Algorithm.
In the same way, $S(g_1, g_3) = (\frac{b}{a^2})g_1 - Xg_3 = \frac{b}{a^2}$ and $\frac{b}{a^2}$ is not divisible by b nor by $\frac{b}{a}$. Thus, one must add $g_4 = \frac{b}{a^2}$, and so on, we observe that Buchberger's Algorithm does not terminate.

Taking the particular case $G = \mathbb{Z} \times \mathbb{Z}$ equipped with the lexicographic order, $a = (0, 1)$, and $b = (1, 0)$. We can prove $\langle \mathrm{LT}(I) \rangle$ is not finitely generated despite that I is finitely generated and that clearly $\langle \mathrm{LC}(I) \rangle = \langle a \rangle$ (there is no such example in the literature).

Proof. To check this, by way of contradiction, suppose that $\langle \mathrm{LT}(I) \rangle = \langle h_1, \ldots, h_s \rangle$, $h_i \in I \setminus \{0\}$, $s \in \mathbb{N}^*$. We can suppose that $h_1, \ldots, h_s$ are terms, that is $h_i = \mathrm{LT}(h_i)$ for each $1 \leq i \leq s$. From Lemma 121, it follows that for each $n \in \mathbb{N}$, there exists $i_n \in \{1, \ldots, s\}$ such that h_{i_n} divides $\frac{b}{a^n}$. We infer that there exists $1 \leq i_0 \leq s$ such that h_{i_0} is constant ($h_{i_0} \in V \setminus \{0\}$) and such that

$$\forall n \in \mathbb{N},\ h_{i_0} \text{ divides } \frac{b}{a^n}.$$

That is, $v(h_{i_0}) \leq (1, -n)\ \forall n \in \mathbb{N}$. It follows that there exists $k \in \mathbb{N}$ such that $v(h_{i_0}) = (0, k)$ and hence there exists u invertible in V such that $h_{i_0} = ua^k$.
Now $\left\{ \begin{array}{l} a^k \in I \\ aX + 1 \in I \end{array} \right. \Rightarrow \left\{ \begin{array}{l} a^k \in I \\ a^{k-1}(aX + 1) \in I \end{array} \right. \Rightarrow\ a^{k-1} \in I\ \Rightarrow\ \cdots\ \Rightarrow\ a \in I\ \Rightarrow\ 1 \in I$, a contradiction.

□

As a consequence of this example, keeping the notations above, we know that a necessary condition so that Buchberger's Algorithm terminates in the integral case is that the group G is archimedian (this is in fact equivalent to $\dim \mathbf{V} \leq 1$, see for example Proposition 8 page 116 in [12]). Moreover, we already know that a sufficient condition is that $\mathbf{V}$ Noetherian. This encourages us to set the following definition and conjecture:

Definition 127. *A ring $\mathbf{R}$ is said to be a Gröbner ring if for each finitely generated ideal I of $\mathbf{R}[X_1, \ldots, X_n]$, the ideal $\{\mathrm{LT}(f), f \in I\}$ of $\mathbf{R}[X_1, \ldots, X_n]$ is finitely generated.*

Conjecture 128. (One-dimensional valuation ⇒ Gröbner) *For a valuation ring $\mathbf{V}$, the following assertions are equivalent:*

(i) *It is always possible to compute a Gröbner basis for each finitely generated nonzero ideal of $\mathbf{V}[X_1, \ldots, X_n]$ by the generalized version of Buchberger's Algorithm for valuation rings in a finite number of steps.*

(ii) $\dim \mathbf{V} \leq 1$.

(iii) $\mathbf{V}$ *is a Gröbner ring.*

7.2 How to construct a dynamical Gröbner basis over a Dedekind ring ?

Let $\mathbf{R}$ be a Dedekind ring (that is, a Noetherian arithmetical ring which may have zero-divisors), $I = \langle f_1, \ldots, f_s \rangle$ a nonzero finitely generated ideal of $\mathbf{R}[X_1, \ldots, X_n]$, and fix a monomial order $>$. The purpose is to construct a dynamical Gröbner basis G for I.

Dynamical version of Buchberger's Algorithm

This algorithm is analogous to the dynamical version of Buchberger's algorithm over principal rings given in [73]. It works like Buchberger's Algorithm for Noetherian valuation rings. The only difference is when it has to handle two incomparable (under division) elements a, b in $\mathbf{R}$. In this situation, one should first compute $u, v, w \in \mathbf{R}$ such that

$$\left\{ \begin{array}{l} ub = va \\ wb = (1 - u)a. \end{array} \right.$$

Now, one opens two branches: the computations are pursued in $\mathbf{R}_u$ and $\mathbf{R}_{1+u\mathbf{R}} := \{\frac{x}{y}, x \in \mathbf{R}$ and $\exists z \in \mathbf{R}$ such that $y = 1 + zu\}$. Note that contrary to [73], we use the localization $\mathbf{R}_{1+u\mathbf{R}}$ instead of $\mathbf{R}_{1-u}$ in order to avoid redundancies.

-First possibility: the two incomparable elements a and b are encountered when performing the division algorithm (analogous to the division algorithm in the case of a Noetherian valuation ring). Suppose that one has to divide a term $aX^\alpha = \mathrm{LT}(f)$ by another term $bX^\beta = \mathrm{LT}(g)$ with X^β divides X^α.

In the ring $\mathbf{R}_{1+u\mathbf{R}}$: $f = \frac{w}{1-u}\frac{X^\alpha}{X^\beta}g + r$ ($\mathrm{mdeg}(r) < \mathrm{mdeg}(f)$) and the division is pursued with f replaced by r.

In the ring $\mathbf{R}_u$: $\mathrm{LT}(f)$ is not divisible by $\mathrm{LT}(g)$ and thus $f = \overline{f}^{\{g\}}$.

-Second possibility: the two incomparable elements a and b are encountered when computing $S(f,g)$ with $\mathrm{LT}(f) = aX^\alpha$ and $\mathrm{LT}(g) = bX^\beta$. Denote $\gamma = (\gamma_1, \ldots, \gamma_n)$, with $\gamma_i = \max(\alpha_i, \beta_i)$ for each i.

In the ring $\mathbf{R}_{1+u\mathbf{R}}$: $S(f,g) = \frac{X^\gamma}{X^\alpha}f - \frac{w}{1-u}\frac{X^\gamma}{X^\beta}g$.

In the ring $\mathbf{R}_u$: $S(f,g) = \frac{v}{u}\frac{X^\gamma}{X^\alpha}f - \frac{X^\gamma}{X^\beta}g$.

At each new branch, if $S = \overline{S(f,g)}^{G'} \neq 0$ where G' is the current Gröbner basis, then S must be added to G'.

Comments

1) Of course, when localized at the multiplicative subsets described above, the obtained rings remain Dedekind rings. Let's sketch the proof of this fact. The only non trivial fact to prove is that if $\mathbf{R}$ is a Dedekind ring and $S = c^{\mathbb{N}}(1 + \langle a_1, \ldots, a_m\rangle) := \{c^n(1+d),\ n \in \mathbb{N},\ d \in \langle a_1, \ldots, a_m\rangle\}$ is a multiplicative subset of $\mathbf{R}$ with c, $a_i \in \mathbf{R}$, then $S^{-1}\mathbf{R}$ remains strongly discrete. Since $S^{-1}\mathbf{R}$ is coherent, it suffices to prove that we can test if $1 \in J$ for any finitely generated ideal J in $S^{-1}\mathbf{R}$. Denoting $J = \langle b_1, \ldots, b_k\rangle$, $b_i \in \mathbf{R}$, proving that $1 \in J$ is nothing but proving that there exist $x_1, \ldots, x_k, y_1, \ldots, y_m \in \mathbf{R}$ and $n \in \mathbb{N}$ such that $c^n(1 + a_1y_1 + \cdots + a_my_m) = b_1x_1 + \cdots + b_kx_k$. For fixed n, consider the ideal $J_n = \{z \in \mathbf{R},\ \exists\ x_1, \ldots, x_k, y_1, \ldots, y_m \in \mathbf{R}$ and $n \in \mathbb{N}$ such that $c^n(z + a_1y_1 + \cdots + a_my_m) = b_1x_1 + \cdots + b_kx_k\}$. Since $\mathbf{R}$ is coherent, the J_n are finitely generated. The increasing sequence (J_n) becomes constant when two consecutive terms J_N and J_{N+1} coincide and then it suffices to test if $1 \in J_N$.

2) This algorithm must terminate after a finite number of steps. Indeed, if it does not stop then this would be the coefficients' fault and not the monomials' fault since $\mathbb{N}^n$ is well ordered (see Dickson's Lemma [24], page 69). That is, the Dynamical version of Buchberger's Algorithm would produce infinitely many polynomials g_i with the same multidegree such that $\langle \mathrm{LC}(g_1)\rangle \subset \langle \mathrm{LC}(g_2)\rangle \subset \langle \mathrm{LC}(g_2)\rangle \subset \cdots$ in contradiction with the fact that a Dedekind ring is Noetherian.

7.3 A conjecture about arithmetical rings

We will extend our conjecture (one-dimensional valuation ⇒ Gröbner) to arithmetical rings.

Conjecture 129. (One-dimensional arithmetical ⇒ Gröbner) *For an arithmetical ring* $\mathbf{R}$*, the following assertions are equivalent:*

(i) *It is always possible to compute a Gröbner basis for each finitely generated nonzero ideal of* $\mathbf{R}[X_1, \ldots, X_n]$ *by the dynamical version of Buchberger's Algorithm in a finite number of steps.*

(ii) $\dim \mathbf{R} \leq 1$.

(iii) $\mathbf{R}$ *is a Gröbner ring.*

7.4 The ideal membership problem over Dedekind rings

Proposition 130. *Let* $\mathbf{R}$ *be a Dedekind ring,* $I = \langle f_1, \ldots, f_s\rangle$ *a nonzero finitely generated ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*,* $f \in \mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order. Suppose that* $G = \{g_1, \ldots, g_t\}$ *is a special Gröbner basis for* I *in* $\mathbf{R}[X_1, \ldots, X_n]$*. Then,* $f \in I$ *if and only if* $\overline{f}^G = 0$.

Proof. Of course, if $\overline{f}^G = 0$ then $f \in \langle g_1, \ldots, g_t\rangle = I$. For the converse, suppose that $f \in I$ and that the remainder r of f on division by G in $\mathbf{R}[X_1, \ldots, X_n]$ is nonzero. This means that $\mathrm{LT}(r)$ is not divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.
Observe that G is also a Gröbner basis for $\langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}_{\mathfrak{p}}[X_1, \ldots, X_n]$ for each prime ideal $\mathfrak{p}$ of $\mathbf{R}$.
Let $\mathfrak{p}$ be any prime ideal of $\mathbf{R}$. Since G is also a Gröbner basis for $\langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}_{\mathfrak{p}}[X_1, \ldots, X_n]$, then $\mathrm{LM}(r)$ is divisible by at least one of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)$, but for each g_i such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(r)$, $\mathrm{LC}(g_i)$ does not divide $\mathrm{LM}(r)$. Let $g_{i_1}, \ldots, g_{i_k}$ be such polynomials and suppose that
$\mathrm{LC}(g_{i_1})/\mathrm{LC}(g_{i_2})/\cdots/\mathrm{LC}(g_{i_k})$ (by definition of a special Gröbner basis we can make this hypothesis). Since the basic ring is a Dedekind ring, we can write $\langle \mathrm{LC}(g_{i_1})\rangle = \mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_\ell^{\alpha_\ell}$ and $\langle \mathrm{LC}(r)\rangle = \mathfrak{p}_1^{\beta_1}\cdots\mathfrak{p}_\ell^{\beta_\ell}$, where the p_i are distinct prime ideals of $\mathbf{R}$, and $\alpha_i, \beta_i \in \mathbb{N}$. Necessarily, there exists $1 \leq i_0 \leq \ell$ such that $\alpha_{i_0} > \beta_{i_0}$. But this would imply that the problem persists in the ring $\mathbf{R}_{\mathfrak{p}_{i_0}}[X_1, \ldots, X_n]$, in contradiction with the fact that G is a Gröbner basis for $\langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}_{\mathfrak{p}_{i_0}}[X_1, \ldots, X_n]$. □

Theorem 131. (Dynamical gluing)
Let $\mathbf{R}$ *be a Dedekind ring,* $I = \langle f_1, \ldots, f_s \rangle$ *a nonzero finitely generated ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*,* $f \in \mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order. Suppose that* $G = \{(S_1, G_1), \ldots, (S_k, G_k)\}$ *is a dynamical Gröbner basis for* I *in* $\mathbf{R}[X_1, \ldots, X_n]$*. Then,* $f \in I$ *if and only if* $\overline{f}^{G_i} = 0$ *in* $(S_i^{-1}\mathbf{R})[X_1, \ldots, X_n]$ *for each* $1 \leq i \leq k$*.*

Proof. " $\Rightarrow$ " This follows from Proposition 130.
" $\Leftarrow$ " Since $\overline{f}^{G_i} = 0$, then $f \in \langle f_1, \ldots, f_s \rangle$ in $(S_i^{-1}\mathbf{R})[X_1, \ldots, X_n]$, for each $1 \leq i \leq k$. This means that for each $1 \leq i \leq k$, there exist $s_i \in S_i$ and $h_{i,1}, \ldots, h_{i,s} \in \mathbf{R}[X_1, \ldots, X_n]$ such that

$$s_i f = h_{i,1} f_1 + \cdots + h_{i,s} f_s.$$

Using the fact that $S_1, \ldots, S_k$ are comaximal, there exist $a_1, \ldots, a_k \in \mathbf{R}$ such that $\sum_{i=1}^{k} a_i s_i = 1$. It follows that

$$f = (\sum_{i=1}^{k} a_i h_{i,1}) f_1 + \cdots + (\sum_{i=1}^{k} a_i h_{i,s}) f_s \in I.$$

□

7.5 Syzygy modules over valuation rings

The following theorem gives a generating set for syzygies of monomials with coefficients in a valuation ring. It is a generalization of Proposition 8 ([24], page 104) to valuation rings.

Theorem 132. (Syzygy generating set of monomials over valuation rings)
Let $\mathbf{V}$ *be a valuation ring,* $c_1, \ldots, c_s \in \mathbf{V} \setminus \{0\}$*, and* $M_1, \ldots, M_s$ *monomials in* $\mathbf{V}[X_1, \ldots, X_n]$*. Denoting* $LCM(M_i, M_j)$ *by* $M_{i,j}$*, the syzygy module* $\mathrm{Syz}(c_1 M_1, \ldots, c_s M_s)$ *is generated by:*

$$\{S_{ij} \in \mathbf{V}[X_1, \ldots, X_n]^s \mid 1 \leq i < j \leq s\},$$

where

$$S_{ij} = \begin{cases} \frac{M_{i,j}}{M_i} e_i - \frac{c_i}{c_j} \frac{M_{i,j}}{M_j} e_j & \text{if } c_j \mid c_i \\ \frac{c_j}{c_i} \frac{M_{i,j}}{M_i} e_i - \frac{M_{i,j}}{M_j} e_j & \text{else.} \end{cases}$$

Here $(e_1, \ldots, e_s)$ *is the canonical basis of* $\mathbf{V}[X_1, \ldots, X_n]^{s \times 1}$*.*

Proof. It is clear that for all $i < j$, S_{ij} is a syzygy of $M = (c_1 M_1, \ldots, c_s M_s)$.
Now, in order to verify that $\{S_{ij}, 1 \leq i < j \leq s\}$ is really a syzygy basis, we need to show that every syzygy H of M can be written as $H = \sum_{i \neq j} u_{ij} S_{ij}$ where $u_{ij} \in \mathbf{V}[X_1, \ldots, X_n]$. For this, let $H = {}^{\mathrm{t}}(h_1, \ldots, h_s)$ be a syzygy of M, that is, such that $MH = 0$. Letting $\gamma(H) = \max_{1 \leq i \leq s} \mathrm{mdeg}(h_i M_i)$, we have

$$\sum_{\mathrm{mdeg}(h_i M_i) = \gamma(H)} c_i h_i M_i + \sum_{\mathrm{mdeg}(h_i M_i) < \gamma(H)} c_i h_i M_i = 0.$$

Thus,

$$\sum_{\mathrm{mdeg}(h_i M_i) = \gamma(H)} c_i LT(h_i) M_i + \sum_{\mathrm{mdeg}(h_i M_i) = \gamma(H)} c_i (h_i - LT(h_i)) M_i + \sum_{\mathrm{mdeg}(h_i M_i) < \gamma(H)} c_i h_i M_i = 0.$$

We can write $H = G + \widetilde{G}$, where $G = (g_1, \ldots, g_s)$ with $g_i = LT(h_i)$ if $\mathrm{mdeg}(h_i M_i) = \gamma(H)$, 0 else; $\widetilde{G} = (\widetilde{g}_1, \ldots, \widetilde{g}_s)$ with $\widetilde{g}_i = h_i - LT(h_i)$ if $\mathrm{mdeg}(h_i M_i) = \gamma(H)$, 0 else.
Since $\gamma(\widetilde{G}) < \gamma(H)$, it suffices, by induction on $\gamma(H)$, to prove the result for G. In particular we can assume that $h_i = a_i M_i'$ with $a_i \in \mathbf{V}$ (a_i can be zero). Let $i_1 < i_2 \ldots < i_t$ be the indices corresponding to the nonzero a_i's, and denote $\gamma(H)$ by γ. The facts that $a_1 M_1' c_1 M_1 + \cdots + a_s M_s' c_s M_s = 0$ and $a_i M_i' c_i M_i = a_i c_i X^\gamma$ imply that

$$a_{i_1} c_{i_1} + \cdots + a_{i_t} c_{i_t} = 0. \quad (*)$$

It follows that

$$(h_1, \ldots, h_s) = (a_1 M_1', \ldots, a_s M_s') = a_{i_1} M_{i_1}' e_{i_1} + \ldots + a_{i_t} M_{i_t}' e_{i_t}$$
$$= a_{i_1} \frac{X^\gamma}{M_{i_1}} e_{i_1} + \cdots + a_{i_t} \frac{X^\gamma}{M_{i_t}} e_{i_t}.$$

As $\mathbf{V}$ is a valuation ring, there exists an integer $q \in \{1, \ldots, t\}$ such that c_{i_q} divide all the c_{i_j}'s. So the previous expression can be written as:

$$a_{i_1}\frac{X^\gamma}{M_{i_1}}e_{i_1} + \ldots + a_{i_t}\frac{X^\gamma}{M_{i_t}}e_{i_t} = \sum_{1\leq j\leq q-1} a_{i_j}\frac{X^\gamma}{M_{i_j,i_q}}[\frac{M_{i_j,i_q}}{M_{i_j}}e_{i_j} - \frac{c_{i_j}}{c_{i_q}}\frac{M_{i_j,i_q}}{M_{i_q}}e_{i_q}]$$

$$- \sum_{q+1\leq j\leq t} a_{i_j}\frac{X^\gamma}{M_{i_j,i_q}}[\frac{c_{i_j}}{c_{i_q}}\frac{M_{i_j,i_q}}{M_{i_q}}e_{i_q} - \frac{M_{i_j,i_q}}{M_{i_j}}e_{i_j}] + [\sum_{j\neq q} a_{i_j}\frac{c_{i_j}}{c_{i_q}} + a_{i_q}]\frac{X^\gamma}{M_{i_q}}e_{i_q}. \quad (**)$$

Note that $\sum_{j\neq q} a_{i_j}\frac{c_{i_j}}{c_{i_q}} + a_{i_q} = 0$ from $(*)$, for $1 \leq j \leq q-1$, $\frac{M_{i_j,i_q}}{M_{i_j}}e_{i_j} - \frac{c_{i_j}}{c_{i_q}}\frac{M_{i_j,i_q}}{M_{i_q}}e_{i_q} = S_{i_j i_q}$, and for each $q+1 \leq j \leq t$,

$$\frac{c_{i_j}}{c_{i_q}}\frac{M_{i_j,i_q}}{M_{i_q}}e_{i_q} - \frac{M_{i_j,i_q}}{M_{i_j}}e_{i_j} = \begin{cases} \frac{c_{i_j}}{c_{i_q}}S_{i_q i_j} \text{ if } c_{i_j}/c_{i_q} \\ S_{i_q i_j} \text{ if } c_{i_j} \text{does not divide } c_{i_q}. \end{cases}$$

Thus, $\mathrm{Syz}(c_1M_1, \ldots, c_sM_s) \subseteq \langle S_{ij}, 1 \leq i < j \leq s\rangle$, the desired conclusion.

□

Example 133. Let $\mathbf{V} = \mathbb{Z}/8\mathbb{Z}$, $f_1 = 4X^2, f_2 = 2XY^3, f_3 = 6Y, f_4 = 5$ in $\mathbf{V}[X, Y]$. With the previous notations, since $c_4/c_3/c_2/c_1$, the syzygy module $\mathrm{Syz}(f_1, \ldots, f_4)$ is generated by $\{S_{ij} = \frac{M_{i,j}}{M_i}e_i - \frac{c_i}{c_j}\frac{M_{i,j}}{M_j}e_j \ 1 \leq i < j \leq 4\}$, that is,

$$\mathrm{Syz}(f_1, \ldots, f_4) = \langle {}^{\mathrm{t}}(Y^3, 6X, 0, 0), {}^{\mathrm{t}}(Y, 0, 6X^2, 0), {}^{\mathrm{t}}(1, 0, 0, 4X^2), {}^{\mathrm{t}}(0, 1, 5XY^2, 0),$$

$${}^{\mathrm{t}}(0, 1, 0, 6XY^3), {}^{\mathrm{t}}(0, 0, 1, 2Y)\rangle.$$

Notation 134. *Let $\mathbf{V}$ be a valuation ring, $>$ a monomial order, $f_1, \ldots, f_s \in \mathbf{V}[X_1, \ldots, X_n] \setminus \{0\}$, and $\{g_1, \ldots, g_t\}$ a Gröbner basis for $\langle f_1, \ldots, f_s\rangle$. Let $c_i = LC(g_i)$, and $M_i = LM(g_i)$. In order to determinate the syzygy module $\mathrm{Syz}(f_1, \ldots, f_s)$, we will first compute $\mathrm{Syz}(g_1, ..., g_t)$. Recall that for each $1 \leq i < j \leq t$, the S-polynomial of g_i and g_j is given by:*

$$S(g_i, g_j) = \begin{cases} \frac{M_{ij}}{M_i}g_i - \frac{c_i}{c_j}\frac{M_{ij}}{M_j}g_j & \text{if } c_j \mid c_i \\ \frac{c_j}{c_i}\frac{M_{ij}}{M_i}g_i - \frac{M_{ij}}{M_j}g_j & \text{else.} \end{cases}$$

And for some $h_{ijk} \in \mathbf{V}[X_1, ..., X_n]$, we have

$$S(g_i, g_j) = \sum_{k=1}^{t} g_k h_{ijk} \text{ with } \mathrm{mdeg}(S(g_i, g_j)) = max_{1\leq k\leq t}\mathrm{mdeg}(g_k h_{ijk}) \quad (\star).$$

(The polynomials h_{ijk} are given by the division algorithm.)
Let:

$$\epsilon_{ij} = \begin{cases} \frac{M_{ij}}{M_i}e_i - \frac{c_i}{c_j}\frac{M_{ij}}{M_j}e_j & \text{if } c_j \mid c_i \\ \frac{c_j}{c_i}\frac{M_{ij}}{M_i}e_i - \frac{M_{ij}}{M_j}e_j & \text{else.} \end{cases}$$

And

$$s_{ij} = \epsilon_{ij} - \sum_{k=1}^{t} e_k h_{ijk}.$$

Theorem 135. *(Syzygy module of a Gröbner basis over a valuation ring) With the previous notations,*

$$\mathrm{Syz}(g_1, \ldots, g_t) = \langle s_{ij} \mid 1 \leq i < j \leq t\rangle.$$

Proof. "$\Longleftarrow$" Let $G = (g_1, \ldots, g_t)$. For each $1 \leq i < j \leq t$, we have $Gs_{ij} = S(g_i, g_j) - \sum_{k=1}^{t} g_k h_{ijk} = 0$. Thus, $s_{ij} \in \mathrm{Syz}(g_1, \ldots, g_t)$.
"$\Longrightarrow$" Let $U = {}^{\mathrm{t}}(u_1, \ldots, u_t) \in \mathrm{Syz}(g_1, \ldots, g_t)$, and set $\gamma(U) = \max_{1\leq i\leq t}\{\mathrm{mdeg}(u_i g_i)\}$. We will proceed by induction on $\gamma(U)$.
Letting $S = \{i \in \{1, \ldots, t\} \setminus \mathrm{mdeg}(u_i g_i) = \gamma(U)\}$, we have

$$\sum_{i\in S} u_i g_i + \sum_{i\notin S} u_i g_i = 0 \Rightarrow \sum_{i\in S} LT(u_i)g_i + \sum_{i\in S}(u_i - LT(u_i))g_i + \sum_{i\notin S} u_i g_i = 0$$

and so $\sum_{i\in S} LT(u_i)LT(g_i) = 0$, that is, $(LT(u_i))_{i\in S} \in \mathrm{Syz}(LT(g_i))_{i\in S}$. Following Theorem 132, we can write

$$(LT(u_i))_{i\in S} = \sum_{1\leq i<j\leq t,\ i,j\in S} h_{ij}\epsilon_{ij}. \qquad (\star\star)$$

Let $U = W + {}^{\mathrm{t}}(u'_1,\ldots,u'_t)$ with $W = {}^{\mathrm{t}}(w_1,\ldots,w_t)$ and $w_i = \begin{cases} 0 & \text{if } i \notin S \\ LT(u_i) & \text{if } i \in S, \end{cases}$

in such a way we have

$$U = \sum_{1\leq i<j\leq t,\ i,j\in S} h_{ij}\epsilon_{ij} + {}^{\mathrm{t}}(u'_1,\ldots,u'_t).$$

We can write $U = \overline{V} + V$ where

$$\overline{V} = \sum_{1\leq i<j\leq t,\ i,j\in S} h_{ij}s_{ij} \text{ and } V = \sum_{1\leq i<j\leq t,\ i,j\in S} h_{ij}\sum_{k=1}^{t} h_{ijk}e_k + {}^{\mathrm{t}}(u'_1,\ldots,u'_t).$$

It is clear that $\overline{V} \in \langle s_{ij}\ ,\ 1 \leq i < j \leq t\rangle$. Denoting by $V = {}^{\mathrm{t}}(v_1,\ldots,v_t)$, we have

$$\mathrm{mdeg}(v_l g_l) = \mathrm{mdeg}(u'_l g_l + \sum_{1\leq i<j\leq t, i,j\in S} h_{ij}h_{ijl}g_l)$$

$$\leq max_{1\leq i<j\leq t,\ i,j\in S}\{\mathrm{mdeg}(u'_l g_l), \mathrm{mdeg}(h_{ij}h_{ijl}g_l)\}.$$

By definition of ${}^{\mathrm{t}}(u'_1,\ldots,u'_t)$, we have $\mathrm{mdeg}(u'_l g_l) < \gamma(U)$. Moreover, from $(\star\star)$, we have

$$(LT(u_i))_{i\in S}\,{}^{\mathrm{t}}(g_i)_{i\in S} = \sum_{1\leq i<j\leq t,\ i,j\in S} h_{ij}\,S(g_i,g_j). \qquad (\star\star\star)$$

In the equality $(\star\star\star)$, all the terms $LT(u_i)g_i$ on the left-hand side are homogeneous with multidegree $\gamma(U)$ since $\mathrm{mdeg}(LT(u_i)LT(g_i)) = \gamma(U)\ \ \forall\, i \in S$. This property must also be satisfied on the right-hand side. Thus, $\mathrm{mdeg}(h_{ij}\frac{M_{ij}}{M_i}M_i) \leq \gamma(U)$, $\mathrm{mdeg}(h_{ij}\frac{c_i}{c_j}\frac{M_{ij}}{M_j}M_j) \leq \gamma(U)$, and $\mathrm{mdeg}(h_{ij}M_{ij}) \leq \gamma(U)$.
On the other hand, $\forall\ 1 \leq k \leq t$, $\mathrm{mdeg}(h_{ijk}g_k) \leq \mathrm{mdeg}(S(g_i,g_j))$ since by $(\star)$ we have $\mathrm{mdeg}(S(g_i,g_j)) = max_{1\leq k\leq t} mdeg(h_{ijk}g_k)$.
Hence $\mathrm{mdeg}(h_{ij}h_{ijl}g_l) \leq \mathrm{mdeg}(h_{ij}S(g_i,g_j)) < \mathrm{mdeg}(h_{ij}M_{ij}) \leq \gamma(U)$, $\mathrm{mdeg}(v_l g_l) < \gamma(U)\ \ \forall\ 1 \leq l \leq t$, and finally, $\gamma(V) < \gamma(U)$ as desired.

□

Example 136. Let $\mathbf{V} = \mathbb{Z}/8\mathbb{Z}$ and $g_1 = 2X^3 + 6X^2, g_2 = 6Y^2, g_3 = 5XY - 5Y \in \mathbf{V}[X,Y]$. Let us fix the lexicographic order as monomial order with $X > Y$. Then $G = \{g_1,g_2,g_3\}$ is a Gröbner basis for $\langle g_1,g_2,g_3\rangle$ in $(\mathbb{Z}/8\mathbb{Z})[X,Y]$ as

$S(g_1,g_2) = Y^2g_1 - 3X^3g_2 = X^2g_2 \xrightarrow{g_2} 0$,
$S(g_1,g_3) = Yg_1 - 2X^2g_3 = 0$,
$S(g_2,g_3) = Xg_2 - 6Yg_3 = g_2 \xrightarrow{g_2} 0$.

Keeping the previous notations, we have

$$h_{121} = 0, h_{122} = X^2, h_{123} = 0 \ \Rightarrow\ s_{12} = {}^{\mathrm{t}}(Y^2, -3X^3 - X^2, 0).$$

In the same way, we obtain that $s_{13} = {}^{\mathrm{t}}(Y, 0, -2X^2)$ and $s_{23} = {}^{\mathrm{t}}(0, X-1, -6Y)$. And finally

$$\mathrm{Syz}(g_1,g_2,g_3) = \langle {}^{\mathrm{t}}(Y^2,-3X^3-X^2,0),\ {}^{\mathrm{t}}(Y,0,-2X^2),\ {}^{\mathrm{t}}(0,X-1,-6Y)\rangle.$$

Denoting by $F = [f_1\cdots f_s]$ and $G = [g_1\cdots g_t]$, there exist two matrices S and T respectively of size $t\times s$ and $s\times t$ such that $F = GS$ and $G = FT$. We can first compute a generator set $\{s_1,\ldots,s_r\}$ of $\mathrm{Syz}(G)$. For each $i \in \{1,\ldots,r\}$, we have $0 = Gs_i = (FT)s_i = F(Ts_i)$. So $\langle Ts_i \mid\ i \in \{1,\ldots,r\}\rangle \subseteq \mathrm{Syz}(F)$. Also denoting by $\mathbf{I}_s$ the identity matrix of size $s\times s$, we have

$$F(\mathbf{I}_s - TS) = F - FTS = F - GS = F - F = 0.$$

This equality shows that the columns $r_1,\ldots,r_s$ of $\mathbf{I}_s - TS$ are also in $\mathrm{Syz}(F)$. The converse holds as stated by the following theorem whose proof is identical to that in case the base ring is a field [24].

Theorem 137. *(Syzygy computation over valuation rings: general case) With the previous notations, we have*

$$\mathrm{Syz}(f_1,\ldots,f_s)=\langle Ts_1,\ldots,Ts_r,r_1,\ldots,r_s\rangle.$$

Proof. Let $s=(a_1,\ldots,a_s)\in Syz(f_1,\ldots,f_s)$. As $0=Fs=GSs$, we have $Ss\in Syz(g_1,\ldots,g_t)$. By definition of $s_1,\ldots,s_r$, we have $Ss=\sum_{i=1}^{r}h_is_i$ for $h_i\in V[X_1,\ldots,X_n]$, which implies that $TSs=\sum_{i=1}^{r}h_i(Ts_i)$. Thus, $s=s-TSs+TSs=(I_s-TS)s+\sum_{i=1}^{r}h_i(Ts_i)=\sum_{i=1}^{s}a_ir_i+\sum_{i=1}^{r}h_i(Ts_i)$, and $Syz(f_1,\ldots,f_s)\subseteq\langle Ts_1,\ldots,Ts_r,r_1,\ldots,r_s\rangle$. We conclude that $Syz(f_1,\ldots,f_s)=\langle Ts_1,\ldots,Ts_r,r_1,\ldots,r_s\rangle$. □

Example 138. Let $f_1=2XY,f_2=3Y^3+3,f_3=X^2-3X\in\mathbf{V}[X,Y]=(\mathbb{Z}/4\mathbb{Z})[X,Y]$, and $F=[f_1\ f_2\ f_3]$. Computing a Gröbner basis for $\langle f_1,f_2,f_3\rangle$ using the lexicographic order with $X>Y$ as monomial order, we obtain:

$S(f_1,f_2)=Y^2f_1-2Xf_2=2X=:f_4$,
$S(f_1,f_3)=Xf_1-2Yf_3=2XY\xrightarrow{f_1}0$,
$S(f_2,f_3)=X^2f_2-3Y^3f_3=3X^2+XY^3\xrightarrow{f_3}X+XY^3\xrightarrow{f_2}0$,
$f_1\xrightarrow{f_4}0$, $S(f_2,f_4)=2Xf_2-Y^3f_4=2X\xrightarrow{f_4}0$,
$S(f_3,f_4)=2f_3-Xf_4=2X\xrightarrow{f_4}0$.

Thus, $\{f_2,f_3,f_4\}$ is a Gröbner basis for $\langle f_1,f_2,f_3\rangle$ in $\mathbf{V}[X,Y]$. Denoting by $G=[f_2\ f_3\ f_4]$, we have $G=FT$ with $T=\begin{pmatrix}0&0&Y^2\\1&0&-2X\\0&1&0\end{pmatrix}$ and $F=GS$ with $S=\begin{pmatrix}0&1&0\\0&0&1\\Y&0&0\end{pmatrix}$.
Computing $s_{ij}=\epsilon_{ij}-\sum_{k=1}^{t}e_kh_{ijk}$ for all $i<j$, we obtain:

$$s_{12}=(X^2-3X,-3Y^3-3,0),s_{13}=(2X,0,-Y^3-1),s_{23}=(0,2,-X-1).$$

And so

$$Ts_{12}=\begin{pmatrix}0\\X^2-3X\\-3Y^3-3\end{pmatrix},Ts_{13}=\begin{pmatrix}-Y^5-Y^2\\4X+2XY^3\\0\end{pmatrix},Ts_{23}=\begin{pmatrix}-XY^2-Y^2\\2X^2+2X\\2\end{pmatrix}.$$

Moreover, we have $\mathbf{I}_3-TS=\begin{pmatrix}1-Y^3&0&0\\2XY&0&0\\0&0&0\end{pmatrix}$. So, denoting the first column of $\mathbf{I}_3-TS$ by r_1, we have:

$$\begin{aligned}\mathrm{Syz}(F)&=\langle Ts_{12},Ts_{13},Ts_{23},r_1\rangle\\&=\langle\,{}^{\mathrm{t}}(-XY^2-Y^2,2X^2+2X,2),\\&\ {}^{\mathrm{t}}(-Y^5-Y^2,4X+2XY^3,0),\ {}^{\mathrm{t}}(0,X^2-3X,-3Y^3-3),\ {}^{\mathrm{t}}(1-Y^3,2XY,0)\rangle.\end{aligned}$$

7.6 Computing dynamically a generating set for syzygies of polynomials over Dedekind rings

Let $\mathbf{R}$ be a Dedekind ring and consider $f_1,\ldots,f_s\in\mathbf{R}[X_1,\ldots,X_n]\setminus\{0\}$. Our goal is to compute a generating set for $\mathrm{Syz}(f_1,\ldots,f_s)$. We have first to compute a dynamical Gröbner basis $G=\{(S_1,G_1),...,(S_k,G_k)\}$ for the ideal $\langle f_1,\ldots,f_s\rangle$ of $\mathbf{R}[X_1,\ldots,X_n]$. Denoting by $H_j=\{h_{j,1},...,h_{j,p_j}\}$ a generating set for $\mathrm{Syz}(f_1,\ldots,f_s)$ over $(S_j^{-1}\mathbf{R})[X_1,\ldots,X_n]$, $1\le j\le k$, for each $1\le i\le p_j$, there exists $d_{j,i}\in S_j$ such that $d_{j,i}h_{j,i}\in\mathbf{R}[X_1,\ldots,X_n]$. Under these hypotheses, we have:

Theorem 139. *(Syzygies over Dedekind rings) As an $\mathbf{R}[X_1,\ldots,X_n]$-module,*

$$\mathrm{Syz}(f_1,\ldots,f_s)=\langle d_{1,1}h_{1,1},\ldots,d_{1,p_1}h_{1,p_1},\ldots,d_{k,1}h_{k,1},\ldots,d_{k,p_k}h_{k,p_k}\rangle.$$

Proof. It is clear that $\langle d_{1,1}h_{1,1},\ldots,d_{1,p_1}h_{1,p_1},\ldots,d_{k,1}h_{k,1},\ldots,d_{k,p_k}h_{k,p_k}\rangle\subseteq\mathrm{Syz}(f_1,\ldots,f_s)$. For the converse, let $h\in\mathrm{Syz}(f_1,\ldots,f_s)$ over $\mathbf{R}[X_1,\ldots,X_n]$. It is also a syzygy for $(f_1,\ldots,f_s)$ over $(S_j^{-1}\mathbf{R})[X_1,\ldots,X_n]$ for each $1\le j\le k$. Hence, for some $d_j\in S_j$, $d_jh\in\langle d_{j,1}h_{j,1},\ldots,d_{j,p_j}h_{j,p_j}\rangle$ over $\mathbf{R}[X_1,\ldots,X_n]$. On the other hand, as $S_1,\ldots,S_k$ are comaximal multiplicative subsets of $\mathbf{R}$, there exist $\alpha_1,\ldots,\alpha_k\in\mathbf{R}$ such that $\sum_{j=1}^{k}\alpha_jd_j=1$.

From the fact that $h = \sum_{j=1}^{k} \alpha_j d_j h$, we infer that $h \in \langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k}\rangle$ over $\mathbf{R}[X_1, \ldots, X_n]$. □

A dynamical method for computing the syzygy module for polynomials over a Dedekind ring

Let $\mathbf{R}$ be a Dedekind ring and consider $f_1, \ldots, f_s \in \mathbf{R}[X_1, \ldots, X_n] \setminus \{0\}$. Our goal is to give a dynamical way of computing a generating set for $\mathrm{Syz}(f_1, \ldots, f_s)$. This method works like the case where the base ring is a Noetherian valuation ring (Paragraph 7.5). Here we add the Noetherian hypothesis so that the dynamical version of Buchberger's algorithm terminates. The only difference is when one has to handle two incomparable (under division) elements a, b in $\mathbf{R}$. In that situation, one should first compute $u, v, w \in \mathbf{R}$ such that

$$\begin{cases} ub = va \\ wb = (1-u)a. \end{cases}$$

Now, one opens two branches: the computations are pursued in $\mathbf{R}_u$ and $\mathbf{R}_{1+u\mathbf{R}}$.

7.7 Examples of dynamical computations

Example 140. $I = \langle f_1 = X^2 + 2X + 2,\ f_2 = 3,\ f_3 = 2X^2 + 11X - 3\rangle$ in $\mathbb{Z}[X]$.
As $LC(f_2)$ et $LC(f_3)$ are not comparable under division in $\mathbb{Z}$, we open two branches:

$$\begin{array}{ccc} & \mathbb{Z} & \\ \swarrow & & \searrow \\ \mathbb{Z}_3 & & \mathbb{Z}_2 \end{array}$$

In $\mathbb{Z}_3$: $\{f_2\}$ is a special Gröbner basis for $\langle f_1,\ f_2,\ f_3\rangle$. Letting $F = [f_1,\ f_2,\ f_3]$ and $G_1 = [f_2]$, we have $G_1 = FT$ with $T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $F = G_1 S$ with $S = \begin{pmatrix} \frac{1}{3}f_1 & 1 & \frac{1}{3}f_3 \end{pmatrix}$.
Note that, in this case, over $\mathbb{Z}_3[X]$, $\mathrm{Syz}(F) = \langle r_i,\ 1 \le i \le 3\rangle$, where the r_i are the columns of the matrix $\mathbf{I}_3 - TS = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{3}f_1 & 0 & -\frac{1}{3}f_3 \\ 0 & 0 & 1 \end{pmatrix}$. Thus, over $\mathbb{Z}_3[X]$,

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} 1 \\ -\frac{1}{3}f_1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -\frac{1}{3}f_3 \\ 1 \end{pmatrix} \rangle.$$

In $\mathbb{Z}_2$:

$$\begin{array}{l} S(f_1, f_2) = 3f_1 - X^2 f_2 = 6X + 6 \xrightarrow{f_2} 0, \\ S(f_2, f_3) = X^2 f_2 - \frac{3}{2}f_3 = -\frac{3}{2}(11X - 3) \xrightarrow{f_2} 0, \\ S(f_1, f_3) = f_1 - \frac{1}{2}f_3 = -\frac{7}{2}X + \frac{7}{2} =: f_4. \end{array}$$

Since $LC(f_2)$ and $LC(f_4)$ are not comparable under division in $\mathbb{Z}_2$, we open in $\mathbb{Z}_2$ two news branches:

$$\begin{array}{ccc} & \mathbb{Z}_2 & \\ \swarrow & & \searrow \\ \mathbb{Z}_{2.3} & & \mathbb{Z}_{2.7} \end{array}$$

In $\mathbb{Z}_{2.3}$: $\{f_2\}$ is a special Gröbner basis for $\langle f_1,\ f_2,\ f_3\rangle$ and we have, over $\mathbb{Z}_{2.3}[X]$,

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} 1 \\ -\frac{1}{3}f_1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -\frac{1}{3}f_3 \\ 1 \end{pmatrix} \rangle.$$

In $\mathbb{Z}_{2.7}$: A special Gröbner basis for $\langle f_1,\ f_2,\ f_3\rangle$ is $\{f_6 = -2 = (-1 - \frac{2}{7}X)f_1 + Xf_2 + \frac{1}{7}Xf_3\}$, and we have over $\mathbb{Z}_{2.7}[X]$,

$$\mathrm{Syz(F)} = \langle \begin{pmatrix} 1 - (\frac{1}{2} + \frac{1}{7}X)f_1 \\ \frac{1}{2}Xf_1 \\ \frac{1}{14}Xf_1 \end{pmatrix}, \begin{pmatrix} -(\frac{1}{2} + \frac{1}{7}X)f_2 \\ 1 + \frac{1}{2}Xf_2 \\ \frac{1}{14}Xf_2 \end{pmatrix}, \begin{pmatrix} -(\frac{1}{2} + \frac{1}{7}X)f_3 \\ \frac{1}{2}Xf_3 \\ 1 + \frac{1}{14}Xf_3 \end{pmatrix} \rangle.$$

Finally, over $\mathbb{Z}[X]$, we have

$$\mathrm{Syz(F)} = \langle \begin{pmatrix} 3 \\ -f_1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -f_3 \\ 3 \end{pmatrix}, \begin{pmatrix} 14-(7+2X)f_1 \\ 7Xf_1 \\ Xf_1 \end{pmatrix}, \begin{pmatrix} -(7+2X)f_2 \\ 14+7Xf_2 \\ Xf_2 \end{pmatrix}, \begin{pmatrix} -(7+2X)f_3 \\ 7Xf_3 \\ 14+Xf_3 \end{pmatrix} \rangle$$

$$= \langle \begin{pmatrix} 3 \\ -X^2-2X-2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -2X^2-11X+3 \\ 3 \end{pmatrix}, \begin{pmatrix} -2X^3-11X^2-18X \\ 7X^3+14X^2+14X \\ X^3+2X^2+2X \end{pmatrix}, \begin{pmatrix} -21-6X \\ 14+21X \\ 3X \end{pmatrix},$$

$$\begin{pmatrix} -4X^3-36X^2-71X+21 \\ 14X^3+77X^2-21X \\ 2X^3+11X^2-3X+14 \end{pmatrix} \rangle.$$

It is worth pointing out that at each leaf of the constructed dynamical tree, the corresponding special Gröbner basis contains a unit. This simply means that $1 \in \langle f_1, f_2, f_3 \rangle$, or, in other words, the vector ${}^{\mathrm{t}}(f_1, f_2, f_3)$ is unimodular. In particular, $\mathrm{Syz}(f_1, f_2, f_3)$ is rank 2 projective $\mathbb{Z}[X]$-module which is free by the Costa-Brewer-Maroscia Theorem 90. So the basis of $\mathrm{Syz}(f_1, f_2, f_3)$ we have obtained above is not **minimal**. Recall that in Example 58, we obtained

$$\mathcal{B} = (\begin{pmatrix} -3-43713x^2-510x-7182x^3 \\ 38529x^2+3591x^3+408x+2 \\ 9288x^2+3591x^3+66x \end{pmatrix}, \begin{pmatrix} 12+204092x^2+2975x+33516x^3 \\ -179851x^2-16758x^3-2429x-7 \\ -43393x^2-16758x^3-434x+1 \end{pmatrix})$$

as a free basis for $\mathrm{Syz}(f_1, f_2, f_3)$.

Example 141. Let $I = \langle f_1 = 8X^2Y + 1, f_2 = 10X^3 - 2 \rangle$ in $\mathbb{Z}[X, Y]$. Let us fix the lexicographic order with $X > Y$ as monomial order.
Since $8 \wedge 10 = 2,\ 8 = 2 \times 4$, and $10 = 2 \times 5$, we will open two branches: $\mathbb{Z}_4$ and $\mathbb{Z}_5$.

In $\mathbb{Z}_4$: $S(f_1, f_2) = \frac{5}{4}Xf_1 - Yf_2 = \frac{5}{4}X + 2Y =: f_3$. The leadings coefficients of f_1 and f_3 are not comparable under division. Since $8 \wedge \frac{5}{4} = 2 \wedge 5 = 1$, we open in $\mathbb{Z}_4$ two news branches $\mathbb{Z}_{4.2}$ and $\mathbb{Z}_{4.5}$.
In $\mathbb{Z}_{4.2}$:

$S(f_1, f_3) = \frac{5}{32}f_1 - XYf_3 = \frac{5}{32} - 2XY^2 =: f_4,$
$S(f_1, f_4) = Yf_1 + 4Xf_4 = \frac{1}{2}f_3 \xrightarrow{f_3} 0,$
$S(f_2, f_4) = Y^2f_2 + 5X^2f_4 = (\frac{5}{8}X - Y)f_3 \xrightarrow{f_3} 0,$
$S(f_3, f_4) = Y^2f_3 + \frac{5}{8}f_4 = 2Y^3 + \frac{25}{256} =: f_5,$
$S(f_1, f_5) = Y^2f_1 - 4X^2f_5 = (-\frac{5}{16}X + \frac{1}{2}Y)f_3 \xrightarrow{f_3} 0,$
$S(f_2, f_5) = Y^3f_2 - 5X^3f_5 = (-\frac{25}{64}X^2 + \frac{5}{8}XY - Y^2)f_3 \xrightarrow{f_3} 0,$
$S(f_3, f_5) = Y^3f_3 - \frac{5}{8}Xf_5 \xrightarrow{f_3} Yf_5 \xrightarrow{f_5} 0,$
$S(f_4, f_5) = Yf_4 + Xf_5 = \frac{5}{64}f_3 \xrightarrow{f_3} 0.$

Thus $G_1 = \{f_1, f_2, f_3, f_4, f_5\}$ is a special Gröbner basis for $\langle f_1, f_2 \rangle$ in $\mathbb{Z}_{4.2}[X, Y]$.
Seting $G = [f_1\ f_2\ f_3\ f_4\ f_5]$ and $F = [f_1\ f_2]$, we have $G = FT$ with

$$T = \begin{pmatrix} 1 & 0 & \frac{5}{4}X & \frac{5}{32} - \frac{5}{4}X^2Y & \frac{5}{4}XY^2 + \frac{25}{256} - \frac{25}{32}X^2Y \\ 0 & 1 & -Y & XY^2 & -Y^3 + \frac{5}{8}XY^2 \end{pmatrix} \text{ and } F = GS \text{ with } S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

we find

$s_{12} = {}^{\mathrm{t}}(\frac{5}{4}X, -Y, -1, 0, 0), s_{13} = {}^{\mathrm{t}}(\frac{5}{32}, 0, -XY, -1, 0), s_{23} = {}^{\mathrm{t}}(2, 1, -8X^2, 0, 0), s_{14} = {}^{\mathrm{t}}(Y, 0, -\frac{1}{2}, 4X, 0),$
$s_{24} = {}^{\mathrm{t}}(0, Y^2, -\frac{5}{8}X + Y, 5X^2, 0), s_{34} = {}^{\mathrm{t}}(0, 0, Y^2, \frac{5}{8}, -1), s_{15} = {}^{\mathrm{t}}(Y^2, 0, -\frac{5}{16}X + \frac{1}{2}Y, 0, -4X^2),$
$s_{25} = {}^{\mathrm{t}}(0, Y^3, \frac{25}{64}X^2 - \frac{5}{8}XY + Y^2, 0, -5X^3), s_{35} = {}^{\mathrm{t}}(0, 0, Y^3 + \frac{25}{512}, 0, -\frac{5}{8}X - Y), s_{45} = {}^{\mathrm{t}}(0, 0, -\frac{5}{64}, Y, X).$

And so

$$Ts_{12} = Ts_{13} = Ts_{34} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, Ts_{23} = \begin{pmatrix} 2-10X^3 \\ 1+8X^2 \end{pmatrix}, Ts_{14} = \begin{pmatrix} \frac{1}{2}Y(2-10X^2) \\ \frac{1}{2}Y(1+8X^2) \end{pmatrix},$$

$$Ts_{24} = \begin{pmatrix} \frac{5}{8}XY(2-10X^2) \\ \frac{5}{8}XY(1+8X^2) \end{pmatrix}, Ts_{15} = \begin{pmatrix} Y^2 - \frac{5}{8}XY - 5X^3Y^2 + \frac{25}{8}X^4Y \\ \frac{1}{2}Y^2 - \frac{5}{16}XY + 4X^2Y^3 - \frac{5}{2}X^3Y^2 \end{pmatrix},$$

$$Ts_{25} = \begin{pmatrix} -\frac{25}{32}X^2Y + \frac{5}{4}XY^2 - \frac{25}{4}X^4Y^2 + \frac{125}{32}X^5Y \\ -\frac{25}{64}X^2Y + \frac{5}{8}XY^2 + 5X^3Y^3 - \frac{25}{8}X^4Y^2 \end{pmatrix},$$

$$Ts_{35} = \begin{pmatrix} -\frac{25}{512}Y(2-10X^2) \\ -\frac{25}{512}Y(1+8X^2) \end{pmatrix}, Ts_{45} = \begin{pmatrix} \frac{5}{64}Y(2-10X^2) \\ \frac{5}{64}Y(1+8X^2) \end{pmatrix}.$$

We have $\mathbf{I}_2 - TS = 0 \Longrightarrow \text{Syz}(F) = \langle Ts_{ij}, 1 \leq i < j \leq 5 \rangle$. Thus, over $\mathbb{Z}_{4.2}[X,Y]$,

$$\text{Syz}(F) = \langle \begin{pmatrix} 2-10X^3 \\ 1+8X^2 \end{pmatrix}, \begin{pmatrix} Y^2 - \frac{5}{8}XY - 5X^3Y^2 + \frac{25}{8}X^4Y \\ \frac{1}{2}Y^2 - \frac{5}{16}XY + 4X^2Y^3 - \frac{5}{2}X^3Y^2) \end{pmatrix} \rangle.$$

Similarly, we obtain $G_2 = \{1+8X^2, 10X^3-2, \frac{5}{4}X+2Y, 1-\frac{64}{5}XY^2, 2Y^3+\frac{25}{256}\}$ as a special Gröbner basis for $\langle f_1, f_2 \rangle$ in $\mathbb{Z}_{4.5}[X,Y]$. Thus, over $\mathbb{Z}_{4.5}[X,Y]$,

$$\text{Syz}(F) = \langle \begin{pmatrix} 2-10X^3 \\ 1+8X^2Y \end{pmatrix}, \begin{pmatrix} Y^2 - \frac{5}{8}XY - 5X^3Y^2 + \frac{25}{8}X^4Y \\ -\frac{5}{16}XY + \frac{1}{2}Y^2 + 4X^2Y^3 - \frac{5}{2}X^3Y^2 \end{pmatrix} \rangle.$$

Also we obtain $G_3 = \{1+8X^2, 10X^3-2, X+\frac{8}{5}Y, 1-\frac{64}{5}XY^2, -\frac{512}{25}Y^3-1\}$ as a special Gröbner basis for $\langle f_1, f_2 \rangle$ in $\mathbb{Z}_5[X,Y]$ and, over $\mathbb{Z}_5[X,Y]$,

$$\text{Syz}(F) = \langle \begin{pmatrix} 2-10X^3 \\ 1+8X^2Y \end{pmatrix}, \begin{pmatrix} \frac{8}{5}XY - \frac{64}{25}Y^2 - 8X^4Y + \frac{64}{5}X^3Y2 \\ \frac{4}{5}XY - \frac{32}{25}Y^2 - \frac{256}{25}X^2Y^3 + \frac{32}{5}X^3Y^2 \end{pmatrix} \rangle.$$

Finally, we obtain over $\mathbb{Z}[X,Y]$ that

$$\text{Syz}(F) = \langle \begin{pmatrix} 2-10X^3 \\ 1+8X^2Y \end{pmatrix}, \begin{pmatrix} 16Y^2 - 10XY - 80X^3Y^2 + 50X^4Y \\ -5XY + 8Y^2 + 64X^2Y^3 - 40X^3Y^2 \end{pmatrix} \rangle.$$

Example 142. Let $I = \langle f_1 = 3XY + 1,\ f_2 = (4+2\theta)Y + 9 \rangle$ in $\mathbb{Z}[\theta][X,Y]$ where $\theta = \sqrt{-5}$.

Let us fix the lexicographic order with $X > Y$ as monomial order.

a) Computing a dynamical Gröbner basis and the syzygy module:

We will first compute a dynamical Gröbner basis for I in $\mathbb{Z}[\theta][X,Y]$. We will give all the details of the computations only for one leaf. Since $x_1 := 3$ and $x_2 := 4+2\theta$ are not comparable, we have to find $u, v, w \in \mathbb{Z}[\theta]$ such that:

$$\begin{cases} ux_2 = vx_1 \\ wx_2 = (1-u)x_1. \end{cases}$$

A solution of this system is given by: $u = 5+2\theta$, $v = 6\theta$, $w = -3$. Then we can open two branches:

$$\begin{array}{ccc} & \mathbb{Z}[\theta] & \\ \swarrow & & \searrow \\ \mathbb{Z}[\theta]_{4+2\theta} & & \mathbb{Z}[\theta]_{5+2\theta} \end{array}$$

In $\mathbb{Z}[\theta]_{5+2\theta}$:

$S(f_1, f_2) = \frac{6\theta}{5+2\theta} f_1 - X f_2 = -9X + \frac{6\theta}{5+2\theta} =: f_3,$
$S(f_1, f_3) = -3f_1 - Y f_3 = -\frac{6\theta}{5+2\theta} Y - 3 =: f_4,$
$S(f_1, f_4) = -\frac{2\theta}{5+2\theta} f_1 - X f_4 = 3X - \frac{2\theta}{5+2\theta} =: f_5,$
$f_2 \xrightarrow{f_4} 0,\ f_3 \xrightarrow{f_5} 0,$
$S(f_1, f_5) = f_1 - Y f_5 = \frac{2\theta}{5+2\theta} Y + 1 =: f_6,$
$f_4 \xrightarrow{f_6} 0,\ S(f_2, f_5) = X f_2 - \frac{6\theta}{5+2\theta} Y f_5 \xrightarrow{f_5, f_6} 0.$

As 2 and 3 are not comparable under division in $\mathbb{Z}[\theta]_{5+2\theta}$, we open two news branches:

$$\begin{array}{ccc} & \mathbb{Z}[\theta]_{5+2\theta} & \\ \swarrow & & \searrow \\ \mathbb{Z}[\theta]_{(5+2\theta).3} & & \mathbb{Z}[\theta]_{(5+2\theta).2} \end{array}$$

In $\mathbb{Z}[\theta]_{(5+2\theta).3}$:

$S(f_1, f_6) = \frac{2\theta}{3(5+2\theta)} f_1 - X f_6 = -\frac{1}{3} f_5 \xrightarrow{f_5} 0,$

$S(f_5, f_6) = \frac{2\theta}{3(5+2\theta)} Y f_5 - X f_6 = \frac{20}{3(5+2\theta)^2} Y - X \xrightarrow{f_5} \frac{20}{3(5+2\theta)^2} Y - \frac{2\theta}{3(5+2\theta)} \xrightarrow{f_6} 0.$

Thus, $G_1 = \{3XY + 1,\ 3X - \frac{2\theta}{5+2\theta},\ \frac{2\theta}{5+2\theta} Y + 1\}$ is a special Gröbner basis for $\langle 3XY + 1,\ (4 + 2\theta)Y + 9\rangle$ in $\mathcal{M}(5 + 2\theta, 3)^{-1}\mathbb{Z}[\theta] = \mathbb{Z}[\theta]_{(5+2\theta).3}$.

Denoting by $F = [f_1\ f_2]$ and $G = [g_1\ g_2\ g_3]$ with $g_1 = 3XY + 1$, $g_2 = 3X - \frac{2\theta}{5+2\theta}$, $g_3 = \frac{2\theta}{5+2\theta} Y + 1$, we have $G = FT$ with

$T = \begin{pmatrix} 1 & 3X - \frac{2\theta}{5+2\theta} + \frac{6\theta}{5+2\theta} XY & -3XY + \frac{2\theta}{5+2\theta} Y - \frac{6\theta}{5+2\theta} XY^2 + 1 \\ 0 & -X^2Y & X^2Y^2 \end{pmatrix}$, and $F = GS$ with $S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 9 \end{pmatrix}$.

$\mathbf{I}_2 - TS = \begin{pmatrix} 0 & 27XY - 9 - (4 + 2\theta)Y + 3(4 + 2\theta)XY^2 \\ 0 & 1 - 9X^2Y^2 \end{pmatrix},$

$r_1 = \begin{pmatrix} 27XY - 9 - (4 + 2\theta)Y + 3(4 + 2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \in \mathrm{Syz}(F),$

$s_{12} = {}^{\mathrm{t}}(1, -Y, -1), s_{13} = {}^{\mathrm{t}}(\frac{2\theta}{3(5+2\theta)}, \frac{1}{3}, -X), s_{23} = {}^{\mathrm{t}}(0, \frac{2\theta}{3(5+2\theta)} Y + \frac{1}{3}, -X + \frac{2\theta}{3(5+2\theta)}),$

$Ts_{12} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $Ts_{13} = \begin{pmatrix} 3X^2Y + \frac{4+2\theta}{3} X^2Y^2 \\ \frac{-1}{3} X^2Y - X^3Y^2 \end{pmatrix}$, and $Ts_{23} = Ts_{13}$. Thus, over $\mathbb{Z}[\theta]_{(5+2\theta).3}[X, Y]$,

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} 3X^2Y + \frac{4+2\theta}{3} X^2Y^2 \\ \frac{-1}{3} X^2Y - X^3Y^2 \end{pmatrix}, \begin{pmatrix} 27XY - 9 - (4 + 2\theta)Y + 3(4 + 2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle.$$

In $\mathbb{Z}[\theta]_{(5+2\theta).2}$:

$G_2 = \{3XY + 1,\ 3X - \frac{2\theta}{5+2\theta},\ \frac{2\theta}{5+2\theta} Y + 1\}$ is a special Gröbner basis for $\langle 3XY + 1,\ (4 + 2\theta)Y + 9\rangle$. Thus, over $\mathbb{Z}[\theta]_{(5+2\theta).2}[X, Y]$,

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} \frac{9X^2Y(5+2\theta+2\theta Y)}{2\theta} \\ \frac{-(5+2\theta)(3X^3Y^2+X^2Y)}{2\theta} \end{pmatrix}, \begin{pmatrix} 27XY - 9 - (4 + 2\theta)Y + 3(4 + 2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle.$$

In $\mathbb{Z}[\theta]_{(4+2\theta)}$:

$G_3 = \{3XY + 1,\ (4 + 2\theta)Y + 9,\ \frac{-27}{4+2\theta} X + 1\}$ is a special Gröbner basis for $\langle 3XY + 1,\ (4 + 2\theta)Y + 9\rangle$. Over $\mathbb{Z}[\theta]_{(4+2\theta)}[X, Y]$, we have

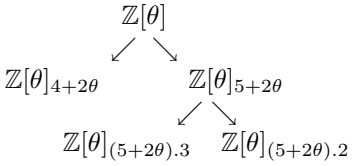
$$\mathrm{Syz}(F) = \langle \begin{pmatrix} -\frac{9}{4+2\theta} - Y \\ \frac{1}{4+2\theta} + \frac{3XY}{4+2\theta} \end{pmatrix} \rangle.$$

Finally, in $\mathbb{Z}[\theta]$: Over $\mathbb{Z}[\theta][X, Y]$, we have

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} -(4 + 2\theta)Y - 9 \\ 3XY + 1 \end{pmatrix}, \begin{pmatrix} 27XY - 9 - (4 + 2\theta)Y + 3(4 + 2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle$$

$$= \langle \begin{pmatrix} -(4 + 2\theta)Y - 9 \\ 3XY + 1 \end{pmatrix} \rangle.$$

As a conclusion, the dynamical evaluation of the problem of constructing a Gröbner basis for I produces the following evaluation tree:



The obtained dynamical Gröbner basis of I is

$$G = \{(\mathcal{M}(5 + 2\theta), G_1),\ (\mathcal{M}(4 + 2\theta), G_2)\}.$$

b) The ideal membership problem: Suppose that we have to deal with the ideal membership problem:

$f = (4\theta - 1)X^2Y + 6\theta XY^2 + 9\theta X^2 + 3X - 4Y - 9\ \in?\ I$

Let us first execute the dynamical division algorithm of f by $G_1 = \{f_1 = 3XY + 1,\ f_5 = -3X + \frac{2\theta}{5+2\theta},\ f_6 = \frac{2\theta}{5+2\theta}Y + 1\}$ in the ring $\mathbb{Z}[\theta]_{(5+2\theta).3}[X, Y]$.
With the same notations as in [24], one obtains:

q_1	q_5	q_6	p
$\frac{4\theta-1}{3}X$	0	0	$6\theta XY^2 + 9\theta X^2 + \frac{10-4\theta}{3}X - 4Y - 9$
$\frac{4\theta-1}{3}X + 2\theta Y$	0	0	$9\theta X^2 + \frac{10-4\theta}{3}X - (4 + 2\theta)Y - 9$
$\frac{4\theta-1}{3}X + 2\theta Y$	$-3\theta X$	0	$-(4 + 2\theta)Y - 9$
$\frac{4\theta-1}{3}X + 2\theta Y$	$-3\theta X$	-9	0

Thus, the answer to this ideal membership problem in the ring $\mathbb{Z}[\theta]_{(5+2\theta).3}[X, Y]$ is positive and one obtains:

$f = (\frac{4\theta-1}{3}X + 2\theta Y)f_1 - 3\theta X f_5 - 9f_6$.

But since

$f_5 = (\frac{-6\theta}{5+2\theta}XY - 3X + \frac{2\theta}{5+2\theta})f_1 - X^2Y f_2$, and
$f_6 = (\frac{-6\theta}{5+2\theta}XY^2 - 3XY + \frac{2\theta}{5+2\theta}Y + 1)f_1 - X^2Y^2 f_2$, one infers that

$$f = [\tfrac{-90}{5+2\theta}X^2Y + 9\theta X^2 + \tfrac{54\theta}{5+2\theta}XY^2 + 27XY + \tfrac{6\theta+15}{5+2\theta}X - 4Y - 9]f_1 + [3\theta X^3Y + 9X^2Y^2]f_2.$$

Seeing that 3 does not appear in the denominators of the relation above, we can say that we have a positive answer to our ideal membership problem in the ring $\mathbb{Z}[\theta]_{5+2\theta}[X, Y]$ without dealing with the leaf $\mathbb{Z}[\theta]_{(5+2\theta).2}$. Clearing the denominators, we get:

$$(5 + 2\theta)f = [-90X^2Y + 45(\theta - 2)X^2 + 54\theta XY^2 + 27(5 + 2\theta)XY + (6\theta + 15)X - 4(5 + 2\theta)Y - 9(5 + 2\theta)]f_1 + [15(\theta - 2)X^3Y + 9(5 + 2\theta)X^2Y^2]f_2. \qquad (A)$$

It remains to execute the dynamical division algorithm of f by $G_2 = \{f_1 = 3XY + 1,\ f_7 = -\frac{27}{4+2\theta}X + 1,\ f_8 = Y + \frac{9}{4+2\theta}\}$ in the ring $\mathbb{Z}[\theta]_{4+2\theta}[X, Y]$. The division is as follows:

q_1	q_7	q_8	p
0	0	$(4\theta - 1)X^2$	$6\theta XY^2 - \frac{81}{4+2\theta}X^2 + 3X - 4Y - 9$
$2\theta Y$	0	$(4\theta - 1)X^2$	$\frac{-81}{4+2\theta}X^2 + 3X - (4 + 2\theta)Y - 9$
$2\theta Y$	$3X$	$(4\theta - 1)X^2$	$-(4 + 2\theta)Y - 9$
$2\theta Y$	$3X$	$(4\theta - 1)X^2 - (4 + 2\theta)$	0

Thus, the answer to this ideal membership problem in the ring $\mathbb{Z}[\theta]_{4+2\theta}[X, Y]$ is positive and one obtains:

$f = 2\theta Y f_1 + 3X f_7 + ((4\theta - 1)X^2 - (4 + 2\theta))f_8$.

But since

$f_7 = f_1 - \frac{3}{4+2\theta}X f_2$, and
$f_8 = (Y + \frac{9}{4+2\theta})f_1 - \frac{3}{4+2\theta}XY f_2$, one infers that

$$(4 + 2\theta)f = [(14\theta - 44)X^2Y + 9(4\theta - 1)X^2 - 4(4 + 2\theta)Y + 3(4 + 2\theta)X - 9(4 + 2\theta)]f_1 + [-9X^2 - 3(4\theta - 1)X^3Y + 3(4 + 2\theta)XY]f_2. \qquad (B)$$

Using the Bezout identity $(5 + 2\theta) - (4 + 2\theta) = 1$, $(A) - (B) \Rightarrow$

$$f = [(46 - 14\theta)X^2Y + 9(\theta - 9)X^2 + 54\theta XY^2 + 27(5 + 2\theta)XY + 3X - 4Y - 9]f_1 + [3(9\theta - 11)X^3Y + 9(5 + 2\theta)X^2Y^2 + 9X^2 - 3(4 + 2\theta)XX]f_2,$$

a complete positive answer.

8 Some problems

Problem 143. (An algorithm for the divisors of monic polynomials and doubly monic Laurent polynomials [9, 71])
1) Prove constructively that for any ring $\mathbf{R}$, if $r^{n+1}y = r^n$ for some $r, y \in \mathbf{R}$ and $n \in \mathbb{N}$, then $r^2y - r$ is nilpotent and ry^n is idempotent. If, in addition, $\mathbf{R}$ is reduced then ry is idempotent and $r\mathbf{R} = (ry)\mathbf{R}$.

2) Let $\mathbf{R}$ be a reduced ring, and $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_dX^d \in \mathbf{R}[X]$ such that $fg = c_0 + c_1X + \cdots + c_mX^m$ with $c_m = 1$.

a) Prove that $a_n^{n+d-m+1}b_{m-n} = a_n^{n+d-m}$.

b) By induction on $n+d-m$, prove that there exists a direct sum decomposition $\mathbf{R} = \mathbf{R}_0 \oplus \cdots \oplus \mathbf{R}_m$ $(m \leq n)$ of $\mathbf{R}$ such that if $f = f_0 + \cdots + f_m$ is the decomposition of f with respect to the induced decomposition $\mathbf{R}[X] = \mathbf{R}_0[X] \oplus \cdots \oplus \mathbf{R}_m[X]$, then the degree coefficient of f_i is a unit of $\mathbf{R}_i$ for each i.

3) Prove that if $\mathbf{R}$ is a non necessarily reduced ring, then $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{R}[X]$ divides a monic polynomial if and only if there exist a nilpotent polynomial N and a direct sum decomposition $\mathbf{R} = \mathbf{R}_0 \oplus \cdots \oplus \mathbf{R}_m$ $(m \leq n)$ of $\mathbf{R}$ such that if $f - N = f_0 + \cdots + f_m$ is the decomposition of $f - N$ with respect to the induced decomposition $\mathbf{R}[X] = \mathbf{R}_0[X] \oplus \cdots \oplus \mathbf{R}_m[X]$, then the degree coefficient of f_i is a unit of $\mathbf{R}_i$ for each i.

4) Deduce that if $\mathbf{R}$ is a non necessarily reduced ring, then $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{R}[X]$ divides a monic polynomial if and only if $\langle a_0, \ldots, a_n\rangle = \mathbf{R}$ and, for each $j \in \{0, \ldots, n\}$, we can find $\beta_j \in \mathbf{R}$ and $k_j \in \mathbb{N}$ such that $(a_j(a_j\beta_j - 1))^{k_j} \equiv 0 \bmod \langle a_{j+1}, \ldots, a_n\rangle$.

5) Let U and V be two indeterminates over a field $\mathbf{K}$, and consider the reduced ring $\mathbf{R} = \mathbf{K}[U, V]/\langle U^2 - U, UV\rangle = \mathbf{K}[u, v] = \mathbf{K}[v] \oplus \mathbf{K}[v]u$, where $u^2 = u$ and $uv = 0$. Take $f = u - (1 + u)X^2 + uX^3$ and $g = v + uX^2 + (u - 1)X^3$. Verify that $fg = (u - v)X^2 - 2uX^4 + X^5$. Using the algorithm coming out of your constructive proof of Question 2), find the corresponding decomposition of f.

6) Recall that a Laurent polynomial $f \in \mathbf{R}[X, X^{-1}]$ is said to be *doubly monic* if the coefficients of the highest and lowest terms are equal to 1.

a) Prove that for any ring $\mathbf{R}$, $f \in \mathbf{R}[X, X^{-1}]$ divides a doubly monic Laurent polynomial if and only if there exist $n, m \in \mathbb{N} \setminus \{0\}$ such that both $X^n f(X)$ and $X^m f(X^{-1})$ divide a monic polynomial.

b) Deduce that if $\mathbf{R}$ is a reduced ring, then $f \in \mathbf{R}[X, X^{-1}]$ divides a doubly monic Laurent polynomial if and only if there exists a direct sum decomposition $\mathbf{R} = \mathbf{R}_0 \oplus \cdots \oplus \mathbf{R}_m$ of $\mathbf{R}$ such that if $f = f_0 + \cdots + f_m$ is the decomposition of f with respect to the induced decomposition $\mathbf{R}[X, X^{-1}] = \mathbf{R}_0[X, X^{-1}] \oplus \cdots \oplus \mathbf{R}_m[X, X^{-1}]$, then the coefficients of the highest and lowest terms of f_i are units in $\mathbf{R}_i$ for each i.

c) Deduce that if $\mathbf{R}$ is a reduced ring, then $f = a_kX^k + a_{k+1}X^{k+1} + \cdots + a_lX^l \in \mathbf{R}[X, X^{-1}]$, $k, l \in \mathbb{Z}$, divides a doubly monic Laurent polynomial if and only if $\langle a_k, \ldots, a_l\rangle = \mathbf{R}$ and, for each $j \in \{k, \ldots, l\}$, we can find $\beta_j, \delta_j \in \mathbf{R}$ and $m_j, n_j \in \mathbb{N}$ such that $(a_j(a_j\beta_j - 1))^{m_j} \equiv 0 \bmod \langle a_{j+1}, \ldots, a_n\rangle$ and $(a_j(a_j\delta_j - 1))^{n_j} \equiv 0 \bmod \langle a_k, \ldots, a_{j-1}\rangle$.

7) For any ring $\mathbf{R}$, $\mathbf{R}\langle X, X^{-1}\rangle$ will denote the localization of $\mathbf{R}[X, X^{-1}]$ at doubly monic polynomials.

a) Prove that $\mathbf{R}\langle X, X^{-1}\rangle = \mathbf{R}\langle X\rangle \cap R\ \langle X^{-1}\rangle$.

b) Prove that $R\langle X^{-1} + X\rangle \subsetneq R\langle X, X^{-1}\rangle$ (one may consider the polynomial $X^{-1} + X^2$).

c) Prove that for any doubly monic Laurent polynomial $g \in \mathbf{R}[X, X^{-1}]$, there exists $h \in \mathbf{R}[X, X^{-1}]$ such that gh is a monic polynomial at $X^{-1} + X$.

d) Prove that for any ring $\mathbf{R}$, $\mathbf{R}[X, X^{-1}]$ is a finitely generated free $\mathbf{R}[X^{-1} + X]$-module (with $(1, X)$ as basis).

e) Deduce that for any ring $\mathbf{R}$, $\mathbf{R}\langle X, X^{-1}\rangle$ is a finitely generated free $R\langle X^{-1} + X\rangle$-module (with $(1, X)$ as basis).

Problem 144. (Stably free modules over Laurent polynomial rings [5, 6])
1) (An analogue of Proposition 47 for Laurent polynomials) Prove constructively that for any ring $\mathbf{R}$, and $u, v \in \mathbf{R}[X]$ with u doubly monic, we have the equivalence:

$$\langle u, v\rangle = \langle 1\rangle \text{ in } \mathbf{R}[X, X^{-1}] \quad \Longleftrightarrow \quad \mathrm{Res}_X(u, v) \in \mathbf{R}^\times.$$

2) (An analogue of Theorem 48 for Laurent polynomials) If $f \in \mathbf{R}[X, X^{-1}]$, a minimal shifted version of f is $\widetilde{f} = X^n f \in \mathbf{R}[X]$ where $n \in \mathbb{Z}$ is the minimal possible. For example a minimal shifted version of $X^{-3} + X + X^2$ is $1 + X^4 + X^5$, a minimal shifted version of $X^2 + X^4$ is $1 + X^2$.

Prove constructively that for any ring $\mathbf{R}$, if $\langle v_1(X), \ldots, v_n(X)\rangle = \mathbf{R}[X, X^{-1}]$ where v_1 is doubly monic and $n \geq 3$, then there exist $\gamma_1, \ldots, \gamma_s \in \mathrm{E}_{n-1}(\mathbf{R}[X])$ such that:

$$\langle \mathrm{Res}(\widetilde{v}_1, e_1.\gamma_1\, {}^{\mathrm{t}}(\widetilde{v}_2, \ldots, \widetilde{v}_n)), \ldots, \mathrm{Res}(\widetilde{v}_1, e_1.\gamma_s\, {}^{\mathrm{t}}(\widetilde{v}_2, \ldots, \widetilde{v}_n))\rangle = \mathbf{R}.$$

In particular $1 \in \langle \widetilde{v}_1, \ldots, \widetilde{v}_n\rangle$ in $\mathbf{R}[X]$. Here $e_1.x$, where x is a column vector, stands for the first coordinate of x, and $\widetilde{v}_i$ is a shifted version of v_i.

3) (An analogue of Theorem 52 for Laurent polynomials) Let $\mathbf{R}$ be a ring, $v_1, \ldots, v_n, u_1, \ldots, v_n \in \mathbf{R}[X, X^{-1}]$ such that $\sum_{i=1}^n u_i v_i = 1$, v_1 doubly monic, and $n \geq 3$. Denote by $\ell = \deg v_1$, $s = (n-2)\,\ell + 1$, and suppose that $\mathbf{R}$ contains a set $E = \{y_1, \ldots, y_s\}$ such that $y_i - y_j$ is invertible for each $i \neq j$. For each $1 \leq r \leq n$ and $1 \leq i \leq s$, let $\widetilde{v}_r$ be a minimal shifted version of v_r and denote by $r_i = \mathrm{Res}_X(\widetilde{v}_1, \widetilde{v}_2 + y_i\widetilde{v}_3 + \cdots + y_i^{n-2}\widetilde{v}_n)$. Prove constructively that $\langle r_1, \ldots, r_s\rangle = \mathbf{R}$, that is, there exist $\alpha_1, \ldots, \alpha_s \in \mathbf{R}$ such that $\alpha_1 r_1 + \cdots + \alpha_s r_s = 1$. In particular $1 \in \langle \widetilde{v}_1, \ldots, \widetilde{v}_n\rangle$ in $\mathbf{R}[X]$. Moreover, let us suppose that $\mathbf{R}$ is a polynomial ring in a finite number of variables over a basic ring $\mathbf{T}$ and that $\max_{1\leq i\leq n}\{\deg u_i\} \leq D$, $1 + \max_{1\leq i\leq n}\{\deg v_i\} \leq d$ (where $d \geq 2$). Prove that for each $1 \leq i \leq s$, $\deg(\alpha_i) \leq \frac{d^4}{16}(d + D + 2)^2$ and $\deg(\alpha_i r_i) \leq \frac{d^4}{16}(d + D + 3)^2$ (here, by degree we mean total degree).

4) (Producing doubly monic Laurent polynomials over a field)

a) Let $\mathbf{K}$ be a field and consider $f = \sum_{i=1}^t a_i X^{n_i} Y^{m_i}$, $a_i \in \mathbf{K}$, where t is the number of monomials appearing in f. Set

$$E = \{\frac{m_j - m_i}{n_i - n_j},\ 1 \leq i, j \leq t,\ n_i \neq n_j\}.$$

Prove that for each $\alpha \in \mathbb{Z}\backslash E$, denoting φ_α the change of variables $(X, Y) \mapsto (XY^\alpha, Y)$, the correspondence $X^{n_i}Y^{m_i} \mapsto \deg_Y(\varphi_\alpha(X^{n_i}Y^{m_i}))$ is a one-to-one. In particular, $\varphi_\alpha(f)$ is doubly monic at Y (here, in order to lighten he notations, doubly monic means that the coefficients of the highest and lowest terms are invertible). Moreover, if the total degree of f is $\leq d$, and if $\alpha_0 \in \mathbb{Z}$ is such that $|\alpha_0| = \min\{|\ell|,\ \ell \in \mathbb{Z} \setminus E\}$, then $|\alpha_0| \leq d$.

b) Take $f = Y + Y^2 + Y^3 + X + XY + X^2Y + X^2Y^2$. Compute E, α_0, $\varphi_{\alpha_0}(X, Y)$, and $\varphi_{\alpha_0}(f)$.

c) What can you say about the general case (more than two variables) ?

d) From Questions 3), 4) and Agorithm 55, deduce an algorithm for unimodular completion over a Laurent polynomial ring $\mathbf{K}[X_1^{\pm 1}, X_2^{\pm 1} \ldots, X_k^{\pm 1}]$, where $\mathbf{K}$ is an infinite field.

5) (An analogue of Lemma 103 for Laurent polynomials) Let $\mathbf{R}$ be a ring and I an ideal of $\mathbf{R}[X, X^{-1}]$ containing a doubly monic polynomial. Prove constructively that if J is an ideal of $\mathbf{R}$ such that $I + J[X, X^{-1}] = \mathbf{R}[X, X^{-1}]$, then $(I \cap \mathbf{R}) + J = \mathbf{R}$.

6) (An analogue of Lemma 107 for Laurent polynomials) Let ${}^{\mathrm{t}}(v_0(X), v_1(X), \ldots, v_n(X)) \in \mathrm{Um}_{n+1}(\mathbf{R}[X, X^{-1}])$, where $\mathbf{R}$ is an integral local ring of Krull dimension ≤ 1 and $n \geq 2$. Prove constructively that

$${}^{\mathrm{t}}(\widetilde{v}_0(X), \widetilde{v}_1(X), \ldots, \widetilde{v}_n(X)) \sim_{\mathrm{E}_{n+1}(\mathbf{R}[X])} {}^{\mathrm{t}}(w_0(X), w_1(X), \ldots, c_2, \ldots, c_n),$$

where the c_i's are constant for $i \geq 2$, $w_i \in \mathbf{R}[X]$ with $\deg\ w_1(X) \leq 1$.

7) Prove constructively that for any ring $\mathbf{R}$, if $\mathrm{Kdim}\,\mathbf{R} \leq 0$, then $\mathbf{R}(X) = \mathbf{R}\langle X\rangle = \mathbf{R}\langle X, X^{-1}\rangle$. Moreover, $\mathrm{Kdim}\,\mathbf{R}(X) = \mathrm{Kdim}\,\mathbf{R}\langle X\rangle = \mathrm{Kdim}\,\mathbf{R}\langle X, X^{-1}\rangle \leq 0$.

8) (An analogue of Corollary 109 for Laurent polynomials) Deduce from the previous questions that for any integral local ring $\mathbf{R}$ of Krull dimension ≤ 1 and $n \geq 2$, $\mathrm{GL}_{n+1}(\mathbf{R}[X, X^{-1}])$ acts transitively on $\mathrm{Um}_{n+1}(\mathbf{R}[X, X^{-1}])$ and thus that all finitely generated stably free modules over $\mathbf{R}[X, X^{-1}]$ are free.

Problem 145. (A converse to Rabinowitsch's trick)

1) (Rabinowitsch's trick) Prove that for any ring $\mathbf{R}$ and $b, a_1, \ldots, a_r \in \mathbf{A}$, we have the equivalence:

$$b \in \sqrt{\langle a_1, \ldots, a_r\rangle} \text{ in } \mathbf{R} \ \Leftrightarrow\ 1 \in \langle a_1, \ldots, a_r, bX - 1\rangle \text{ in } \mathbf{R}[X].$$

We will say that a ring $\mathbf{B}$ is equipped with a unimodularity test if given $f_1, \ldots, f_n \in \mathbf{B}$, there is an algorithm to determine whether $1 \in \langle f_1, \ldots, f_n\rangle$ and if it is, to compute $g_1, \ldots, g_n \in \mathbf{B}$ such that $1 = f_1 g_1 + \cdots + f_n g_n$.

We will also say that a ring $\mathbf{A}$ is equipped with a radical ideal membership test if given $b, a_1, \ldots, a_s \in \mathbf{A}$, there is an algorithm to determine whether $b \in \sqrt{\langle a_1, \ldots, a_s \rangle}$ and if it is, to compute $m \in \mathbb{N}$, $b_1, \ldots, b_s \in \mathbf{A}$ such that $b^m = b_1 a_1 + \cdots + b_s a_s$. The goal of this problem is to show, using Suslin's lemma (Theorem 48), that for any ring $\mathbf{R}$, *having a unimodularity test in* $\mathbf{R}[X]$ $\Leftrightarrow$ *having a radical ideal membership test in* $\mathbf{R}$.

2) (Case $n = 1$) Prove that for any ring $\mathbf{R}$,

$$v_1 = a_0 X^s + \cdots + a_s \in \mathbf{R}[X]^\times \;\Leftrightarrow\; a_s \in \mathbf{R}^\times \text{ and } a_0, \ldots, a_{s-1} \in \sqrt{(0)}.$$

3) (Case $n = 2$, Generalization of Proposition 47) Let $\mathbf{R}$ be a ring and consider $v_1 = a_0 X^s + \cdots + a_s$, $v_2 = b_0 X^m + \cdots + b_m$ with $a_i, b_j \in \mathbf{R}$, and $0 \le k \le \min(m, s)$. Define $r_k := \mathrm{Res}(a_k X^{s-k} + \cdots + a_s,\, b_k X^{m-k} + \cdots + b_m)$ (the polynomials being taken respectively of formal degrees $s-k$ and $m-k$), that is, r_k is the determinant of the following $(m+s-2k) \times (m+s-2k)$ matrix:

$$S_k = \begin{pmatrix}
a_k & & & & b_k & & & \\
a_{k+1} & a_k & & & b_{k+1} & b_k & & \\
a_{k+2} & a_{k+1} & \ddots & & b_{k+2} & b_{k+1} & \ddots & \\
\vdots & & \ddots & a_k & \vdots & & \ddots & b_k \\
 & \vdots & & a_{k+1} & & \vdots & & b_{k+1} \\
a_s & & & & b_m & & & \\
 & a_s & & \vdots & & b_m & & \vdots \\
 & & \ddots & & & & \ddots & \\
 & & & a_s & & & & b_m
\end{pmatrix}.$$

$$\underbrace{\qquad\qquad}_{m-k \text{ columns}} \quad \underbrace{\qquad\qquad}_{s-k \text{ columns}}$$

Prove constructively that $1 \in \langle v_1, v_2 \rangle \;\Leftrightarrow\; 1 \in \langle a_s, b_m \rangle$ and $\forall\, 0 \le k \le \min(m, s),\; a_k, b_k \in \sqrt{\langle r_0, \ldots, r_k \rangle}$.

4) (Case $n \ge 3$) Let $\mathbf{R}$ be a ring and $v_1, \ldots, v_n \in \mathbf{R}[X] \setminus \{0\}$ with $n \ge 3$. Denote by a be the leading coefficient of v_1.

a) Prove that $1 \in \langle v_1, v_2 \ldots, v_n \rangle$ if and only if there exist $\gamma_1, \ldots, \gamma_\ell \in \mathrm{E}_{n-1}(\mathbf{R}[X])$ such that, denoting $r_i := \mathrm{Res}(v_1, e_1.\gamma_i\, {}^{\mathrm{t}}(v_2, \ldots, v_n))$, we have $a \in \sqrt{\langle r_1, \ldots, r_\ell \rangle}$.

b) Deduce an algorithm producing from an ideal membership test in $\mathbf{R}$, a unimodularity test in $\mathbf{R}[X]$.

Problem 146. (Seminormality following Coquand [18])

1) Let $\mathbf{R}$ be a ring and $M \in \mathbf{R}^{n \times n}$. Prove that the matrix M is idempotent with rank r free image if and only if there exist $X \in \mathbf{R}^{n \times r}$ and $Y \in \mathbf{R}^{r \times n}$ such that $Y X = \mathrm{I}_r$ and $M = X Y$. Moreover,

a) $\mathrm{Im}\, M = \mathrm{Im}\, X \simeq \mathrm{Im}\, Y$.

b) For all matrices X', Y' with the same sizes as X and Y and such that $M = X' Y'$, there exists a unique matrix $U \in \mathrm{GL}_r(\mathbf{R})$ such that $X' = U X$ and $Y = U Y'$ (in fact, $U = Y X'$, $U^{-1} = Y' X$, $Y' X' = \mathrm{I}_r$, and the columns of X' form a free basis of $\mathrm{Im}\, M$).

c) Reformulate this result in case $r = 1$.

2) Let $\mathbf{R}$ be a ring and $M \in \mathbf{R}^{n \times n}$ with $M^2 = M$. Prove that $\mathrm{Im}\, M$ has rank one if and only if M has trace one and all 2×2 minors of M are zero.

3) Prove that for any ring $\mathbf{R}$, the natural homomorphism $\mathrm{Pic}\, \mathbf{R} \;\to\; \mathrm{Pic}\, \mathbf{R}[X]$ is an isomorphism (in short, $\mathrm{Pic}\, \mathbf{R} = \mathrm{Pic}\, \mathbf{R}[X]$) if and only if for every rank one idempotent matrix $M = (m_{i,j})_{1 \le i,j \le n}$ over $\mathbf{R}[X]$ such that $M(0) = \begin{pmatrix} 1 & 0 \\ 0 & 0_{n-1} \end{pmatrix} =: \mathrm{I}_{n,1}$ there exist $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{R}[X]$ such that $m_{i,j} = f_i g_j$ for all i, j.

4) A ring $\mathbf{R}$ will be called *seminormal* if for every b, $c \in \mathbf{R}$ satisfying $b^2 = c^3$ there exists $a \in \mathbf{R}$ such that $a^3 = b$ and $a^2 = c$.

a) Prove that seminormal $\Rightarrow$ reduced.

b) (Schanuel's example) Let $\mathbf{R}$ be a reduced ring such that $\operatorname{Pic}\mathbf{R} = \operatorname{Pic}\mathbf{R}[X]$. Let b, $c \in \mathbf{R}$ satisfying $b^2 = c^3$. Consider $\mathbf{T} = \mathbf{R}[a] = \mathbf{R} + a\mathbf{R}$ a reduced ring containing $\mathbf{R}$ with $a^3 = b$ and $a^2 = c$ (one can take for example $\mathbf{T} = (\mathbf{R}[T]/\langle T^2 - c, T^3 - b\rangle)_{\mathrm{red}}$). Consider the matrix $M(X) = (f_i g_j)_{1\leq i,j\leq 2}$ with $f_1 = 1 + aX$, $f_2 = cX^2 = g_2$ and $g_1 = (1-aX)(1+cX^2)$, that is, $M(X) = \begin{pmatrix} (1-a^2X^2)(1+cX^2) & (1+aX)cX^2 \\ (1-aX)(1+cX^2)cX^2 & c^2X^4 \end{pmatrix}$.

Verify that $M(X)$ is rank one idempotent. Deduce that $a \in \mathbf{R}$.

c) Prove that a gcd domain is seminormal.

(Hints: Use 1.c). Consider a rank one idempotent matrix $(m_{i,j})_{1\leq i,j\leq n}$. Suppose that $m_{1,1}$ is regular and consider the gcd f of the elements on the first row.)

5) Prove that if $\mathbf{R}$ is seminormal and $\mathbf{T}$ is a reduced extension of $\mathbf{R}$ then the conductor of $\mathbf{T}$ in $\mathbf{R}$ (i.e., $\{r \in \mathbf{R} \mid r\mathbf{T} \subseteq \mathbf{R}\}$) is a radical ideal of $\mathbf{T}$.

6) Let $\mathbf{R} \subseteq \mathbf{T}$ with $\mathbf{T} = \mathbf{R}[c_1, \ldots, c_q]$ reduced and finite over $\mathbf{R}$. Let I be the conductor of $\mathbf{T}$ in $\mathbf{R}$ and suppose that it is a radical ideal. Prove that I is equal to $\{r \in \mathbf{R} \mid rc_1, \ldots, rc_q \in \mathbf{R}\}$.

7) Let $\mathbf{R}$ be a seminormal domain. Our purpose is to prove that $\operatorname{Pic}\mathbf{R} = \operatorname{Pic}\mathbf{R}[X]$ (the Traverso-Querré theorem). Let $M(X) = (m_{i,j}(X))_{1\leq i,j\leq n}$ be a rank one idempotent matrix over $\mathbf{R}[X]$ such that $M(0) = \mathrm{I}_{n,\,1}$. Denote by $\mathbf{F}$ the field of fractios of $\mathbf{R}$. By 4.a) we know that there exist $f_1, \ldots, f_n, g_1, \ldots, g_n \in \mathbf{F}[X]$ such that $m_{i,j} = f_i g_j$ for all i, j (note that $f_1(0) = g_1(0) = 1$). Let us denote by $\mathbf{T}$ the subring of $\mathbf{F}$ generated by $\mathbf{R}$ and the coefficients of the f_i's and the g_j's and by I the conductor of $\mathbf{T}$ in $\mathbf{R}$. Our goal is to prove that $\mathbf{T} = \mathbf{R}$, or equivalently, $1 \in I$.

Let us first recall **Kronecker's theorem**: *Let* $\mathbf{A}$ *be a ring,* $f, g \in \mathbf{A}[X]$ *and* $h = fg$. *Let* a *be a coefficient of* f *and* b *a coefficient of* g. *Then* ab *is integral over the subring of* $\mathbf{A}$ *generated by the coefficients of* h.

a) Prove that $\mathbf{T}$ is a finitely generated $\mathbf{R}$-module.

b) By way of contradiction, we will suppose that $1 \notin I$. Consider a minimal prime ideal $\mathfrak{p}$ of $\mathbf{R}$ over I (that is, $\mathfrak{p}/I$ is a minimal prime ideal of $\mathbf{R}/I$). Denote by $S = \mathbf{R} \setminus \mathfrak{p}$ and S' the image of S in $\mathbf{R}/I$. We have that $\mathbf{R}/I$ is a reduced ring, $(\mathbf{R}/I)_{S'} =: \mathrm{L}$ is a field contained in the reduced ring $(\mathbf{T}/I)_{S'}$.

Using Question 6, find a contradiction (there exists $s \in S$ such that $s \in \mathfrak{p}$).

c) Being inspired by the method explained in Subsection 3.4, find a method for eliminating the use of minimal prime ideals in the proof above (it will be a dual method for eliminating maximal ideals: maximal ideal $\mathfrak{m} \leftrightarrow$ minimal prime ideal $\mathfrak{p}$, $\mathbf{R}/\mathfrak{m} \leftrightarrow (\mathbf{R}/\mathfrak{p})_{\overline{\mathfrak{p}}}$). Infer a general method "by backtracking" for making the use of minimal prime ideals constructive (it will be a dual method to Elimination of maximal ideals by backtracking 51).

References

[1] Adams W.W., Laustaunau P. *An introduction to Gröbner bases.* Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] Aschenbrenner M. *Ideal membership in polynomial rings over the integers.* J. Amer. Math. Soc. **17** (2004), 407-441.

[3] Ayoub C. *On constructing bases for ideals in polynomial rings over the integers.* J. Number theory **17** (1983), no. 2, 204-225.

[4] Amidou M., Hadj Kacem A., Yengui I. *A dynamical method for computing the syzygy module over polynomials with coefficients in a Dedekind ring.* Preprint (2007).

[5] Amidou M., Mnif A., Yengui I. *Stably free modules over Laurent polynomial rings.* Preprint (2008).

[6] Amidou M., Yengui I. *An algorithm for unimodular completion over Laurent polynomial rings.* Linear Algebra Appl, to appear.

[7] Barhoumi S., Lombardi H. *An algorithm for the Traverso-Swan theorem over seminormal rings.* J. Algebra **320** (2008) 1531–1542.

[8] Barhoumi S., Lombardi H., Yengui I. *Projective modules over polynomial rings: a constructive approach.* Math. Nachr., to appear.

[9] Barhoumi S., Yengui I. *On a localization of the Laurent polynomial ring.* JP. Algebra, Number Theory and Appl. 5 **(3)** (2005) 591-602.

[10] Bass H. *Libération des modules projectifs sur certains anneaux de polynômes*, Sém. Bourbaki 1973/74, exp. 448, Lecture Notes in Math., vol. 431, Springer-Verlag, Berlin and New York (1975) 228-254.

[11] Basu S., Pollack R., Roy M.-F. *Algorithms in real algebraic geometry.* Second edition. Algorithms and Computation in Mathematics, 10. Springer-Verlag, Berlin, 2006.

[12] Bourbaki N. *" Algèbre commutative", Chapitres 5-6.* Masson, Paris, 1985.

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

[14] Byrne E., Fitzpatrick P. *Gröbner bases over Galois rings with an application to decoding alternant codes.* J. Symbolic Comput. **31** (2001) 565-584.

[15] Cahen P.-J. *Construction B,I,D et anneaux localement ou résiduellement de Jaffard.* Archiv. Math. **54** (1990) 125-141.

[16] Cahen P.-J., Elkhayyari Z., Kabbaj S. *Krull and valuative dimension of the Serre conjecture ring $R\langle n\rangle$.* Lect. Not. Pure and Appl. Math. **185** (1997) 173-185.

[17] Buchberger B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen polynomideal.* Ph.D. thesis, University of Innsbruck, Austria, 1965.

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

[19] Coquand T. *A refinement of Forster's theorem.* Preprint (2007).

[20] 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.

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

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

[23] 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.

[24] Cox D., Little J., O'Shea D. *Ideals, varieties and algorithms*, 2^{nd} edition. New York, Springer-Verlag, 1997.

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

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

[27] Duval D., Reynaud J-C. *Sketches and computation (Part II) Dynamic evaluation and applications.* Mathematical Structures in computer Sciences **4** (1994), 239–271.

(see http://www.Imc.imag.fr/Imc-cf/Dominique.Duval/evdyn.html)

[28] Ellouz A., Lombardi H., Yengui I. *A constructive comparison of the rings $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$ and application to the Lequain-Simis induction theorem*, J. Algebra **320** (2008) 521-533.

[29] Fitchas N., Galligo A. *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel.* Math. Nachr. **149** (1990) 231–253.

[30] Gallo S., Mishra B. *A solution to Kronecker's problem.* Appl. Algebra in Engrg. Comm. Comput. **5** (1994) 343-370.

[31] Glaz S. *Finite conductor properties of $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$.* Ideal theoretic methods in commutative algebra (Columbia, MO, 1999). Lecture Notes in Pure and Appl. Math., 220. Dekker, New York (2001) 231–249.

[32] Greuel G.M., Pfister G. *A Singular introduction to commutative algebra.* Springer Verlag Berlin, Heidelberg, New York, 2002.

[33] Hadj Kacem A., Yengui I. *Dynamical Gröbner bases over Dedekind rings.* 2006. (Preprint).

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

[35] Huckaba J. *Commutative rings with zero-divisors.* Marcel Dekker, 1988.

[36] Kandry-Rody A., Kapur D. *Computing a Gröbner basis of a polynomial ideal over a Euclidean domain.* J. Symbolic Comput. **6** (1988) no. 1, 37-57.

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

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

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

[40] 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.

[41] Logar A., Sturmfels B. *Algorithms for the Quillen-Suslin theorem.* J. Algebra **145** no. 1 (1992) 231–239.

[42] 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.

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

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

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

[46] Lombardi H. *Hidden constructions in abstract algebra (1) Integral dependance relations.* J. Pure Appl. Algebra **167** (2002) 259–267.

[47] 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.

[48] 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.

[49] 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.

[50] Lombardi H., Quitté C. *Seminormal rings (following Thierry Coquand).* Theoretical Computer Science **392** (2008) 113-127.

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

[52] Lombardi H., Quitté C., Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* J. Pure Appl. Algebra **212** (2008) 1575–1582.

[53] Lombardi H., Yengui I. *Suslin's algorithms for reduction of unimodular rows.* J. Symb. Comp. **39** (2005) 707–717.

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

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

[56] Mnif A., Yengui I. *An algorithm for unimodular completion over Noetherian rings.* J. Algebra **316** (2007) 483-498.

[57] Mora T. *Solving Polynomial Equation Systems I: The Kronecker-Duval Philosophy.* Cambridge University Press (2003)

[58] Norton G.H., Salagean A. *Strong Gröbner bases and cyclic codes over a finite-chain ring.* Applicable algebra in engineering, communication and computing, **10** (2000) 489-506.

[59] Norton G.H., Salagean A. *Strong Gröbner bases for polynomials over a principal ideal ring.* Bull. of the Australian Mathematical Soc., **64** (2001) 505-528.

[60] Norton G.H., Salagean A. *Gröbner bases and products of coefficient rings.* Bull. of the Australian Mathematical Soc., **65** (2002) 145-152.

[61] Norton G.H., Salagean A. *Cyclic codes and minimal strong Gröbner bases over a principal ideal ring.* Finite fields and their applications, **9** (2003) 237-249.

[62] Park H., Woodburn C. *An algorithmic proof of Suslin's stability theorem for polynomial rings.* J. Algebra **178** (1995) 277–298.

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

[64] R.A. Rao, *The Bass-Quillen conjecture in dimension three but characteristic $\neq 2, 3$ via a question of A. Suslin*, Invent. Math. 93 (1988) 609-618.

[65] Roitman M. *On projective modules over polynomial rings.* J. Algebra **58** (1979) 51–63.

[66] Roitman M. *On stably extended projective modules over polynomial rings*, Proc. Amer. Math. Soc. 97 (1986) 585-589.

[67] Rosenberg J. *Algebraic K-Theory and its applications.* Graduate Texts in Mathematics, 1996.

[68] Serre J.-P. *Faisceaux algébriques cohérents.* Ann. Math. **61** (1955) 191–278.

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

[70] Suslin A. A. *Projective modules over a polynomial ring are free.* Soviet Math. Dokl. **17** (1976) 1160–1164.

[71] Yengui I. *An algorithm for the divisors of monic polynomials over a commutative ring.* Math. Nachr. **260** (2003) 1-7.

[72] Yengui I. *Making the use of maximal ideals constructive.* Theoretical Computer Science **392** (2008) 174-178.

[73] Yengui I. *Dynamical Gröbner bases.* J. Algebra **301** (2006) 447–458.

[74] Yengui I. *The Hermite ring conjecture in dimension one.* J. Algebra **320** (2008) 437-441.

[75] Yengui I. *Stably free modules over $\mathbf{R}[X]$ of rank $>$ $\dim \mathbf{R}$ are free.* Preprint 2007.