CONSTRUCTIONS IN $R[x_1,\ldots,x_n]$. APPLICATIONS TO K-THEORY

JESÚS GAGO-VARGAS

ABSTRACT. A classical result in K-Theory about polynomial rings like the Quillen-Suslin theorem admits an algorithmic approach when the ring of coefficients has some computational properties, associated with Gröbner bases. There are several algorithms when we work in $\mathbb{K}[x_1,\ldots,x_n]$, $\mathbb{K}$ a field. In this paper we compute a free basis of a finitely generated projective module over $R[x_1,\ldots,x_n]$, R a principal ideal domain with additional properties, test the freeness for projective modules over $D[x_1,\ldots,x_n]$, with D a Dedekind domain like $\mathbb{Z}[\sqrt{-5}]$ and for the one variable case compute a free basis if there exists any.

1. Introduction

The Quillen-Suslin theorem asserts that if $A = D[x_1,\ldots,x_n]$ is a polynomial ring over a Dedekind domain D then every finitely generated projective A-module is extended from D ([21, 22]). When D is a principal ideal domain every finitely generated projective A-module is free. This is equivalent to say that if R is a principal ideal domain and $\mathbf{f} = (f_1,\ldots,f_m)$ is a unimodular row of $R[x_1,\ldots,x_n]^m$ then there exists a matrix $U \in \mathrm{GL}(m, R[x_1,\ldots,x_n])$ such that $\mathbf{f}\cdot U = (1,0,\ldots,0)$, or that we can complete $\mathbf{f}$ to an invertible matrix. An algorithm for the Quillen-Suslin theorem produces such matrix, and we call it a QS-algorithm. The last $m-1$ columns of the matrix U form a free basis of the module defined by $\ker(\mathbf{f}) \subset R[x_1,\ldots,x_n]^m$. There are several algorithms when R is a field ([16, 6, 14, 15], [20] as a corollary). The main tool in the procedure is the algorithm to compute Gröbner bases, which we can find in other rings like $\mathbb{Z}$.

In Section 2 we give some algorithmic results over the ring $R[x_1,\ldots,x_n]$ that we need later, namely, the construction of a maximal ideal that contains an ideal of $R[x_1,\ldots,x_n]$ and how to compute in $S^{-1}R[x]$ and $R[x_1,\ldots,x_n]_{\mathcal{M}}$, rings obtained from $R[x_1,\ldots,x_n]$.

In Section 3 we present two QS-algorithms for $R[x_1,\ldots,x_n]$, that avoid the normalization step used in [7]. The first one follows [14, 15] and the second one [19, 17]. Our starting point is a projective module P given as kernel of a unimodular row or as a submodule of a free module. Then we can generalize the results in [14] to monoid rings $R[M]$, because the induction step reduces the problem to a free monoid, where we have solved the problem. In a similar way the QS-algorithm

2000 *Mathematics Subject Classification.* Primary: 13C10, 13P10, 19A49, 68W30. Secondary: 15A33.

Key words and phrases. Serre Conjecture, Quillen-Suslin Theorem, Gröbner bases, Dedekind domains, projective modules.

Partially supported by DGICYT PB97-0723 and Junta de Andalucía FQM-218.

This is a preliminary version of this article.

for quotients of polynomial rings by monomial ideals, that is, rings of the form $R[x_1,\dots,x_n]/I$, with I a monomial ideal and R a PID, is easily extended, such as appears in [13].
In Section 4 we consider D the ring of integers of a number field, a Dedekind domain in which it is possible to compute. First we give a new algorithm using Gröbner bases to get the factorization of an ideal of D as product of prime ideals, and we apply it to find a free basis of a projective module over D, if there exists one. The next step is to study the freeness of a projective module P over $D[x_1,\dots,x_n]$. We can do it by reducing the problem to a module over D, and for one variable, we give an algorithm to compute a free basis when there exists one.

2. Preliminary algorithmse

Let R be a ring. We recall that linear equations are solvable in R if we have an algorithm to decide the membership problem of a element with respect to an ideal and we can compute a set of generators of the module $Syz(a_1,\dots,a_m)$, with $a_1,\dots,a_m \in R$. With these conditions we can build Gröbner bases in the ring $R[x_1,\dots,x_n]$ ([1, chapter 4]). We need to add another one.

Definition 1. Let R be a ring. We say that R is an MC-ring if we can solve linear equations in R and, given $I \subset R$ a proper ideal, it is possible to compute a set of generators of a maximal ideal that contains I.

For example, $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-5}]$ are MC-rings. Additionally, we need the factorization of polynomials in $(R/\langle p\rangle)[x]$, $p \in R$ a prime element, and $Q(R)[x]$, $Q(R)$ the field of fractions of R.

Definition 2. Let R be a ring. We say that R has effective coset representatives if given J an ideal of R it is possible to find a complete set $\mathcal{C}$ of coset representatives of R/J, and there is a procedure to find, for all $a \in R$, an element $c \in \mathcal{C}$ such that $a \equiv c \ (mod\ J)$.

This definition appears in [1, p. 226], and we need this property in R to compute the normal form of a polynomial with respect to an ideal.
We include here the algorithm described in [7] to compute a set of generators of a maximal ideal of $R[x_1,\dots,x_n]$, R an MC-PID, that contains an ideal.

Algorithm 1. *Input:* $F = \{f_1,\dots,f_r\}$ *set of generators of an ideal* I *of* $R[x_1,\dots,x_n]$.
Output: $H = \{g_1,\dots,g_m\}$ *set of generators of a maximal ideal* $\mathcal{M} \subset R[x_1,\dots,x_n]$ *that contains* I.

(1) *Compute* $\langle s\rangle = \langle F\rangle \cap R$.
(2) *If* $s \neq 0$*, let* $p \in R$ *be a prime element such that* p *divides* s.
  (a) *Compute* $\bar g_1,\dots,\bar g_k \in (R/\langle p\rangle)[x_1,\dots,x_n]$ *generators of a maximal ideal* $\overline{\mathcal{M}}$ *that contains* $\bar I$ *in* $(R/\langle p\rangle)[x_1,\dots,x_n]$.
  (b) *Lift to* $g_1,\dots,g_k \in R[x_1,\dots,x_n]$ *and let* $H = \{p, g_1,\dots,g_k\}$. **STOP**.
(3) *If* $s = 0$*, compute* $d \in R, d \neq 0$ *such that* $I = (I,d) \cap I^{ec}$*, where* $I^{ec} = IQ(R)[x_1,\dots,x_n] \cap R[x_1,\dots,x_n]$ *(*[9]*).*
(4) *If* $(I,d) \neq R$*, set* $F \leftarrow F \cup \{d\}$*, and go to step* 1. *Otherwise, compute* $\tilde g_1,\dots,\tilde g_k \in Q(R)[x_1,\dots,x_n]$ *generators of a maximal ideal* $\widetilde{\mathcal{M}}$ *that contains* $\tilde I$ *in* $Q(R)[x_1,\dots,x_n]$.

(5) *Let J be ideal of $R[x_1,\dots,x_n]$ such that $J^e = \widetilde{\mathcal{M}}$. Compute r the least common multiple of the coefficients of a Gröbner basis of J. Let $p \in R$ be a prime element that does not divide r. Set $F \leftarrow F \cup \{p\}$, and go to step 1.*

Example 1. Let $I = \langle xy+1\rangle$ be ideal of $\mathbb{Z}[x,y]$. Then $I \cap \mathbb{Z} = 0$, so there exists $d \in R, d \neq 0$ such that $I = (I,d) \cap I^{ec}$. In this case, $d = 1$. The ideal $\widetilde{\mathcal{M}} = \langle x-1, y+1\rangle$ is a maximal ideal in $\mathbb{Q}[x,y]$ that contains I^e. Set $J_1 = \langle x-1, y+1\rangle \subset \mathbb{Z}[x,y]$, and $s = 1$. Take $p = 2$ and set $I' = (J_1, 2) \supset I$. Applying the algorithm to I', we get $\mathcal{M} = \langle 2, x-1, y-1\rangle$ maximal ideal of $\mathbb{Z}[x,y]$ that contains I.

Let S be the set of monic polynomials of $R[x]$, and write $R' = S^{-1}R[x]$. When R is a field, the ring R' is the field of rational functions over $R[x]$.

Lemma 1. *Let R be a principal ideal domain where we can divide and compute the greatest common divisor and $I = \langle f,g\rangle \subset R'$ be an ideal of R'. Then it is possible to compute $h, f', g' \in R'$ such that $I = \langle h\rangle$, $f = f'h$ and $g = g'h$.*

Proof. By [11, p. 117], we know that R' is a principal ideal domain. Then $I = \langle h'\rangle$, where h' is the greatest common divisor of f and g in R'. We can assume $f, g \in R[x]$ taking off denominators and compute $h = \gcd(f,g)$ in $R[x]$ with the pseudo-division algorithm ([4, algorithms 3.2.10, 3.1.2]). Every irreducible element of $R[x]$ is irreducible or a unit of R'. Then $I = \langle h\rangle$, and by division we obtain $f', g' \in R[x]$ such that $f = f'h, g = g'h$. $\square$

Remark 1. In [2] it is shown that if R is an euclidean domain, then $S^{-1}R[x]$ is an euclidean domain too. However, the division algorithm passes through a formal power serie.

Corollary 1. *Let R be an MC-PID. Then R' is an MC-PID.*

Proof. Given $I = \langle f_1,\dots,f_n\rangle \subset R'$ ideal of R', by iterative applications of Lemma 1, we compute h a generator of I. If $f \in R'$, we can check whether $f \in I$ by reducing to $R[x]$ and making the division by h. If $f \in I$, we obtain $f' \in R'$ with $f = f'h$. The syzygy module of a set $f_1,\dots,f_m$ in R' is easily reduced to a computation of a syzygy module in $R[x]$.
Let I be a proper ideal of R'. By Lemma 1, we find a not monic polynomial $f(x) \in R[x]$ such that $I = \langle f(x)\rangle R'$. We get $f_1(x) \in R[x]$ an irreducible and not monic polynomial that divides $f(x)$ in $R[x]$, by factoring in $Q(R)[x]$ and Gauss's Lemma. Then $I \subset \langle f_1(x)\rangle R'$, maximal ideal in R'. $\square$

Proposition 1. *Let R be an MC-ring. If $\mathcal{M}$ is a maximal ideal of $R[x_1,\dots,x_n]$ then $R[x_1,\dots,x_n]_{\mathcal{M}}$ is an MC-ring.*

Proof. The construction of a maximal ideal that contains a given ideal is trivial, because $R[x_1,\dots,x_n]_{\mathcal{M}}$ is local. We have to check the conditions about linear equations. Note that through Gröbner bases in $R[x_1,\dots,x_n]$ we can check if a polynomial f belongs to an ideal I, and if so, express it as linear combination of generators, and this procedure is valid in $R[x_1,\dots,x_n]_{\mathcal{M}}$. Let $I_{\mathcal{M}} = \langle f_1,\dots,f_m\rangle$ be an ideal in $R[x_1,\dots,x_n]_{\mathcal{M}}$, and $f \in R[x_1,\dots,x_n]_{\mathcal{M}}$. We can suppose $f, f_1,\dots,f_m \in R[x_1,\dots,x_n]$. If any f_i is not in $\mathcal{M}$, then $I_{\mathcal{M}} = R[x_1,\dots,x_n]_{\mathcal{M}}$, and we are done. Then assume that $I \subset \mathcal{M}$, and $f \in \mathcal{M}$. We have that $f \in I_{\mathcal{M}}$ if and only if there exists $s \notin \mathcal{M}$ such that $s \cdot f \in I$, i.e., $s \in (I : f)$. We can compute $c_1,\dots,c_m \in R[x_1,\dots,x_n]$ a set of generators of $(I : f)$. If every c_i is in $\mathcal{M}$ then

$f \notin I_{\mathcal{M}}$. If, for example, $c_1 \notin \mathcal{M}$, then $c_1 \cdot f \in I$, and we can express f as a linear combination of the generators of $I_{\mathcal{M}}$ with coefficients in $R[x_1, \ldots, x_n]_{\mathcal{M}}$.
In a similar way to Corollary 1, we can get a set of generators of the module $Syz(f_1, \ldots, f_m)$ wit $f_1, \ldots, f_m \in R[x_1, \ldots, x_n]_{\mathcal{M}}$. □

Remark 2. If R has effective coset representatives then, for a given $I_{\mathcal{M}}$ proper ideal of $R[x_1, \ldots, x_n]_{\mathcal{M}}$, we can compute the cosets of $R[x_1, \ldots, x_n]/I$ and the same set is valid for $R[x_1, \ldots, x_n]_{\mathcal{M}}/I_{\mathcal{M}}$.

3. QS-algorithms in $R[x_1, \ldots, x_n]$

Let R be an MC-PID, $\mathbf{f} = (f_1, \ldots, f_m)$ a unimodular row in $R[x_1, \ldots, x_n]^m$ and $P = \ker(\mathbf{f})$. Then P is a projective module, and we want to get a free basis of it. The process described in [7] uses the primary decomposition of an ideal of $R[x_1, \ldots, x_n]$. To avoid it, we give two new QS-algorithms. The procedures are by induction on n, the number of variables. If $n = 0$ we have a projective module over an MC-PID, and we can compute the Smith normal form. Assume that $n \geq 0$ and that we have an algorithm for rings of polynomials with n variables and coefficients in an MC-PID. Now consider the polynomial ring $R[x_1, \ldots, x_n][y]$ in $n + 1$ variables. The first step is reducing the problem to find a free basis of the modules $P_{\mathcal{M}}$ over the rings $R[x_1, \ldots, x_n]_{\mathcal{M}}[y]$ for a finite set of maximal ideals $\mathcal{M}$ of $R[x_1, \ldots, x_n]$. Here we need Algorithm 1 to compute a maximal ideal that contains an ideal in $R[x_1, \ldots, x_n]$. These free bases are patched together to obtain a basis of the module P, as shown in [16], so the problem is reduced to give an algorithmic proof of Horrocks' theorem ([17, p. 28]).

3.1. First QS-algorithm in $R[x_1, \ldots, x_n]$.

Theorem 1. *Let P be a projective module over $R[x_1, \ldots, x_n][y]$, defined as the kernel of a unimodular row $\mathbf{f} = (f_1, \ldots, f_m)$, and $\mathcal{M}$ a maximal ideal of $R[x_1, \ldots, x_n]$. Then there exists a $m \times m$-invertible matrix U with entries in $R[x_1, \ldots, x_n]_{\mathcal{M}}[y]$ such that $\mathbf{f} \cdot U = (1, 0, \ldots, 0)$. The last $m - 1$ columns of U form a free basis of $P_{\mathcal{M}}$.*

Proof. Write $A = R[x_1, \ldots, x_n]_{\mathcal{M}}[y]$. Let S be the multiplicative set of monic polynomials of A, and $S_0 \subset R[y]$ the set of monic polynomials. As $\mathbf{f}$ is a unimodular row, we can compute a column $\mathbf{g}$ such that $\mathbf{f} \cdot \mathbf{g} = 1$, and $M = I - \mathbf{g} \cdot \mathbf{f}$ is a matrix whose columns form a set of generators of the $R[x_1, \ldots, x_n][y]$-module $Syz(\mathbf{f})$. From the commutative diagram

$$\begin{array}{ccc} R[x_1, \ldots, x_n][y] & \rightarrow & (S_0^{-1} R[y])[x_1, \ldots, x_n] \\ \downarrow & & \downarrow \\ R[x_1, \ldots, x_n]_{\mathcal{M}}[y] & \longrightarrow & A_S \end{array}$$

we see that the module $S^{-1} P_{\mathcal{M}}$ is extended from $S_0^{-1} P$. By Corollary 1, $S_0^{-1} R[y]$ is an MC-PID, and by the induction hypothesis and extension we compute a matrix $U_S \in \mathrm{GL}(m, S^{-1} R[y])$ such that $\mathbf{f} \cdot U_S = (1, 0, \ldots, 0)$. Let $v_1, \ldots, v_{m-1} \in P_{\mathcal{M}}$ be the last $m - 1$ columns of U_S. These vectors form a free basis of $S^{-1} P_{\mathcal{M}}$ in A_S. Let $k = R[x_1, \ldots, x_n]/\mathcal{M}$, $\overline{A} = A/\mathcal{M}A = k[y]$ and $\overline{A}_S = k(y)$. Compute a matrix $\overline{U} \in \mathrm{GL}(m, k[y])$ such that $\mathbf{f} \cdot \overline{U} = (1, 0, \ldots, 0)$ and let $\overline{e}_1, \ldots, \overline{e}_{m-1}$ be the last $m - 1$ columns of $\overline{U}$. This set is a free basis of $\overline{P_{\mathcal{M}}}$. Take $a_1, \ldots, a_{m-1} \in A$ such that $\overline{a}_i = \overline{e}_i, i = 1, \ldots, m - 1$. Then $e_i = a_i - \mathbf{g} \cdot \mathbf{f} \cdot a_i, i = 1, \ldots, m - 1$, are elements of $P_{\mathcal{M}}$ that go over $\overline{e}_1,\dots,\overline{e}_{m-1}$. By solving a linear system, we get $\overline{W}\in \mathrm{GL}((m-1),k(y))$ such that

$$(\overline{v}_1,\dots,\overline{v}_{m-1})\overline{W}=(\overline{e}_1,\dots,\overline{e}_{m-1})$$

because $\overline{v}_1,\dots,\overline{v}_{m-1}$ and $\overline{e}_1,\dots,\overline{e}_{m-1}$ are bases of the vector space $\overline{P}_S$ over the field $k(y)$. As pointed in [3, 14], we can take $W\in \mathrm{GL}(m-1,A_S)$ that lifts to $\overline{W}$. Change the basis $v_1,\dots,v_{m-1}$ of $S^{-1}P_{\mathcal{M}}$ by the basis $(v_1,\dots,v_{m-1})\cdot W$. Then

$$e_i=v_i+h_i,\quad h_i\in \mathcal{M}S^{-1}P_{\mathcal{M}},\quad i=1,\dots,m-1.$$

Following [12, 3], if C is the subring of $S^{-1}R[y]$ formed by f/g, with $g\in S$ and $\deg(f)\le\deg(g)$, then $\mathcal{M}S^{-1}P_{\mathcal{M}}=\mathcal{M}P_{\mathcal{M}}+\mathcal{M}Q$, where $Q=\bigoplus v_iy^{-1}C$. By the division algorithm, decompose $h_i=g_i+g_i'$, where $g_i\in A^m$, and the degree of the denominators of g_i' are greater than the degree of numerators. Compute z_i the normal form of g_i with respect the module $\mathcal{M}P_{\mathcal{M}}$ over the ring A. Then, by [12, 3], the elements $v_i'=v_i+z_i+g_i', i=1,\dots,m-1$ form a basis of $P_{\mathcal{M}}$. □

Remark 3. The algorithm described in [14, algorithm 4] is incomplete, because to extract the component in $\mathcal{M}P_{\mathcal{M}}$ we need normal forms, and not only quotients. An analogous remark is applied to [14, p. 418].

Example 2. Consider the polynomial ring $\mathbb{Z}[x]$, the unimodular row $\mathbf{f}=(13,x^2-1,2x-3)$ and P the projective module defined by $\ker(\mathbf{f})$. We can compute $\mathbf{g}=(2,-20,10x+15)^t$ with $\mathbf{f}\cdot\mathbf{g}=1$. A basis of $S^{-1}P$ over $S^{-1}\mathbb{Z}[x]$ is formed by the vectors

$$v_1=\left(1,-\frac{13}{x^2-1},0\right)^t,v_2=\left(0,-\frac{2x-3}{x^2-1},1\right)^t.$$

For every maximal ideal $\mathcal{M}$ in $\mathbb{Z}$, a basis of the module $S^{-1}P_{\mathcal{M}}$ is obtained by extension. Let $\mathcal{M}=\langle 2\rangle$ maximal ideal of $\mathbb{Z}$, and $\overline{A}=(\mathbb{Z}/\mathcal{M})[x]$. By Euclidean algorithm in $\overline{A}$, we get a basis of $\overline{P}_{\mathcal{M}}$ with elements $\overline{e}_1=\left(-x^2+1,1,0\right)^t,\overline{e}_2=(1,0,1)^t$. Then

$$\overline{W}=\begin{pmatrix}-x^2+1 & 1\\ 0 & 1\end{pmatrix}\in \mathrm{GL}(2,\overline{A}_S)$$

is a matrix with

$$(\overline{v}_1|\overline{v}_2)\overline{W}=(\overline{e}_1|\overline{e}_2).$$

Lift to

$$W=\begin{pmatrix}-x^2+1 & 1\\ 0 & 1\end{pmatrix}\in \mathrm{GL}(2,A_S)$$

and a new basis of $S^{-1}P_{\mathcal{M}}$ is

$$v_1=\left(-x^2+1,13,0\right)^t,v_2=\left(1,-\frac{2(5+x)}{x^2-1},1\right)^t.$$

We can compute elements $e_1=\overline{e}_1-\mathbf{g}\cdot\mathbf{f}\cdot\overline{e}_1,e_2=\overline{e}_2-\mathbf{g}\cdot\mathbf{f}\cdot\overline{e}_2\in P_{\mathcal{M}}$ such that they apply over $\overline{e}_1,\overline{e}_2$. Let $h_1=e_1-v_1=g_1+g_1',h_2=e_2-v_2=g_2+g_2'$, where $g_1=h_1,g_1'=0$, and

$$g_2=\left(-20-4x,200+40x,-150-130x-20x^2\right)^t,\quad g_2'=\left(0,2\tfrac{x+5}{x^2-1},0\right)^t.$$

The respective normal forms of g_1,g_2 with respect to $\mathcal{M}P_{\mathcal{M}}$ are

$$z_1=(0,0,0)^t,z_2=\left(\frac{-4x^2+x^3+4x-1}{x^3-2x^2-1},-\frac{(x-1)x^2(x^2-3x+1)}{x^3-2x^2-1},0\right)^t.$$

Then $v_1' = v_1, v_2' = \left(0, 2x-3, -x^2+1\right)^t$ form a free basis of $P_{\mathcal{M}}$. If $U = (\mathbf{g}|v_1'|v_2')$, then $\det(U) = -13$ is a unit in $\mathbb{Z}_{\mathcal{M}}$. To obtain a matrix with determinant 1, we consider $U_1 = \left(\mathbf{g}| -\frac{1}{13}v_1'|v_2'\right)$. Let $r_1 = 13$.
We repeat the process for $\mathcal{M}_2 = \langle 13 \rangle$, and obtain the matrix

$$U_2 = \begin{pmatrix} 2 & 1 & 0 \\ -20 & -\frac{52}{5} & 2x-3 \\ 10x+15 & \frac{26}{5}x + \frac{39}{5} & -x^2+1 \end{pmatrix}.$$

In this case, $r_2 = 5$, and $\langle r_1, r_2 \rangle = \mathbb{Z}$. By patching together the solutions as described in [16], we get

$$V = \begin{pmatrix} -128x^2+60x^3+60x & 1+1144x^2-780x^3 & -144x^2+100x^3-4x \\ -1-30x & 13+390x & -50x-3 \\ 270x-375x^2 & -130x+4875x^2 & 1-625x^2 \end{pmatrix}$$

with $\det(V) = 1$ and $\mathbf{f} \cdot V = (1 \quad 0 \quad 0)$.

3.2. **Second QS-algorithm in $R[x_1, \ldots, x_n]$.** The algorithm described in the previous section uses the normal form of a vector with respect to a module. We give another method, based on [19, 17], where is not needed. We begin with an easy lemma.

Lemma 2. *(*[17, Lemma 3.2.5]*.) Let R be an MC-PID and M a free R-module. Let v be a nonzero element of M. Then M has a basis $v_1, \ldots, v_r$ such that $v = \alpha v_1$ for some $\alpha \in R$.*

The following algorithm solves the local step, i.e., compute a basis of the $R[x_1, \ldots, x_n]_{\mathcal{M}}$-module $P_{\mathcal{M}}$. Our starting point is a set of generators of $P_{\mathcal{M}}$ as a submodule of a free module, and proceed by induction over $\operatorname{rank}(P) = m$. We build a set of generators of a projective module P' with rank $m-1$. Remember that if P' is projective then it is torsion free, so it is isomorphic to a submodule of a free module of finite rank ([10, Prop. 10.11]). This isomorphism can be computed, because the relations between the generators of P' can be found by solving a linear system in the field $Q(R)$. Then we apply the induction hypothesis.

Theorem 2. *(*[17, Thm. 3.2.1] *Let P be a projective $R[x_1, \ldots, x_n][y]$-module, generated by a set of vectors of $R[x_1, \ldots, x_n][y]^s$, and $\mathcal{M}$ a maximal ideal of $R[x_1, \ldots, x_n]$. Then we can find a free basis of $P_{\mathcal{M}}$.*

Proof. Let M be a matrix whose columns are the generators of P, and $m = \operatorname{rank}(P)$.

(1) If $m = 1$ then P is isomorphic to an ideal of $R[x_1, \ldots, x_n][y]$. Then $S_0^{-1}P$ is a projective ideal of $(S_0^{-1}R[y])[x_1, \ldots, x_n]$, so it is free, hence principal. Using a Gröbner basis we can find its generator, that is a basis.
(2) If $m \geq 2$, let $v_1, \ldots, v_m$ a basis of $S_0^{-1}P_{\mathcal{M}}$, that we can compute because $S_0^{-1}(R[x_1, \ldots, x_n][y]) = (S_0^{-1}R[y])[x_1, \ldots, x_n]$. Choose $v_i \in P_{\mathcal{M}}$ taking off denominators.
(3) Let $\bar{e}_1, \ldots, \bar{e}_m$ be a basis of $\overline{P}_{\mathcal{M}}$ over $k[y]$, with $k = R[x_1, \ldots, x_n]/\mathcal{M}$.
(4) Compute a basis $\bar{q}_1, \ldots, \bar{q}_m$ of $\overline{P}_{\mathcal{M}}$ with $\bar{v}_1 = \alpha \bar{q}_2$ (Lemma 2). Let $\overline{V}$ be a change basis matrix and V a lifting with entries in A.
(5) Lift q_1 to $P_{\mathcal{M}}$ through $M \cdot V$.
(6) By solving a linear system, let $q_1 = \sum_{i=1}^m a_i' v_i$ in $S^{-1}A$, so we can find $s \in A$ such that $sq_1 = \sum_{i=1}^m a_i v_i, a_i \in A$.

(7) Take k such that $a_1 + sy^k$ is a monic polynomial in the variable y.
(8) Let $p = q_1 + y^k v_1$, and $P' = P/pA$. Then P' is projective and $\operatorname{rank}(P') = m-1$ ([17, 19]), so is torsion free, and we can compute a set of generators. Set $P \leftarrow P'$, and go to step 1.

□

Example 3. Consider Example 2, and let $\mathcal{M} = \langle 2\rangle \subset \mathbb{Z}$. We want to compute a free basis of the $A = \mathbb{Z}_{\mathcal{M}}[x]$-module $P_{\mathcal{M}}$. A set of generators of P is formed by the columns s_1, s_2, s_3 of $M = I - \mathbf{g}\cdot\mathbf{f}$. It is easy to see that $\operatorname{rank}(P) = 2$. As $S_0^{-1}\mathbb{Z}[x]$ is an MC-PID, we can find the Smith normal form of the module $S_0^{-1}P_{\mathcal{M}}$. Then

$$\begin{pmatrix} 10 & 1 & 0 \\ 10x+15 & 0 & -2 \\ 13 & x^2-1 & 2x-3 \end{pmatrix} M \begin{pmatrix} 0 & 1 & 2 \\ 1 & -10 & -20 \\ 0 & 5x+7 & 10x+15 \end{pmatrix} = V_1 M V_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The nonzero columns $\{v_1, v_2\}$ of $M \cdot V_2$ form a basis of $S_0^{-1}P$. Now it is easy to see that the vectors $\overline{e}_1 = (-1,0,-1)^t, \overline{e}_2 = \left(0,-1,-x^2+1\right)^t$ are a basis of the module $\overline{P}_{\mathcal{M}}$. As $\overline{v}_1 = \overline{e}_2$, we take $\overline{q}_1 = \overline{e}_1, \overline{q}_2 = \overline{e}_2$, and $q_1 = (-25, 260, -130x-195)^t \in P_{\mathcal{M}}$ goes over $\overline{q}_1$. Then $sq_1 = a_1v_1 + a_2v_2$ with $a_1 = 10, s = 1$ and $a_1 + sx$ is monic in x, so

$$\begin{aligned} &p = q_1 + xv_1 = \\ &\left(-25 - 2x^3 + 2x, 260 - 19x + 20x^3, -115x - 195 - 10x^4 + 10x^2 - 15x^3\right)^t. \end{aligned}$$

We know that $P' = P_{\mathcal{M}}/pA$ is a projective A-module with rank equal to 1. Now we have to compute a free basis $w + \langle p\rangle$ of P', which is generated by $s_1 + \langle p\rangle, s_2 + \langle p\rangle, s_3 + \langle p\rangle$. The first step is to find $d_2, d_3 \in A$ such that $d_2(s_2 + \langle p\rangle) = \lambda_2(s_1 + \langle p\rangle), d_3(s_3 + \langle p\rangle) = \lambda_3(s_1 + \langle p\rangle)$, so we solve the system

$$\left(\begin{array}{c|c} s_2 & s_3 \end{array}\right) = \left(\begin{array}{c|c} p & s_1 \end{array}\right) \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

in the field of fractions of A. Let $d = 5x(2x+3), \lambda_2 = -5(2x+3), \lambda_3 = -2(10+x)$, and consider the morphism between A-modules $\varphi : P' \to (s_1 + \langle p\rangle)A$ defined by $\varphi(v) = d \cdot v$. Then φ is injective, and $P' \simeq \varphi(P') \subset (s_1 + \langle p\rangle)A$. Since $\varphi(P')$ is generated by only one element, it must be a multiple of $s_1 + \langle p\rangle$. Then consider the ideal $J = \langle d, \lambda_2, \lambda_3\rangle A$. By computing a Gröbner basis in A we obtain $u = 85 = 0\cdot d + \lambda_2 - 5\lambda_3$, a unit in A, so P' is generated by $\varphi^{-1}(s_1 + \langle p\rangle) = u^{-1}(s_2 - 5s_3) + \langle p\rangle$. Let

$$\begin{aligned} &w = u^{-1}(s_2 - 5s_3) = \\ &\tfrac{1}{85}\left(-2x^2 + 20x - 28, 20x^2 - 200x + 281, -10x^3 + 85x^2 + 10x - 215\right)^t. \end{aligned}$$

Then $\{p, w\}$ is a free basis of $P_{\mathcal{M}}$.

Remark 4. These algorithms allow us to extend the results in [14] to find bases of projective modules over a monoid ring $R[M]$, because all we need are the constructions in $S^{-1}R[x]$ described in Section 2 and the Quillen-Suslin algorithm in $R[x_1,\ldots,x_n]$ ([8]). In the same way, we have a QS-algorithm for quotients of the form $R[x_1,\ldots,x_n]/I$, with I a monomial ideal, extending [13].

4. QS-algorithm in $D[x]$

4.1. **Ideal factorization in a Dedekind domain.** Let D be the ring of integers of a number field, and I an ideal of D. Then D is a Dedekind domain, and there is an algorithm ([5, algorithm 2.3.22]) to compute the factorization of I as product of prime ideals of D. We present here another algorithm based in Gröbner bases. We know that D is a free $\mathbb{Z}$-module of finite rank, and we can find $\omega_0 = 1, \omega_1, \ldots, \omega_n$ a free basis ([4, algorithm 6.1.8]). Then $\omega_i \omega_j = \sum_{k=0}^n a_{i,j,k}\omega_k, i, j \in \{0, 1, \ldots, n\}$ for some $a_{i,j,k} \in \mathbb{Z}$. Let $s_{ij} = x_i x_j - \sum_{k=0}^n a_{i,j,k} x_k$ be polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$, and call J the ideal generated by them.

Lemma 3. (1) $D \simeq \mathbb{Z}[x_1, \ldots, x_n]/J$.
(2) *There is a primality testing algorithm for ideals of D.*
(3) *Let I be a proper ideal of D. Then there exists an algorithm to find a set of generators of a maximal ideal $\mathcal{M}$ of D that contains I.*
(4) *Let $\mathcal{M}$ be a maximal ideal of D. Then it is possible to compute a set of generators of the D-module $\mathcal{M}^{-1}$.*

Proof. (1) Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial such that $p(\omega_1, \ldots, \omega_n) = 0$. By reducing p by the polynomials s_{ij}, we have that $p \equiv q \pmod{J}$, where $q(x_1, \ldots, x_n) = a_0 + a_1 x_1 + \ldots + a_n x_n, a_i \in \mathbb{Z}$. Since $p(\omega_1, \ldots, \omega_n) = 0$, then $q(\omega_1, \ldots, \omega_n) = 0$, so $a_0 = a_1 = \ldots = a_n = 0$, because of linear independence of ω_i in $\mathbb{Z}$, and then $p \in J$.
If I is an ideal of D, we note $\tilde{I}$ the lifted ideal of $\mathbb{Z}[x_1, \ldots, x_n]$.
(2) I is a prime ideal of D if and only if $\tilde{I}$ is a prime ideal of $\mathbb{Z}[x_1, \ldots, x_n]$, and by [9, prop. 4.3] we have an algorithm to test the primality of $\tilde{I}$.
(3) Apply Algorithm 1 to $\tilde{I}$.
(4) Follow [4, p. 199]. Observe that we can always find $p \in \mathbb{Z} \cap \mathcal{M}$ a prime element through $\widetilde{\mathcal{M}} \cap \mathbb{Z}$.

□

Proposition 2. *Let I be a proper ideal of D. Then we can find prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of D such that $I = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$.*

Proof. If I is prime, we are done. Otherwise, let $\mathfrak{p}_1$ be a maximal ideal that contains I. Let $I_1 = \mathfrak{p}_1^{-1} I$. Then I_1 is an integer ideal and $I \subsetneq I_1$ ([18]). We apply again the process to the ideal I_1, and we obtain an ascending chain of ideals $I \subset I_1 \subset \ldots \subset I_r$ that becomes stationary because D is a noetherian ring. If $I_r = I_{r+1}$, we know that $I_{r+1} = \mathfrak{p}^{-1} I_r$, where $\mathfrak{p}$ is a maximal ideal of D that contains I_r. Then $I_r = \mathfrak{p}^{-1} I_r$ and this would imply that $\mathfrak{p} = D$. So I_r is a maximal ideal, the algorithm stops and we obtain the expression $I = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$. □

Example 4. Let $I = \langle 6 \rangle$ be ideal of $D = \mathbb{Z}[\omega]$, with $\omega = \sqrt{-5}$. An integral basis of D is $\{1, \omega\}$. Now consider $\tilde{I} = \langle 6, t^2 + 5 \rangle$ ideal of $\mathbb{Z}[t]$. Then $\tilde{I}$ is not prime, because $\langle 6 \rangle \mathbb{Z} = \tilde{I} \cap \mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$. Let $p_1 = 2$ be a prime number that divides 6, and consider the ideal $\tilde{I}' = \langle p_1, t^2 + 5 \rangle$, that contains $\tilde{I}$. We compute $\overline{\mathcal{M}}_1 = \langle t + 1 \rangle$, a maximal ideal of $(\mathbb{Z}/p_1)[t]$ that contains the polynomial $t^2 + \bar{5}$. Then $\mathfrak{p}_1 = \langle 2, 1 + \omega \rangle$ is a maximal ideal that contains I and $\mathfrak{p}_1^{-1} = D + \frac{1+\omega}{2} D$. Hence we obtain $I_1 = \mathfrak{p}_1^{-1} I = \langle 6, 3 + 3\omega \rangle$.
Again, I_1 is not a prime ideal, so we apply the process to it. It is contained in the maximal ideal $\mathfrak{p}_2 = \langle 2, 1 + \omega \rangle$, so we define $I_2 = \mathfrak{p}_2^{-1} I_1 = \langle 3 \rangle$. The ideal I_2 is not

prime, because $t^2+\bar{5}$ is reducible in $(\mathbb{Z}/3)[t]$. A maximal ideal that contains I_2 is $\mathfrak{p}_3=\langle 3,1+\omega\rangle$, and $\mathfrak{p}_3^{-1}=D+\frac{1-\omega}{3}D$. Now $I_3=\mathfrak{p}_3^{-1}I_2=\langle 3,1-\omega\rangle$, that it is prime. Putting $\mathfrak{p}_4=I_3$ we get $I=\mathfrak{p}_1^2\mathfrak{p}_3\mathfrak{p}_4$.

4.2. **Projective modules over** $D[x]$**.** Let M be a finitely generated D-module. Then M is projective if and only if M is torsion free. In this case, if $\operatorname{rank}(M)=r$, then $M\simeq D^{r-1}\oplus\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of D. M is free if and only if $\mathfrak{a}$ is principal ([5, Thm. 1.2.23]). This decomposition can be computed when D is the ring of integers of a number field ([5, Thm. 1.2.19]), and the crucial step is the following lemma.

Lemma 4. *If I and J are fractional ideals of D then $I\oplus J\simeq D\oplus IJ$ as D-modules.*

A way to obtain this isomorphism is through the prime decomposition of ideals in D (see [5, Prop. 1.3.12]) or applying [5, Algorithm 1.3.16]. Then, if we have determined the freeness of a torsion free module M we can compute a basis using this isomorphism.
If $\mathcal{M}$ is a maximal ideal in D then the local ring $D_{\mathcal{M}}$ is a discrete valuation ring, so a PID. If $P(x)$ is a projective module over $D[x]$, then for each maximal ideal $\mathcal{M}$ of D, the module $P(x)_{\mathcal{M}}$ is projective over $D_{\mathcal{M}}[x]$, and by the Quillen-Suslin theorem $P(x)_{\mathcal{M}}$ is free. Then $P(x)$ is extended from $P(0)$ ([21]). When D is the ring of integers of a number field, we have an algorithm for the previous result analogous to [14]. This shows us that for checking the freeness of $P(x)$ over $D[x]$ is enough to test $P(0)$ over D. The problem is reduced to compute a free basis of the module $P(x)_{\mathcal{M}}$ over $D_{\mathcal{M}}[x]$ for a maximal ideal $\mathcal{M}$ of D. But $D_{\mathcal{M}}$ is an MC-PID, and by sections 3.1, 3.2 we have two algorithms to get a free basis.

Example 5. In $D=\mathbb{Z}[\omega],\omega=\sqrt{-5}$ consider $\mathbf{f}(x)=(f_1(x)\quad f_2(x)\quad f_3(x))$ the unimodular row in $D[x]^3$ where

$$f_1(x)=-5x^2-2\omega x+2x+\omega-2, f_2(x)=x^2-x, f_3(x)=\omega x-\omega+1.$$

Let $P(x)$ be the projective module defined by $\ker(\mathbf{f}(x))$, whose generators in $D[x]^3$ are given by the columns of the matrix $M(x)=I_3-\mathbf{g}(x)\mathbf{f}(x)$, where $\mathbf{g}(x)=(x-1,5x-2,2x-1)^t$. To check the freeness of $P(x)$ we consider the D-module $P(0)$ generated by the columns of $M(0)$. We can see that $P(0)\simeq D\oplus J$, where $J=\langle 2-\omega\rangle$. Then $P(0)$ is free, so $P(x)$. Let $\mathcal{M}=\langle 2,1+\omega\rangle$ be maximal ideal of D. Applying Theorem 2 to $P_{\mathcal{M}}$ we get the matrix

$$\begin{aligned}
&[x-1,-5x^4+6x^3+\omega x^2-3x^2+\omega x-\omega x^4-\omega+1,-(x-1)(10086662778x\\
&+20424937041\omega-6861175910\omega x-27394274848x^2+8528154248\omega x^3\\
&-5214150542\omega x^2-45243672650x^3+28030914183)\,/\beta]\\
&\big[5x-2\,,-25x^4-2\omega x^3+14x^3+2\omega x^2-12x^2+5\omega x-x-6\omega x^4-2\omega+2\,,\\
&-(144679169033x-61623674056\omega+99695086617\omega x+120872168654x^2\\
&-36583582778\omega x^3-17235547982\omega x^2+36521518173\omega x^4-44295714782x^3\\
&-240865770565x^4-18225840353)\,/\beta\big]\\
&\big[2x-1,2-4x^2-11x^4-\omega x^3+7x^3+\omega x^2+2\omega x-2\omega x^4-\omega+x^5\,,\\
&(-65754728708x+28500912245\omega-41229027211\omega x-52828252348x^2\\
&-6119253067x^5+15325343098\omega x^3+13191112346\omega x^2-18717821941\omega x^4\\
&+14918939512x^3+94101342265x^4+2929481463x^5\omega+15681952346)\,/\beta\big]\,,
\end{aligned}$$

with $\beta=(-37835988013+20773799974\,\omega)$.

References

[1] W.W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, (Amer. Math. Soc., Providence, RI 1994).

[2] D.D. Anderson, D.F. Anderson and R. Markanda, The Rings $R(X)$ and $R\langle X\rangle$, J. Algebra, **95** (1985), 96–115.

[3] V.A. Artamonov, Serre's quantum problem, Russian Math. Surveys, **53:4**, (1998), 657–730.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, (Springer, Berlin, 1993).

[5] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, (Springer, New York, 2000).

[6] N. Fitchas and A. Galligo, Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel, Math. Nachr., **149** (1990), 231–253.

[7] J. Gago-Vargas, On Suslin's Stability Theorem for $R[x_1, \dots, x_m]$, in *Ring Theory and Algebraic Geometry*, Lecture Notes in Pure and Applied Mathematics, vol. 221, 203–210, (Marcel Dekker, New York, 2001).

[8] J. Gago-Vargas, *Algoritmo para el teorema de Quillen-Suslin en* $R[M]$, Comunicación en EACA-2000, Barcelona (2000).

[9] P. Gianni, B. Trager and G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, J. Symbolic Comput., **6** (1988), 149–167.

[10] N. Jacobson, *Basic Algebra II*, (W.H. Freeman and Co., San Francisco, 1980).

[11] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, (Birkhäuser, Boston, 1985).

[12] T.Y. Lam, *Serre's Conjecture*, Lecture Notes in Math., vol. 635, (Springer, New York, 1978).

[13] R. Laubenbacher and K. Schlauch, An algorithm for the Quillen-Suslin theorem for quotients of polynomial rings by monomial ideals, J. Symbolic Comput, **30** (2000), no. 5, 555–571.

[14] R. Laubenbacher and C. Woodburn, An algorithm for the Quillen-Suslin theorem for monoid rings, J. Pure Appl. Algebra, **117-118** (1997), 395–429.

[15] R. Laubenbacher and C. Woodburn, A new algorithm for the Quillen-Suslin theorem, Beiträge Algebra Geom., **41** (2000), 23–31.

[16] A. Logar and B. Sturmfels, Algorithms for the Quillen-Suslin theorem, J. Algebra, **145** (1992), 231–239.

[17] S. Mandal, *Projective modules and Complete Intersections*, Lecture Notes in Math., vol. 1672, (Springer, Berlin, 1997).

[18] M.P. Malliavin, *Algèbre commutative. Applications en géométrie et théorie des nombres*, (Masson, Paris, 1985).

[19] B. Nashier and W. Nichols, Ideals containing monics, Proc. Amer. Math. Soc., **99** (1987), 634–636.

[20] H. Park and C. Woodburn, An algorithmic proof of Suslin's stability theorem for polynomial rings, J. Algebra, **178** (1995), 277–298.

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

[22] A.A. Suslin, Projective modules over polynomial rings are free, Soviet Math. Dokl. **17** (1976), no. 4, 1160–1164.

Dpto. de Álgebra, Universidad de Sevilla, Apdo. 1160, 41080 Sevilla, España

E-mail address: gago@algebra.us.es.