Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 41 (2000), No. 1, 23-31.

A New Algorithm for the Quillen-Suslin Theorem

Reinhard C. Laubenbacher **Cynthia J. Woodburn**

Department of Mathematics, New Mexico State University
Las Cruces, NM 88003, USA
e-mail: reinhard@nmsu.edu

Department of Mathematics, Pittsburg State University
Pittsburg, KS 66762-7502, USA
e-mail: cwoodbur@pittstate.edu

Abstract. In this paper we present a new algorithm for the Quillen-Suslin Theorem for polynomial rings.

MSC 1991: 13C10, 13P10, 19A49
Keywords: Gröbner basis, polynomial ring, projective module, Quillen-Suslin Theorem

1. Introduction

In 1955, J.-P. Serre remarked [12, p. 243] that it was not known whether there exist finitely generated projective modules over $k[x_1, \ldots, x_r]$, k a field, which are not free. This remark turned into the "Serre Conjecture", stating that indeed there were no such modules. Proven independently in 1976 by D. Quillen [11] and by A. A. Suslin [13], it became subsequently known as the Quillen-Suslin Theorem (QS).

Several algorithms have been given for QS [9, 3, 4]. Given a suitable presentation of a finitely generated projective module over $k[x_1, \ldots, x_r]$, k a field, these algorithms produce a free basis for the module. Such algorithms might be of interest in applications of QS to problems within as well as outside mathematics. See [15] for applications of QS to problems in control theory. To mention an application to the solution of linear systems of equations with polynomial coefficients, one may interpret the theorem as follows. Let A be an $n \times m$-matrix with entries in $R = k[x_1, \ldots, x_r]$, and let

$$A \cdot \mathbf{y} = 0$$

be a system of linear equations. Define a module P via the presentation

$$R^m \xrightarrow{A} R^n \longrightarrow P \longrightarrow 0,$$

and suppose that P is a projective R-module. Then the Quillen-Suslin Theorem implies that the solution space of the system $A\mathbf{y} = 0$ has a free basis, and an algorithm for the theorem will compute such a free basis.

This paper contains a new algorithm for QS. It is a variant of the algorithm in [9], and appears implicitly in [7], which contains a more general algorithm for the Quillen-Suslin Theorem for seminormal monoid rings, based on results in [5]. (See also [14].)

All rings which appear are either subrings of polynomial rings over a field, quotients of polynomial rings, or localizations thereof. Thus, all required computations can be carried out using the theory of Gröbner bases, as described in [1], [2], [8]. Since the study of projective modules is properly part of algebraic K-theory, the present paper may be considered a contribution to the computational side of that subject.

Following is a precise statement of the result.

Theorem 1.1. *Let k be a field, and P a finitely generated $R = k[x_1, \ldots, x_r]$-module, given as the kernel or cokernel of a matrix with entries in R. Then there is an algorithm to test whether P is projective, in which case it computes a free basis for P.*

In order to put the result of the present paper in context we describe briefly the algorithm in [9]. It proceeds by induction on the number of variables. In the case of a polynomial ring in one variable, one can use the Smith normal form algorithm. Suppose the theorem is true for all polynomial rings in less than or equal to r variables over any field. Now consider the polynomial ring

$$R[y] = k[x_1, \ldots, x_r][y]$$

in $r + 1$ variables. The first step in [9] is to reduce the problem to the case of a stably free module. Recall that, for a ring S, a projective S-module P is *stably free*, if $P \oplus S^n \cong S^m$ for some non-negative integers n and m. Using Gröbner basis techniques, one can compute a free resolution for an arbitrary projective S-module. All the cokernels of the maps in the resolution are projective, so, in particular, the cokernel of the last map in the resolution is stably free. With an algorithm to find free bases for stably free modules, one can now construct a shorter free resolution for P. Proceeding inductively, one obtains a free resolution

$$0 \longrightarrow R^n \longrightarrow R^m \longrightarrow P \longrightarrow 0$$

of P, from which one can compute a free basis. If P is stably free, then we can assume that the matrix in Theorem 1.1 is unimodular, that is, has a left inverse. Given such a unimodular matrix, its left inverse can be computed with standard Gröbner basis methods (see [9, pp. 236–237]).

The next step in the algorithm is to reduce the problem to that of finding a free basis for the localized modules $P_{\mathcal{M}}$ over the rings

$$k[x_1, \ldots, x_r]_{\mathcal{M}}[y],$$

for a suitable finite collection of maximal ideals $\mathcal{M}$ of $k[x_1, \ldots, x_r]$. These free bases for the local modules are then "patched together" to obtain a basis for the module P.

In this paper we present an alternative algorithm for the local problem, that is, to find a free basis for the module $P_{\mathcal{M}}$ over $k[x_1, \ldots, x_r]_{\mathcal{M}}[y]$, for a maximal ideal $\mathcal{M} \subset k[x_1, \ldots, x_r]$. We conclude the paper with an example.

2. The local algorithm

Proposition 2.1. *Let P be a finitely generated $k[x_1, \ldots, x_r, y]$-module, given as the kernel or cokernel of a matrix C with entries in $k[x_1, \ldots, x_r, y]$. Let $\mathcal{M}$ be a maximal ideal of $k[x_1, \ldots, x_r]$. Then there is an algorithm which tests whether $P_{\mathcal{M}}$ is projective, in which case it computes a free basis for it.*

The conceptual basis for the algorithm is a version of Roberts' Theorem (even though we will not explicitly use it).

Theorem 2.2. ([14, Theorem 3.2]) *Let R be a commutative local ring with maximal ideal $\mathcal{M}$. Let A be an R-algebra, and let P be a finitely generated A-module. Let S be a central multiplicative set of A which is regular on A and on P. Let n be a nonnegative integer. Assume*

(1) *If $f \in S$, then A/fA is finite over R.*
(2) *$GL_n(A_S) \setminus GL_n(\overline{A_S})/GL_n(\overline{A}) = \{1\}$, where $\overline{A} = A/\mathcal{M}A$.*
(3) *There is an R-subalgebra $B \subset A_S$ with $A_S = A + B$ and $\mathcal{M}B \subset J(B)$, where $J(B)$ is the Jacobson radical of B.*
(4) *$P_S \cong A_S^n$ and $\overline{P} \cong \overline{A}^n$.*

Then $P \cong A^n$.

Let $R = k[x_1, \ldots, x_r]_{\mathcal{M}}$ and $A = R[y]$. To simplify notation, denote the localization of P at $\mathcal{M}$ again by P. Let $S \subset A$ be the multiplicative set of polynomials, which, when viewed as a polynomial in y, have leading coefficient a unit in R. Taking quotients modulo $\mathcal{M}$, we obtain the commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & A_S \\ \downarrow & & \downarrow \\ \overline{A} & \longrightarrow & \overline{A_S}. \end{array}$$

Here $\overline{A} = A/\mathcal{M}A = k'[y]$ is a polynomial ring in one variable over the field $k' = k[x_1, \ldots, x_r]/\mathcal{M}$. Furthermore, the localization A_S can be described as

$$A_S = (k[x_1, \ldots, x_r]_{\mathcal{M}}[y])_S = k(y)[x_1, \ldots, x_r]_{\widetilde{\mathcal{M}}},$$

where $\widetilde{\mathcal{M}}$ is the extension of the maximal ideal $\mathcal{M}$ to the polynomial ring over the larger field $k(y)$. Since there are finitely many maximal ideals $\mathcal{N}_1, \ldots, \mathcal{N}_s$ of $k(y)[x_1, \ldots, x_r]$ lying over $\mathcal{M}$, it follows that A_S is a semi-local ring. Furthermore, it is the localization of a polynomial ring in r variables, which will allow us to apply our induction hypothesis later on. Consequently,

$$\overline{A_S} = \prod_{i=1}^{s} k(y)[x_1, \ldots, x_r]/\mathcal{N}_i$$

is a product of fields, each of which contains k'. The kernel of the right-hand vertical projection is equal to the intersection of the $\mathcal{N}_i$, which is the Jacobson radical of A_S.

Outline of the proof of Proposition 2.1. We will only present the proof for a module presented as the kernel of a matrix with polynomial entries. The proof for a cokernel is entirely similar. The proof proceeds by induction on the number of variables of A. A polynomial ring in one variable over a field is a PID, so we can apply the Smith normal form algorithm to C to check whether P is projective, and to compute a free basis for it. Now assume the proposition is true for polynomial rings in r variables over a field. Suppose we are given the following presentation:

$$0 \longrightarrow P \longrightarrow k[x_1, \ldots, x_r, y]^m \xrightarrow{C} k[x_1, \ldots, x_r, y]^n$$

of P.

First assume that $P_{\mathcal{M}}$ is projective. Using the reduction algorithm in [9] we can assume that $P_{\mathcal{M}}$ is stably free. If we reduce modulo the maximal ideal $\mathcal{M}$ we get a projective module $\overline{P_{\mathcal{M}}}$ over the principal ideal domain $k'[y]$. Using the Smith normal form algorithm, we find a free basis $\bar{u}_1, \ldots, \bar{u}_t$ for $\overline{P_{\mathcal{M}}}$ over $\overline{A}$. Extending scalars from $\overline{A}$ to $\overline{A_S}$, we obtain a free basis $\bar{u}_1, \ldots, \bar{u}_t$ of $\overline{(P_{\mathcal{M}})_S}$ over $\overline{A_S}$. Now lift the elements $\bar{u}_1, \ldots, \bar{u}_t$ to elements $u_1, \ldots, u_t \in P_{\mathcal{M}} \subset (P_{\mathcal{M}})_S$, using normal forms with respect to a Gröbner basis for $\mathcal{M} \subset k[x_1, \ldots, x_r]$.

To simplify notation, denote $P_{\mathcal{M}}$ by P. The module P_S over A_S has the same presentation matrix C as P. Since A_S is the localization of a polynomial ring in r variables, P_S is free by induction, and we can find a free basis $v_1, \ldots, v_t$. Let $\overline{v_1}, \ldots, \overline{v_t}$ be the induced basis of $\overline{P_S}$ over the product of fields $\overline{A_S}$. Let $\overline{W}$ be a base change matrix that transforms the basis $\{\overline{v_i}\}$ into the basis $\{\bar{u}_i\}$. It is possible to lift $\overline{W}$ to a matrix W over A_S, which restricts to an invertible matrix on the image of C. Transforming the basis $\{v_1, \ldots, v_t\}$ via W, we obtain another free basis of P_S, again denoted by $\{v_i\}$, which maps to the basis $\{\bar{u}_i\}$ over $\overline{A_S}$. Hence the differences $u_i - v_i$ lie in the radical of P_S. We can now transform the v_i into a free A_S-basis of P_S which is actually contained in $P \subset P_S$, so they also form a free A-basis of P.

If $P = P_{\mathcal{M}}$ is not projective, then the algorithm fails to either find a free basis for $\overline{P}$ or for P_S. Thus, it can be used to test $P_{\mathcal{M}}$ for projectivity.

Proof. To begin the proof, assume that P is projective. Using the reduction algorithm in [9] we can assume further that P is in fact stably free, that is, C has a right inverse

$$D : A^n \longrightarrow A^m,$$

such that CD is the identity on A^n. Let S be the multiplicative subset of A consisting of those elements which are monic when viewed as polynomials in y. Consider the ring

$$A_S = (k[x_1,\ldots,x_r]_{\mathcal{M}}[y])_S = k(y)[x_1,\ldots,x_r]_{\widetilde{\mathcal{M}}}.$$

Let

$$0 \longrightarrow P \longrightarrow A_S^m \xrightarrow{C} A_S^n \longrightarrow 0$$

be the presentation of P_S obtained from C by extending scalars to A_S. Our goal is to find a free basis for P_S. Since C has a right inverse, we have an effective decomposition

$$A_S^m \cong \ker(C) \oplus A_S^n = P_S \oplus A_S^n,$$

given by $x = (x - DCx) + DCx$ for all $x \in A_S^m$. There is a commutative diagram

$$\begin{array}{ccc} k[x_1,\ldots,x_r][y] & \longrightarrow & k(y)[x_1,\ldots,x_r] \\ \downarrow & & \downarrow \\ k[x_1,\ldots,x_r]_{\mathcal{M}}[y] & \longrightarrow & A_S. \end{array}$$

Thus, the module P_S is extended from $k(y)[x_1,\ldots,x_r]$. By induction, we can find a free basis for projective modules over this ring. Thus, we can extend P to this ring, find a free basis, and then extend to A_S. In this way we obtain a free basis $v_1,\ldots,v_t$ of P_S.

We now construct the elements $u_i \in P \subset P_S$. First we reduce the above presentation matrix C over A modulo $\mathcal{M}$ to obtain a presentation matrix over

$$k[x_1,\ldots,x_r]_{\mathcal{M}}[y]/\mathcal{M} = k'[y].$$

Since $k'[y]$ is a principal ideal domain, we can use the Smith normal form algorithm to find an invertible matrix U such that

$$\overline{C}U = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix},$$

where I is an $(m \times m)$-identity matrix. Then the last $t = n - m$ rows of U^{-1} form a free basis $\bar{u}_1,\ldots,\bar{u}_t$ for $\overline{P}$.

We now choose a term order for $k[x_1,\ldots,x_r]$ and compute a Gröbner basis for the ideal $\mathcal{M} \subset k[x_1,\ldots,x_r]$. Now compute normal forms in $k[x_1,\ldots,x_r]$ for the polynomials in the entries of $\bar{u}_i$. Using these normal forms we obtain elements

$$u_1,\ldots,u_t \in A^m,$$

which map onto the basis for $\overline{P}$. We modify the u_i by elements in $\mathcal{M} \cdot A^m$, so that they lie in P as follows. If we replace u_i by $u_i - DCu_i$, then

$$C(u_i - DCu_i) = Cu_i - (CD)Cu_i = 0.$$

Thus, we have elements $u_i \in P \subset P_S$ which map onto the initial free basis $\{\bar{u}_i\}$ of $\overline{P}$.

Now consider the basis $\{\bar{u}_i\}$ of $\overline{P_S}$. Since $\overline{A_S}$ is a product of fields we can compute base change matrices in each component and use the Chinese Remainder Theorem to assemble them to a base change matrix $\overline{W} \in GL_t(\overline{A_S})$ which maps $\{\bar{v}_i\}$ to $\{\bar{u}_i\}$. We compute normal forms of the polynomials making up the entries of $\overline{W}$ with respect to the Gröbner basis of $\mathcal{M}$. Using these normal forms we can lift $\overline{W}$ to a matrix

$$W : A_S^m \longrightarrow A_S^m.$$

Now replace W by $W - DCW$. The new W still reduces to the old $\overline{W}$, and, furthermore, $C(W - DCW) = 0$. While this new W need not be invertible, it restricts to an invertible transformation on P_S. Now replace the basis $v_1, \ldots, v_t$ of P_S by the basis $Wv_1, \ldots, Wv_t$. Then for this new basis $\{v_i\}$ of P_S we have that $\bar{u}_i = \overline{v_i}$ for all i. Consequently, the differences $u_i - v_i$ lie in the radical of P_S. Using the division algorithm we decompose $u_i - v_i$ as the sum

$$u_i - v_i = f_i - g_i,$$

where $f_i \in A^m$, and the degrees of the denominators of the entries in g_i are greater than or equal to the degrees of the numerators. Then

$$u_i - f_i = v_i - g_i,$$

so that $v_i - g_i$ is denominator-free (with respect to elements in S). Replace v_i by $v_i - g_i$. The new v_i are still linearly independent since they map to a free basis modulo the Jacobson radical of A_S. If we now further alter the v_i by replacing them with

$$v_i - DCv_i,$$

then the new v_i are still linearly independent and lie in $P \subset P_S$. Furthermore, they differ from the initial basis for P_S by elements in $\text{rad}(A_S)P_S$, hence they form a free basis for P_S. Also, we still have that $\bar{u}_i = \overline{v_i}$ is a free basis for $\overline{P}$ over $\overline{A}$.

Now consider the free A-submodule P' of P generated by $v_1, \ldots, v_t$. Since $\overline{v_i} = \bar{u}_i$ generates $\overline{P}$, it follows that

$$P = P' + \text{rad}(A)P.$$

Nakayama's Lemma implies that $P' = P$. Hence we have found a free basis for P.

If P is not projective, then the algorithm fails to find a free basis for either $\overline{P}$ or P_S. $\square$

3. An example

Consider the polynomial ring $\mathbb{Q}[x, y]$. Let $\mathcal{M}$ be the maximal ideal of $\mathbb{Q}[x]$ generated by $x - 1$, and let $P = P_{\mathcal{M}}$ be the stably free $A = \mathbb{Q}[x]_{\langle x-1\rangle}[y]$-module given by the kernel of the unimodular row $C = (x^2y + 1, x + y - 2, 2xy)$. Notice that $D = (1, 0, -x/2)^t$ is a right inverse of C.

First we find elements $\bar{u}_i$ which form a free basis of $\overline{P_S}$. Reducing C modulo $\langle x - 1\rangle$, we obtain $\overline{C} = (y + 1, y - 1, 2y)$. Computing the Smith normal form of $\overline{C}$ yields

$$\begin{aligned}(1,0,0) &= \overline{C}U \\ &= \overline{C} \cdot \begin{pmatrix} 1 & -y+1 & -1 \\ 0 & y+1 & -1 \\ -\frac{1}{2} & 0 & 1 \end{pmatrix}\end{aligned}$$

So, the last two columns of U form a free basis $\bar{u}_1 = (-y+1, y+1, 0)^t, \bar{u}_2 = (-1,-1,1)^t$ for $\overline{P}$.

Now lift these to elements $u_1 = (-y+1, y+1, 0)^t$, $u_2 = (-1,-1,1)^t$ over A, and then modify them so that they lie in P by replacing each u_i by $u_i - DCu_i$:

$$\begin{aligned} u_1 &= \left(y + 2 + x^2y^2 - x^2y - xy - x - y^2, y+1, \frac{-x}{2}\left(x^2y^2 - x^2y + 2y + 1 - xy - x - y^2\right)\right)^t \\ u_2 &= \left(-2 + x^2y + x + y - 2xy, -1, \frac{1}{2}\left(2 - x^3y + x - x^2 - xy + 2x^2y\right)\right)^t. \end{aligned}$$

Next, using Gaussian elimination, we find

$$V = \begin{pmatrix} 1 & -x-y+2 & -2xy \\ 0 & 1 & 0 \\ \frac{-x}{2} & \frac{x}{2}(x+y-2) & x^2y+1 \end{pmatrix},$$

with $CV = (1,0,0)$. Thus, the last two columns of V,

$$v_1 = \left(-x-y+2, 1, \frac{x}{2}(x+y-2)\right)^t,$$

and

$$v_2 = \left(-2xy, 0, x^2y+1\right)^t,$$

form a free basis of P_S, and $\overline{v_1} = \left(-y+1, 1, \frac{1}{2}(y-1)\right)^t$, $\overline{v}_2 = (-2y, 0, y+1)^t$ form a free basis of $\overline{P_S}$. (Notice that $\{v_1, v_2\}$ is actually a free basis for P. We continue with the example, however, in order to demonstrate the algorithm.)

A base change matrix $\overline{W}$, which maps $\{\overline{v_i}\}$ to $\{\bar{u}_i\}$, is

$$\begin{pmatrix} -\frac{1}{2} & -y+1 & -1 \\ -\frac{1}{2} & y+1 & -1 \\ \frac{2y+1}{2y} & \frac{y-1}{2y} & 2 \end{pmatrix}$$

which has determinant 1. Lifting $\overline{W}$ to A_S, we obtain the same matrix W. Now replace W with $W = W - DCW =$

$$\begin{pmatrix} \frac{1}{2}(x^2y - x + y - 4xy - 2) & y + 2 + x^2y^2 - x^2y - 2xy - y^2 & x^2y + x + y - 4xy - 2 \\ -1/2 & y+1 & -1 \\ W_{3,1} & W_{3,2} & W_{3,3} \end{pmatrix},$$

with

$$\begin{aligned} W_{3,1} &= \frac{1}{4y}(4y + 2 - x^3y^2 + xy + x^2y - xy^2 + 4x^2y^2), \\ W_{3,2} &= \frac{1}{2y}(y - 1 - x^3y^3 + x^3y^2 - 2xy^2 - xy + 2x^2y^2 + xy^3), \\ W_{3,3} &= \frac{1}{2}(4 - x^3y + x - x^2 - xy + 4x^2y). \end{aligned}$$

Although W is not invertible, when restricted to P_S, it gives an invertible transformation. Next, replace v_1 with

$Wv_1 =$

$$\begin{pmatrix} \frac{1}{2}\left(6y+4x-3x^2y^2-3x^2-16xy-7x^3y+14x^2y-3y^2+x^3+x^3y^2+5xy^2+x^4y\right) \\ \frac{1}{2}\left(3x+3y-x^2-xy\right) \\ \frac{-1}{4y}\left(2x-8y-2-15x^2y^2+12xy-2x^3y-3x^2y+4y^2-3x^3y^3+14x^3y^2+3xy^2-3xy^3+x^4y-7x^4y^2+5x^2y^3+x^5y^2+x^4y^3\right) \end{pmatrix},$$

and v_2 with

$$Wv_2 = \begin{pmatrix} -2xy-5x^3y^2-xy^2+5x^2y^2-2+x^4y^2+x^3y+x+y \\ xy-1-x^2y \\ \frac{1}{2}\left(-5xy-x+5x^4y^2+7x^2y-x^3y+x^2y^2-5x^3y^2+4-x^5y^2-x^4y-x^2\right) \end{pmatrix}.$$

Notice that the following differences lie in the radical of P_S:

$u_1 - v_1 =$

$$\begin{pmatrix} \frac{1}{2}\left(-4y+4+7x^3y+5x^2y^2-16x^2y+3x^2+14xy+y^2-5xy^2-6x-x^4y-x^3y^2-x^3\right) \\ \frac{1}{2}\left(-y+2-3x+x^2+xy\right) \\ \frac{1}{4y}\left(2x-8y-13x^2y^2+10xy-2x^3y-x^2y+4y^2-2-5x^3y^3+16x^3y^2-xy^2-xy^3+x^4y-7x^4y^2+5x^2y^3+x^5y^2+x^4y^3\right) \end{pmatrix}$$

$$= (x-1)\cdot\begin{pmatrix} \frac{1}{2}\left(-x^3y+6x^2y-x^2y^2-x^2+4xy^2-10xy+2x+4y-y^2-4\right) \\ \frac{1}{2}(x+y-2) \\ \frac{1}{4y}\left(x^4y^2+x^3y-6x^3y^2+x^3y^3-x^2y-4x^2y^3+10x^2y^2-2xy-3\,xy^2+xy^3+2-4y^2+8y\right) \end{pmatrix}$$

and

$$\begin{aligned} u_2 - v_2 &= \begin{pmatrix} x^2y+5x^3y^2+xy^2-5x^2y^2-x^4y^2-x^3y \\ -xy+x^2y \\ \frac{1}{2}(2x-2+4xy-5x^2y-5x^4y^2-x^2y^2+5x^3y^2+x^5y^2+x^4y) \end{pmatrix} \\ &= (x-1)\cdot\begin{pmatrix} -\left(x^2y-4xy+x+y\right)xy \\ xy \\ \frac{1}{2}(x^4y^2-4x^3y^2+x^3y+x^2y^2+x^2y-4xy+2) \end{pmatrix}. \end{aligned}$$

So, ignoring the denominator-free part of $u_1 - v_1$ and $u_2 - v_2$, respectively, we have $g_1 = \left(0, 0, \dfrac{x-1}{-2y}\right)^t$ and $g_2 = (0,0,0)^t$. Then $v_2 = v_2 - g_2$ and replacing v_1 with $v_1 - g_1$ yields

$$v_1 = \begin{pmatrix} \frac{1}{2}\left(6y+4x+x^3-3x^2y^2-3x^2-16xy-7x^3y+14x^2y-3y^2+x^3y^2+5xy^2+x^4y\right) \\ \frac{1}{2}\left(3x+3y-x^2-xy\right) \\ \frac{1}{4}\left(8+15x^2y-12x+2x^3+3x^2-4y+3x^3y^2-14x^3y-3xy+3xy^2-x^4+7x^4y-5x^2y^2-x^5y-x^4y^2\right) \end{pmatrix}$$

To move v_1 back to $P = \ker C$, replace v_1 with $v_1 - DCv_1$. Then

$$v_1 = \begin{pmatrix} \frac{1}{2}\left(6x+6y-16xy-3x^2y^2+x^3y^2+5xy^2+14x^2y-7x^3y-5x^2+x^3-3y^2+x^4y\right) \\ \frac{1}{2}\left(3x+3y-x^2-xy\right) \\ \frac{1}{4}(8-12x+15x^2y-14x^3y-3xy+x^2+4x^3+3xy^2+3x^3y^2-4y+7x^4y-5x^2y^2-x^4-x^5y-x^4y^2) \end{pmatrix}$$

and

$$v_2 = \begin{pmatrix} -2xy-5x^3y^2-xy^2+5x^2y^2-2+x^4y^2+x^3y+x+y \\ xy-1-x^2y \\ \frac{1}{2}(-5xy-x+5x^4y^2+7x^2y-x^3y+x^2y^2-5x^3y^2+4-x^5y^2-x^4y-x^2) \end{pmatrix}$$

lie in P and form the desired free basis.

References

[1] Adams, W.; Loustaunau, P.: *An Introduction to Gröbner Bases.* Amer. Math. Soc., Graduate Studies in Math. **3**, Providence 1994.

[2] Cox, D.; Little, J.; O'Shea, D.: *Ideals, Varieties, and Algorithms.* Undergrad. Texts in Math., Springer Verlag, New York 1992.

[3] Fitchas, N. (working group): *Algorithmic Aspects of Suslin's Proof of Serre's Conjecture.* Comp. Complexity **3** (1993), 31–55.

[4] Fitchas, N.; Galligo, A.: *Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel.* Math. Nachr. **149** (1990), 231–253.

[5] Gubeladze, I. Dzh.: *Anderson's Conjecture and the Maximal Monoid Class Over Which Projective Modules Are Free.* Math. USSR Sbornik **63** (1989), 165–180.

[6] Lam, T. Y.: *Serre's Conjecture.* Lecture Notes in Math. **635**, Springer Verlag, New York 1978.

[7] Laubenbacher, R. C.; Woodburn, C. J.: *An Algorithm for the Quillen-Suslin Theorem for Monoid Rings.* J. Pure Appl. Algebra, to appear.

[8] Logar, A.: *Computational Aspects of the Coordinate Ring of an Algebraic Variety.* Comm. Algebra **18** (1990), 2641–2662.

[9] Logar, A.; Sturmfels, B.: *Algorithms for the Quillen-Suslin Theorem.* J. Algebra **145** (1992), 231–239.

[10] Park, H.; Woodburn, C.: *An Algorithmic Proof of Suslin's Stability Theorem for Polynomial Rings.* J. Algebra **178** (1995), 277–298.

[11] Quillen, D.: *Projective Modules Over Polynomial Rings.* Invent. Math. **36** (1976), 167–171.

[12] Serre, J.-P.: *Faisceaux Algébriques Cohérents.* Ann. Math. **61** (1955), 191–278.

[13] Suslin, A. A.: *Projective Modules Over a Polynomial Ring Are Free.* Soviet Math. Dokl. **17** (1976), 1160-1164.

[14] Swan, R. G.: *Gubeladze's Proof of Anderson's Conjecture.* Contemporary Mathematics **124**, Amer. Math. Soc. 1992, 215–250.

[15] Youla, D. C.; Pickel, P. F.: *The Quillen-Suslin Theorem and the Structure of n-Dimensional Elementary Polynomial Matrices.* IEEE Trans. on Circuits and Systems **31** (1994), 513–517.

Received February 24, 1997; revised version March 23, 1999