An algorithm for the divisors of monic polynomials over a commutative ring

Ihsen Yengui

Equipe de Mathématiques, CNRS UMR 6623,
UFR des Sciences et Techniques, Besançon, France
Correspondence address: Département de Mathématiques,
Faculté des Sciences, 3018 Sfax, Tunisia
e.mail ihsen.yengui@fss.rnu.tn

Math. Nachr. 260 (2003), 1-7

Gilmer and Heinzer proved that given a reduced ring R, a polynomial f divides a monic polynomial in $R[X]$ if and only if there exists a direct sum decomposition of $R = R_0 \oplus \cdots \oplus R_m$ ($m \leq \deg f$), associated to a fundamental system of idempotents $e_0, ..., e_m$, such that the component of f in each $R_i[X]$ has degree coefficient which is a unit of R_i. We propose to give an algorithm to explicitly find such a decomposition. Moreover, we extend this result to divisors of doubly monic Laurent polynomials.

INTRODUCTION

Let R be a ring and $U(X)$ the multiplicative subset of $R[X]$ formed by monic polynomials, that is polynomials with degree coefficient 1. The ring $R\langle X\rangle = R[X]_{U(X)}$ received a considerable amount of attention due to its role in Quillen's solution to Serre's conjecture. As soon as Serre's conjecture was settled, there were many research papers presenting results and algorithms dealing with Serre's conjecture and its ramifications [2,4,6,7,8,9,10].

In [2], the authors determined by an abstract way the group of units of $R\langle X\rangle$, this is equivalent to determining the saturation $U(X)^*$ of $U(X)$, that is all divisors of monic polynomials over R. Our purpose in this paper is to determine for a given polynomial f in $R[X]$ dividing some monic polynomial, the explicit decomposition into a direct sum of polynomials with invertible degree coefficients. Our proof is constructive, it does not use that of Gilmer and Heinzer and extends it to the non reduced case.

Also, we give the analogue to this result for doubly monic Laurent polynomials, that is polynomials in $R[X, X^{-1}]$ such that the coefficient of the highest and lowest terms are equal to 1. Furthermore, we prove that any doubly monic Laurent polynomial divides some monic polynomial in $X + X^{-1}$. As a consequence, we retrieve a constructive proof of the fact that

finitely generated projective modules over $K[X_1^{\pm 1}, X_2^{\pm 1} \ldots, X_n^{\pm 1}]$, K a field, are stably free.

1. THE UNITS OF $R\langle X\rangle$

Proposition 1. *Let $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$.*
1) If R is reduced, then $f \in U(X)^*$ if and only if there exists a direct sum decomposition $R = R_0 \oplus \cdots \oplus R_m$ $(m \leq n)$ of R such that if $f = f_0 + \cdots + f_m$ is the decomposition of f with respect to the induced decomposition $R[X] = R_0[X] \oplus \cdots \oplus R_m[X]$, then the degree coefficient of f_i is a unit of R_i for each i.
2) If R is not reduced, then $f \in U(X)^*$ if and only if there exist a nilpotent polynomial N and a direct sum decomposition $R = R_0 \oplus \cdots \oplus R_m$ $(m \leq n)$ of R such that if $f - N = f_0 + \cdots + f_m$ is the decomposition of $f - N$ with respect to the induced decomposition $R[X] = R_0[X] \oplus \cdots \oplus R_m[X]$, then the degree coefficient of f_i is a unit of R_i for each i.
3) $f \in U(X)^*$ if and only if $\langle a_0, \ldots, a_n\rangle = R$ and, for each $j \in \{0, \ldots, n\}$, we can find $\beta_j \in R$ and $k_j \in \mathbb{N}$ such that $(a_j(a_j\beta_j - 1))^{k_j} \equiv 0 \bmod \langle a_{j+1}, \ldots, a_n\rangle$.
4) $f \in U(X)^*$ if and only if $\langle a_0, \ldots, a_n\rangle = R$ and, for each prime ideal p of R, the relations $a_{j+1}, \ldots, a_n \in p$, $a_j \notin p$, imply that a_j is a unit modulo p.

Proof. We make the proof without assuming we have an equality test inside R.

1) If R is reduced. Let $f = a_0 + a_1X + ... + a_nX^n$ and $g = b_0 + b_1X + ... + b_dX^d$ in $R[X]$ such that $fg = c_0 + c_1X + ... + c_mX^m$ with $c_m = 1$.
We prove the result by induction on $n + d - m$.
– If $m = n + d$ then $a_nb_d = 1$.
– If $m < n+d$. We write all the relations between the a_i's, b_j's and c_k's in which a_n appears:

$$(S): \begin{cases} a_nb_d = \epsilon_0 \ (= 0) \\ a_nb_{d-1} + a_{n-1}b_d = \epsilon_1 \\ a_nb_{d-2} + a_{n-1}b_{d-1} + a_{n-2}b_d = \epsilon_2 \\ \quad\vdots \\ a_nb_0 + a_{n-1}b_1 + ... + a_{n-v}b_v = \epsilon_d \end{cases}$$

Where $v = \min\{d, n\}$, $\epsilon_i = 0$ if $i < n + d - m$.

If $m < n$, then multiplying each k^{th} equality in (S) by a_n^{k+1}, we obtain the system

$$(S'): \begin{cases} a_nb_d = 0 \\ a_n^2b_{d-1} = 0 \\ \quad\vdots \\ a_n^{d+1}b_0 = 0 \end{cases}$$

Thus, $a_n^{d+1}g = 0$ and $a_n^{d+1}fg = 0$. Hence, $a_n^{d+1} = 0$, and $a_n = 0$ since R is reduced. It follows by induction that all a_i's and b_i's with $i > m$ are zero and we can assume $n, d \leq m$.
By identification, $\epsilon_{n+d-m} = c_m = 1$.
Considering the $(n + d - m + 1)^{\text{th}}$ equality in (S) and multiplying each k^{th} equality $(1 \leq k \leq n + d - m)$ by a_n^{k-1}, we obtain

$$a_n^{n+d-m+1}b_{m-n} = a_n^{n+d-m}.$$

We need the following lemma.

Lemma 1. *Let R be a ring. If $r^{n+1}y = r^n$ for some $r, y \in R$ and $n \in \mathbb{N}$, then $r^2y - r$ is nilpotent and $r^n y^n$ is idempotent. If in addition, R is reduced then ry is idempotent and $rR = (ry)R$.*

Proof. Let $u = ry$. It is clear that $r^n(u-1) = 0$, $r^n(u^n - 1) = 0$ and $u^n(u^n - 1) = 0$. In the reduced case, we get $r(u-1) = 0$, $u(u-1) = 0$ and $rR = ruR \subseteq uR \subseteq rR$. $\diamondsuit$

Using lemma 1, $e_0 = a_n b_{m-n}$ is idempotent and $a_n^2 b_{m-n} - a_n = a_n(e_0 - 1) = 0$.
Set $e_0' = 1 - e_0$, $R_0 = Re_0$, $R_0' = Re_0'$, $f_0 = fe_0$, $g_0 = ge_0$, $f_0' = fe_0'$, $g_0' = ge_0'$. In R_0, $e_0 a_n$ is a unit, so $\deg(f_0) = n$ and $\deg(g_0) = m - n$.
We have $R = R_0 \oplus R_0'$. In R_0', $\deg f_0' g_0' = m$, the degree coefficient of $f_0' g_0'$ is a unit, $\deg(f_0') < n$ (since $a_n e_0' = 0$), and $\deg(g_0') \leq d$. We are done by induction.

Concretely, if we continue the process, we find an idempotent e_1 in R_0' (e_1 is also an idempotent in R) and a decomposition $R = R_0 \oplus R_1 \oplus R_1'$, and so on. So we find a priori $n + d - m + 1$ terms in the final decomposition, where $n, d \leq m$ since we first killed all a_i's and b_i's with $i > m$. In the most general case this means $m + 1$ terms in the final decomposition. Remark that without zero test inside R it is possible that we do not know which terms in the decomposition are useless, i.e., zero.

2) General case. R is not necessarily reduced.

– Let $\mathcal{N}$ be the nilradical of R. The proof for the case "R reduced" works with $R/\mathcal{N}$. In the first case we have proved $a_i = b_i = 0$ for $i > m$ and we computed idempotents $e_0, \ldots, e_m$ verifying $\sum e_i = 1$, $e_i e_j = 0$ if $j \neq i$, $e_i a_j = 0$ if $j > m - i$ (i.e., $\deg(e_i f) \leq m - i$), $e_i b_k = 0$ if $k > i$ (i.e., $\deg(e_i g) \leq i$) and $e_i(a_{m-i} b_i - 1) = 0$.
In the general case we explicitly get with the same proof all these equalities modulo $\mathcal{N}$, i.e., we know for each previous equality $t = 0$ (in the reduced case) an exponent k for which, in the general case $t^k = 0$. This gives the desired result.

It is of interest to recall a folklore result stating that each idempotent in $R/\mathcal{N}$ lifts in R. In more details, let $r \in R$ be an approximate root of the polynomial $f(X) = X^2 - X$, that is $f(r) = r^2 - r \in \mathcal{N}$. Say $f(r) = r^2 - r = \eta = c_0\eta$, where $\eta \in \mathcal{N}$ and $c_0 = 1$.
We have $f'(X) = 2X - 1$ and $f'(X)^2 = 4f(X) + 1$. Thus, $f'(r) = 1 + 4\eta$ is invertible. We replace "à la Newton" the approximate root r by $r + h$ as follows

$$f(r + h) = f(r) + hf'(r) + h^2 f_2(r, h), f_2(r, h) \in R.$$

Taking $h = \frac{-\eta}{f'(r)}$ and setting $r_1 = r_0 - \frac{\eta}{f'(r)}$, we obtain $f(r_1) = c_1\eta^2$ for some $c_1 \in R$.
Repeating this process, we find $r_2, c_2, \ldots, r_k, c_k \in R$ such that $f(r_2) = c_2\eta^4, \ldots, f(r_k) = c_k\eta^{2^k}$. For sufficiently large k, we get $f(r_k) = 0$ and $r - r_k \in \langle \eta \rangle \subseteq \mathcal{N}$.

Example: Let $n = 4$, $d = 5$, $m = 3$. We have $a_n^{d+1} = a_4^6 = 0$ and $b_d^{n+1} = b_5^5 = 0$. Thus, in the ring $R/\langle a_4, b_5 \rangle$, the degrees are cut down at 3 and 4, and consequently $b_4^4 = 0$. Here, one may wonder if it is possible to explicitly bound the nilpotence order of b_4 in R. Since $b_4^4 = 0$ in $R/\langle a_4, b_5 \rangle$, we obtain an equality $b_4^4 = a_4 A + b_5 B$ in R (A and B can be computed but it is not necessary). Hence, in R, $b_4^{4\times 10} = a_4^6 A' + b_5^5 B' = 0$. This suggests that a function bounding the nilpotence order will be exponential at n and d.
In the ring $R/\langle a_4, b_5, b_4 \rangle$, the degrees are cut down at 3 and 3, that is $n = d = m = 3$, and we are in the second case. The equality $a_n^{n+d-m+1} b_{m-n} = a_n^{n+d-m}$ signifies that $a_3^4 b_0 = a_3^3$. The Lemma says that $(r(ry-1))^3 = 0$ with $r = a_3$ and $y = b_0$ in $R/\langle a_4, b_5, b_4 \rangle$. One can precisely get

$(r(ry-1))^{3\times(40+5+6-2)} = (r(ry-1))^{147} = 0$ in R. In $S = R/\langle a_4, b_5, b_4, a_3(a_3b_0-1)\rangle$, $a_3b_0 = ry$ is idempotent and corresponds to an idempotent of R. Indeed, ry is an approximate solution of the equation $X^2 - X = 0$ which lifts "à la Hensel" since $2X-1$ is, at $X = ry$, a unit: indeed $(2X-1)^2 = 1 + 4(X^2 - X)$ and $4(X^2 - X)$ is, at $X = ry$, nilpotent with order less than 147. Denote by $e = a_3b_0+$ a nilpotent element, the idempotent lifting a_3b_0 in R. This decomposes R and S into two parts. In $eS \simeq S/\langle e-1\rangle$, f is quasimonic with degree 3 and $b_1 = b_2 = b_3 = 0$. This means that in $eR \simeq R/\langle e-1\rangle$, f is quasimonic with degree 3 and b_1, b_2, b_3 are nilpotent. And so on ...

– Another wording:

With the same notations as in the reduced case, we prove the result by induction on n.

If $a_n^{n+d-m} = 0$ or $a_n^{d+1} = 0$.
Let $k = \max\{n+d-m, d+1\}$, we have $a_n^k = 0$. Since $((f - a_nX^n)g - fg)^k = 0$, we can explicitly find a polynomial h in $R[X]$ such that $(f - a_nX^n)gh = (fg)^k$ is monic with degree mk, and we are done by the induction hypothesis.

If $a_n^{n+d-m} \neq 0$ and $a_n^{d+1} \neq 0$.
By the calculations done in the reduced case, we have

$$a_n^{n+d-m+1}b_{m-n} = a_n^{n+d-m}.$$

By Lemma 1, $e_0 = (a_nb_{m-n})^{n+d-m}$ is idempotent and $\alpha = a_n(a_nb_{m-n} - 1)$ is nilpotent.
We have $a_n = a_n^2b_{m-n} - \alpha$ where $\alpha^{n+d-m} = 0$. Hence $a_n^2 = a_n^3b_{m-n} - \alpha a_n$ and $a_n = a_n^3b_{m-n}^2 - \alpha a_nb_{m-n} - \alpha$. And so on, we can see that $a_n = b_{m-n}^{n+d-m}a_n^{n+d-m+1} + \beta = a_n(a_nb_{m-n})^{n+d-m} + \beta$, where $\beta^{n+d-m} = 0$. Thus with $a'_n = a_ne_0 = b_{m-n}^{n+d-m}a_n^{n+d-m+1}$ it holds

$$b_{m-n}^2(a'_n)^2 - b_{m-n}a'_n = b_{m-n}^2a_n^2(a_nb_{m-n})^{2(n+d-m)} - b_{m-n}a_n(a_nb_{m-n})^{n+d-m} = 0$$

as $b_{m-n}a_n^{n+d-m+1} = a_n^{n+d-m}$. As $b_{m-n}a'_n$ is idempotent, $b_{m-n}a'_n = e_0$, and

$$e_0R = b_{m-n}a'_nR \subseteq a'_nR = a_ne_0R \subseteq e_0R,$$

that is a'_nR is generated by the idempotent e_0.
Denoting $f_1 = f - a_nX^n + a'_nX^n$, $f = f_1 - N$, where N is nilpotent.
We have $f_1g = fg + Ng$ and thus $(f_1g - fg)^{n+d-m} = 0$ and we can explicitly find a polynomial D in $R[X]$ such that $f_1gD = (fg)^{n+d-m}$ monic with degree $m(n+d-m)$.
Of course, the degree coefficient of f_1 is a'_n. It remains only to do as in the reduced case, just replace f by f_1, a_n by a'_n, a_nb_{m-n} by $(a_nb_{m-n})^{n+d-m}$, g by gD, and m by $(n+d-m)m$.

3) Suppose that $f \in U(X)^*$. It is clear that one easily obtains an equality asserting that $\langle a_0, \ldots, a_n\rangle = R$. For each $j \in \{0, \ldots, n\}$, considering the ring $R/\langle a_{j+1}, \ldots, a_n\rangle$ and reviewing the proof of part 2), we see that the first step of the algorithm produces an equality of the form $\bar{a_j}^{k_j} = \bar{0}$ or $\bar{a_j}^{k_j+1}\bar{\beta_j} = \bar{a_j}^{k_j}$ for some $\beta_j \in R$. Hence, $(a_j(a_j\beta_j - 1))^{k_j} \equiv 0 \bmod \langle a_{j+1}, \ldots, a_n\rangle$.

Conversely, suppose that $\langle a_0, \ldots, a_n\rangle = R$ and, that for each $j \in \{0, \ldots, n\}$, we can find $\beta_j \in R$ and $k_j \in \mathbb{N}$ such that $(a_j(a_j\beta_j - 1))^{k_j} \equiv 0 \bmod \langle a_{j+1}, \ldots, a_n\rangle$. Since $(a_n(a_n\beta_n - 1))^{k_n} = 0$, we have $a_n^{k_n+1}\gamma_n = a_n^{k_n}$, where $\gamma_n = \sum_{i=1}^{k_n} \mathrm{C}_{k_n}^i(-1)^{k_n-i}a_n^{i-1}\beta_n^i$. Now, as in the proof of part 2), we can write $f = f_1 - N$, where $f_1 = f - a_nX^n + \gamma_n^{k_n}a_n^{k_n+1}X^n$, and $N^{k_n} = 0$. To prove that f divides some monic polynomial, it suffices to do the same for f_1.
Denoting by $e_0 = (a_n\gamma_n)^{k_n}$, e_0 is idempotent by Lemma 1, $R = Re_0 \oplus R(1-e_0)$, $f_1 = f_1e_0 + f_1(1-e_0)$, and the degree coefficient of f_1e_0 is a unit of $Re_0[X]$. Our task is then reduced to

prove that $f_1(1-e_0)$ divides some monic polynomial in $R(1-e_0)[X]$. Since $\deg(f_1(1-e_0)) < n$ and all the hypotheses on f are inherited by $f_1(1-e_0)$, the desired result can be obtained by induction on n. Note that the condition $\langle a_0, \ldots, a_n\rangle = R$ is needed to get the induction started.

4) This equivalence was given in [2]. The condition:

$$a_{j+1}, \ldots, a_n \in p,\ a_j \notin p \text{ imply that } a_j \text{ is a unit modulo } p$$

is easily seen to be necessary as a consequence of 2). The proof that the condition is sufficient needs at least the axiom saying that any non trivial ring has a prime ideal (this is a weak version of choice). So it cannot be constructive. However, 3) can be seen as a constructive reformulation of 4) obtained by mean of the notion of "idealistic prime" [1,5]. $\diamondsuit$

Example 1. Let U and V be two indeterminates over a field K, and consider the reduced ring $R = K[U,V]/(U^2-U, UV) = K[u,v] = K[v] \oplus K[v]u$, where $u^2 = u$ and $uv = 0$.
Setting $f = u-(1+u)X^2+uX^3$ and $g = v+uX^2+(u-1)X^3$, we have $fg = (u-v)X^2-2uX^4+X^5$.

Using the algorithm described in the proof of Proposition 1, we find:
$e_0 = a_3b_2 = u^2 = u$, $R_0 = Ru = uK[u,v]$, $f_0 = uf = u - 2uX^2 + uX^3$, $g_0 = uX^2$, $R_0' = R_1 = R(1-u) = (1-u)K[u,v]$, $f_0' = f_1 = (u-1)X^2$, $g_0' = g_1 = v + (u-1)X^3$.
Thus, in $K[u,v] = uK[u,v] \oplus (1-u)K[u,v]$, the decomposition of f is $f = (u-2uX^2+uX^3) + ((u-1)X^2)$.
Of course, $R_0 = uK[u,v] \simeq R$, by this isomorphism $f_0 \leftrightarrow 1 - 2X^2 + X^3$, $g_0 \leftrightarrow X^2$;
$R_1 = (1-u)K[u,v] \simeq R$, by this isomorphism $f_1 \leftrightarrow -X^2$, $g_1 \leftrightarrow v - X^3$.

Example 2. Let U and V be two indeterminates over a field K such that Char$K \neq 2$, and consider the non reduced ring $R = K[U,V]/(U^2-U, UV^2) = k[u,v] = K[v] \oplus Ku \oplus Kuv$, where $u^2 = u$ and $uv^2 = 0$. The nilradical of R is $\mathcal{N} = (uv)$ and $R/\mathcal{N} = K[U,V]/(U^2-U, UV) = K[u', v']$ with $u'^2 = u'$ and $u'v' = 0$.
Setting $f = u-(1+u)X^2+uX^3+uvX^4$ and $g = -v^4+uX^2+2v^2X^3-2uX^4+uX^5+(u-1-uv)X^6$, we have $fg = (u+v^4)X^2 - 4uX^4 + (u-v^2)X^5 + 4uX^6 - 4uX^7 + X^8$.

- If we want to decompose $R/\mathcal{N}$, we consider the images modulo $\mathcal{N}$, $f' = u' - (1+u')X^2 + u'X^3$, $g' = -v'^4 + u'X^2 + 2v'^2X^3 - 2u'X^4 + u'X^5 + (u'-1)X^6$, $f'g' = (u'+v'^4)X^2 - 4u'X^4 + (u'-v'^2)X^5 + 4u'X^6 - 4u'X^7 + X^8$, respectively of f, g , and fg.
As in Example 1, our algorithm yields to the direct sum decompositions:
$R/\mathcal{N} = u'K[u',v'] \oplus (1-u')K[u',v']$,
$f' = (u' - 2u'X^2 + u'X^3) + ((u'-1)X^2)$.
$f - uvX^4 = (u - 2uX^2 + uX^3) + ((u-1)X^2)$, where $(uvX^4)^2 = 0$.

- If we want to decompose R, using the algorithm described in the proof of Proposition 1 for the non reduced case, we have:
$((f-uvX^4)g - fg)^2 = 0$ and thus $(f-uvX^4)(g^2(f+uvX^4)) = (fg)^2$.
Note that g^2 has degree 12 and highest coefficient $1-u$, $f+uvX^4$ has degree 4 and highest coefficient $2uv$, whereas $g^2(f+uvX^4)$ has degree 14 and highest coefficient $u-1-uv$.
The first idempotent element found is $e_0 = (a_3b_{13})^{17-16} = a_3b_{13} = a_3((g^2)_{12}(f+uvX^4)_1 + (g^2)_{11}(f+uvX^4)_2 + (g^2)_{10}(f+uvX^4)_3 + (g^2)_9(f+uvX^4)_4 = uu = u$.
Thus, $f_0 = (f-uvX^4)u = u - 2uX^2 + uX^3$, $f_0' = f_1 = (f-uvX^4)(1-u) = (u-1)X^2$, $R = K[u,v] = uK[u,v] \oplus (1-u)K[u,v]$, and $f - uvX^4 = (u-2uX^2+uX^3) + ((u-1)X^2)$, where $(uvX^4)^2 = 0$.

2. THE UNITS OF $R[X, X^{-1}]_{\mathcal{V}}$

We consider the following regular multiplicative subsets of $R[X]$:

$U(X) = \{f \in R[X], f \text{ is monic}\}$,
$S = \{X^n, n \in \mathbb{N}\}$,
$W = \{f \in R[X], f(0) = 1\}$,
$V = U(X) \cap W = \{1 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n, n \in \mathbb{N} \setminus \{0\}, a_i \in R\}$,
$\mathcal{V} = \{f \in R[X, X^{-1}],$ the coefficient of the highest and lowest terms are equal to $1\}$.

Note that $R[X, X^{-1}]_{\mathcal{V}} = R[X]_{SV}$. By the following two propositions, we give characterizations of the saturations of V and $\mathcal{V}$. The proofs of parts 1), 2), 3) and 4) in Proposition 2 and Proposition 3 are constructive.

Proposition 2. *Let $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n \in R[X]$.*
1) If R is reduced, then $f \in V^*$ if and only if there exists a direct sum decomposition $R = R_0 \oplus \cdots \oplus R_m$ $(m \leq n)$ of R such that if $f = f_0 + \cdots + f_m$ is the decomposition of f with respect to the induced decomposition $R[X] = R_0[X] \oplus \cdots \oplus R_m[X]$, then both of the constant and degree coefficients of f_i are units in R_i for each i.
2) If R is not reduced, then $f \in V^*$ if and only if there exist a nilpotent polynomial N and a direct sum decomposition $R = R_0 \oplus \cdots \oplus R_m$ $(m \leq n)$ of R such that if $f - N = f_0 + \cdots + f_m$ is the decomposition of $f - N$ with respect to the induced decomposition $R[X] = R_0[X] \oplus \cdots \oplus R_m[X]$, then both of the constant and degree coefficients of f_i are units in R_i for each i.
3) $V^* = \{f \in R[X], f(0)$ and the degree coefficient of f are units$\}$ if and only if R is reduced and indecomposable.
4) $f \in V^*$ if and only if a_0 is a unit and, for each $j \in \{0, \ldots, n\}$, we can find $\beta_j \in R$ 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) $f \in V^*$ if and only if a_0 is a unit and, for each prime ideal p of R, the relations $a_{j+1}, \ldots, a_n \in p$, $a_j \notin p$, imply that a_j is a unit modulo p.

Proof. 1) For the necessity, the system of idempotents corresponding to the direct sum decomposition $R = R_0 \oplus \cdots \oplus R_m$ is given by Proposition 1.1). It is clear that for each i, the constant coefficient of f_i is a unit in R_i. For the sufficiency, for each i, denote by α_i and β_i respectively the inverses of the constant and degree coefficients of f_i in R_i, and by n_i the degree of f_i $(n_i \leq n)$. Then

$$\left(\sum_{i=0}^{m}(\alpha_i + \beta_iX^{n-n_i})\right) f$$

has 1 as constant and degree coefficient and $f \in V^*$.
2) Do as in Proposition 1.2).
3) By virtue of 2), it suffices to prove that the result fails if R is not reduced or is decomposable. If R is not reduced, let γ be a nonzero nilpotent in R. Since $1 + \gamma X$ is a unit in $R[X]$, then $1 + \gamma X \in V^*$, while γ is not a unit. If R is decomposable, write $1 = e_1 + e_2$, where e_1 and e_2 are two orthogonal idempotents in R. Then $(1 + e_1X)(1 + e_2X) = 1 + X$ and thus $1 + e_1X \in V^*$, while e_1 is not a unit in R.
4) Do exactly as in Proposition 1.3).
5) Same remarks as for Proposition 1.4). $\diamondsuit$

Proposition 3. *Let $f(X) = a_kX^k + a_{k+1}X^{k+1} + \cdots + a_lX^l \in R[X, X^{-1}]$, $k, l \in \mathbb{Z}$.*
1) $f \in \mathcal{V}^*$ if and only if there exist $n \in \mathbb{N} \setminus \{0\}$ and $m \in \mathbb{N} \setminus \{0\}$ such that $X^n f(X) \in U(X)^*$ and $X^m f(X^{-1}) \in U(X)^*$,
2) In the case R is reduced, $f \in \mathcal{V}^*$ if and only if there exists a direct sum decomposition $R = R_0 \oplus ... \oplus R_m$ of R such that if $f = f_0 + \cdots + f_m$ is the decomposition of f with respect to the induced decomposition $R[X, X^{-1}] = R_0[X, X^{-1}] \oplus \cdots \oplus R_m[X, X^{-1}]$, then the coefficients of the highest and lowest terms of f_i are units in R_i for each i.
3) $\mathcal{V} = \{f \in R[X, X^{-1}]$, the coefficient of the highest and lowest terms are units$\}$ if and only if R is reduced and indecomposable.
4) $f \in \mathcal{V}^*$ if and only if $\langle a_k, \ldots, a_l\rangle = R$ and, for each $j \in \{k, \ldots, l\}$, we can find $\beta_j, \delta_j \in R$ 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 $(a_j(a_j\delta_j - 1))^{n_j} \equiv 0 \bmod \langle a_k, \ldots, a_{j-1}\rangle$.
5) $f \in \mathcal{V}^*$ if and only if $\langle a_k, \ldots, a_l\rangle = R$ and, for each prime ideal p of R, the relations $a_{j+1}, \ldots, a_l \in p$, $a_j \notin p$ or $a_k, \ldots, a_{j-1} \in p$, $a_j \notin p$, imply that a_j is a unit modulo p.

Proof. 1) It is clear that the condition is necessary. For the sufficiency, suppose that we can find two polynomials $g, h \in R[X]$ such that $X^n f(X)h(X) \in U(X)$ and $X^m f(X^{-1})g(X) \in U(X)$. Then, $(X^n h(X) + X^{-m}g(X^{-1}))f \in \mathcal{V}$ and $f \in \mathcal{V}^*$.
2) Using Proposition 1 and part 1), if $x_0, \ldots, x_p$ and $y_0, \ldots, y_q$ are two systems of nonzero orthogonal idempotents associated respectively to $X^n f(X)$ and $X^m f(X^{-1})$, then denoting $\{x_iy_j, 0 \leq i \leq p, 0 \leq j \leq q\} = \{\epsilon_0, \ldots, \epsilon_m\}$, we take $R_i = R\epsilon_i$. For the sufficiency, for each i, denote by α_i and β_i respectively the inverses of the lowest and highest coefficients of f_i in R_i, and by k_i and l_i respectively the lowest and highest degrees of f_i ($k \leq k_i$, $l_i \leq l$). Then

$$\left(\sum_{i=0}^{m}(\alpha_i X^{k-k_i} + \beta_i X^{l-l_i})\right) f$$

has 1 as lowest and highest coefficient and $f \in \mathcal{V}^*$.
3) Do exactly as in Proposition 2.3).
4) Do exactly as in Proposition 1.3).
5) Same remarks as for Proposition 1.4). $\diamondsuit$

It is clear that for any ring R, $U(X + X^{-1}) \subseteq \mathcal{V}$ and $U(X + X^{-1}) \neq \mathcal{V}$. Next, we prove that $U(X + X^{-1})^* = \mathcal{V}^*$ in $R[X, X^{-1}]$, that is, each doubly monic Laurent polynomial divides some monic polynomial in $X + X^{-1}$.

Proposition 4. *For each $f \in \mathcal{V}$, there exists $g \in \mathcal{V}$ such that $fg \in U(X + X^{-1})$.*

Proof. Remark that a Laurent polynomial q is in $R[X + X^{-1}]$ iff $q(X) = q(X^{-1})$. Let γ the degree coefficient of $f(X)f(X^{-1})$. We take $g = \gamma^{-1}f(X^{-1})$. $\diamondsuit$

Corollary 1. *For any ring R, $R[X, X^{-1}]_{\mathcal{V}} = R[X, X^{-1}]_{U(X+X^{-1})}$ and $R[X, X^{-1}]_{\mathcal{V}}$ is a finitely generated free $R\langle X + X^{-1}\rangle$-module generated by 1 and X.*

Proof. This follows from Proposition 4 and the fact that $R[X, X^{-1}]$ is a finitely generated free $R[X + X^{-1}]$-module generated by 1 and X [3, Lemma 1]. $\diamondsuit$

We also obtain an alternative constructive proof of the following well-known result.

Corollary 2. *If K is a field then every finitely generated projective module over $K[X_1^{\pm 1}, X_2^{\pm 1} \ldots, X_n^{\pm 1}]$ is stably free.*

Proof. We reasone by induction on n. Let P be a finitely generated projective module over $A = K[X_1^{\pm 1}, X_2^{\pm 1} \ldots, X_n^{\pm 1}]$. By [4, Lemma 2.1 p. 90], we can find a finite rank free A-submodule F of P and $f \in A - \{0\}$ such that $fP \subseteq F$.
After the change of variables $X_1 = Y_1$, $X_2 = Y_2 Y_1^m$,..., $X_n = Y_n Y_1^{m^{n-1}}$, for sufficiently large m, f becomes doubly monic in Y_1. By Proposition 4, we can find $g \in A$ such that $fg \in B = K[Y_2^{\pm 1}, \ldots, Y_{n-1}^{\pm 1}][Y_1 + Y_1^{-1}]$ and fg is monic relatively to $Y_1 + Y_1^{-1}$.
Since $(fg)gF \subseteq (fg)P \subseteq gF$, the Towber presentation applies [5, Proposition 2.2 p. 91], where the modules are considered as B-modules ($A = B^2$). $\diamondsuit$

Note that we can also obtain a constructive proof of the fact that finitely generated projective modules over $A = K[X_1^{\pm 1}, X_2^{\pm 1} \ldots, X_n^{\pm 1}]$ are free using Corollary 2 and the fact that $\mathrm{GL}_r(A)$ acts transitively on $\mathrm{Um}_r(A)$ for $r \geq 1$ [9].

ACKNOWLEDGMENTS

I am thankful to Henri Lombardi for suggesting to me this problem and many useful comments.

References

[1] Th. Coquand, H. Lombardi, Hidden constructions in abstract algebra (3) Krull dimension, going-up, going-down. Preprint 2001.

[2] R. Gilmer, W. Heinzer, On the divisors of monic polynomials over a commutative ring, Pac. J. Math. **78** (1978), 121–131.

[3] S. Glaz, On the weak dimension of coherent group rings, Comm. Algebra **15**(9) (1987), 1841–1858.

[4] S.K. Gupta, M.P. Murthy, Suslin's work on linear groups over polynomial rings and Serre problem, Indian Statistical Institute Lecture Notes Series, Vol. 8, Macmillan, New Delhi, 1980.

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

[6] H. Lombardi, C. Quitté, Constructions cachées en algèbre abstraite (2) Le principe local global. To appear in Proceeding of the Fourth International Conference on Commutative Ring Theory and Applications held June 7-11, 2001 in Fez, Morocco, Marcel Dekker (2002).

[7] S. Mandal, About direct summands of projective modules over Laurent polynomial rings, Proc. Amer. Math. Soc. **112** (1991), 915–918.

[8] S. Mandal, Projective modules and complete intersections, Lect. Notes. Math. 1672, Springer-Verlag, Berlin, 1997.

[9] H. Park, A computational theory of Laurent polynomial rings and multidimensional fir systems, Ph.D. Thesis, UC Berkeley, Berkeley, CA, 1995.

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