JOURNAL OF ALGEBRA 103, 1–17 (1986)

On the Computation of Minimal Polynomials

DAVID R. RICHMAN

Department of Mathematics and Statistics, University of South Carolina, Columbia, South Carolina 29208

Communicated by David Buchsbaum

Received February 7, 1984

Let K be a field and let f and g be non-constant elements of $K[T]$. Assume that $\gcd(\deg f, \deg g)$ is not divisible by the characteristic of K. This paper describes an algorithm to compute the polynomial $p(X, Y)$ of minimal degree such that $p(f, g) = 0$. Using ideas needed to justify the algorithm, a new proof is given of the fact that if $K[f, g] = K[T]$, then either $\deg g$ divides $\deg f$ or $\deg f$ divides $\deg g$.

1. INTRODUCTION

Let f and g be non-constant polynomials in one variable, and let $p(X, Y)$ be the polynomial of minimal degree such that $p(f, g) = 0$. In [PR] an algorithm to compute $p(X, Y)$ is described. The authors remark without proof that the algorithm simplifies considerably when the characteristic of the scalar field does not divide the greatest common divisor of $\deg f$ and $\deg g$. The main goal of this paper is to explain this simplified algorithm. Using the principles involved in justifying the algorithm, a new proof is given of the following result.

THEOREM A. *Let $f, g \in K[T] - \{0\}$. Assume that the characteristic of K does not divide $\gcd(\deg f, \deg g)$. If $K[f, g]$ equals $K[T]$ then either $\deg f$ divides $\deg g$ or $\deg g$ divides $\deg f$.*

This result, in the case that K is an algebraically closed field of characteristic zero, first appears in [S], but the proof is incorrect. The first correct proof of Theorem A appears in [AM2] and a simplification of the proof can be found in [A] and in [M]. This paper presents a proof of Theorem A which differs from the previous ones in that it does not involve any Puiseux expansions.

Section 2 describes results which are needed to justify the minimal polynomial algorithm. This section also contains a proof of Theorem A.

0021-8693/86 $3.00

Section 3 describes two algorithms to compute the minimal polynomial $p(X, Y)$, assuming that the characteristic of K does not divide $\gcd(\deg f, \deg g)$. It also describes algorithms to compute generators for the semigroup

$$\{\deg y\colon y \in K[f, g], y \neq 0\}.$$

Abhyankar has a somewhat different algorithm to compute these generators, based on ideas found in [A].

2. Some Algebraic Results

Let N denote the degree of the field extension $K(f, g)/K(g)$. It is assumed thoughout this section that $N > 1$. Let d be the greatest common divisor of $\deg f$ and $\deg g$. The following is the main result of this section.

($*$) *Assume that the characteristic of K does not divide* $\deg g$. *There exists elements $h_1, \ldots, h_{N-1}$ of $K[T]$ such that*

(i) *for each i, $h_i \in f^i + K[g] f^{i-1} + \cdots + K[g]$, and*

(ii) *the numbers* 0, $\deg h_1, \ldots, \deg h_{N-1}$ *are pairwise incongruent* mod-$\deg g$.

Proposition 1. *Assume that ($*$) is true. If the characteristic of K does not divide d and if $K[f, g]$ contains an element of degree d, then either* $\deg f$ *divides* $\deg g$ *or* $\deg g$ *divides* $\deg f$.

Proof. By interchanging f and g if necessary, we assume that the characteristic of K does not divide $\deg g$. Let $h_1, \ldots, h_{N-1}$ be polynomials satisfying the conditions of ($*$). Define $h_0 = 1$. One can easily show by induction on j that the space $K[g] + K[g] f + \cdots + K[g] f^j$ is generated as a $K[g]$ module by the elements $h_0, \ldots, h_j$, whenever $0 \leqslant j < N$. Hence, if w is a non-zero element of the space

$$K[g] + \cdots + K[g] f^j,$$

there exists elements $c_0, \ldots, c_j$ in $K[g]$ such that

$$w = c_0 h_0 + \cdots + c_j h_j.$$

Combining this equation with the fact that the numbers $\deg h_0, \ldots, \deg h_j$

are pairwise incongruent mod $\deg g$, one concludes that for some subscript i, $\deg w$ equals $\deg c_i h_i$. Hence there are non-negative integers s, i such that

$$\deg w = \deg g^s h_i, \qquad 0 \leqslant i \leqslant j. \tag{1}$$

Define $e = (\deg g)/d$. Observe that the numbers

$$0, \deg f, ..., (e-1) \deg f$$

are pairwise incongruent mod $\deg g$. Hence any non-zero element of the space $K[g] + \cdots + K[g] f^{e-1}$ has the same degree as some element of

$$K[g] \cup \cdots \cup K[g] f^{e-1}.$$

In particular, if $0 \leqslant j < e$ there exist non-negative integers p, q such that

$$\deg h_j = \deg f^p g^q. \tag{2}$$

Since $\deg f/d$ and e and relatively prime, there exist integers m and n such that

$$(m)(\deg f)/d + ne = 1.$$

One may furthermore choose m so that

$$0 \leqslant m < e;$$

we assume that m satisfies these inequalities. Observe that

$$m \deg f \equiv d \bmod \deg g. \tag{3}$$

Suppose that w is an element of $K[f, g]$ of degree d. Since

$$K[f, g] = K[g] + K[g] f + \cdots + K[g] f^{N-1}$$

Eq. (1) implies that there are non-negative integers s, J such that

$$d = \deg g^s h_J. \tag{4}$$

This equation and Eq. (3) imply that

$$m \deg f \equiv \deg h_J \bmod \deg g. \tag{5}$$

Equation (1) implies that there is a subscript i for which

$$\deg f^m \equiv \deg h_i \bmod \deg g, \tag{6}$$

where $0 \leqslant i \leqslant m$. Congruences (5) and (6) imply that $\deg h_J$ is congruent to $\deg h_i \bmod \deg g$; hence $i = J$. Therefore $J \leqslant m < e$. Equations (4) and (2) imply that

$$d = \deg g^{q+s} f^p.$$

Since $q + s$ and p are non-negative integers, the preceding equation implies that $d \geqslant \min(\deg f, \deg g)$. On the other hand, d divides both $\deg f$ and $\deg g$, so $d = \min(\deg f, \deg g)$. Therefore either $\deg f$ divides $\deg g$ or $\deg g$ divides $\deg f$. This finishes the proof.

Observe that Theorem A is an immediate consequence of (*) and Proposition 1. The rest of this section is devoted to proving (*).

DEFINITION. Let S be a subset of $K[T] - \{0\}$ whose elements have distinct degrees. If h is an element of $K[T]$, define $R(h, S)$ as follows. Set $R(h, S) = h$ if $\deg h$ is different from the degree of any element of S. In general set

$$R(h, S) = h - s_1 - \cdots - s_t,$$

where $s_1, \ldots, s_t$ are scalar multiples of elements of S such that

$$\deg h > \deg(h - s_1) > \cdots > \deg(h - s_1 - \cdots - s_t)$$

and such that

> $\deg(h - s_1 - \cdots - s_t)$ is different from the degree of any element of S.

Observe that $R(h, S) = 0$ if and only if h lies in the span of S.

The following result is implicit in [PR, Sect. 4].

PROPOSITION 2. *There exist non-zero polynomials $h_1, \ldots, h_{N-1}$ such that*

(i) *for each subscript i, $h_i \in K[g]f^i + K[g]f^{i-1} + \cdots + K[g]$,*

(ii) *the numbers 0, $\deg h_1, \ldots, \deg h_{N-1}$ are pairwise incongruent* $\bmod \deg g$.

Proof. Set $S = \{g^n : n = 0, 1, 2, \ldots\}$. Define $h_1 = R(f, S)$. By definition of the function R, $\deg h_1$ is not equal to the degree of any element of S, so $\deg h_1$ is not divisible by $\deg g$.

Assume that $h_1, \ldots, h_i$ have been defined so that the properties of the Proposition hold. Define $h_0 = 1$ and set

$$T = T_i = \{h_t g^n : 0 \leqslant t \leqslant i, 0 \leqslant n\}.$$

Define a sequence of elements $y_0, y_1,..$ in $K[g]f^{i+1}+K[g]f^i+\cdots+K[g]$ by

$$y_0=R(f^{i+1}, T)$$
$$y_1=R(gf^{i+1}, T\cup\{y_0\})$$
$$\vdots$$
$$y_m=R(g^m f^{i+1}, T\cup\{y_0, y_1,..., y_{m-1}\})$$
$$\vdots$$

Observe that if $i+1<N$, the elements $y_0, y_1,...$ are all non-zero. By definition of the function R, the degrees of the y_i's are distinct and, for each i, $\deg y_i$ is different from the degree of any element of T.

For each integer t satisfying $0\leqslant t\leqslant i$, there are only finitely many non-negative integers which are congruent to, but strictly less than, $\deg h_t$. Therefore, if $i+1<N$, there must exist a subscript m for which $\deg y_m$ is not congruent mod $\deg g$ to the degree of any element of T. Set $h_{i+1}=y_m$ and observe that the elements $h_0,..., h_{i+1}$ have the desired properties. By induction this finishes the proof.

Proposition 2 implies that there exist elements $h_1,..., h_{N-1}$ in $K(f, g)$ which satisfy the following conditions.

(**) (i) *For each* i, $h_i\in f^i+K(g)f^{i-1}+\cdots+K(g)$.

(ii) *The numbers* $0, \deg h_1,..., \deg h_{N-1}$ *are pairwise incongruent* mod $\deg g$.

To establish (*) it suffices to find elements $h_1,..., h_{N-1}$ which lie in $K[f, g]$ and which satisfy the condition (**). The following proposition gives a criterion for an element of $K(f, g)$ to lie in $K[f, g]$. This criterion was also used in the earlier proofs of Theorem A (cf. [A, pp. 265–270; AM1, pp. 42–49]); for the sake of keeping the exposition selfcontained, the proof is repeated here.

PROPOSITION 3 (Abhyankar and Moh). *Let* e *and* D *be positive integers such that* $eD\leqslant N$ *and such that the characteristic of* K *does not divide* e. *Let* $h\in f^D+K(g)f^{D-1}+\cdots+K(g)$ *and let* $t\in f^{eD}+K[g]f^{eD-1}+\cdots+K[g]$. *Assume that* $h^e-t\in K(g)+K(g)f+\cdots+K(g)f^{eD-D-1}$; *then* $h\in K[f, g]$.

Proof. Let $H(Y)$ and $T(Y)$ be the monic elements of $K(g)[Y]$ such that $H(f)=h$, $T(f)=t$, $\deg H=D$, and $\deg T=eD$. Since $eD\leqslant N$, $H(Y)$ and $T(Y)$ are uniquely determined by h and by t, respectively; the coefficients of $T(Y)$ must lie in $K[g]$. If j is an integer satisfying $eD\geqslant j\geqslant eD-D$, the coefficient of Y^j in $H^e(Y)$ is the same as the coefficient of Y^j in $T(Y)$. It follows that the coefficients of $H(Y)$ are expressible as polynomial functions of the coefficients of $T(Y)$. Therefore they lie in $K[g]$. Therefore $h = H(f)$ lies in $K[f, g]$.

In order to apply Proposition 3 it is useful to focus on certain divisors of N. The next definition and proposition identify such divisors.

DEFINITION. Let $h_1, \ldots, h_{N-1}$ be elements of $K(f, g)$ which possess properties (**). Set $h_0 = g$. Define the gcd-decreasing sequence of $h_1, \ldots, h_{N-1}$, denoted $c(1), \ldots, c(k)$, as follows.

Set $c(1) = 1$.

Suppose that $c(1), \ldots, c(t)$ have been defined. If for every subscript i one has

$$\deg h_i \in \mathbb{Z} \deg h_0 + \mathbb{Z} \deg h_1 + \cdots + \mathbb{Z} \deg h_{c(t)}$$

then $c(t)$ is the last element in the gcd-decreasing sequence. Otherwise let i be the smallest subscript such that $i > c(t)$ and such that

$$\deg h_i \notin \mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{i-1};$$

define $c(t+1) = i$.

Note that a positive integer c lies in the gcd-decreasing sequence if and only if the space $f^c + K(g) f^{c-1} + \cdots + K(g)$ contains an element whose degree does not lie in the additive group generated by the set

$$\{\deg y : y \in K(g) + K(g) f + \cdots + K(g) f^{c-1}\}.$$

Thus the gcd-decreasing sequence depends only on the pair (f, g) and not on the choice of the sequence $h_1, \ldots, h_{N-1}$.

For the rest of this section $h_1, \ldots, h_{N-1}$ will denote elements of $K(f, g)$ satisfying (**) and $c(1), \ldots, c(k)$ will denote the gcd-decreasing sequence of $h_1, \ldots, h_{N-1}$. Set $h_0 = g$ and set $c(k+1) = N$.

PROPOSITION 4. *If $1 \leqslant t \leqslant k$, let $e = e_t$ be the smallest positive integer such that*

$$e \deg h_{c(t)} \in \mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)-1};$$

then $ec(t) = c(t+1)$. In particular $c(t)$ divides $c(k+1) = N$ for all t.

Proof. Set

$$B = B_t = \{h_n h_{c(t)}^j : 0 \leqslant n < c(t), 0 \leqslant j < e_t\}.$$

Observe that the set B contains one element from each of the sets

$$\{g\}, f + K(g), \ldots, f^{ec(t)-1} + K(g) f^{ec(t)-2} + \cdots + K(g).$$

Therefore the $K(g)$ span of B is the set $K(g)+K(g)f+\cdots+K(g)f^{ec(t)-1}$. Furthermore the degrees of the elements of B are pairwise incongruent mod deg g. Therefore, for any non-zero element $w \in K(g)+\cdots+K(g)f^{ec(t)-1}$, deg w is congruent mod deg g to the degree of some element of B. In particular

$$\deg h_m \in \mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)} \qquad \text{when} \quad 0 \leqslant m < ec(t).$$

On the other hand, by the definition of gcd-decreasing sequence,

$$\deg h_{c(t+1)} \notin \mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)} \qquad \text{when} \quad t \leqslant k-1.$$

Therefore

$$ec(t) \leqslant c(t+1) \tag{7}$$

when $t \leqslant k-1$. The elements of B are linearly independent over $K(g)$ because their degrees are pairwise incongruent mod deg g. Therefore

$$ec(t) = |B| \leqslant N;$$

this shows that (7) also holds when $t=k$.

It will be shown that $ec(t)=c(t+1)$ by induction on t.

Claim. Let $D=D_t$ be the additive group generated by the numbers $\deg h_0, \deg h_1, ..., \deg h_{c(t)}$. For any $d \in D$ there exists an element $b \in B$ such that $d \equiv \deg b \bmod \deg g$.

Let $\bar{D}$ denote the natural image of D in $\mathbb{Z}/\deg g\mathbb{Z}$ and observe that $|\bar{D}_t| = e_t e_{t-1} \cdots e_1$. Furthermore $|B| = e_t c(t)$, so by applying the induction hypothesis repeatedly one gets $|B| = e_t e_{t-1} \cdots e_1$. Thus $|B| = |\bar{D}|$. The claim is an immediate consequence of this and of the fact that the degrees of the elements of B are pairwise incongruent mod deg g.

Set $n=ec(t)$ and suppose that $n<N$. Since by (**), the numbers $\deg h_0, ..., \deg h_n$ are pairwise incongruent mod deg g, $\deg h_n$ is different from the degree of any element in the $K(g)$ span of $h_0, ..., h_{n-1}$. Therefore $\deg h_n$ is different from the degree of any element of B, so by the Claim, $\deg h_n$ does not lie in D_t. Hence by the definition of gcd-decreasing sequence, $\deg h_n$ does not lie in the additive group generated by $\deg h_0, ..., \deg h_{c(t+1)-1}$. Therefore $n \geqslant c(t+1)$. This inequality and (7) imply that $ec(t)=c(t+1)$ whenever $ec(t)<N$. If $ec(t) \geqslant N$ then by (7) $t=k$ and $ec(t)=N=c(k+1)$. This finishes the proof.

PROPOSITION 5. *Define $e=e_t$ as in Proposition 4. Set $h=h_{c(t)}$ and set $h_N=0$. There exist elements $w_1, ..., w_e$ in $K(g)+K(g)f+\cdots+K(g)f^{c(t)-1}$ such that*

$$h^e - h_{c(t+1)} = w_1 h^{e-1} + w_2 h^{e-2} + \cdots + w_e. \tag{8}$$

The elements $w_1, \ldots, w_e$ are uniquely determined by (8). Furthermore, $\deg w_1 < \deg h$.

Proof. Set $B = \{h_n h^j : 0 \leqslant n < c(t),\ 0 \leqslant j < e_t\}$. Since the $K(g)$ span of B is the space $K(g) + K(g) f + \cdots + K(g) f^{ec(t)-1}$ and since, by Proposition 4, $ec(t) = c(t+1)$, it is possible to express $h^e - h_{c(t+1)}$ as a $K(g)$ linear combination of the elements of B. Thus one can write

$$h^e - h_{c(t+1)} = a_1(g)\, b_1 + \cdots + a_s(g)\, b_s \tag{9}$$

where $b_1, \ldots, b_s$ are distinct elements of B. Equation (9) is equivalent to (8). The elements $w_1, \ldots, w_e$ are uniquely determined because the elements of B are linearly independent over $K(g)$.

Since the degrees of the elements of B are pairwise incongruent mod $\deg g$, the non-zero elements in the sequence $a_1(g)\, b_1, \ldots, a_s(g)\, b_s$ have distinct degrees. Therefore, for some subscript I,

$$\deg a_I(g)\, b_I = \deg(h^e - h_{c(t+1)}), \tag{10}$$

and

$$\deg a_i(g)\, b_i < \deg(h^e - h_{c(t+1)}) \qquad \text{for all } i \neq I. \tag{11}$$

Observe that $\deg a_I(g)\, b_I$ and $\deg h^e$ lie in the set $\mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)}$, whereas $\deg h_{c(t+1)}$ does not. From this and from (10) one concludes that $\deg h_{c(t+1)} < \deg h^e$, so $\deg(h^e - h_{c(t+1)}) = e \deg h$. Therefore (11) implies that

$$\deg a_i(g)\, b_i < e \deg h \tag{12}$$

whenever $\deg b_i$ is not congruent to $e \deg h \bmod \deg g$. Therefore (12) holds whenever $\deg b_i$ does not lie in the set $\mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)-1}$. By the definition of e and of gcd-decreasing sequence, $\deg h_n h^{e-1} \notin \mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)-1}$ when $0 \leqslant n < c(t)$. Therefore $\deg w_1 h^{e-1} < e \deg h$, so $\deg w_1 < \deg h$. This finishes the proof.

The next proposition is a special case of a result which can be found in [A, pp. 268–270] and in [AM1, pp. 42–49].

PROPOSITION 6. *Fix an integer t such that $1 \leqslant t \leqslant k$. Let $h = h_{c(t)}$ and let $e = e_t$ as in Proposition 4. Assume that the characteristic of K does not divide e and set $\bar{h} = h - (1/e)\, w_1$, where w_1 is as in (8). Write*

$$\bar{h}^e - h_{c(t+1)} = y_1 \bar{h}^{e-1} + \cdots + y_e$$

where each y_i lies in $K(g) + \cdots + K(g) f^{c(t)-1}$. Either $y_1 = 0$ or $\deg y_1 < \deg w_1$.

Proof. Observe that

$$\bar{h}^e - h_{c(t+1)} = (h - (1/e)\, w_1)^e - h_{c(t+1)}$$
$$= w_2 h^{e-2} + \cdots + w_e + R,$$

where $\deg R < \deg w_1 h^{e-1}$ when $w_1 \neq 0$. There exists elements $\bar{w}_2, \ldots, \bar{w}_e$, $z_1, \ldots, z_e$ in $K(g) + \cdots + K(g) f^{c(t)-1}$ such that

$$w_2 h^{e-2} + \cdots + w_e = \bar{w}_2 \bar{h}^{e-2} + \cdots + \bar{w}_e,$$

and

$$R = z_1 \bar{h}^{e-1} + z_2 \bar{h}^{e-2} + \cdots + z_e.$$

Note that z_1 must equal y_1. By Proposition 5, $\deg h = \deg \bar{h}$, so the numbers 0, $\deg \bar{h}, \ldots, (e-1) \deg \bar{h}$ are pairwise incongruent $\bmod\, \mathbb{Z} \deg h_0 + \cdots + \mathbb{Z} \deg h_{c(t)-1}$. Therefore the non-zero terms in the sequence $z_1 \bar{h}^{e-1}$, $z_2 \bar{h}^{e-2}, \ldots, z_e$ have distinct degrees, so $\deg R \geqslant \deg z_i \bar{h}^{e-i}$ for all i. In particular

$$\deg z_1 \bar{h}^{e-1} \leqslant \deg R < \deg w_1 h^{e-1} \qquad \text{when } w_1 \neq 0.$$

Since $\deg \bar{h} = \deg h$, this inequality implies that $\deg z_1 < \deg w_1$ when $w_1 \neq 0$. When $w_1 = 0$, $h = \bar{h}$ and $y_1 = w_1 = 0$. This finishes the proof.

It is now possible to present a proof of (*).

PROPOSITION 7 *Assume that the characteristic of K does not divide $\deg g$. There exists a sequence $h_1, \ldots, h_{N-1}$ satisfying (**) such that $h_i \in f^i + K[g] f^{i-1} + \cdots + K[g]$ for all i.*

Proof. Since $K(f, g)$ is a subfield of $K(T)$ and since $[K(T): K(g)] = \deg g$, N divides $\deg g$. Therefore the characteristic of K does not divide N. Hence, by Proposition 4, it does not divide e_t for any t.

By successively applying Proposition 6 one can construct a sequence $H_1, \ldots, H_{N-1}$ satisfying (**) such that

$$H_{c(t)}^e - H_{c(t+1)} \in K(g) + K(g) f + \cdots + K(g) f^{ec(t) - c(t) - 1} \tag{13}$$

for all t; here e denotes $c(t+1)/c(t)$.

Recall (see Proposition 5) that $H_{c(k+1)}$ is defined to be 0. If $p(Y)$ is the monic minimal polynomial of f over $K(g)$, then $p(f) = H_{c(k+1)}$ and the coefficients of $p(Y)$ lie in $K[g]$. Therefore, applying Proposition 3 with $h = H_{c(k)}$ and with $t = p(f)$, one concludes that $H_{c(k)}$ lies in $K[f, g]$.

Assume that $H_{c(t+1)}$ lies in $K[f, g]$. Relation (13) and Proposition 3 imply that $H_{c(t)}$ lies in $K[f, g]$. This shows by induction that $H_{c(t)}$ lies in

$K[f, g]$ for all t. A suitable ordering of the set $\{H_{c(1)}^{j_1} \cdots H_{c(k)}^{j_k} : 0 \leqslant j_s < e_s$ for all $s\}$ yields a sequence $h_1, \ldots, h_{N-1}$ having the desired properties.

Recall that d denotes $\gcd(\deg f, \deg g)$.

PROPOSITION 8. *Assume that the characteristic of K does not divide d. There exist elements $h_1, \ldots, h_{N-1}$ such that*

(i) *for each i, $h_i \in f^i + K[g] f^{i-1} + \cdots + K[g]$, and*

(ii) *the numbers $0, \deg h_1, \ldots, \deg h_{N-1}$ are pairwise incongruent mod $\deg g$.*

Proof. Let $M = [K(f, g) \colon K(f)]$. If $M = 1$ there is a polynomial $H(T)$ such that $g(T) = H(f(T))$, and the sequence of polynomials $f, f^2, \ldots, f^{(\deg H) - 1}$ has the desired properties. Assume for the rest of the proof that $M > 1$.

In the case that the characteristic of K does not divide $\deg g$, Proposition 8 reduces to Proposition 7. Assume that the characteristic of K divides $\deg g$. Since the characteristic of K does not divide d, it does not divide $\deg f$. By Proposition 7 there is a sequence of polynomials $g_1, \ldots, g_{M-1}$ such that

(i) for each i, g_i lies in $g^i + K[f] g^{i-1} + \cdots + K[f]$,

(ii) the numbers 0, $\deg g_1, \ldots, \deg g_{M-1}$ are pairwise incongruent mod $\deg f$, and

(iii) if $\deg g$ is not divisible by $\deg f$, $g_1 = g$.

Let $c(1), \ldots, c(k)$ denote the gcd-decreasing sequence of $g_1, \ldots, g_{M-1}$. Define $w_0 = f$ and define D_j to be the additive group generated by $\deg g_0$, $\deg g_1, \ldots, \deg g_j$. Let $c(k+1) = M$ and define e_t to be the smallest positive integer such that $e_t \deg g_{c(t)}$ lies in $D_{c(t)-1}$. By Proposition 4, $e_t c(t) = c(t+1)$ when $1 \leqslant t \leqslant k$. Repeated applications of this equation imply that

$$c(t+1) = e_t e_{t-1} \cdots e_1 \qquad \text{when} \quad 1 \leqslant t \leqslant k. \tag{15}$$

Observe that

$$\deg f = [K(T) \colon K(f)] = [K(T) \colon K(f, g)]\, [K(f, g) \colon K(f)]$$

and

$$\deg g = [K(T) \colon K(g)] = [K(T) \colon K(f, g)]\, [K(f, g) \colon K(g)].$$

Therefore

$$(\deg f)/M = (\deg g)/N. \tag{16}$$

Define

$$B_0 = \{f^n : n \geqslant 0\},$$
$$B_1 = \{f^n g_{c(1)}^{j_1} : n \geqslant 0,\ 0 \leqslant j_1 < e_1\},$$
$$\vdots$$
$$B_k = \{f^n g_{c(1)}^{j_1} g_{c(2)}^{j_2} \cdots g_{c(k)}^{j_k} : n \geqslant 0, 0 \leqslant j_i < e_i \text{ for all } i\}.$$

The sequence $h_1, ..., h_{N-1}$ will be constructed by altering certain elements of B_k.

Let t be an integer such that $1 \leqslant t \leqslant k$. Define $g_M = 0$. By Proposition 5 there are distinct elements $b_1 = b_1(t), ..., b_v = b_v(t)$ in B_t and non-zero scalars $s_1 = s_1(t), ..., s_v = s_v(t)$ such that

$$g_{c(t)}^{e_t} - g_{c(t+1)} = s_1 b_1 + \cdots + s_v b_v. \tag{17a}$$

The definitions of e_1, $e_2, ..., e_t$ imply that the elements of B_t have distinct degrees. Therefore

$$\deg(s_1 b_1 + \cdots + s_v b_v) = \max\{\deg b_1, ..., \deg b_v\}. \tag{17b}$$

Observe that the degrees of $g_{c(t)}^{e_t}$, $b_1, ..., b_v$ all lie in $D_{c(t)}$. On the other hand, by the definition of gcd-decreasing sequence, either $g_{c(t+1)} = 0$ or the degree of $g_{c(t+1)}$ does not lie in $D_{c(t)}$. These remarks and Eqs. (17a) and (17b) imply that

$$\deg(g_{c(t)}^{e_t} - g_{c(t+1)}) = \deg g_{c(t)}^{e_t} > \deg g_{c(t+1)} \tag{17c}$$

and

$$e_t \deg g_{c(t)} = \max\{\deg b_1, ..., \deg b_v\}. \tag{17d}$$

Suppose that $\deg f$ does not divide $\deg g$. By property (iii) of the definition of $g_1, ..., g_{M-1}$, $g_1 = g$. Therefore $B_1 = \{f^n g^j :\ n \geqslant 0,\ 0 \leqslant j < e_1\}$ and $e_1 = (\deg f)/d$. Set

$$q = (\deg g)/(\deg f).$$

By Eq. (17c) there is a non-zero scalar u such that

$$\deg(g_{c(2)} - g^{e_1} - u f^{e_1 q}) < e_1 \deg g = q e_1 \deg f.$$

This inequality, Eq. (17a), and the fact that the elements of B_1 have distinct degrees imply that $g_{c(2)} - g^{e_1} - uf^{e_1 q}$ is a linear combination of elements in the set $\{f^n g^j\colon 0 \leqslant n < e_1 q,\ 0 \leqslant j < e_1\}$. Therefore

$$\text{if } \deg f \text{ does not divide } \deg g,\ g_{c(2)} \text{ lies in } uf^{e_1 q} + K[g] f^{e_1 q - 1} + \cdots + K[g]. \tag{18a}$$

Suppose now that $\deg f$ divides $\deg g$. There is a polynomial $H(T)$ such that $g_1 = g - H(f)$. Since $\deg f$ divides $\deg g$, since $\deg f$ does not divide $\deg g_1$ and since $g_1 = g - H(f)$,

$$\deg g_1 < \deg g = \deg H(f) = \deg H(T) \deg f.$$

Thus

$$\text{if } \deg f \text{ divides } \deg g,\ \deg g_1 < \deg g \text{ and there is a polynomial } H(T) \text{ of degree } q \text{ such that } g_1 = g - H(f). \tag{18b}$$

Set $t_0 = 1$ if $\deg f$ divides $\deg g$ and set $t_0 = 2$ otherwise. The next goal will be to show that, if $t_0 \leqslant t \leqslant k$, there is a non-zero scalar u_t such that $g_{c(t)}$ lies in $u_t f^{c(t)q} + K[g] f^{c(t)q-1} + \cdots + K[g]$. This relation will be established by induction on t. Statements (18a) and (18b) imply that the relation holds when $t = t_0$. Suppose now that $t_0 \leqslant t < k$. By the induction hypothesis one may assume that there are non-zero scalars $u_1, \ldots, u_t$ such that

$$\text{when } t_0 \leqslant j \leqslant t, \quad g_{c(j)} \text{ lies in } u_j f^{c(j)q} + K[g] f^{c(j)q-1} + \cdots + K[g]. \tag{19a}$$

I want to show that this relation also holds when $j = t+1$. Suppose that b_r is an element of B_t which appears in Eq. (17a). Since b_r lies in B_t there are non-negative integers $n, j_1, \ldots, j_t$ such that $j_i < e_i$ for all i and such that

$$b_r = f^n g_{c(1)}^{j_1} g_{c(2)}^{j_1} \cdots g_{c(t)}^{j_t}. \tag{19b}$$

Set

$$m = n + j_2 c(2)q + j_3(3)q + \cdots + j_t c(t)q$$

if $\deg f$ does not divide $\deg g$ and set

$$m = n + j_1 c(1)q + j_2 c(2)q + \cdots + j_t c(t)q$$

if $\deg f$ divides $\deg g$.

Recall that $g_1 = g$ if $\deg f$ does not divide $\deg g$ and that there is a polynomial $H(T)$ of degree q such that $g_1 = g - H(f)$ if $\deg f$ divides $\deg g$. These remarks and statements (19a) and (19b) imply that

$$b_r \text{ lies in } K[g] f^m + K[g] f^{m-1} + \cdots + K[g]. \tag{19c}$$

I want to show that $m < qc(t+1)$. Relations (17d) and (19b) imply that

$$n \deg f \leqslant e_t \deg g_{c(t)} - j_1 \deg g_{c(1)} - \cdots - j_t \deg g_{c(t)}. \tag{19d}$$

Observe that

$$\begin{aligned}
m &\leqslant n + j_1 c(1)q + j_2 c(2)q + \cdots + j_t c(t)q \\
&= (1/\deg f)\,(n \deg f + j_1 c(1) \deg g + j_2 c(2) \deg g \\
&\quad + \cdots + j_t c(t) \deg g) \\
&\leqslant (1/\deg f)\,[e_t \deg g_{c(t)} \\
&\quad + j_1(c(1) \deg g - \deg g_{c(1)}) + \cdots \\
&\quad + j_t(c(t) \deg g - \deg g_{c(t)})] \qquad \text{(by (19d))} \\
&\leqslant (1/\deg f)(e_t \deg g_{c(t)} \\
&\quad + (e_1 - 1)(c(1) \deg g - \deg g_{c(1)}) \\
&\quad + (e_2 - 1)(c(2) \deg g - \deg g_{c(2)}) + \cdots \\
&\quad + (e_t - 1)(c(t) \deg g - \deg g_{c(t)})) \quad \text{(since } j_i < e_i \text{ and by (17c) and (15),} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \deg g_{c(j)} \leqslant c(j) \deg w_1 \leqslant c(j) \deg g) \\
&= (1/\deg f)(e_t \deg g_{c(t)} - (e_t - 1) \deg g_{c(t)} \\
&\qquad\qquad - (e_{t-1} - 1) \deg g_{c(t-1)} - \cdots \\
&\qquad\qquad - (e_1 - 1) \deg g_{c(1)}) \\
&\quad + q((e_1 - 1)\, c(1) + (e_2 - 1)\, c(2) + \cdots \\
&\qquad + (e_t - 1)\, c(t)) \\
&= (1/\deg f)((\deg g_{c(t)} - e_{t-1} \deg g_{c(t-1)}) + \cdots \\
&\qquad\qquad + (\deg g_{c(2)} - e_1 \deg g_1)) + (\deg g_1)/(\deg f) \\
&\qquad\qquad + q(c(t+1) - 1) \qquad \text{(by (15b))} \\
&\leqslant qc(t+1) \text{ with strict inequality when } t > 1 \qquad \text{(by (17c))}.
\end{aligned} \tag{19e}$$

Note also that the definition of g_1 and relation (18b) imply that $\deg g_1 \leqslant \deg g$ and $\deg g_1 < \deg g$ when $\deg f$ divides $\deg g$. Therefore relation (19e) implies that $m < qc(t+1)$. This inequality and statement (19c) imply that the polynomials $b_1, \ldots, b_v$ all lie in $K[g] f^{qc(t+1)-1} + K[g] f^{qc(t+1)-2} + \cdots + K[g]$. This observation and statements (15), (17a), and (19a) imply that $g_{c(t+1)}$ lies in $u_t^{e_t} f^{c(t+1)q} + K[g] f^{c(t+1)q-1} + \cdots + K[g] f + K[g]$. This proves by induction that

$$g_{c(t)} \text{ lies in } u_t f^{c(t)q} + K[g] f^{c(t)q-1} + \cdots + K[g] \quad \text{when } t_0 \leqslant j \leqslant k. \tag{20}$$

If $\deg f$ does not divide $\deg g$, define

$$S = \{ f^n g_{c(2)}^{j_2} \cdots g_{c(k)}^{j_k} \colon 0 \leqslant n < e_1 q,\ 0 \leqslant j_i < e_i \text{ for all } i \geqslant 2 \}.$$

If $\deg f$ divides $\deg g$, define

$$S = \{ f^n g_{c(1)}^{j_1} \cdots g_{c(k)}^{j_k} \colon 0 \leqslant n < q,\ 0 \leqslant j_i < e_i \text{ for all } i \geqslant 1 \}.$$

By Eqs. (15), (16), and (20) there are non-zero scalars $u_1, \ldots, u_{N-1}$ such that the set S contains an element of $u_i f^i + K[g] f^{i-1} + \cdots + K[g] f + K[g]$ when $1 \leqslant i < N$. Note that the degrees of the elements of S are pairwise incongruent mod $\deg g$. Therefore, by multiplying the elements of $S - \{1\}$ by suitable scalars, one obtains polynomials $h_1, \ldots, h_{N-1}$ having the desired properties.

3. Some Algorithms

As in the previous section, f and g denote non-constant elements of $K[T]$ and N denotes $[K(f, g) \colon K(g)]$. It is assumed throughout this section that the characteristic of K does not divide $\gcd(\deg f, \deg g)$. If $n \geqslant 0$ we let L_n denote the space $K[g] + \cdots + K[g] f^n$.

The goal of this section is to describe algorithms which solve the following problems:

1. If $0 < n < N$, find an element h_n in $f^n + L_{n-1}$ whose degree is incongruent mod $\deg g$ to the degree of any element of L_{n-1}.
2. Find semigroup generators for the set $\{\deg y \colon y \in K[f, g],\ y \neq 0\}$.
3. Compute the polynomial $p(X, Y) \in K[X, Y]$ of minimal degree such that $p(f, g) = 0$.
4. Given $h \in K[T]$, determine if h lies in $K[f, g]$.

Define a sequence $h_0, \ldots, h_{N-1}$ recursively as follows:

Set $h_0 = 1$.

Assume that $h_0, \ldots, h_j$ have been defined. Set $S_j = \{ h_i g^q \colon 0 \leqslant i \leqslant j,\ q \geqslant 0 \}$ and define

$$h_{j+1} = R(f h_j, S_j);$$

the function R is defined in the previous section, just before Proposition 2.

An easy induction argument shows that h_n lies in $f^n + L_{n-1}$ for all n.

Claim 1. If $0<n<N$, $\deg h_n$ is incongruent mod $\deg g$ to the degree of any element of L_{n-1}.

Proof. By Proposition 8 there exists an element $\bar{h}_n$ in f^n+L_{n-1} whose degree is not congruent mod $\deg g$ to that of any element of L_{n-1}. Since $h_n-\bar{h}_n$ lies in L_{n-1}, $\deg \bar{h}_n$ does not equal $\deg(h_n-\bar{h}_n)$. Hence

$$\deg h_n=\max(\deg \bar{h}_n, \deg(h_n-\bar{h}_n)). \tag{21}$$

By the definition of h_n, $\deg h_n$ must be different from the degree of any element of S_{n-1}. Observe that S_{n-1} spans L_{n-1}; furthermore by induction we may assume that the numbers $0, \deg h_1,..., \deg h_{n-1}$ are pairwise incongruent mod $\deg g$, so the elements of S_{n-1} have distinct degrees. Therefore the degree of any non-zero element of L_{n-1} equals the degree of some element of S_{n-1}. Hence $\deg h_n$ must be different from the degree of any element of L_{n-1}. In particular $\deg h_n$ does not equal $\deg(h_n-\bar{h}_n)$, so by Eq. (21) $\deg h_n=\deg \bar{h}_n$. This establishes the claim.

The claim implies that the elements $\deg g$, $\deg h_1,..., \deg h_{N-1}$ generated the set $\{\deg y: y\in K[f, g] \text{ and } y\neq 0\}$ as a semigroup.

Observe that S_{N-1} is a K basis for $K[f, g]$ whose elements have distinct degrees. Hence an element h in $K[T]$ lies in $K[f, g]$ if and only if $R(h, S_{N-1})=0$. The equation $R(f^N, S_{N-1})=0$ (or $R(h_{N-1}f, S_{N-1})=0$) is equivalent to an expression for f^N as an element of L_{N-1}. This expression is in turn equivalent to the minimal polynomial $p(X, Y)$ relating f and g.

The following is another approach for constructing a K basis for $K[f, g]$ whose elements have distinct degrees.

Define elements $A_0, A_1,..., A_t$ recursively as follows.

Set $S_0=\{g^q: 0\leqslant q\}$ and define $A_0=R(f, S_0)$.

Assume that $A_0,..., A_n$ have been defined. If $A_n=0$, stop. Otherwise define A_{n+1} as follows. Let

$$\begin{aligned} e_0 &= \deg g,\\ e_1 &= \gcd(\deg A_0, \deg g),...,\\ e_{n+1} &= \gcd(\deg A_n, \deg A_{n-1},..., \deg A_0, \deg g). \end{aligned}$$

Set

$$S_{n+1}=\{g^q A_0^{b_0}\cdots A_n^{b_n}: 0\leqslant q,\ 0\leqslant b_j<e_j/e_{j+1} \text{ for all } j\}$$

and set

$$A_{n+1}=R(A_n^{e_n/e_{n+1}}, S_{n+1}).$$

Note that, by the definition of the b_i's and the e_i's, the elements of S_n

have distinct degrees for all n. Hence the expression $R(A_n^{e_n/e_{n+1}}, S_{n+1})$ makes sense.

An easy induction argument shows that A_n lies in $f^{\deg g/e_n} + L_{(\deg g/e_n)-1}$ for all n. Hence if $0 \leqslant j < \deg g/e_n$, the set S_n contains an element of $f^j + L_{j-1}$. Therefore S_n spans $L_{(\deg g/e_n)-1}$ over K. On the other hand S_n is a subset of $L_{(\deg g/e_n)-1}$ and the elements of S_n have distinct degrees. Therefore S_n is a basis for $L_{(\deg g/e_n)-1}$.

It is necessary to show that the sequence $e_0, e_1, \ldots, e_t$ is strictly decreasing, otherwise the sequence $A_0, A_1, \ldots$ would eventually become constant without every hitting zero.

Suppose that $0 \leqslant n < t$. The proof of Claim 1 implies that $\deg A_n$ is incongruent mod $\deg g$ to the degree of any element of $L_{(\deg g/e_n)-1}$, and hence to that of any element of S_n. For any integer c, it is possible to find integers $B, b_0, \ldots, b_{n-1}$ such that

$$B \deg g + b_0 \deg A_0 + \cdots + b_{n-1} \deg A_{n-1} = ce_n$$

and such that $0 \leqslant b_j < e_j/e_{j+1}$ for all j. Since $A_0^{b_0} \cdots A_{n-1}^{b_{n-1}}$ lies in S_n, $\deg A_n$ is incongruent mod $\deg g$ to $b_0 \deg A_0 + \cdots + b_{n-1} \deg A_{n-1}$ and hence to ce_n. Therefore $\deg A_n$ is not a multiple of e_n, so $e_{n+1} < e_n$. Thus $e_0, e_1, \ldots$ is strictly decreasing, so for some subscript t, $A_t = 0$. Therefore S_t is a basis for $K[f, g]$ whose elements have distinct degrees. The numbers $\deg A_0, \ldots, \deg A_{t-1}$ generate $\{\deg y : y \in K[f, g] \text{ and } y \neq 0\}$ as a semigroup.

Since S_t is a K basis for $K[f, g]$, the set $\{A_0^{b_0} \cdots A_{t-1}^{b_{t-1}} : 0 \leqslant b_j < e_j/e_{j+1}\}$ is a $K(g)$ basis for $K(f, g)$. There are $\deg g/e_t$ t-tuples $(b_0, \ldots, b_{t-1})$ such that $0 \leqslant b_j < e_j/e_{j+1}$ for all j; hence $N = \deg g/e_t$. The equation

$$A_t = R(A_{t-1}^{e_{t-1}/e_t}, S_t) = 0$$

is equivalent to an expression for f^N as an element of L_{N-1}. Thus the calculation of the A_i's leads to the minimal polynomial $p(X, Y)$ relating f and g.

Acknowledgment

I am grateful to Professor S. S. Abhyankar for his encouragement of this work.

References

[A] S. S. Abhyankar, On the semigroup of a meromorphic curve, I, *in* "Proceedings, International Symposium on Algebraic Geometry, Kyoto" (M. Nagata, Ed.), pp. 249–414, Kinokuniya Book-Store Co., Ltd., Tokyo, 1978.

[AM1] S. S. Abhyankar and T. T. Moh, Newton–Puiseux expansion and generalized Tchirnhausen transformation, II, *J. Reine Angew. Math.* **261** (1973), 29–54.

[AM2] S. S. Abhyankar and T. T. Moh, Embeddings of the line in the plane, *J. Reine Angew. Math.* **276** (1975), 149–166.

[M] T. T. Moh, On the concept of approximate roots for algebra, *J. Algebra* **65** (1980), 347–360.

[PR] B. R. Peskin and D. R. Richman, A method to compute minimal polynomials, *SIAM J. Algebraic Discrete Methods* **6** (1985), 292–299.

[S] B. Serge, Corrispondenze di Mobius e Transformazioni cremoniane intere, *Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Nat.* **91** (1956–1957), 3–19.