Ideal Bases and Primary Decomposition:
Case of Two Variables

D. LAZARD†
Institut de Programmation, Université Paris VI, F-75230 Paris Cedex 05
(Received 24 September 1984)

A complete structure theorem is given for standard (= Gröbner) bases for bivariate polynomials over a field and lexicographical orderings or for univariate polynomials over a Euclidian ring. An easy computation of primary decomposition in such rings is deduced. Another consequence is a natural factorisation of the resultant of two univariate polynomials over the integers which is a generalisation of the "reduced discriminant" of a polynomial of degree 2.

1. Introduction

In his celebrated paper, Hironaka (1964), introduced the notion of a standard basis of an ideal of formal power series. One year later, Buchberger (1965) defined independently the same notion for polynomial ideals, which he termed Gröbner basis, and gave an algorithm for computing such a basis. He proved also that the roots of a system of algebraic equations can easily be deduced from a Gröbner basis relative to a lexicographical ordering. In this paper we use Hironaka's terminology of standard basis for the general notion and Buchberger's term of Gröbner basis for the particular case of lexicographical orderings.

There are now many papers on this subject (see Buchberger (1985) for a large bibliography and also EUROSAM 84 and EUROCAL 85 for more recent references). It appears that the computational complexity of standard bases is strongly dependent on the ordering of monomials and on the irregularity of the ideal.

However, once a standard basis is computed, most "properties" of an ideal can be easily (i.e. polynomially) deduced. The main exception to the last assertion is the computation of the primary decomposition of an ideal. Seidenberg (1974) gave an algorithm for this, but it is impracticable. However, some particular subproblems are much easier: the above mentioned problem of systems of algebraic equations is one, which can be solved from Gröbner bases for lexicographical ordering by means of Buchberger's algorithm or from standard bases for degree compatible orderings by our algorithm (Lazard, 1981, 1983). The latter also computes the multiplicities which are the indices of the primary components in the corresponding prime ideal. In Lazard (1982) we gave also an algorithm which computes prime components and multiplicities for pure equidimensional ideals.

In the present paper, we solve the problem of primary decomposition for polynomials in two variables (over a field). We first give a complete structure theorem for Gröbner bases relative to pure lexicographic orderings. There follows an easier computation of the
roots than in Buchberger’s algorithm and an easy computation of the whole primary decomposition. Finally we show a surprising relation between Gröbner bases and resultants which gives a natural factorisation of the resultant.

2. Structure of Grobner Bases

We consider polynomials of $K[x, y]$, the ring of polynomials in two variables over any field $K$. The monomials are ordered by the lexicographical ordering

$$1 < x < x^2 < \ldots < y < xy < yx^2 < \ldots < y^2 < y^2x < \ldots$$

The polynomials which depend on $y$ are generally considered as polynomials in $y$ with coefficients in $K[x]$; if $f$ is such a polynomial, $\text{content}(f) = \text{content}(f, y)$ is the polynomial in $K[x]$ of greatest degree which divides $f$, and

$$\text{primpart}(f) = \text{primpart}(f, y) := f/\text{content}(f);$$

$f$ is monic (in $y$) if its leading monomial is a power of $y$, the leading monomial being the greatest monomial (for the above ordering) with non-zero coefficient.

We refer to Buchberger (1985) for the definition of a Grobner basis and recall that a Grobner basis is reduced if no monomial of a member of it is a multiple of the leading monomial of another member of the Grobner basis, and minimal if there is no relation of divisibility between the leading monomials of its members.

**Theorem I** (Structure Theorem). (i) Let $f_0, \ldots, f_k$ be a minimal Grobner basis, sorted by increasing leading monomials, of an ideal in $K[x, y]$. Then

$$f_0 = PG_1 \ldots G_{k+1}, \quad f_k = PH_k G_{k+1},$$

$$f_i = PH_i G_{i+1} \ldots G_{k+1} \quad \text{for } i \in 1 \ldots k-1,$$

where: $G_i \in K[x]$ for $i \in 1 \ldots k+1$,

$P = \text{primpart}(f_0), \ G_{k+1} = \text{content}(f_k),$

$H_i$ is monic (in $y$) of degree $d(i)$ (in $y$),

$d(1) < d(2) < \ldots < d(k),$

$$H_{i+1} \in (H_i, H_{i-1} G_i, \ldots, H_1 G_2 \ldots G_i, G_1 G_2 \ldots G_i) \quad \text{for } i \in 1 \ldots k-1.$$

(ii) Every set of polynomials which satisfies the preceding conditions is a Grobner basis; it is minimal if and only if $G_i$ is not a unit for $i \neq k+1$.

**Remark 1.** Once $P$ is computed as $\text{primpart}(f_0)$, the computation of the $G_i$ and the $H_i$ from the $f_i$ needs only exact divisions: the product $G_{i+1} \ldots G_{k+1}$ is the coefficient of the highest power of $y$ in $f_i$.

**Proof.** Let $P = \text{primpart}(\text{GCD}(f_0, \ldots, f_k))$ and $G_{k+1} = \text{content}(\text{GCD}(f_0, \ldots, f_k))$. It follows clearly from the definitions that $g_0, \ldots, g_k$ is a minimal Gröbner basis if and only if the same is true for $h g_0, \ldots, h g_k$. Thus we may divide by $PG_{k+1}$ and suppose that the $f_i$ have no common divisors.

We suppose now that the $f_i$ have no common factor; this implies that $P = G_{k+1} = 1$.

**Lemma 1.** Let $d(i)$ be the degree of $f_i$ in $y$: we have

$$d(i) < d(i+1).$$
Otherwise we would have \( d(i) = d(i+1) \), the leading monomial of \( f_i \) would divide the one of \( f_{i+1} \) and the basis would not be minimal (recall that the \( f_i \) are sorted by increasing leading monomials).

**Lemma 2.** The coefficient (which is in \( K[x] \)) of the highest power of \( y \) in \( f_{i+1} \) divides the coefficient of the highest power of \( y \) in \( f_i \).

Let \( d(i) := \text{degree}(f_i) \) be the degree in \( y \) and \( g_i := \text{coeff}(f_i, y^{d(0)}) \); the polynomials \( y^{d(i+1)} - d(0)f_i \) and \( f_{i+1} \) are in the ideal. Successive divisions of their leading terms (which have the same degree in \( y \)) leads to a polynomial of degree \( d(i+1) \) in \( y \) in which the coefficient of \( y^{d(i+1)} \) is \( \text{GCD}(g_i, g_{i+1}) \).

The leading monomial of this polynomial is a multiple of the leading monomial of some \( f_j \). If \( g_{i+1} \neq \text{GCD}(g_i, g_{i+1}) \), we must have \( j < i+1 \) and the leading monomial of \( f_j \) divides the one of \( f_{i+1} \). The basis being minimal this is not possible and \( g_{i+1} \) divides \( g_i \).

**Lemma 3.** \( f_0 \in K[x], \ g_i \) divides \( f_i \) and \( f_k \) is monic in \( y \).

In fact \( (g_i/g_{i+1})f_{i+1} = y^{d(i+1)} - d(0)f_i \) is a polynomial of degree less than \( d(i+1) \) in \( y \) which reduces to zero modulo the Gröbner basis. It follows that \( (g_i/g_{i+1})f_{i+1} \in (f_i, f_{i-1}, \ldots, f_0) \); if, by induction hypothesis, \( \text{primpart}(f_0) \) (resp. \( g_i \)) divides \( f_0, \ldots, f_i \), then \( \text{primpart}(f_0) \) (resp. \( g_{i+1} \)) divides \( f_{i+1} \). Thus, if the \( f_i \) have no common factors, we have \( g_k = 1 \), \( \text{primpart}(f_0) = 1 \) and \( g_i \) divides \( f_i \) for \( i \in 1, \ldots, k \).

Let \( G_{i+1} := g_i/g_{i+1} \) and \( H_i := f_i/g_i \). We have proved that \( G_{i+1}f_{i+1} \in (f_i, f_{i-1}, \ldots, f_0) \). Dividing by \( G_{i+1} \) we get the last assertion of (i) and this completes the proof of (i).

**Lemma 4.** If \( j > i \geq 1 \), we have \( H_j \in (H_i, H_{i-1}G_i, \ldots, H_iG_{i-1}, G_{i-1}, \ldots, G_j) \) and \( H_j \in (H_i, G_i) \).

This is an easy consequence of the last assertion of (i).

To prove the assertion (ii) of theorem 1, let us compute the S-relation

\[ S := x^d f_j - y^{d(0)} - d(0)f_i \]

with \( d = \text{degree}(G_{i+1} \ldots G_j) \) and \( j > i \); the coefficient of \( y^{d(0)} \) in \( S \) is

\[-g_i + x^dg_j.\]

Reducing \( S \) by \( f_j \) gives then

\[ S' := S + (g_i/g_j - x^d)f_j = (g_i/g_j)f_j - y^{d(0)} - d(0)f_i;\]

by lemma 4, \( S' \in (f_0, \ldots, f_j) \) and \( S' \) reduces to zero if we have proved by induction that \( f_1, \ldots, f_j \) is a Gröbner base of the ideal they generate. Thus every S-relation reduces to zero and the theorem is proved.

**Proposition 1.** Let \( f_0, \ldots, f_k \) be a Gröbner base satisfying the conditions of theorem 1(i).

For each integer \( j \) let \( h_j := f_jy^{-d(0)} \) where \( d(i) \leq j < d(i+1) \) (notations of theorem 1 with \( d(0) := 0 \) and \( d(k+1) := +\infty \)).

Then, for every \( t \geq d(k) \), the set \( h_0, \ldots, h_t \) is a Gröbner basis of the same ideal which satisfies the conclusions of theorem 1(i) and such that \( d(j) = j \).

This is almost immediate; the basis \( h_0, \ldots, h_t \) is what Ayoub (1983) calls a detaching base.
THEOREM 2. Suppose that the \( f_i \) are as in theorem 1 and that they have no common factors (i.e. \( PG_{k+1} = 1 \)). Then

(i) The common zeros of the \( f_i \)'s are the union of the sets of common zeros of the pairs \((G_i, H_i)\).

(ii) A maximal ideal contains all the \( f_i \)'s if and only if it contains at least one pair \((G_i, H_i)\).

(iii) Such a maximal ideal is generated by an irreducible factor \( u(x) \) of \( G_i \) in \( K[x] \) and an irreducible factor \( v(x, y) \) of \( H_i \) in \( (K[x]/u(x))[y] \).

(iv) The multiplicity of a common zero of the \( f_i \) (resp. of a maximal ideal containing the \( f_i \)) is the sum of the corresponding multiplicities for the pairs \((G_i, H_i)\).

(v) The multiplicity of a common zero \((a, b)\) of \((G_i, H_i)\) is the product of the multiplicities of \( a \) as a root of \( G_i \) and of \( b \) as a root of \( H_i \).

(vi) The multiplicity of a maximal ideal \((u(x), v(x, y))\) containing \((G_i, H_i)\) is the product of the multiplicities of \( u(x) \) as a factor of \( G_i \) and of \( v(x, y) \) as a factor of \( H_i \) in \((K[x]/u(x))[y]\).

REMARK 2. We have stated the case of the common zeros for the convenience of the reader. In fact it is the particular case of a maximal ideal \((x - a, y - b)\).

PROOF. By lemma 4, the ideal generated by the \( f_i \)'s is contained in the ideal \((G_i, H_i)\), for \( i = 1, \ldots, k \); thus the common zeros of \((G_i, H_i)\) are common zeros of the \( f_i \)'s and the maximal ideals containing \((G_i, H_i)\) contain the \( f_i \)'s. Conversely, if \((a, b)\) is a common zero of the \( f_i \)'s (resp. if \((a, b)\) is a maximal ideal containing the \( f_i \)), let \( j \) be the highest integer such that \( G_j(a) = 0 \) (resp. \( G_j \in m \)). Such an integer exists, because \( f_0(a) = 0 \) (resp. \( f_0 \in m \)). We immediately have \( H_j(a, b) = 0 \) (resp. \( H_j \in m \)); this proves (i) and (ii).

If \( m \) is a maximal ideal containing \((G_i, H_i)\), it contains an irreducible factor \( u(x) \) of \( G_i \). The image of \( m \) in \( L := (K[x]/u(x))[y] \) is a maximal ideal containing the image of \( H_i \) and, thus, an irreducible factor \( v(x, y) \) of \( H_i \). The quotient \( L/v(x, y) \) being a field, the ideal \((u(x), v(x, y))\) is maximal and equal to \( m \); this proves (iii).

To prove (iv) and (v) we shall use the fact that the multiplicities are additive for the exact sequences (Serre, 1965). For this, define inductively the ideals \( I_i \) by \( I_1 = (G_1, H_1) \) and \( I_i = (H_{i-1}) + G_i I_{i-1} \) for \( i > 1 \). By theorem 1 and our hypothesis that \( PG_{k+1} = 1 \), it is easy to see that \( I_k \) is the ideal \((f_0, \ldots, f_k)\). To prove (iv) and (v) we have only to provide an exact sequence:

\[ 0 \to A/I_{i-1} \to A/I_i \to A/(G_i, H_i) \to 0, \]

where \( A := K[x, y] \). The right arrow is the natural epimorphism (we have \( I_i \subset (G_i, H_i) \)). The left arrow is the multiplication by \( G_i \); it is well defined and injective because

\[ (G_i) \cap I_i = G_i I_{i-1} + (G_i) \cap (H_i) = G_i I_{i-1} + (G_i H_i) = G_i I_{i-1}; \]

in fact \( H_i \in I_{i-1} \) by the last assertion of theorem 1(i), and \( G_i \) and \( H_i \) have no common factors. The sequence is exact because

\[ (G_i, H_i)/I_i = ((G_i) + I_i)/I_i = (G_i)/((G_i) \cap I_i). \]

By remark 2 it remains only to prove (vi); for this we use Serre's definition of multiplicities (Serre, 1965). Let \( m \) be the multiplicity of \( u(x) \) as a factor of \( G_i \) and \( n \) be that
of \( v(x, y) \) as a factor of \( H_i \) modulo \( u(x) \). By Hensel’s lemma we are able to decompose \( H_i \mod u(x)^m \) as a product \( w_1 w_2 \) where \( w_1 = (v(x, y)^m \mod u(x)) \) and \( w_2 \neq 0 \mod (u(x), v(x, y)) \). Thus the localisation at the prime \( (u(x), v(x, y)) \) of \( A/(G_i, H_i) \) is the same as the localisation of \( A/(u(x)^m, w_i) \) and also the same as that of \( A/(u(x)^m, w_i) \); the ideal \( (u(x)^m, w) \) is \( (u(x), v(x, y)) \)-primary, containing \( u^m \) and \( v^m \). Thus, the required multiplicity is the dimension of the last quotient over \( A/(u(x), v(x, y)) \). The dimension over \( K \) of this field is degree \((u) \cdot \text{degree}_y(u) \) and the dimension over \( K \) of \( A/(u(x)^m, w_i) \) is \( m \cdot \text{degree}_y(u) \cdot \text{degree}_x(v) \) because \( w_i \) is of the same degree in \( y \) as \( (u(x))^m \). This proves that the multiplicity is \( mn \), as asserted, and terminates the proof of theorem 2.

**Corollary.** If all common zeros of \( (f_0, \ldots, f_k) \) in an algebraic closure of \( K \) have multiplicity one, the polynomial \( f_0 = G_1 \ldots G_k \) is square free.

The fact that each \( G_i \) is square free comes from (v) or (vi). Lemma 4 asserts that \( H_i \in (G_i, H_i) \) for \( j > i \); if \( G_i \) and \( G_j \) would have a common irreducible factor \( u \), then \( H_i \) would divide \( H_j \) modulo \( u \) and any common zero of \( u \) and \( H_i \) would be a common zero of \( u \) and \( H_j \); thus we would have common zeros with multiplicity more than 1, by (iv).

Theorem 2 allows us to compute the prime components and the multiplicities of an ideal given by a Gröbner basis. It now remains to compute the primary component corresponding to a particular prime \( (u(x), v(x, y)) \). This can be done by the following:

**Algorithm**

**Input:** \((f_0, \ldots, f_k)\) a zero dimensional ideal given by a Gröbner basis as in theorem 1 with \( PG_k+1 = 1 \);

\((u(x), v(x, y))\) a maximal ideal containing the \( f_i \), which has been computed by means of theorem 2.

**Output:** a Gröbner basis of the corresponding primary component.

1. Replace \( f_0 \) by the highest power of \( u(x) \) which divides it.
2. We have \( H_k = (v(x, y)^m w(x, y)) \mod u(x) \), with \( w \) prime to \( v \mod u(x) \); use Hensel lemma to compute polynomials \( s, t \), such that

\[
H_k = st \mod f_0 \quad \text{(which is now a power of } u(x)\text{),}
\]

\[
s = v(x, y)^m \mod u(x) \quad \text{and} \quad t = w(x, y) \mod u(x).
\]

Replace \( H_k \) by \( s \).

3. {Optionally} Replace each \( G_i \) in each \( f_j \) by the highest power of \( u(x) \) which divides it and remove the \( f_i \) for which the corresponding \( G_i \) becomes 1.

4. Output a Gröbner base of the ideal generated by the new \( f_i \)’s.

**Proof.** The aim of the steps (1), (2) and (3) is to drop out components which are removed by localisation at \((u(x), v(x, y))\). We have to prove:

(a) the ideal computed in steps (1), (2) and (3) has same localisation at \((u(x), v(x, y))\): this is true for the step (1) and the first part of step (3) because we remove factors of \( f_i \) which become invertible by localisation. The same argument works for step (2) if we remark that changing \( H_k \) to \( st \) does not change the ideal. The last assertion of theorem 1(i) asserts that \( f_j G_i \in (f_0, \ldots, f_{i-1}) \); thus \( f_j \in (f_0, \ldots, f_{i-1}) \) after localisation, if \( G_i \) becomes invertible; thus removing \( f_j \) does not change the localisation.

(b) the produced ideal is \((u(x), v(x, y))\) primary: it suffices to prove that \( u \) and \( v \) have
powers in this ideal. For \( u \), it results immediately from step (1) that there exists \( m \) such that \( u(x)^m \) is in the ideal. From step (2), we have \( f_k = H_k = s = v^n + u \cdot r \) and thus \( v^{mn} = (f_k - u \cdot r)^m \in (f_k, f_0) \).

**Remark 3.** The optional step (3) does not change the result, but, being easy to compute, it may increase the speed of step (4) and thus of the whole algorithm.

**Remark 4.** The work of step (2) may be done on each \( H_i \); but it seems that repeated use of computations in algebraic extensions and of Hensel lemma would be more costly than the above algorithm.

*Case of 1-dimensional ideals:* The above algorithm works after removing the GCD of the generators \( (PG_k+1) \). In the case where the GCD is not 1, the prime components of the ideal are the irreducible factors of \( PG_k+1 \) and the maximal ideals given by algorithm 1 after removing \( PG_k+1 \). The 1-dimensional primary components are the highest power of an irreducible factor of \( PG_k+1 \) which divides it. For the zero dimensional primes which do not contain \( PG_k+1 \), the primary component is that which is given by the algorithm after removing \( PG_k+1 \). In the case where a maximal ideal \( m = (u(x), v(x, y)) \) contains \( PG_k+1 \), we have an imbedded component and neither the primary component nor the multiplicity are well defined. Thus we prefer to describe this component as the product of the irreducible factors of \( PG_k+1 \) which are in \( m \) and of the primary component given by algorithm 1, even if it is not the usual primary decomposition. However, the latter may easily be computed, as found after the submission of this paper.

**Remark 5.** A generating set of a primary component at \( (u(x), v(x, y)) \) may easily be obtained in all cases: it suffices to add to the generating set \( (f_0, \ldots, f_4) \) of the ideal the highest power of \( u(x) \) which divides \( f_0 \) and the polynomial \( v(x, y)^{s+t} \) where \( s \) is the sum of the multiplicities of the \( (G_i, H_i) \)'s at \( (u(x), v(x, y)) \) given by theorem 2, and \( t \) is the multiplicity of \( v \) as a factor of \( P \mod u \) (Bonet, 1985).

### 4. An Example

We conclude by an illustration of the usefulness of the above results which comes from Davenport *et al.* (1985).

Let \( f(z) \) be a polynomial with real coefficients and define

\[
\begin{align*}
  f_1(x, y) &:= \text{Real-Part} \left( f(x+iy) \right) = \frac{f(x+iy)+f(x-iy)}{2} \\
  f_2(x, y) &:= \text{Imag-Part} \left( f(x+iy) \right) = \frac{f(x+iy)-f(x-iy)}{2i}.
\end{align*}
\]

Clearly the roots of \( f \) correspond to the real common zeros of \( f_1 \) and \( f_2 \). Conversely, the common zeros of \( f_1 \) and \( f_2 \) are the pairs \((x, 0)\) where \( f(x) = 0 \), and the pairs \((x, y)\) such that there exists two roots \( a, b \) of \( f \) such that \( x = (a+b)/2 \), \( y = (a-b)/2i \). It follows that, if \( f \) is square free, the sums of two roots are all distinct, and they are distinct from the double of a root, then the Gröbner basis of \((f_1, f_2)\) has the form \( y^2-h(x), \ yG(x), \ f(x)G(x) \). Theorem 2 asserts that it suffices to solve the two systems \((f(x), y)\) and \((G(x), y^2-h(x))\)
for solving the system \((f_1, f_2)\); this is computationally easier than solving the system of three equations, given by the Gröbner basis.

In the general case, the structure of the Gröbner base is different but may also be used to improve the computations. If, for example, \(f(z) = z^4 + 1\) we have

\[
f_1(x, y) = y^4 - 6x^2y^2 + x^4 + 1
\]

\[
f_2(x, y) = 4xy^3 - 4x^3y.
\]

The Gröbner basis has the form

\[
(G_1 G_2 G_3, H_1 G_2 G_3, H_2 G_3, H_3),
\]

where

\[
G_1 = x^4 + 1, \quad G_2 = 4x^4 - 1, \quad G_3 = x,
\]

\[
H_1 = y, \quad H_2 = y^2 - \frac{3}{2}x^5 - \frac{5}{2}x^3, \quad H_3 = y^4 - \frac{5}{2}x^8 - \frac{5}{2}x^6 + 1.
\]

The \(G_i\)'s and the \(H_i\)'s are easily obtained from the Gröbner basis by exact divisions; theorem 2 asserts that solving the system is equivalent to solving the three very simple systems \((G_i = 0, H_i \mod G_i = 0)\) for \(i = 1, 2, 3\), where \(H_1 \mod G_1 = y, H_2 \mod G_2 = y^2 - x^2\) and \(H_3 \mod G_3 = y^4 + 1\); only the second system \(y^2 - x^2 = 4x^4 - 1 = 0\) has real solutions.

It is also interesting to note that, conversely, starting from the knowledge of the roots of \(f\), the computation of \(G_1, G_2, G_3, H_1, H_2 \mod G_2\) and \(H_3 \mod G_3\) is almost immediate.

## 5. Resultant and Sylvester Matrices

From now on we consider univariate polynomials in the ring \(R[y]\) where \(R\) is a Euclidian ring (\(\mathbb{Z}\) for example). All the preceding results remain true, except that the part of theorem 2 relative to "roots" becomes meaningless and that the syzygy \(S\) in the proof of lemma 4 becomes \((g_i/g_j)f_j - y^{a_i}d_j - d_i'f_j\); moreover we have to replace "multiple of" and "divisibility" in the definition of minimal and reduced Gröbner base by "reducible by" and "reducibility". All results would remain true when \(A\) is a principal ideal domain, if we had defined Gröbner bases of polynomial ideals over such a ring; this is not very difficult, but needs preliminaries which are beyond the scope of this paper.

Given two polynomials \(A\) and \(B\) in \(R[y]\):

\[
A = a_0y^m + a_1y^{m-1} + \ldots + a_m,
\]

\[
B = b_0y^m + b_1y^{m-1} + \ldots + b_m,
\]

we shall compare the Gröbner base of the ideal generated by \(A\) and \(B\) and the resultant \(\text{Res}(A, B)\) which is the determinant of the Sylvester matrix

\[
\begin{bmatrix}
  a_0 & b_0 \\
  \vdots & \vdots \\
  a_m & b_m \\
  \vdots & \vdots \\
  a_{m-1} & b_{m-1} \\
  \vdots & \vdots \\
  a_1 & b_1 \\
  a_0 & b_0
\end{bmatrix}
\]

The main results are as follows:
THEOREM 3. Given $A, B$ in $R[y]$, let $G_i \in R$ and $P_i \in R[y]$ be obtained by applying theorem 1 to a Grobner base of the ideal generated by $A$ and $B$. Let $d(i) = \text{degree}_y(H_i)$ and $d(k+1) = m+n$; then

(i) $\prod G_i^{d(i)}$ divides $\text{Res}(A,B)$.

(ii) $\text{Res}(A,B)/\prod G_i^{d(i)}$ is a unit in $R$ if and only if $1 = \text{GCD}(a_0, b_0)$ and $P = 1$ (i.e. $\text{Res}(A,B) = 0$).

Recall that given any matrix $M$ over $R$ there is an invertible square matrix $S$ such that $MS = N$ and (a) $N(i,j) = 0$ for $j > i$, (b) $N(i,j) = \text{remainder}(N(i,j), N(i,i))$. The matrix $N$ is called the Hermite normal form of $M$.

THEOREM 4. Suppose that $\text{GCD}(a_0, b_0) = 1$. Then

(i) The Hermite normal form $N$ of the Sylvester matrix of $A$ and $B$ satisfies $N(i,i)$ divides $N(j,k)$ for $i < j$.

(ii) The coefficients of the columns $i$ such that $N(i,i)$ strictly divides $N(i+1,i+1)$ are the coefficients of the polynomials of a reduced Grobner basis.

(iii) The coefficients of the columns of $N$ are the coefficients of the polynomials of a Grobner basis.

PROOF. Let $f_0, \ldots, f_k$ be a Grobner basis of the ideal generated by $A$ and $B$ which satisfies the conditions of theorem 1, and let $g_0, \ldots, g_{m+n}$ the corresponding detaching base (cf. proposition 1).

LEMMA 5. The products $\prod G_i^{d(i)}$ corresponding to the basis $f_0, \ldots, f_k$ and to the base $g_0, \ldots, g_{m+n}$ are equal.

It is easy to see that Buchberger's algorithm to compute the Grobner base of $A$ and $B$ provides only polynomials of degree in $y$ at most $\max(m,n) \leq m+n$; so $k \leq m+n$ and the products differ only by factors equal to 1.

Now, to prove the theorems we have only to consider the base $g_0, \ldots, g_{m+n}$ for which $d(i) = i$ (except that $d(m+n+1) = m+n$). Let us consider the polynomials

$$h_i = \sum_{j} N(m+n-j, m+n-i) y^j$$

which occur in theorem 4(iii). The definition of Hermite normal form implies that degree $(h_i) \leq i$ and that $\text{Res}(A,B) = \prod N(i,i)$. This resultant is zero iff $\text{GCD}(A,B)$ depends on $y$ or $a_0$ and $b_0$ are 0; in these cases, theorem 3 is immediate and theorem 4 is vacuous; thus we may suppose that $P = 1$ (notation of theorem 1) and that degree $(h_i) = i$. The first part of theorem 3 follows easily from

LEMMA 6. The leading coefficient $G_i^{d(i+1)} \cdots G_{m+n+1}$ of $g_i$ divides the leading coefficient $N(m+n-i, m+n-i)$ of $h_i$.

In fact, $h_i$ is in the ideal generated by $A$ and $B$ or by the $g_i$. The set of the $g_i$'s being a Grobner base, the leading coefficient of $h_i$ is in the ideal generated by the leading coefficients of those $g_j$ of degree at most $i$, which is generated by the leading coefficient of $g_i$. 

COROLLARY. \( h_i \) is in the \( R \)-module generated by \( g_0, \ldots, g_i \).

The above proof is valid if \( h_i \) is any polynomial of degree \( i \) in the ideal \((A, B)\). Dividing \( h_i \) by \( g_i \), an easy induction leads to the result.

**Lemma 7.** Suppose that \( \gcd(a_0, b_0) = 1 \). If \( C = AP + BQ \) is a polynomial of degree less than \( m + n \), we can choose \( P' \) and \( Q' \) such that

\[
\text{degree}(P') < n, \quad \text{degree}(Q') < m \quad \text{and} \quad C = AP' + BQ'.
\]

We use induction on degree \( (P) \): if degree \( (P) < n \) we have degree \( (BQ) < m + n \) and degree \( (Q) < m \). Let \( d := \text{degree}(P) \) be at least \( n \) and let \( e = \text{degree}(Q) \); we have \( e + n = \text{degree}(BQ) = \text{degree}(AP) = d + m \); thus the leading terms of \( AP' \) and \( BQ' \) cancel and, \( R \) being principal, there is an element \( c \) in \( R \) such that the leading term of \( P' \) (resp. \( Q' \)) is \( cb_0 y^d \) (resp. \( -ca_0 y^e \)); let \( P_1 := P - cb_0 y^{d-n} \) and \( Q_1 := Q + cA y^{e-m} \). The relation \( C = AP_1 + BQ_1 \) inductively gives the result.

**Lemma 8.** If \( \gcd(a_0, b_0) = 1 \) then \( g_0, \ldots, g_i \) and \( h_0, \ldots, h_i \) generate the same \( R \)-module for every \( i < m + n \).

The definitions of Sylvester matrix and of Hermite normal form show that \( h_0, \ldots, h_{m+n-1} \) generate the \( R \)-module of polynomials \( C = AP + BQ \) such that degree \( (P) < n \) and degree \( (Q) < m \). Lemma 7 implies that \( g_0, \ldots, g_{m+n-1} \) are in this module and degree considerations give the result.

It follows that \( g_i \) and \( h_i \) are associate; taking the product of the leading coefficient proves theorem 3. To prove theorem 4 we need the classical:

**Lemma 9.** A set of polynomials \( f_1, \ldots, f_s \) is a Gröbner basis of the ideal \( I \) they generate if and only if the ideal generated by initial terms of the \( f_i \) is the ideal of initial terms of the elements of \( I \).

Thus the property to be a Gröbner basis depends only on the ideal and on the set of initial terms; \( g_i \) and \( h_i \) having the same leading terms, the polynomials \( h_i \) form a Gröbner basis. In the proof of theorem 1, the property of the basis to be minimal is used only in the proof of lemma 2 which is satisfied by the \( h_i \); this proves that the polynomials \( h_i \) satisfy the conditions of theorem 1. The minimal basis extracted from the \( h_i \) is a reduced Gröbner basis in view of part (b) of the definition of Hermite normal form. Thus the polynomials \( h_i \) satisfy all assertions of theorem 4.

**Remark 6.** Theorems 3 and 4 may be used for computing the resultant from a Gröbner basis; more interesting is the fact that factorisation of theorem 1 gives informations on the structure of the resultant which seems promising as the following examples show.

**Example 1.** Let \( R := \mathbb{Z}, \ A := y^2 + by + c, \ B = A' = 2y + b. \) An easy computation shows that the polynomials \( G_i \) are:

\[
G_3 = 1, \quad G_2 = \gcd(b, 2), \quad G_1 = \left( \frac{b}{G_2} \right)^2 - \left( \frac{2}{G_2} \right)^2 c;
\]

they give the factorisation

\[
\text{discriminant}(A) = \text{Res}(A, B) = G_1 G_2^2;
\]

which is \( b^2 - 4c \) for odd \( b \) and \( 2^2((b/2)^2 - c) \) for even \( b \). Thus the "reduced discriminant" \( G_1 \) appears as a particular case of a natural general object.
Example 2. With \( R : = \mathbb{Z} \), \( A = y^3 + py + q \), \( B = A' = 3y^2 + p \), we get also a natural factorisation of \( 4p^3 + 27q^2 \):

\[
G_4 = 1, \quad G_3 = \text{GCD}(p, 3), \quad G_2 = \text{GCD}\left( \frac{2p}{G_3}, q \right), \quad G_1 = \frac{4p^3 + 27q^2}{G_2^3 G_3^3},
\]

\( 4p^3 + 27q^2 = G_1 G_2^3 G_3^3 \).

Remark 7. The minimal pseudo-resultant of Rothstein (1984) is clearly \( h_0 = N(m + n, m + n) \). If \( \text{GCD}(a_0, b_0) = 1 \) the minimal pseudo-resultant is then \( \prod G_i \), while the resultant is \( \prod G_i^{d(i)} \). The relation between \( \prod G_i^{d(i)} \) and \( \text{Res}(A, B) \) when \( \text{GCD}(a_0, b_0) \neq 1 \) is an open problem.

References


Briançon, J. (1977). Description de Hilb \( \{x, y\} \). *Inventiones Mathematicae* 41, 45–89.


