

Iterated discriminants

Daniel Lazard*
LIP6 (Université Paris VI)
and Project SALSA (INRIA)

Scott McCallum†
Macquarie University

June 1, 2007

Abstract

It is shown that the discriminant of a discriminant has the same irreducible factors as the product of seven polynomials which are defined as the GCD of the generators of an elimination ideal. Under tame conditions of genericity, three of these polynomials are irreducible and generate the corresponding elimination ideal, while the four other are equal to one. Moreover the factors of two of these polynomials are factors of multiplicity at least two of the iterated discriminant and the factors of two others of the seven polynomials have multiplicity at least three.

The proof involves an extended use of the notion of generic point of an algebraic variety and a careful study of the singularities of the hypersurface defined by a discriminant, which are interesting by them selves.

1 Introduction

It has been remarked, for a rather long time, that the discriminant of a discriminant has a natural factorization of the shape cPQ^2R^3 . The first author remarked this for polynomials of degree 4, when writing the paper [4] and studying Rozier's example in 1990 (see Section 6). He did not write anything on the subject, having no idea, at that time, for a general proof. This factorization has been stated as a general conjecture by the second author ([7], see also [5, 6]); in this manuscript, he gave an explicit description of the cubic factor R by means of a multivariate resultant.

In fact, such a factorization was known since nineteenth century and proved in [3] for generic bivariate polynomials of given degrees for each variable.

Recently, L. Busé and B. Mourrain proved a similar result for generic bivariate polynomials of a given total degree [1]. Their result is much stronger, as they prove the irreducibility of the factors and the fact that the factorization remains true for non generic coefficients, if the first discriminant has the degree which is expected. More precisely, they prove:

Theorem 1 (Busé – Mourrain) *Let A be a commutative ring and $f \in A[x, y]$ be a polynomial such that $\deg_x(f) = \deg_{\{x,y\}}(f) = n$ and $\deg_y(\text{disc}_x(f)) = n(n-1)$. Then we have $\text{disc}_y(\text{disc}_x(f)) = cPQ^2R^3$ where $c \in A$ is the coefficient of x^n in f and $P, Q, R \in A$ are defined by multivariate resultants.*

In practice, iterated discriminants appear frequently in Cylindrical Algebraic Decomposition (CAD) [2]. Therefore, the direct computation of the factors may improve dramatically the efficiency of CAD algorithm.

This led us, independently from Busé and Mourrain, to study this factorization. We got some results in the generic case which are now superseded by [1]. We did not publish them because they were not

*E-mail: Daniel.Lazard@lip6.fr

†E-mail: scott@ics.mq.edu.au

satisfactory in the non generic case. In fact, like Busé and Mourrain, we used multivariate resultant, which give no information when they vanish because irrelevant zeros at infinity.

Therefore, we use now elimination ideals and we have devoted this paper to the non generic case, without the degree restriction of Busé–Mourrain Theorem. We prove the following result.

Theorem 2 *Let K be a field and $f \in K[x, y, z, \dots]$. There exist seven polynomials $P, Q, R, S, P^\infty, Q^\infty, R^\infty$ such that either $\text{disc}_y(\text{disc}_x(f)) = PQRSP^\infty Q^\infty R^\infty = 0$ or the product $PQRSP^\infty Q^\infty R^\infty$ and the double discriminant $\text{disc}_y(\text{disc}_x(f))$ have the same irreducible factors. These polynomials are defined as the GCD of the generators of an elimination ideal. Under tame conditions of genericity, the polynomials P, Q, R are irreducible and generate a principal elimination ideal, while the other polynomials are equal to 1.*

Moreover, the square (resp. the cube) of the irreducible factors of QQ^∞ (resp. RR^∞) divide $\text{disc}_y(\text{disc}_x(f))$.

The replacement of the resultants by elimination ideals allows to take off the degree hypotheses of Busé–Mourrain Theorem, but implies to lose part of the information on the multiplicity of the factors.

These results allow a dramatic improvement of the computation of the factors of the iterated discriminant, as needed, for example, in Cylindrical Algebraic Decomposition (CAD) [2].

Three main ingredients are used in the proofs.

The first one consists in looking on the polynomials as finite Taylor series and comparing the order at a point (as a series) of a polynomial and its discriminant.

The second one is a careful description of the various singularities of the hypersurface defined by a discriminant. As this study is interesting by itself, we provide it with more details than needed for the main results of the paper.

The last ingredient is a systematic use of the Weil’s notion of a generic point of an irreducible variety. Although the word “generic” appears frequently in papers of Computer Algebra or of Applied Algebraic Geometry, the notion of a generic point of a variety is rarely used in its precise meaning. It is very powerful to avoid the problems set by the singularities when one try to show inclusions of varieties. Therefore it is a touchstone to apply the results on the singularities of the discriminant to the factorization of the double discriminant.

In all this paper, A will denote an integral ring, which is usually a polynomial ring $K[z, \dots]$ over a field or over the integers. We consider a polynomial $f = f(x, y) = f(x, y, z, \dots)$ in $A[x, y]$, and we study the factorization of its double discriminant $\text{disc}_y(\text{disc}_x(f))$.

We denote the partial derivatives of f such as $f'_x, f'_y, f''_{x^2}, f''_{x^2y}, f^{iv}_{x^3y}, \dots$

2 Discriminant and Sylvester matrix

Let A be any ring and $f \in A[x]$ be a polynomial. Let us write f as $f = a_0 + a_1x + \dots + a_nx^n$ with $a_i \in A$. We define $a_i := 0$ for $i < 0$ and $i > n$.

The Sylvester matrix of f and f'_x is the $(2n - 1) \times (2n - 1)$ matrix S such that the coefficient $S_{i,j}$ of the i -th row and the j -th column is a_{i-j} for $j < n$ and $(i - j + n) a_{i-j+n}$ for $j \geq n$:

$$S = \begin{pmatrix} a_0 & & & & a_1 & & & & \\ a_1 & a_0 & & & 2a_2 & a_1 & & & \\ a_2 & a_1 & a_0 & & 3a_3 & 2a_2 & a_1 & & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \end{pmatrix}$$

In fact we have reversed the usual order of the rows, in order to have the coefficients of low degrees at the beginning, but this does not change the sign of the determinant. Thus, the resultant of f and f'_x is $\text{res}_x(f, f'_x) = \det(S)$.

The discriminant $\text{disc}_x(f)$ of f with respect to x is defined as $\text{res}_x(f, f'_x)/a_n$. Thus, it is equal, up to the sign, to the determinant of the matrix S' in which a_n is replaced by 1 in the last row,

$$\begin{pmatrix} 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & na_n \end{pmatrix},$$

of S .

When $\deg_x(f) = 1$, then the matrix S' reduces to (1), and when f is independent of x , then S' is the empty matrix (with no row and no column). In both cases, we set $\text{disc}_x(f) = 1$.

When A is a polynomial ring, we need to compute the rank of S and S' when the indeterminates of A are replaced by values in some field. This is the aim of the following lemma, which, although not new, is not very well known.

Lemma 1 *Let φ be any homomorphism of A in some field K . We denote also by φ the extension of φ to an homomorphism of $A[x]$ into $K[x]$ or to a map from matrices over A to matrices over K . If $\varphi(S)$ is not the zero matrix, the rank of $\varphi(S)$ is $2n - k - l - 1$ where k is the degree in x of the GCD of $\varphi(f'_x) = \varphi(f)'_x$ and $\varphi(f)$, and l is the smallest integer such that $\varphi(a_{n-l}) \neq 0$.*

The rank of $\varphi(S')$ is $2n - k - l$ or $2n - k - 1$ depending on $\varphi(a_n) = 0$ or not (i.e. $l > 0$ or $l = 0$).

Proof. We may suppose that $\varphi(S)$ is not the zero matrix and thus that $\varphi(f) \neq 0$. Let F and F' be the quotients of $\varphi(f)$ and $\varphi(f'_x)$ by their GCD. Thus the degree of F is $n - k - l$ and that of F' is at most $n - k - l - 1$ (equality in characteristic 0).

The linear map

$$(A, B) \mapsto AF + BF'$$

where A (resp. B) is a polynomial in $K[x]$ of degree less than $n - k - l - 1$ (resp. less than $n - k - l$, the degree of F) is surjective onto the polynomials of degree less than $2n - 2k - 2l - 1$; in fact, the matrix of this application is the Sylvester matrix of F and F' and is invertible, because its determinant is not zero, being the resultant of F and F' , which are co-prime. Multiplying by the GCD of $\varphi(f)$ and $\varphi(f'_x)$ and by any power of x up to x^{k+l} , we see that the linear map

$$(A, B) \mapsto A\varphi(f) + B\varphi(f'_x)$$

(with A and B of respective degrees less than $n - 1$ and n) contains in its image the product of the GCD by any power of x less than $x^{2n-k-l-1}$. As this image may only contain multiples of the GCD, this shows that the dimension of the image, i.e. the rank of $\varphi(S)$, is $2n - k - l - 1$.

If $a_n \neq 0$, the rank of $\varphi(S')$ is clearly the same. If $a_n = 0$, the rank of $\varphi(S')$ could be $2n - k - l - 1$ or $2n - k - l$. The first principal subresultant coefficient of $\varphi(f)$ and $\varphi(f'_x)$ which is not 0 is the determinant of a submatrix of $\varphi(S')$ of rank $2n - 2l - 2k - 1$. This matrix may consist in rows $k + 1$ to $2n - 2l - k - 1$ and in columns 1 to $n - k - l - 1$ and n to $2n - k - l - 1$. Extending it by adding rows $2n - 2l - k$ to $2n - l - 1$ and $2n - 1$ and columns $n - k - l$ to $n - 1$ and $2n - 1$, we get a bloc triangular matrix which is regular of rank $2n - k - l$. \square

In preceding Lemma, the parameters k and l seems to be very different. In fact, l is the multiplicity of infinity as a root of f . This may be seen by the remark that the discriminants of $f = a_0 + a_1x + \cdots + a_nx^n$ and its reverse polynomial $a_n + a_{n-1}x + \cdots + a_0x^n$ may only differ by their sign. We will use the more general well known fact :

Lemma 2 *If a, b, c, d are elements of A such $ad - bc = \pm 1$, then f and $(cx + d)^n f(\frac{ax+b}{cx+d})$ have discriminants which differ only by their sign.*

We may now close the case of characteristic 2 by following result.

A point of a hypersurface defined by f in \tilde{K}^N is singular if it is not a zero of all partial derivative of f . A point which is not singular is regular. The multiplicity of a singular point is the smallest order of differentiation for which the point is not a zero of some partial derivative of f . (Note that, with this definition, we consider as different the hypersurfaces defined by f and f^2 , although they have the same points.)

The following lemmas are classic. They are corollaries of the first one, which follows itself from the isomorphism between the field generated by the coordinates of a generic point and the field of fractions of the ring associated to the variety. We refer to the text books of algebraic geometry or to [8] for more details

Lemma 3 Let $p = (\alpha, \beta, \dots)$ be a generic point of an irreducible variety V defined by polynomials with coefficients in K . If p belongs to a variety W , also defined over K , then $V \subset W$.

Lemma 4 A generic point of an irreducible variety is regular.

Lemma 5 Let I be an ideal of $K[x, y, z, \dots]$ and $J = I \cap K[z, \dots]$. For any generic point (γ, \dots) of any component of the variety defined by J , there exist α and β such $(\alpha, \beta, \gamma, \dots)$ is a zero of I .

We finish this subsection by a lemma which recalls the geometrical meaning of the hypersurface defined by the discriminant.

Lemma 6 Let $f \in K[x, y, z, \dots]$ of degree n in x . The point (β, γ, \dots) is a zero of $\text{disc}_x(f)$ if and only if either there exists α such $(\alpha, \beta, \gamma, \dots)$ is a common zero of f and f'_x or the degree in x of $f(x, \beta, \gamma, \dots)$ is at most $n - 2$.

In other words (β, γ, \dots) is a zero of $\text{disc}_x(f)$ if and only if $f(x, \beta, \gamma, \dots)$ has a multiple root, possibly at infinity.

Proof. This is very classical and is an immediate corollary of Lemma 1 : The rank of $\varphi(S')$ is not maximal if and only if $k \geq 1$ or $l \geq 2$. \square

We examine now the various possibilities for the relations between the zeros of $\text{disc}_x(f)$ and the corresponding multiple roots of f . For this purpose it may be useful to recall some basic facts and definitions of algebraic geometry.

The polynomial $f \in K[x, y, z, \dots]$ defines an hypersurface which is the set of points $(\alpha, \beta, \gamma, \dots)$ such that $f(\alpha, \beta, \gamma, \dots) = 0$. The *order* of a polynomial (at the origin) is the degree of its homogeneous part of lowest degree which is not null (i.e. its order as a Taylor series). If the origin $(0, 0, 0, \dots)$ belongs to the hypersurface defined by f (i.e. if $f(0, 0, 0, \dots) = 0$), then the origin is a *regular point* if the order of f is 1; otherwise the origin is a *singular point* and its *multiplicity* is the the order of f . If the origin is a regular point, the *tangent hyperplane* at the origin is the hypersurface defined by the homogeneous part of degree 1 of f . In the case of a singular point, of multiplicity m , the *tangent cone* is the hypersurface defined by the homogeneous part of degree m .

3.2 Regular points of the discriminant

Proposition 2 Given a polynomial $f \in K[x, y, z, \dots]$ such that $\deg_x(f) \geq 2$ and $\text{disc}_x(f) \neq 0$, let $(\alpha, \beta, \gamma, \dots)$ be a point such that α is a multiple root of $f(x, \beta, \gamma, \dots)$. Then (β, γ, \dots) is a zero of $\text{disc}_x(f)$, which is regular if and only if all the following conditions are satisfied: the characteristic of K is not 2; $(\alpha, \beta, \gamma, \dots)$ is a regular point of the hypersurface defined by f ; α is a root of multiplicity 2 of $f(x, \beta, \gamma, \dots)$; α is the only multiple root of $f(x, \beta, \gamma, \dots)$; $\deg_x(f(x, \beta, \gamma, \dots)) \geq \deg_x(f) - 1$.

If these conditions are fulfilled, the tangent hyperplanes of $f = 0$ at $(\alpha, \beta, \gamma, \dots)$ and of $\text{disc}_x(f) = 0$ at (β, γ, \dots) are defined by the same linear polynomial.

Proof. Remark first that the last condition means that there is no multiple root at infinity. Thus this condition becomes included in the preceding after the change of variable which follows.

By extending K to $K(\alpha)$ and applying Lemma 2, we may suppose that $\alpha = 0$ and $\deg_x(f) = \deg_x(f(x, \beta, \gamma, \dots))$. By a linear change of variables we may also suppose that $0 = \beta = \gamma = \dots$

Recall that $f = a_0 + a_1 x + \dots + a_n x^n$ and that its discriminant is the determinant of the matrix

$$S' = \begin{pmatrix} a_0 & & & & a_1 & & & & \\ a_1 & a_0 & & & 2a_2 & a_1 & & & \\ a_2 & a_1 & a_0 & & 3a_3 & 2a_2 & a_1 & & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \end{pmatrix}$$

in which the last row has been divided by a_n .

As $\alpha = 0$ is a multiple root, a_0 and a_1 vanish at the origin, which means that their order is at least 1. When expanding the determinant of S' , one may have a term of order 1 only if it contains $2a_2$ in the second row, which implies that the element in the first row is a_0 . Thus, the homogeneous part of degree one of the discriminant is that of $2a_0 a_2 D_1$, where D_1 is the minor of S' obtained by removing the two first rows and the first and n -th columns.

If one substitutes a_0 and a_1 by 0 in the corresponding submatrix, one gets a Sylvester matrix showing that $D_1 - \text{resultant}_x((f - a_0 - a_1 x)/x, (f'_x - a_1)/x)/a_n$ belongs to the ideal $\langle a_0, a_1 \rangle$. Therefore the substitution of y, z, \dots by $0, 0, \dots$ in this expression shows that $D_1(0, 0, \dots) = 0$ if and only if $(\gcd(f(x, 0, 0, \dots), f'_x(x, 0, 0, \dots)))/x$ is not constant, which means that either 0 is a root of multiplicity at least 3 or that there is another multiple root.

Thus the origin is a regular point of $\text{disc}_x(f)$ if and only if a_0 has order one and $2a_2 D_1$ does not vanish at the origin. Since $a_1 x + a_2 x^2 + \dots$ has order at least 2, the polynomial f has order 1 if and only a_0 has. This shows the first assertion of the proposition. This shows also the second part, since, if the conditions are fulfilled, the homogeneous parts of degree 1 of f and $\text{disc}_x(f)$ differ only by a constant factor, the constant term of $2a_2 D_1$. \square

3.3 Cusp like points of the discriminant

Proposition 3 *Given a polynomial $f \in K[x, y, z, \dots]$ such that $\deg_x(f) \geq 3$ and $\text{disc}_x(f) \neq 0$, let $(\alpha, \beta, \gamma, \dots)$ be a point such that α is a root of $f(x, \beta, \gamma, \dots)$ of multiplicity at least 3. Then (β, γ, \dots) is a singular zero of $\text{disc}_x(f)$, which has multiplicity 2 if and only if all the following conditions are satisfied: $(\alpha, \beta, \gamma, \dots)$ is a regular zero of f ; the characteristic is not 3; the root α of $f(x, \beta, \gamma, \dots)$ has multiplicity 3; $f(x, \beta, \gamma, \dots)$ has no other multiple root; $\deg_x(f(x, \beta, \gamma, \dots)) \geq \deg_x(f) - 1$.*

If these conditions are fulfilled, the equation of the tangent cone to $\text{disc}_x(f)$ at β, γ, \dots is, up to a constant factor, the square of the equations of the tangent hyperplane to f at $(\alpha, \beta, \gamma, \dots)$.

Proof. Remark, as above, that the last condition means that there is no multiple root at infinity. Thus this condition becomes included in the preceding one after the change of variable which follows.

As above, we may change the variables in order that $(\alpha, \beta, \gamma, \dots)$ becomes the origin and that $\deg_x(f(x, 0, 0, \dots)) = \deg_x(f)$

If $\alpha = 0$ is a root of multiplicity at least 3 of $f(x, 0, 0, \dots)$, then a_0, a_1 and a_2 have an order at least 1 at the origin. Thus the two first rows of S' have an order at least 1 and the order of the discriminant is at least 2. We have to look further at the Sylvester matrix

$$S' = \begin{pmatrix} a_0 & & & & a_1 & & & & \\ a_1 & a_0 & & & 2a_2 & a_1 & & & \\ a_2 & a_1 & a_0 & & 3a_3 & 2a_2 & a_1 & & \\ a_3 & a_2 & a_1 & a_0 & 4a_4 & 3a_3 & 2a_2 & a_1 & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \end{pmatrix}$$

The last block consists in the remaining row and columns. It is the Sylvester matrix of $(f - a_0 - a_1x - a_{n-1}x^{n-1} - a_nx^n)/x$ and $(f'_x - a_1 - (n-1)a_{n-1}x^{n-2} - na_nx^{n-1})/x$. Thus its determinant, say D_3 , vanishes at the origin if and only if either the multiplicity of α_1 or α_2 is higher than 2 or if $f(x, 0, 0, \dots)$ has another multiple root.

This proves that the homogeneous part of degree 2 of $\text{disc}_x(f)$ is that of $8a_0a_2a_{n-2}^2a_nD_3$, which proves the result, since the equations of the tangent planes at the origin are the linear part of a_0 and a_n . \square

3.5 Projection of an ordinary singularity

Proposition 5 *Given a polynomial $f \in K[x, y, z, \dots]$ such that $\deg_x(f) \geq 2$ and $\text{disc}_x(f) \neq 0$, let $(\alpha, \beta, \gamma, \dots)$ be a singular zero of the hypersurface defined by f . Then (β, γ, \dots) is a singular zero of $\text{disc}_x(f)$, which has multiplicity 2 if and only if all the following conditions are satisfied: the singular point $(\alpha, \beta, \gamma, \dots)$ has multiplicity 2 and the equation of its tangent cone is not a square; the root α of $f(x, \beta, \gamma, \dots)$ has the multiplicity 2; $f(x, \beta, \gamma, \dots)$ has no other multiple root; $\deg_x(f(x, \beta, \gamma, \dots)) \geq \deg_x(f) - 1$.*

If these conditions are fulfilled, the equation of the tangent cone to $\text{disc}_x(f)$ at β, γ, \dots is, up to a constant factor, $\text{disc}_x(T)$, where T is the equation of the tangent cone of f at $\alpha, \beta, \gamma, \dots$

Proof. As in the preceding propositions, we may suppose that $0 = \alpha = \beta = \gamma = \dots$ and that a_n does not vanish at the origin.

The hypothesis implies thus that the order of a_0 (resp. a_1) is at least 2 (resp. 1). A term of order at most 2 in the expansion of the determinant of S' should contain either $2a_0a_2$ or a_1^2 in the two first rows. It is thus of order at least 2 and should contain $3a_3$ or $2a_2$ in the third row.

This shows that the order of $\text{disc}_x(f)$ is at least 2, i.e. $\text{disc}_x(f)$ is singular at the origin. Moreover the homogeneous part of degree 2 of the determinant of S' is the same as the determinant of the matrix deduced from S' by substituting a_0 and a_1 by 0 in all rows of S' but the two first ones. This matrix is block triangular with two blocks on the diagonal. The first block is

$$\begin{pmatrix} a_0 & a_1 & & \\ a_1 & 2a_2 & a_1 & \\ a_2 & 3a_3 & 2a_2 & \end{pmatrix}.$$

Since the term $3a_0a_1a_3$ in its determinant has order at least 3, the homogeneous part of degree 2 of this determinant is that of $a_2(4a_0a_2 - a_1^2)$. It is null if either $a_2(0, 0, \dots) = 0$ i.e. α is a root of multiplicity at least 3 of $f(x, \beta, \gamma, \dots)$ or $4a_0a_2 - a_1^2$ has an order higher than 2. Let h_2 be the homogeneous part of degree 2 of f ; it is also the homogeneous part of degree 2 of $a_0 + a_1x + a_2x^2$. This shows that the homogeneous part of degree 2 of $4a_0a_2 - a_1^2$ is $\text{disc}_x(h_2)$. If a_2 does not vanish at the origin, $\text{disc}_x(h_2) = 0$ if and only if h_2 is the square of a linear polynomial.

The second block is obtained by removing the three first rows and the first, n -th and $(n+1)$ -th columns from S' and substituting a_0 and a_1 by 0. It is a Sylvester matrix whose determinant is the quotient by a_n of the resultant of $(f - a_0 - a_1x)/x^2$ and $(f'_x - a_1)/x$. It vanishes at the origin if and only if either α is a root of $f(x, \beta, \gamma, \dots)$ of multiplicity at least 3 or if $f(x, \beta, \gamma, \dots)$ has another multiple root. \square

3.6 Projection of a cusp like singularity

Proposition 6 *Given a polynomial $f \in K[x, y, z, \dots]$ such that $\deg_x(f) \geq 2$ and $\text{disc}_x(f) \neq 0$, let $(\alpha, \beta, \gamma, \dots)$ be a singular zero of multiplicity 2 of $f = 0$, with the square of an hyperplane as a tangent cone.*

4.2 Critical values of the double projection

Let I_1 be the ideal of $K[x, y, z, \dots]$ generated by (f, f'_x, f'_y) . We set $P = \gcd(I_1 \cap K[z, \dots])$.

As we have to take into account the values “at infinity” for x , we introduce also the ideal I_1^∞ generated by $(a_n, a_{n-1}, \partial a_n / \partial y)$ and the polynomial $P^\infty = \gcd(I_1^\infty \cap K[z, \dots])$.

Lemma 8 *If $PP^\infty \neq 0$, any irreducible factor of PP^∞ divides the polynomial $\text{disc}_y(\text{disc}_x(f))$. If $PP^\infty = 0$ then $\text{disc}_y(\text{disc}_x(f)) = 0$.*

Proof. Let (γ, \dots) be a generic zero of some irreducible factor of P . By lemma 5, there exist α and β s.t. $(\alpha, \beta, \gamma, \dots)$ is a common zero of the elements of I_1 .

If $(\alpha, \beta, \gamma, \dots)$ is singular on $f = 0$ then Proposition 5 applied to f and then to $\text{disc}_c(f)$ shows that (γ, \dots) is a singular zero of $\text{disc}_y(\text{disc}_x(f))$. If $(\alpha, \beta, \gamma, \dots)$ is non singular, then Proposition 2 shows that $\text{disc}_x(f)'_y = 0$. As we have also $\text{disc}_x(f) = 0$ at this point, it follows that, in any case, (γ, \dots) is a zero of the hypersurface defined by $\text{disc}_y(\text{disc}_x(f))$. Lemma 3 implies thus that every irreducible factor of P divides $\text{disc}_y(\text{disc}_x(f))$.

Similarly, if (γ, \dots) is a generic zero of some irreducible factor of P^∞ , there exists β such that β, γ, \dots is a common zero of the elements of I_1^∞ . As a_n and a_{n-1} are null at this point, we have $\text{disc}_x(f) = 0$ at this point.

Let us homogenize f with respect to x , i.e let us consider the polynomial $g(x, t) = \text{numer}(\text{subs}(x = x/t, f))$. We have $\text{disc}_t(g(1, t)) = \text{disc}_x(f)$ by Lemma 2. The term independent from t in $\partial g(1, t) / \partial y$ is $\partial a_n / \partial y$. Thus, the above proof applied to $g(1, t)$ instead of f and with $\alpha = 0$, shows that (γ, \dots) is a zero of $\text{disc}_y(\text{disc}_x(f))$, and therefore that every irreducible factor of P^∞ divides the double resultant.

Finally, if $PP^\infty = 0$, the above proof applies by taking for (γ, \dots) a generic point of the whole affine space (the algebraic variety defined by the null polynomial). This shows that the whole space is included in the variety defined by $\text{disc}_y(\text{disc}_x(f))$, i.e. that this polynomial is identically null. \square

Remarks. We have $P = 0$ when $f = 0$ has a singular locus of codimension 1. This is especially the case when the polynomial f is reducible.

Usually (and generically, as it will be shown below), $I_1 \cap K[z, \dots]$ is a principal ideal and there is no need of computing a GCD for computing P . However, if $f = ay + \varphi(x + by + c)$ for some univariate polynomial $\varphi(u) \in K[u, z, \dots]$ and $a, b, c \in K[z, \dots]$, the ideal $I_1 \cap K[z, \dots]$ contains a and $\text{disc}_u(\varphi)$. Generally, these elements are relatively prime, and $P = 1$.

Similarly, P^∞ is usually equal to one. However, if $a_{n-1} = 0$, it has the same irreducible factors as $\text{disc}_y(a_n)$. If a_n is independent from y and a_{n-1} depends from y , then $P^\infty = a_n$; this is especially the case when f is homogeneous with respect to x, y and some other variables.

4.3 One triple root of f

Let I_3 be the ideal of $K[x, y, z, \dots]$ generated by (f, f'_x, f''_{x^2}) . We set $R = \gcd(I_3 \cap K[z, \dots])$ if $\deg_x(f) \geq 3$, and $R = 1$ for smaller degrees.

For the case where the triple root is at infinity, we define also I_3^∞ , the ideal generated by a_n, a_{n-1} and a_{n-2} and we set $R^\infty = \gcd(I_3^\infty \cap K[z, \dots])$. If $n < 3$ we set $R^\infty = 1$.

Lemma 9 *If $RR^\infty \neq 0$, the cube of any irreducible factor of RR^∞ divides $\text{disc}_y(\text{disc}_x(f))$. If $RR^\infty = 0$ then $\text{disc}_y(\text{disc}_x(f)) = 0$.*

Proof. An irreducible factor R_i of RR^∞ defines a hypersurface which is an irreducible component of the variety defined by the intersection with $K[z, \dots]$ of either I_3 or I_3^∞ . Therefore if (γ, \dots) is a generic zero of R_i , then, by Lemma 5, either there exist α and β s.t. $(\alpha, \beta, \gamma, \dots)$ is a common zero of the elements of I_3 or there exists β s.t. (β, γ, \dots) is a common zero of a_n, a_{n-1}, a_{n-2} . By definition

of I_3 and I_3^∞ , the infinity or α is a triple root of $f(x, \beta, \gamma, \dots)$ and in both cases, Propositions 3 and 6 show that either $\text{disc}_y(\text{disc}_x(f)) = 0$ or (γ, \dots) is a singular zero of $\text{disc}_y(\text{disc}_x(f))$ of multiplicity at least three. It follows that the variety $\text{disc}_y(\text{disc}_x(f)) = 0$ contains the variety $RR^\infty = 0$, even in the case where RR^∞ is identically null.

If $RR^\infty \neq 0$, then (γ, \dots) is a regular zero of a factor R_i of RR^∞ (Lemma 4) and is not a zero of the other factors of $RR^\infty \neq 0$ (Lemma 3). If the multiplicity of R_i as a factor of $\text{disc}_y(\text{disc}_x(f))$ would be lower than three, then the multiplicity of (γ, \dots) as a point of the hypersurface defined by $\text{disc}_y(\text{disc}_x(f))$ would thus be also lower than three, contradicting above assertion. This finishes the proof. \square

Remarks. Generally $I_3 \cap K[z, \dots]$ is a principal ideal and R may be computed without computing a GCD. We will show that this is always the case with a very tame condition of genericity.

On the other hand, R^∞ is usually equal to 1. However, if $a_{n-1} = 0$, the polynomial R^∞ has the same irreducible factors as the resultant of a_n and a_{n-2} with respect to y .

4.4 Two double roots of f

Intuitively, the ideal I_2 corresponding to the β, γ, \dots such that $f(x, \beta, \gamma, \dots)$ has two double roots should be generated by $f(x, y, z, \dots)$, $f'_x(x, y, z, \dots)$, $f(x_1, y, z, \dots)$, $f'_x(x_1, y, z, \dots)$. However, we have to exclude the case where the two roots are equal, which is done in the following way.

Let us introduce two new variables, a and b . Let q and r be the quotient and the remainder of the Euclidean division of f by $(x^2 + ax + b)^2$ w.r.t. x . The remainder r is a polynomial in x of degree at most 3, whose coefficients c_0, c_1, c_2 and c_3 are polynomials in a, b, y, z, \dots . Let $I_2 = \langle c_0, c_1, c_2, c_3 \rangle$ be the ideal generated by these coefficients and $Q = \text{gcd}(I_2 \cap K[z, \dots])$.

Let also I_2^∞ be the ideal generated by a_n, a_{n-1}, f, f'_x and $Q^\infty = \text{gcd}(I_2^\infty \cap K[z, \dots])$.

If $\deg_x(f) < 4$ we set $Q = Q^\infty = 1$.

Lemma 10 *If $QQ^\infty \neq 0$, then the square of any irreducible factor of QQ^∞ divides $\text{disc}_y(\text{disc}_x(f))$. If $QQ^\infty = 0$ then $\text{disc}_y(\text{disc}_x(f)) = 0$.*

Proof. An irreducible factor Q_i of QQ^∞ defines an hypersurface which is an irreducible component of the intersection with $\tilde{K}[z, \dots]$ of either I_2 or I_2^∞ . Therefore, if (γ, \dots) is a generic zero of Q_i , then, by Lemma 3, either there exist α, α_1 and β s.t. $(\alpha, \alpha_1, \beta, \gamma, \dots)$ is a common zero of I_2 or there exist $(\alpha, \beta, \gamma, \dots)$ s.t. $(\alpha, \beta, \gamma, \dots)$ is a common zero of I_2^∞ . By the definition of I_2 and I_2^∞ this means that the polynomial $f(x, \beta, \gamma, \dots)$ has two multiple roots, one of them being possibly at infinity. It follows by Propositions 4 and 5 that (γ, \dots) is a zero of $\text{disc}_y(\text{disc}_x(f))$ whose multiplicity at least two if this polynomial is not identically null.

If $QQ^\infty = 0$, this shows that $\text{disc}_y(\text{disc}_x(f)) = 0$ (Lemma 3). If $QQ^\infty \neq 0$, this shows that the square of any irreducible factor of QQ^∞ divides $\text{disc}_y(\text{disc}_x(f))$, by the same argument as in the proof of Lemma 9. \square

Remarks. We will see below that $I_2 \cap K[z, \dots]$ is generically a principal ideal, and therefore Q may usually be computed without GCD computation.

On the other hand Q^∞ is usually equal to 1. However, if $a_{n-1} = 0$, it has the same irreducible factors as the resultant, with respect to y , of a_n and $\text{disc}_x(f - a_n x^n)$.

4.5 The factorization

We may now state the main result of this paper for the non generic case.

Theorem 3 *If $\deg_x(f) > 1$, $\deg_y(\text{disc}_x(f)) > 1$ and the characteristic of K is not 2, then the polynomials $\text{disc}_y(\text{disc}_x(f))$ and $PQRS P^\infty Q^\infty R^\infty$ are either both 0 or have the same irreducible factors. In the latter case, the irreducible factors of QQ^∞ and RR^∞ have respectively a multiplicity of, at least, 2 or 3 in the factorization of $\text{disc}_y(\text{disc}_x(f))$.*

When the above hypotheses are not satisfied, then $\text{disc}_y(\text{disc}_x(f))$ is 0 or 1.

Proof. The last assertion results immediately from Proposition 1 and the definition of the discriminant of a polynomial of degree lower than two.

According to the preceding results, it remains only to show that if the double discriminant is identically null then $PQRS P^\infty Q^\infty R^\infty = 0$, and that if $\text{disc}_y(\text{disc}_x(f)) \neq 0$, then it has no other irreducible factors than those of $PQRS P^\infty Q^\infty R^\infty$.

To deal with both cases together, we consider a point (γ, \dots) which is either a generic point of the whole space or a generic point of some irreducible factor, say G , of the double discriminant. Several cases may occur, that we list now.

The first case is when (γ, \dots) is a common zero of the ideal I_0 generated by b_d and b_{d-1} , the coefficients of the highest powers of y in $\text{disc}_x(f)$. As we have supposed that $\deg_y(\text{disc}_x(f)) > 1$, this case may only occur if the double discriminant is not null; thus (γ, \dots) is the generic point of G , which is therefore a factor of S (Lemma 3).

If we are not in this case, there is β s.t. (β, γ, \dots) is a zero of $\text{disc}_x(f)$, and thus some α , possibly at infinity, s.t. α is a multiple root of $f(x, \beta, \gamma, \dots)$. If α is not unique, then (γ, \dots) is a zero of $I_2 \cap K[z, \dots]$ or $I_2^\infty \cap K[z, \dots]$, by the definition of these ideals. As (γ, \dots) is a generic point of the whole space or of an hypersurface, it follows from Lemma 3 that one of these ideal is either null or contained in the principal ideal generated by G ; this implies that QQ^∞ is either null or is a multiple of G .

If α is a root of $f(x, \beta, \gamma, \dots)$ of multiplicity higher than two, then the same argument shows that either $RR^\infty = 0$ or G divides RR^∞ .

If α is the unique multiple root of $f(x, \beta, \gamma, \dots)$ and has multiplicity two, then Proposition 2 implies that either $(\alpha, \beta, \gamma, \dots)$ is a singular point of the hypersurface defined by f or the tangent hyperplanes of f and $\text{disc}_x(f)$ have the same equation. As β, γ, \dots is a common zero of $\text{disc}_x(f)$ and $\text{disc}_x(f)'_y$, this equation is thus independent from x and y . This shows that in both cases $(\alpha, \beta, \gamma, \dots)$ is a common zero of the generators of I_1 (or I_1^∞ if α is at infinity). Thus, by the same argument as above, PP^∞ is either null or a multiple of G . \square

It may be useful for the reader to reread the last argument of this proof in the following way : The variety $\text{disc}_y(\text{disc}_x(f)) = 0$ is a union of irreducible hypersurfaces which is contained in the union of the varieties of some ideals ; each of these irreducible hypersurfaces should thus be contained in some irreducible (hypersurface) component of one of the ideals. This is this fact which allows to replace ideals by their GCD.

Remark. In this proof, we have used the fact that, when the variety of an ideal contains a hypersurface, then the GCD of this ideal is a multiple of the (squarefree) equation of the hypersurface.

5 Generic situation

The aim of this section is to prove that, under tame conditions of genericity, the product of polynomials $SPP^\infty(QQ^\infty)^2(RR^\infty)^3$ divides $\text{disc}_y(\text{disc}_x(f))$ and that those of these factors which are not constant are irreducible and distinct. In fact, we have $\text{disc}_y(\text{disc}_x(f)) = PQRS P^\infty Q^\infty R^\infty$ for some kinds of generic polynomials. However, the notion of genericity depends on the support of the polynomial. It is therefore out of the scope of the paper to explicit, for all possible supports the conditions of genericity which induce this equality.

Usually, a generic polynomial is defined as a polynomial whose coefficients are distinct indeterminates. This implies to define the *support* of the polynomial, which is the set of the monomials with a non-zero coefficient. Therefore, for most authors a generic polynomial is a polynomial of a given total degree n (the support is the set of monomials of degree at most n) or a homogeneous polynomial of degree n (the support is the set of monomials of degree n). In most applications, these restricted definitions of a generic polynomial are convenient, because the properties which are studied behave well by specializing to zero some of the coefficients.

Here, things are more complicated, because the double discriminant depends on $\deg_y(\text{disc}(f))$, which itself depends strongly on the support of f . It follows that we have to deal with generic polynomials of any support.

Moreover, for most of our results, we do not need that all coefficients are generic, but only some of them. This is the motivation of the definition which follows.

Definition 2 Let $A = K[z, \dots]$. A generic support of a polynomial $f \in A[x, y]$ is a subset of the monomials $x^i y^j$ of f whose coefficients (in A) have the shape $U_{i,j} + g_{i,j}$ where $g_{i,j} \in A$ and $U_{i,j}$ is an indeterminate which does not occur elsewhere in f .

It may be noted that the usual notion of *generic polynomial* correspond to the case where the set of all monomials (the support of the polynomial) is a generic support and all g_i are null.

We have also to recall that the *height* (also called *codimension*) of a prime ideal J is the maximal length of strictly ascending chains $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \dots \subset \mathcal{P}_h = J$.

The following lemma is the key tool for the proofs involving a generic support

Lemma 11 Let $g_0, v_1 + g_1, \dots, v_k + g_k$ be polynomials in $K[v_1, \dots, v_k, x, y, \dots]$ such that $g_i \in K[x, y, \dots]$ for $i = 0, 1$ and $g_i \in K[v_1, \dots, v_{i-1}, x, y, \dots]$ for $i > 1$. The ideal generated by $v_1 + g_1, \dots, v_k + g_k$ in $K(v_1, \dots, v_k)[x, y, \dots]$ is prime of height k and defines a variety which is not contained in the hypersurface defined by g_0 (if $g_0 \neq 0$).

Proof. To prove that the ideal generated by the $v_i + g_i$ is prime of height k , it suffices to prove that it is true for the ideal I generated by the same polynomials in the ring $K[v_1, \dots, v_k, x, y, \dots]$, because $K(v_1, \dots, v_k)[x, y, \dots] = S^{-1} K[v_1, \dots, v_k, x, y, \dots]$, with $S = K[v_1, \dots, v_k] \setminus \{0\}$.

The ideal I is prime as being the inverse image of the prime ideal 0 by the homomorphism from $K[v_1, \dots, v_k, x, y, \dots]$ into $K[x, y, \dots]$ obtained by substituting the v_i by the $-g_i$ as far as possible. As I is generated by k elements, its height is at most k . It is k because $0 \subset \langle v_1 + g_1 \rangle \subset \langle v_1 + g_1, v_2 + g_2 \rangle \subset \langle v_1 + g_1, v_2 + g_2, v_3 + g_3 \rangle$ is a sequence of prime ideals.

Now, g_0 belongs clearly not to the inverse image of zero by this homomorphism. Therefore it does not belong to I nor to $S^{-1} I$; As the ideal I is prime, this implies the last assertion. \square

Proposition 8 Under Hypothesis 1, if the characteristic of K is 0 and $\{1, x, y, x^2, xy, y^2\}$ is a generic support of f , then the ideal I_1 of Section 4.2 is prime, $I_1 \cap K[z, \dots]$ is a principal ideal, thus generated by P , which is not a constant. Moreover, if $\text{disc}_y(\text{disc}_x(f))$ is not null, then P does not divide $QRSP^\infty Q^\infty R^\infty$.

Proof. Recall that I_1 is generated by f, f'_x, f'_y . The constant terms of these polynomials are respectively $U_{0,0}, U_{1,0}$ and $U_{0,1}$, and Lemma 11 applies with $v_1 = U_{0,1}, v_2 = U_{1,0}$ and $v_3 = U_{0,0}$. Thus I_1 is prime of height 3.

The ideal $I_1 \cap K[z, \dots]$ is thus also prime. To prove that it is principal and not generated by a constant, it suffices to show that its height is one. Thus we have to prove that the dimensions of I_1 and $I_1 \cap K[z, \dots]$ are equal. This will be the case if the implicit functions theorem applies at a generic point,

i.e. if the Jacobian matrix of f, f'_x, f'_y w.r.t. x, y has rank 2 at a generic point of the variety of I_1 . This Jacobian matrix contains the minor

$$\begin{pmatrix} f''_{x^2} & f''_{xy} \\ f''_{xy} & f''_{y^2} \end{pmatrix},$$

whose determinant, $f''_{x^2}f''_{y^2} - f''_{xy}{}^2$, is a polynomial of degree two in U_{xy} , which is not null at a generic point of I_1 , as the coefficient of U_{xy} in it is -1 (Lemma 11).

We prove now that a generic point of the hypersurface $P = 0$ does not belongs to the other factors. Thus, let $\Gamma = (\alpha, \beta, \gamma, \dots)$ be a generic zero of I_1 . By above proof, (γ, \dots) is a generic zero of P .

As the coefficient a_n of x^n in f does not depends on $U_{0,0}, U_{1,0}$ and $U_{0,1}$ (because $n = \deg_x(f) \geq 2$), Lemma 11 shows that Γ is not a zero of a_n and is therefore not a zero of $P^\infty Q^\infty R^\infty$.

The polynomial f''_x which appears in the definition of I_3 (Section 4.3) is not null (as having $2U_{2,0}$ as a constant term) and does not depends on $U_{0,0}, U_{1,0}$ and $U_{0,1}$. Therefore Lemma 11 shows that Γ is not a zero of I_3 and P does not divides Q (Lemma 11).

Similarly the coefficient c_2 which appears in the definition of I_2 (Section 4.4) does not depends on $U_{0,0}, U_{1,0}$ and $U_{0,1}$, but has $U_{2,0}$ as a constant term. Thus Γ is not a zero of I_2 and P does not divides Q .

To show that P does not divides S , it suffices to show that Γ is not a zero of the coefficient b_d of the highest power of y in $\text{disc}_x(f)$. For this, one may remark that the coefficients a_i and therefore $\text{disc}_x(f)$ are polynomials in $y, U_{0,0} + U_{0,1}y + U_{0,2}y^2$ and $U_{1,0} + U_{1,1}y$. It follows that $U_{0,0}, U_{1,0}$ and $U_{0,1}$ do not appear in b_d and Γ is not a zero of b_d , by Lemma 11. \square

Proposition 9 *Under Hypothesis 1, if the characteristic of K is 0 and $\{1, x, x^2, x^3, y, xy, x^2y\}$ is a generic support of f , then the ideal I_3 of Section 4.3 is prime, $I_3 \cap K[z, \dots]$ is a principal ideal, thus generated by R , which is not a constant. Moreover, if $\text{disc}_y(\text{disc}_x(f))$ is not null, then R does not divides $PQSP^\infty Q^\infty R^\infty$.*

Proof. The proof is very similar as that of Proposition 8, and we detail only their differences.

As I_3 is generated by f, f'_x, f''_{x^2} , the constant terms of its generators are $U_{0,0}, U_{1,0}$ and $U_{2,0}$. Therefore I_3 and $I_3 \cap K[z, \dots]$ are prime.

The Jacobian matrix of the generators of I_3 contains the minor

$$\begin{pmatrix} f'_x & f'_y \\ f'''_{x^3} & f'''_{x^2y} \end{pmatrix},$$

whose determinant at a zero of I_3 is $f'_y f'''_{x^3}$. It is not null at a generic zero of I_3 , as containing the term $U_{0,1}U_{3,0}$.

As x^3 belongs to the generic support of f , we have $\deg_x(f) \geq 3$ and $U_{0,0}, U_{1,0}, U_{2,0}$ do not appear in a_n , which implies that R does not divides $P^\infty Q^\infty R^\infty$.

The polynomial R does not divides P nor Q because f'_y and the coefficient c_3 of the definition of I_2 do not depend from $U_{0,0}, U_{1,0}, U_{2,0}$ and are not null, having respectively $U_{0,1}$ and $U_{3,0}$ as constant terms.

The coefficients a_i and therefore $\text{disc}_x(f)$ are polynomials in $y, U_{0,0} + U_{0,1}y, U_{1,0} + U_{1,1}y, U_{2,0} + U_{2,1}y$, with no other occurrences of $U_{0,0}, U_{1,0}, U_{2,0}$. Therefore the coefficient b_d of the highest power of y in $\text{disc}_x(f)$ does nor depends on $U_{0,0}, U_{1,0}, U_{2,0}$. \square

Proposition 10 *Under Hypothesis 1, if $\{1, x, x^2, x^3, x^4, y, xy, x^2y, x^3y\}$ is a generic support of f and the characteristic of K is 0, then the ideal I_2 of Section 4.4 is prime, $I_2 \cap K[z, \dots]$ is a principal ideal, thus generated by Q , which is not a constant. Moreover, if $\text{disc}_y(\text{disc}_x(f))$ is not null, then Q does not divides $PRSP^\infty Q^\infty R^\infty$.*

Proof. It results from the definition of the Euclidean division that, for $i < 4$, the part of the generator c_i of I_2 which is independent from a and b is the coefficient a_i of x in f . Also, the coefficient of a in c_3 and the coefficients of b in c_2 (viewed as polynomials in a and b) are both $-a_4$. Moreover all the other terms of the c_i are of degree at least two in a and b .

It results that Lemma 11 applied with $v_i = U_{i-1,0}$ shows that I_2 and $I_2 \cap K[z, \dots]$ are prime.

The Jacobian matrix of the generators of I_2 contains the minor

$$\begin{pmatrix} \partial c_0 / \partial y & \partial c_0 / \partial a & \partial c_0 / \partial b \\ \partial c_2 / \partial y & \partial c_2 / \partial a & \partial c_2 / \partial b \\ \partial c_3 / \partial y & \partial c_3 / \partial a & \partial c_3 / \partial b \end{pmatrix}.$$

It results from above property of the coefficients of a and b in the c_i that the determinant of this minor contains the term $U_{0,1}U_{4,0}^2$ and that the $U_{i,0}$ do not appear in it for $i = 0, \dots, 3$. Thus this minor is not null at a generic zero of I_2 .

As x^4 belongs to the generic support of f , we have $\deg_x(f) \geq 4$ and $U_{0,0}, U_{1,0}, U_{2,0}, U_{3,0}$ do not appear in a_n , which implies that q does not divide $P^\infty Q^\infty R^\infty$.

The polynomial Q does not divide P because f'_y is not null, does not depend from $U_{0,0}, U_{1,0}, U_{2,0}, U_{3,0}$ and has $U_{0,1}$ as a constant terms. It does not divide R , because, under our hypotheses, Q and R are both irreducible and we have already shown that R does not divide Q .

The coefficients a_i and therefore $\text{disc}_x(f)$ are polynomials in $y, U_{0,0} + U_{0,1}y, U_{1,0} + U_{1,1}y, U_{2,0} + U_{2,1}y, U_{3,0} + U_{3,1}y$, with no other occurrences of $U_{0,0}, U_{1,0}, U_{2,0}, U_{3,0}$. Therefore the coefficient b_d of the highest power of y in $\text{disc}_x(f)$ does not depend on $U_{0,0}, U_{1,0}, U_{2,0}, U_{3,0}$. \square

Proposition 11 *If f is monic as a polynomial in x , then $P^\infty Q^\infty R^\infty = 1$.*

If $\{x^n, x^{n-1}, x^n y\}$, (resp. $\{x^n, x^{n-1}, x^{n-2}\}$, $\{1, x, x^n, x^{n-1}\}$) is a generic support of f , then P^∞ (resp. R^∞, Q^∞) is the polynomial 1.

On the other hand, if $\deg_y(a_n) = 0$ and $\deg_y(a_{n-1}) > 0$, then $P^\infty = a_n$. If $\deg_y(a_n) = \deg_y(a_{n-1}) = 0$, then $P^\infty = \text{gcd}(a_n, a_{n-1})$. (Note that this occurs if $\deg_x(f) = \deg_{x,y}(f)$).

If $a_{n-1} = 0$ and $\{x^n, x^n y, x^n y^2\}$ (resp. $\{x^n, x^{n-2}, x^n y\}$, $\{1, x, x^2, x^n, x^n y\}$) is a generic support of f , then P^∞ , (resp. R^∞, Q^∞) is irreducible and non constant.

Proof. The first assertion is immediate.

The definition of I_1^∞ and I_3^∞ and Lemma 11 show that these ideals are prime of height three. Thus their intersection with $K[z, \dots]$ are prime of height at least two, which implies that their GCD are constant. The same argument applies to Q with height three replaced by height four.

If $\deg_y(a_n) = 0$, both assertions result immediately from the definition of P^∞ .

Finally the hypotheses of genericity imply that the ideals I_1^∞, I_2^∞ and I_3^∞ are prime and that the Jacobian matrix of the projection eliminating y (resp. x and y) does not vanishes at a generic zero of the ideal. \square

Proposition 12 *Let $e_i = \deg_y(a_i)$ for $i = 0, \dots, n$ and $d = \deg_y(\text{disc}_x(f))$. Suppose that the characteristic of K does not divide $n(n-1)$, that $d = (n-1)(e_0 + e_n) = (n-1)(e_1 + e_{n-1})$ and that none term of the expansion of the determinant of the matrix S' has a degree higher than d . If $\{y^{e_0-1}, xy^{e_1}, x^{n-1}y^{e_{n-1}}\}$ is a generic support of f , then $S = 1$.*

Above hypotheses are generically satisfied if the support of f consists in all monomials of degree n in x, y or in all monomials of degrees n in x and e_0 in y .

On the other hand, there exists polynomials for which $S \neq 1$.

Proof. The last assertion will be proved in next section.

The second assertion is almost immediate: In the second case, all a_i have the degree e_0 in y and the result follows that every term of the expansion of the determinant of the matrix S' consists in a product of $2(n-1)$ coefficients a_i . In the first case, is it a classical exercise to show that any term in the expansion of S' has the degree $n(n-1)$ in n .

Let $u_{i,j}$ be the coefficient of y^j in a_i , when $x^i y^j$ does not belong to the generic support under consideration. Let also $f'_\infty = nf - xf'_x = a_{n-1}x^{n-1} + 2a_{n-2}x^{n-2} + \dots + na_0$. We have $\text{disc}_f(x) = \text{res}_x(f'_\infty, f'_x)/n^{n-1}$. Looking at the Sylvester matrix of this resultant, it appears that the expansion of this determinant contains the terms $(a_1 a_{n-1})^{n-1}$ and $n^{2(n-1)}(a_0 a_n)^{n-1}$. It follows that the coefficient b_d of $\text{disc}_x(f)$ is equal to $(U_{n-1, e_{n-1}} U_{1, e_1}/n)^{n-1} + \dots$, where the dots replace a polynomial independent from U_{0, e_0-1} and of degree lower than $n-1$ in $U_{n-1, e_{n-1}}$. Similarly, the coefficient b_{d-1} has the shape $(n-1)n^{n-1}u_{n, e_n}^{n-1}u_{0, e_0}^{n-2}U_{0, e_0-1} + \dots$, where the dots are independent from U_{0, e_0-1} . Thus this coefficient is linear in U_{0, e_0-1} with a leading term involving variables which do not appear in the leading term of b_d . This implies clearly that the GCD of b_d and b_{d-1} is a constant. \square

6 Examples

In this section, we provide first examples showing that each of the factors P, Q, R may be equal to one.

Then we describe an example coming from a challenging problem of Quantifier Elimination, showing that the direct computation of the factors of the double discriminant may be a dramatic improvement of the computation time.

This example shows also that GCD computations may be needed to compute the factors P, Q, S .

This implies that these factors may not be computed straightforwardly by mean of multivariate resultants. In fact, multivariate resultants may define only principal ideals. Thus, to eliminate the non principal components of the elimination ideals, one would need a kind of residual resultant for which we do not know any theory. Another difficulty lies in the fact that multivariate resultants of non homogeneous polynomials may be null even if the iterated discriminant is not null; it is especially the case if the degree condition of Theorem 1 is not satisfied. If one get a non principal elimination ideal, this shows that this degree condition is not satisfied for Theorem 1 and also for all similar theorems involving other resultant theories (usual resultants, resultants for weighted degrees, resultants for product of projective spaces, toric resultants, ...).

All our examples are specializations of the generic monic polynomial of degree four $f = x^4 + px^3 + qx^2 + yx + s$. As f is monic in x , we have $P^\infty Q^\infty R^\infty = 1$ for f as well for any specialization of it. The first discriminant is $\text{disc}_x(f) = -27y^4 + \dots$. It follows that S is constant for any specialization of f .

We consider first simple specializations of this polynomial.

- For the polynomial f itself we have $P = s$ and the factors Q and R are irreducible. we have $\text{disc}_y(\text{disc}_x(f)) = -256PQ^2R^3$. Thus the situation is generic in this case.
- If $f_0 = x^4 + qx^2 + yx + s$, we have $P = s, Q = q^2 - 4s$ and $R = q^2 + 12s$, but $\text{disc}_y(\text{disc}_x(f)) = -2^{16}3^3PQ^2R^6$, showing the double discriminant need not to be equal, up to a constant, to PQ^2R^3 .
- If $f_P = x^4 + qx^2 + yx + 1$, we have $P = 1$, providing an example where the factor P is a constant.
- Similarly, we have $Q = 1$ for the polynomial $f_Q = x^4 + 2ux^2 + yx + u^2 + 1$ and $R = 1$ for $f_R = x^4 + 6ux^2 + yx - 3u^2 + 1$.

Several years ago a problem of quantifier elimination, coming from a stability study in numerical analysis, was submitted to us by a PhD student named Rozier (around 1999). We were unable to solve

it with Cylindrical Algebraic Decomposition (CAD), but we have been able to solve it with an ad-hoc hand written method. Despite the progress of the algorithms and the power of the computers, it is yet a unsolved challenge to solve it by an automatic method.

After some reductions, this problem reduces to eliminate the quantifiers in the formula.

$$\exists(a, b, c, d) \forall x (p > 0 \wedge c + d > 0 \wedge d(a - 1) > 0)$$

where $p = (x + c)(x^3 - u) + (x - d)(bx + av)$.

To solve this problem by CAD, one has first to eliminate x , to compute the discriminant $\text{disc}_x(p)$, and then to eliminate the variables a, b, c, d one after the other, in any order. The second step consists in computing and factoring the second discriminant with respect to one of these variables.

As p is monic in x , we have always $P^\infty Q^\infty R^\infty = 1$.

- $\text{disc}_a(\text{disc}_a(p)) = 256S^4PQ^2R^3$, with $S = v^3$ and $P = (c + d)(d^3 - u)$. In this case, P is not only reducible, but it has been obtained by a GCD computation, the ideal $I_1 \cap K[b, c, d, u, v]$ being not principal. the factor S is the cube of a polynomial which is a factor of multiplicity 12 of the second discriminant. On the other hand, Q and R are irreducible and are obtained without GCD computation.

The second discriminant has 1046 terms whose coefficients have up to 18 decimal digits, while P , Q , R and S have 35 terms together with coefficients not larger than 1296. The direct computation of P , Q , R and S needs around 0.2 second while computing and factoring the double discriminant needs around 12 seconds.

- $\text{disc}_a(\text{disc}_b(p)) = -256PQ^2R^3$. Here $S = 1$ and P , Q and R generate their elimination ideal (no need of GCD computation), but P is again reducible (it has three factors).

The second discriminant has 2199 terms whose coefficients have up to 22 decimal digits, while P , Q , R and S have 54 terms together whose coefficients have no more than four decimal digits. The direct computation of P , Q , R and S also needs around 0.2 second while the double discriminant is computed in 7 seconds and factored in more than 9min.

- $\text{disc}_a(\text{disc}_c(p)) = -4096S^3PQ^2R^3$. Here $S = 27u$ and P , Q and R generate their elimination ideal (no need of GCD computation), but P is again reducible (it has two factors).

The second discriminant has 2461 terms whose coefficients have up to 25 decimal digits, while P , Q , R and S have 54 terms together whose coefficients have no more than three decimal digits. The direct computation of P , Q , R and S needs around 0.2 second while the double discriminant is computed in 9 seconds and factored in more than 15min.

7 Conclusion

The examples show that the direct computation of the factors may dramatically improve the computation of the hypersurface defined by the double discriminant.

They also show that the multiplicity of these factors in the double discriminant may not easily be predicted. Therefore it seems difficult to get a better result than Theorem 3, which is true for any polynomial. Even for the generic polynomials of a given support, general results seems very difficult.

On the other hand, in all the examples we have encountered, the double discriminant is a multiple of $SPP^\infty(QQ^\infty)^2(RR^\infty)^3$. *This is reasonable to conjecture that it is always true*, but we do not know how to prove it.

References

- [1] Laurent Busé and Bernard Mourrain. *Explicit factors of some iterated resultants and discriminants*. Research Report (2006). URL: <http://hal.inria.fr/inria-00119287/en/>
- [2] George E. Collins. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition. In *Automata theory and formal languages* (Second GI Conf., Kaiserslautern, 1975), pages 134-183. Lecture Notes in Comput. Sci., **33**, Springer (Berlin, 1975).
- [3] Olaus Henrici. On certain formulae concerning the Theory of Discriminants; with applications to Discriminants of Discriminants, and to the theory of polar curves, *Proc. London Math. Soc.*, Nov. 1868, 104-116.
- [4] Daniel Lazard. Quantifier Elimination: Optimal solution of Two Classical Examples. *J. Symbolic Comput.* (1988), bf 5, 261-266.
- [5] Scott McCallum. *On certain roots of a repeated discriminant*. Technical report No. 98-15, University of Delaware, Department of Computer and Information Sciences, 11 pages, March 27, 1998.
- [6] Scott McCallum. Factors of iterated resultants and discriminants. *J. Symbolic Comput.*, (1999) bf 27, 367-385.
- [7] Scott McCallum. *Repeated Discriminants*. Unpublished manuscript, 13 pages (January 10, 1999).
- [8] André Weil. *Foundation of Algebraic Geometry*. The American Mathematical Society (New York, 1946).