THE D-RESULTANT, SINGULARITIES
AND THE DEGREE OF UNFAITHFULNESS

ARNO VAN DEN ESSEN AND JIE-TAI YU

(Communicated with Wolmer V. Vasconcelos)

Abstract. We introduce the D-resultant of two polynomials in one variable and show how it can be used to decide if \( k(f(t), g(t)) = k(t) \), \( k[f(t), g(t)] = k[t] \) and to find the singularities of the curve \( x = f(t), y = g(t) \). The second criterion is used to give a very short proof of a special case of the epimorphism theorem of Abhyankar and Moh.

Introduction

Let \( k \) be a field. In lecture 19 of [2] Abhyankar defines the Taylor resultant of two polynomials \( f(t) \) and \( g(t) \) in \( k[t] \) as the resultant (with respect to the variable \( t \)) of the polynomials

\[
f'(s) + \frac{f''(s)}{2!} t + \frac{f'''(s)}{3!} t^2 + \cdots, \quad g'(s) + \frac{g''(s)}{2!} t + \frac{g'''(s)}{3!} t^2 + \cdots.
\]

He introduces this concept to solve the following questions: how can one decide if \( k(t) = k(f(t), g(t)) \) or if \( k[t] = k[f(t), g(t)] \) and how can one compute the singularities of the curve \( x = f(t), y = g(t) \)? The solutions to these questions are described in Theorem on page 153 of [2], however no proof is presented.

An objection to the Taylor resultant is that, apparently, it is only defined for fields of characteristic zero. To overcome this point we introduce in this paper the so-called D-resultant (see §1) of polynomials over arbitrary fields (or more generally over arbitrary domains) and show that in case \( \text{char } k = 0 \) it agrees with Abhyankar’s Taylor resultant. Furthermore we show that the above three questions can be very easily solved by the D-resultant (cf. Theorem 2.1).

At the end of this paper we use the D-resultant to give a very short proof of a special case of the epimorphism theorem of Abhyankar and Moh (cf. [3]); we show that if \( \gcd(\deg f(t), \deg g(t)) = 1 \), then \( k[f(t), g(t)] \neq k[t] \).

It is worth remarking that also the formulas obtained in Proposition 1.1 below turn out to be very useful for applications. More precisely, the results on the D-resultant obtained in this paper are used in [5] to give a new characterisation of polynomial automorphisms of the plane over an arbitrary field \( k \).

Finally we would like to mention that in [6] the D-resultant is used to show that a polynomial map \( F : \mathbb{C}^2 \to \mathbb{C}^2 \) with \( \det JF \in \mathbb{C}^* \) is an automorphism, if there...
exist a point \( p \) in \( \mathbb{C}^2 \) and three lines going through \( p \) such that the restriction of \( F \) to each of these three lines is injective.

0. Preliminaries

0.1 The resultant of two polynomials in one variable. Let \( A \) be a commutative ring without zero-divisors, \( K \) its quotient field and \( A[t] \) the polynomial ring in the variable \( t \) with coefficients in \( A \). Let \( f = f_0 t^n + f_1 t^{n-1} + \ldots + f_n \) be a polynomial in \( A[t] \) with \( f_0 \) \( \neq \) 0. Then \( n \) is called the degree of \( f \), denoted \( \deg_0 f \) or \( \deg f \). Let also \( g = g_0 f^m + g_1 f^{m-1} + \ldots + g_m \) be in \( A[t] \) with \( g_0 \) \( \neq \) 0. Then the resultant of \( f \) and \( g \) with respect to \( t \), denoted \( \text{Res}_t(f, g) \) is a well-defined element of \( A \) (cf. \([7, 9]\)). The next proposition summarises some of its properties (cf. \([7, 9]\)).

Proposition 0.2. Let \( f, g \in A[t] \), \( n = \deg f \), \( m = \deg g \).

1) \( \text{Res}_t(f, g) = (-1)^{nm} \text{Res}_t(g, f) \).
2) If also \( h \in A[t] \), then \( \text{Res}_t(f, g, h) = \text{Res}_t(f, h) \text{Res}_t(g, h) \).
3) If \( a \in A \), then \( \text{Res}_t(a f, a g) = a \text{Res}_t(f, g) \).
4) \( f \) and \( g \) have a common zero (in some field extension of \( K \)) if and only if \( \text{Res}_t(f, g) = 0 \).
5) If \( f \) and \( g \) are polynomials in \( t \) with literal coefficients i.e. \( f, g \in \mathbb{Z}[f_0, \ldots, f_n, g_0, \ldots, g_m][t] \), then

\[
\text{Res}_t(f, g) = \sum m_{i_0 \ldots i_n j_0 \ldots j_m} f_0^{i_0} \cdot \ldots \cdot f_n^{i_n} g_0^{j_0} \cdot \ldots \cdot g_m^{j_m},
\]

where each \( m_{i_0 \ldots i_n j_0 \ldots j_m} \) is an integer and \( 0.i_0 + 1.i_1 + 2.i_2 + \ldots + n.i_n + j_1 + \ldots + m.j_m = mn \).

0.3 Resultants and minimal polynomials. Let \( k \) be an arbitrary field and let \( f = f(t) \) and \( g = g(t) \) be two elements of \( k[t] \), not both constants. Then \( f(t) \) and \( g(t) \) are algebraically dependent over \( k \), so there exists an irreducible polynomial \( m(X, Y) \in k[X, Y] \) such that \( m(f(t), g(t)) = 0 \). It is not difficult to prove that \( m \) is unique up to a non-zero constant factor (cf. \([11, \text{Lemma 1}]\)). We call such an \( m \) a minimal polynomial of \( f \) and \( g \). One has the following useful result (cf. \([1, 8]\)).

Theorem 0.4 (Abhyankar, McKay, Wang). Let \( m \) be a minimal polynomial of \( f \) and \( g \); then there exists \( c \in k^* \) such that

\[
\text{Res}_t(f(t) - X, g(t) - Y) = cm(X, Y)^q
\]

where

\[
q = \lfloor k(t) : k(f, g) \rfloor.
\]

0.5 Branch representations. Let \( C \) be an irreducible plane curve given by the irreducible polynomial \( m(X, Y) \in k[X, Y] \). Suppose \( m(0, 0) = 0 \). A pair of formal power series \( f(t), g(t) \) in \( k[[t]] \), not both constant, satisfying \( f(0) = g(0) = 0 \) and \( m(f(t), g(t)) = 0 \), is called a branch representation of the curve \( C \) at \( (0, 0) \). Such a branch representation is called not primitive if there exists a formal power series \( \tau(t) \) in \( k[[t]] \) with ord \( \tau(t) > 1 \) such that \( f(t) = \tilde{f}(\tau(t)) \) and \( g(t) = \tilde{g}(\tau(t)) \) for some \( \tilde{f}, \tilde{g} \) in \( k[[t]] \). Otherwise a branch representation is called primitive. Two branch representations \((f_1, g_1)\) and \((f_2, g_2)\) of \( m = 0 \) at \((0, 0)\) are called equivalent if there exists a formal power series \( \tau(t) \) of order 1 such that \( f_1(t) = f_2(\tau(t)) \) and \( g_1(t) = g_2(\tau(t)) \). Now suppose that \((0, 0)\) is a simple point of the curve \( m = 0 \),
say \( m_y(0,0) \neq 0 \). Then by the formal implicit function theorem there exists a (primitive) branch representation of \( m \) of the form \((t, g_0(t))\) with \( g_0(t) \in k[[t]] \) and \( g_0(0) = 0 \). Now let \((f(t), g(t))\) be another primitive branch representation of \( m \) at \((0,0)\). By [10, Theorem 12.6] \((f(t), g(t))\) is equivalent with \((t, g_0(t))\); i.e. there exists a formal power series \( \tau(t) \) of order 1 such that \((f(t), g(t)) = (\tau(t), t_0(\tau(t)))\). In particular \( f(t) = \tau(t) \). Consequently \( f'(0) = \tau'(0) \neq 0 \). If \( m_x(0,0) \neq 0 \) a similar argument gives \( g'(0) \neq 0 \). Summarizing we showed

(0.6) If \((0,0)\) is a simple point of the curve \( m = 0 \), then for every branch representation \((f, g)\) of \( m \) at \((0,0)\) we have \((f'(0), g'(0)) \neq (0,0)\).

To conclude this section we give a simple fact which will be used below: let \( A \) be a commutative ring, \( f(t) \in A[t] \) and \( a \in A \). Instead of \( f(a) \) we sometimes write \( f|_{t=a} \). Observe that \( f(t) - f(a) \) is divisible by \( t - a \), so \( \frac{f(t) - f(a)}{t - a} \) belongs to \( A[t] \).

**Lemma 0.7.** \( \frac{f(t) - f(a)}{t - a} \big|_{t = a} = f'(a) \).

**Proof.** For \( f = t^i \) the result follows from the formula \( \frac{t^i - a^i}{t - a} = t^{i-1} + at^{i-2} + \ldots + a^{i-1} \).

Writing \( f(t) = \sum f_{n-i}t^i \) one deduces the general case as a direct consequence. \( \square \)

§1. THE D-RESULTANT AND SINGULARITIES

Let \( A \) be a commutative ring without zero-divisors, \( K \) its quotient field and \( A[t, s] \) or \( A[X, Y] \) denotes the polynomial ring in two variables over \( A \). Let \( f(t), g(t) \) be in \( A[t] \). So we get the polynomials \( \frac{f(t) - f(s)}{t - s} \) and \( \frac{g(t) - g(s)}{t - s} \) in \( A[t, s] \). Now we define the \( D \)-resultant of \( f(t) \) and \( g(t) \) by putting

\[
D \text{Res}_t(f(t), g(t)) := \text{Res}_t \left( \frac{f(t) - f(s)}{t - s}, \frac{g(t) - g(s)}{t - s} \right)
\]

(The \( D \) stands for Divided difference.) Obviously this resultant is an element of \( A[s] \). If no confusion is possible we write \( D(s) \) instead of \( D \text{Res}_t(f(t), g(t)) \). The next useful proposition relates \( D(s) \) with

\[
R(X, Y) := \text{Res}_t(f(t) - X, g(t) - Y).
\]

**Proposition 1.1.**

\[
f'(s)D(s) = (-1)^{\deg f} \text{Res}_Y(f(s), g(s)), \quad g'(s)D(s) = (-1)^{1 + \deg f} \text{Res}_X(f(s), g(s)).
\]

**Proof.** We only prove the first formula (the other one is proved similarly). Writing \( g(t) - g(s) = (t - s)^{2(t) - g(s)} \big|_{t-s} \) we obtain

\[
r(s) := \text{Res}_t \left( \frac{f(t) - f(s)}{t - s}, g(t) - g(s) \right) = \text{Res}_t \left( \frac{f(t) - f(s)}{t - s}, t - s \right) D(s).
\]

So by Proposition 0.2.1, 0.2.3 and Lemma 0.7 we obtain

\[
r(s) = (-1)^{\deg f} f'(s)D(s).
\]

Put \( \tilde{R}(s, Y) := \text{Res}_t \left( \frac{f(t) - f(s)}{t - s}, g(t) - Y \right) \). Then \( r(s) = \tilde{R}(s, Y) \big|_{Y=g(s)} \). Writing \( f(t) - f(s) = (t - s)^{f(t) - f(s)} \big|_{t-s} \) we obtain

\[
\tilde{R}(s, Y) = \text{Res}_t \left( f(t) - f(s), g(t) - Y \right) / \text{Res}_t (t - s, g(t) - Y)
\]

\[= - \text{Res}_t (f(t) - f(s), g(t) - Y) / (Y - g(s)) = -R(f(s), Y) / Y - g(s).
\]
Proof. Let $k$ be a field of characteristic zero and $f(t), g(t)$ in $k[t]$. Then the Taylor resultant of $f(t)$ and $g(t)$ is the polynomial

$$T(s) := \text{Res}_t(f'(s) + \frac{1}{2!}f''(s)t + \frac{1}{3!}f'''(s)t^2 + \cdots, g'(s) + \frac{1}{2!}g''(s)t + \frac{1}{3!}g'''(s)t^3 + \cdots)$$

**Proposition 1.3.** Let $k$ be a field of characteristic zero. Then $D(s) = T(s)$.

**Proof.** By Taylor's formula we get

$$f(t) = f(s) + f'(s)(t - s) + \frac{1}{2!}f''(s)(t - s)^2 + \cdots$$

and a similar result for $g(t)$. Consequently we get

$$D(s) = \text{Res}_t(f'(s) + \frac{1}{2!}f''(s)(t - s) + \cdots) + g'(s) + \frac{1}{2!}g''(s)(t - s) + \cdots).$$

Now observe that in general $\text{Res}_t(F(t-a), G(t-a)) = \text{Res}_t(F(t), G(t))$ for all domains $A, F(t), G(t) \in A[t]$ and all $a \in A$.

So in (1.3.1) we may replace $t - s$ by $t$, which implies that $D(s) = T(s)$. 

§2. The main theorem

Throughout this section $k$ is an arbitrary field. Now we are able to prove the main result of this paper.

**Theorem 2.1.** Let $f(t)$ and $g(t)$ in $k[t]$ be such that both $f'(t)$ and $g'(t)$ are non-zero. Then

1) $k[f(t), g(t)] = k(t)$ if and only if $D(s) \neq 0$.
2) $k[f(t), g(t)] = k[t]$ if and only if $D(s) \in k^*$.
3) If $D(s) \neq 0$, say $D(s) = \prod_{i=1}^{r}(s - s_i)^{e_i}$, where each $e_i$ is a positive integer and all $s_i$ are distinct (and belong to some algebraic closure $\overline{k}$ of $k$), then the singularities of the curve $x = f(t), y = g(t)$ are exactly the points $(f(s_i), g(s_i)), i \leq i \leq r$.

**Proof.** i) Let $m$ be a minimal polynomial of $f$ and $g$ over $k$. Then $R = cm^q$ for some $c \in k^*$ and $q = |k(t) : k(f, g)|$ (by Theorem 0.4). Consequently $R_X = cq^{m^{-1}}m_X$ and $R_Y = cq^{m^{-1}}m_Y$. Now assume that $q > 1$. Then both $R_X$ and $R_Y$ contain a factor $m$, hence $R_X(f, g) = R_Y(f, g) = 0$. So $D(s) = 0$ follows from Proposition 1.1 and the hypothesis that both $f'$ and $g'$ are non-zero. If $q = 1$, then $R_X = cm_X$ and $R_Y = cm_Y$. So again using Proposition 1.1 we conclude that if $D(s) = 0$ then both $m_X(f, g)$ and $m_Y(f, g)$ are zero. Consequently $m$ divides both $m_X$ and $m_Y$. If $\text{char } k = 0$ this is clearly impossible; if $\text{char } k = p > 0$ then $m_X = m_Y = 0$
imply that \( m = \overline{m}^p \) for some \( \overline{m} \) in \( k[X,Y] \) which contradicts the minimal choice of \( m \). So in any case we get a contradiction, and hence \( D(s) \neq 0 \).

ii) Now we show 3). Without loss of generality we may assume that \( f(0) = g(0) = 0 \). First observe that if \( D(s) \neq 0 \), then \( (f(t), g(t)) \) is a primitive branch representation of \( m \) at \((0,0)\); for if \( f(t) = \tilde{f}(\tau(t)) \) and \( g(t) = \tilde{g}(\tau(t)) \) with \( \tilde{f}, \tilde{g} \) in \( k[[t]] \) and \( \tau(t) \in k[[t]] \) with \( \tau(t) > 1 \), then \( \frac{f(t) - f(s)}{t-s} = \frac{(\tau(t) - \tau(s))}{\tau(t) - \tau(s)} \cdot \tau(t) - \tau(s) \), so \( \tau(t) - \tau(s) \) is a factor of \( \frac{f(t) - f(s)}{t-s} \) and by a similar argument also of \( \frac{g(t) - g(s)}{t-s} \). But this implies that \( D(s) = 0 \), a contradiction. Furthermore, since \( D(s) \neq 0 \) it follows from Proposition 1.1 that \( m_{X}(f(s_i), g(s_i)) = m_{Y}(f(s_i), g(s_i)) = 0 \), so \( (f(s_i), g(s_i)) \) is a singular point of the curve \( x = f(t), y = g(t) \). Conversely, if \( m_{X}(f(s_0), g(s_0)) = m_{Y}(f(s_0), g(s_0)) = 0 \) it follows from Proposition 1.1 that \( f'(s_0)D(s_0) = g'(s_0)D(s_0) = 0 \). Now observe that by (0.6) either \( f'(s_0) \neq 0 \) or \( g'(s_0) \neq 0 \), which implies that \( D(s_0) = 0 \), so \( s_0 = s_i \) for some \( 1 \leq i \leq r \), as desired.

iii) Now we show 2). Suppose \( k[[f(t), g(t)] = k[t] \). Then there exists some \( F \in k[X,Y] \) such that \( t = F(f(t), g(t)) \). So \( (F(f(t), g(t)) - F(f(s), g(s)))/(t-s) = 1 \).

\[
(2.2) \quad \frac{F(f(t), g(t)) - F(f(s), g(t))}{t-s} + \frac{F(f(s), g(t)) - F(f(s), g(s))}{t-s} = 1.
\]

Observe that \( F(X, g(t)) - F(a, g(t)) \) is divisible by \( X - a \) (for all \( a \in k[s] \)). So substituting \( X = f(t) \) and \( a = f(s) \) we obtain that

\[
F(f(t), g(t)) - F(f(s), g(t)) = h_1 \cdot (f(t) - f(s)), \quad \text{for some } h_1 \in k[t,s].
\]

Similarly

\[
F(f(s), g(t)) - F(f(s), g(s)) = h_2 \cdot (g(t) - g(s)), \quad \text{for some } h_2 \in k[t,s].
\]

So by (2.2) we get

\[
h_1(t,s) \frac{f(t) - f(s)}{t-s} + h_2(t,s) \frac{g(t) - g(s)}{t-s} = 1.
\]

So for each \( s_0 \in \overline{k} \) the polynomials \( \frac{f(t) - f(s_0)}{t-s_0} \) and \( \frac{g(t) - g(s_0)}{t-s_0} \) have no common zero, hence (by Proposition 0.2.4) \( D(s_0) \neq 0 \) for all \( s_0 \) in \( \overline{k} \). So \( D(s) \in k^* \).

Finally we show the converse: since \( \overline{k}[f(t), g(t)] = \overline{k}[t] \) implies \( k[[f(t), g(t)] = k[[t] \), we may assume that \( k \) is algebraically closed. Now suppose that \( D(s) \in k^* \). Then in particular \( D(s) \neq 0 \), so by 1) \( k(f(t), g(t)) = k[t] \) and by 3) the irreducible plane curve \( m(x,y) = 0 \) has no singularities. So for each maximal ideal \( \eta \) of the ring \( A = k[X,Y]/m \) (\( \simeq [k[f,g]] \)), \( A_{\eta} \) is a discrete valuation ring. Hence by [4, Theorem 9.3] \( A \) is integrally closed. So \( k[f,g] \) is integrally closed in \( k[t] \). Since \( t \) is obviously integral over \( k[f,g] \) it follows that \( t \in k[f,g] \), whence \( k[f,g] = k[t] \) as desired.

\[\Box\]

\section{A remark on the Abhyankar-Moh epimorphism theorem}

In [3] Abhyankar and Moh proved the following well-known result.

**Theorem 3.1.** Let \( k \) be an arbitrary field of characteristic \( p \) (\( p = 0 \) or \( p > 0 \)). Let \( f(t), g(t) \) in \( k[t] \) of degree \( n \) resp. \( m \) be such that \( p \) does not divide \( \text{g.c.d}(n,m) \). If \( k[[f(t), g(t)] = k[t] \), then either \( n \) divides \( m \) or \( m \) divides \( n \).
In other words: if say $m \leq n$ and $m$ does not divide $n$, and $p$ does not divide $\gcd(n, m)$, then $k[f, g] \neq k[t]$. So using Theorem 2.1.2, Theorem 3.1 is equivalent with

(3.2) Let $m \leq n$. If $m$ does not divide $n$ and $\gcd(m, n) \neq 0 \mod p$, then either $D(s) = 0$ or $D(s)$ contains the variable $s$.

In the remainder of this paper we will show (3.2) for the special case that $\gcd(m, n) = 1$. Therefore we need

**Lemma 3.3.** Let $f(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_n$ and $g(t) = b_0 t^m + b_1 t^{m-1} + \cdots + b_m$ be polynomials in the polynomial ring $\mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m, t]$; i.e. $f$ and $g$ have literal coefficients. If $\gcd(m, n) = 1$, then

$$D(s) = da_0^n b_0^m s^{(n-1)(m-1)} + \text{lower order terms in } s,$$

for some $d \in \mathbb{Z} \setminus \{0\}$.

**Proof.**

\[ \frac{f(t) - f(s)}{t - s} = a_0 \left( \frac{t^n - s^n}{t - s} \right) + a_1 \left( \frac{t^{n-1} - s^{n-1}}{t - s} \right) + \cdots + a_n. \]

Similarly

\[ \frac{g(t) - g(s)}{t - s} = b_0 t^{m-1} + (b_0 s + b_1) t^{m-2} + \cdots + (b_0 s^{m-1} + b_1 s^{m-2} + \cdots + b_m). \]

So if we give each $a_i$ weight $i$, each $b_j$ weight $j$ and $s$ weight 1, then according to Proposition 0.2.5 each monomial $a_0^{n-i} a_{n-1}^{n-i-1} \cdots b_0^{m-j} b_{m-1}^{m-j-1}s^{k}$ appearing in $D(s)$ has weight $(m-1)(n-1)$, in particular $\deg s D(s) \leq (m-1)(n-1)$ and the coefficient $c$ of $s^{(m-1)(n-1)}$ can only contain $a_0$ and $b_0$. So we can compute $c$ by setting $a_1 = \cdots = a_n = b_1 = \cdots = b_m = 0$. Therefore consider

\[ r(a_0, b_0, s) := \text{Res}_t \left( a_0 \left( \frac{t^n - s^n}{t - s} \right), b_0 \left( \frac{t^m - s^m}{t - s} \right) \right). \]

Since, as observed above, each monomial in $r(a_0, b_0, s)$ has weight $(m-1)(n-1)$ and $a_0$ and $b_0$ have weight zero it follows that $r(a_0, b_0, s) = c_{s^{(m-1)(n-1)}}$. Consequently

\[ c = r(a_0, b_0, 1) = a_0^m b_0^n \text{Res}_t \left( \frac{t^{n-1} - 1}{t-1}, \frac{t^{m-1} - 1}{t-1} \right). \]

Now observe that $d := \text{Res}_t \left( \frac{t^{n-1} - 1}{t-1}, \frac{t^{m-1} - 1}{t-1} \right)$ is non-zero, since if $(n, m) = 1$ is an $n$-th root of unity $\neq 1$ cannot be an $m$-th root of unity. Then apply Proposition 0.2.4.

**Proof of (3.2) in case $\text{gcd}(m, n) = 1$.** Let $f(t) = f_0 t^n + f_1 t^{n-1} + \cdots + f_n$, $g(t) = g_0 t^m + g_1 t^{m-1} + \cdots + g_m$ with $f_0, g_0 \in k^*$. Then $D(s)$ can be obtained from the resultant of Lemma 3.3 by the substitutions $a_i \rightarrow f_i$, $b_j \rightarrow g_j$ for all $i, j$. Since $f_0$ and $g_0$ are non-zero it follows that $s^{(n-1)(m-1)}$ has non-zero coefficient. Finally $(n-1)(m-1) > 0$. So $D(s) \notin k^*$.
REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NIJMEGEN, TOERNOOIVELD, 6525 ED NIJMEGEN, THE NETHERLANDS
E-mail address: essen@sci.kun.nl

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HONG KONG, HONG KONG
E-mail address: yuji@hkusua.hku.hk