TOPOLOGY AND FACTORIZATION
OF POLYNOMIALS

HANI SHAKER

Abstract

For any polynomial $P \in \mathsf{C}[X_1, X_2, \ldots, X_n]$, we describe a C-vector space $F(P)$ of solutions of a linear system of equations coming from some algebraic partial differential equations such that the dimension of $F(P)$ is the number of irreducible factors of P. Moreover, the knowledge of $F(P)$ gives a complete factorization of the polynomial P by taking gcd's. This generalizes previous results by Ruppert and Gao in the case $n = 2$.

1. Introduction

Let K be the algebraic closure of a field k and let $k[X_1, X_2, \ldots, X_n]$ be the polynomial ring in n indeterminates. The zero set of a polynomial $P \in k[X_1, X_2, \ldots, X_n]$ of $\deg d > 0$ is a hypersurface $V(P)$ in K^n. As the polynomial ring is a factorial ring, we can write $P = \prod_{i=1}^{s} P_i$, where P_i are the irreducible factors of P in $K[X_1, X_2, \ldots, X_n]$.

We assume that the factors P_i are distinct, i.e. P is a *reduced polynomial*. The prime factorization of P corresponds to the decomposition into irreducible components $V(P) = \prod_{i=1}^{s} V(P_i)$ of the hypersurface $V(P)$.

A natural question to ask is: "*How can we compute s, the number of irreducible factors of P (resp. irreducible components of $V(P)$) from the coefficients of P?*" A variant of this problem (called the *absolute factorization problem*) is when P is assumed to be irreducible in $k[X_1, X_2, \ldots, X_n]$, see [1].

In this paper we recall in Section 2 briefly Gao's results in the case $n = 2$, see [3], and then some usual techniques for reducing the case $n > 2$ to the case $n = 2$ by taking generic linear sections, see [1].

Since all these reduction techniques are not easy to use in practice (since the notion of a *generic* linear section is quite subtle as we show by some examples), we develop in Sections 3 and 4 of our note a direct approach to the case $n > 2$.

Unlike Ruppert-Gao's approach, which is purely algebraic and works over any field k of characteristic zero or of relatively large characteristic, our approach is topological, using de Rham cohomology, and hence works only for the algebraically closed subfields of the field of complex numbers C.

---

2. Ruppert-Gao's idea and the reduction techniques

Assume that $n = 2$ and denote by X, Y the two indeterminates. If $P(X, Y) = \prod_{i=1}^{s} P_i(X, Y)$, is the factorization of P into irreducible factors in $K[X, Y]$, then by taking the partial derivatives on both sides, we have

$$(2.1) \quad P_X = \sum_{i=1}^{s} \left(\prod_{j \neq i} P_j \right) \frac{\partial P_i}{\partial X} = \sum_{i=1}^{s} g_i \qquad \text{where} \quad g_i = \left(\prod_{j \neq i} P_j \right) \frac{\partial P_i}{\partial X}$$

and also

$$(2.2) \quad P_Y = \sum_{i=1}^{s} \left(\prod_{j \neq i} P_j \right) \frac{\partial P_i}{\partial Y} = \sum_{i=1}^{s} h_i \qquad \text{where} \quad h_i = \left(\prod_{j \neq i} P_j \right) \frac{\partial P_i}{\partial Y}.$$

Note that we can write

$$\frac{\partial}{\partial X}(\log P_i) = \frac{1}{P_i} \frac{\partial P_i}{\partial X} = \frac{g_i}{P}, \qquad \frac{\partial}{\partial Y}(\log P_i) = \frac{1}{P_i} \frac{\partial P_i}{\partial Y} = \frac{h_i}{P}$$

which yields

$$(2.3) \qquad \frac{\partial}{\partial Y}\left(\frac{g_i}{P} \right) = \frac{\partial}{\partial X}\left(\frac{h_i}{P} \right) \qquad \text{for} \quad i = 1, \ldots, s.$$

DEFINITION 2.1. Let $P(X, Y) \in K[X, Y]$ be such that $\deg_X(P) = m_1$, $\deg_Y(P) = m_2$. Then the bidegree of P is defined as

$$\text{bideg}(P) = \big(\deg_X(P), \deg_Y(P) \big) = (m_1, m_2).$$

In our case, we obviously have

$$\text{bideg}(g_i) \leq (m_1 - 1, m_2) \qquad \text{and} \qquad \text{bideg}(h_i) \leq (m_1, m_2 - 1).$$

DEFINITION 2.2. Let $F(P)$ be the K-vector space of solutions $(v, w) \in K[X, Y]^2$ of the partial differential equation

$$\frac{\partial}{\partial Y}\left(\frac{v}{P} \right) = \frac{\partial}{\partial X}\left(\frac{w}{P} \right)$$

such that $\text{bideg}(v) \leq (m_1 - 1, m_2)$, $\text{bideg}(w) \leq (m_1, m_2 - 1)$.

This partial differential equation was first considered by Ruppert [5], [6]. Moreover, it was clear to Ruppert and Gao that this is just the condition that a certain 1-form is closed, see the comment just before Theorem 2.1 in [3].

THEOREM 2.3 (Gao's Theorem [3]). *If $P(X, Y) = \prod_{i=1}^{s} P_i(X, Y)$ is the factorization of P into irreducible factors in $K[X, Y]$, then $s = \dim_K F(P)$ and the set*

$$\{(g_i, h_i) \mid i = 1, \ldots, s\}$$

is a basis for $F(P)$.

COROLLARY 2.4. (i) *P is irreducible if and only if $\dim_K F(P) = 1$.*
(ii) *$P_i = \gcd(P, v - \lambda_i P_X)$ where $v = \sum_{i=1}^{s} \lambda_i g_i$ is a generic vector in the vector space $E(P)$ obtained from $F(P)$ by projecting on the first factor.*

Here $\lambda = (\lambda_1, \ldots, \lambda_s) \in \mathbf{C}^s$ and the genericity means that λ has to avoid a proper Zariski closed subset of $\mathbf{C}^s$. The first claim is an obvious consequence of Theorem 2.3 and was obtained already by Ruppert [5]. The second one is much more subtle and we will discuss this point in the general case in the last section, see in particular Proposition 4.6.

Now we return to the general case $n \geq 2$. Let $V(P)$ be the affine hyper-surface defined by $P = 0$ in the affine space K^n. Let E be an affine plane in K^n such that $V(P) \cap E$ is a curve in E. One may ask "*Is there some relation between the number of irreducible components of $V(P)$ and $V(P) \cap E$? or, more precisely: Are these numbers always equal?*" The answer is to such questions depends on the choice of E. Let us look at two examples.

EXAMPLE 2.5. (i) Consider the Whitney umbrella $S : x^2 - zy^2 = 0$, an irreducible singular surface in $\mathbf{C}^3$. Choose two planes $E_0 : z = 1$ and $E_1 : y = 1$. One can see that $S \cap E_0$ is the union of two lines, namely $x^2 - y^2 = 0$, and $S \cap E_1$ is irreducible and isomorphic to $\mathbf{C}$.
(ii) Consider the smooth irreducible surface $S' : x^2 y - x - z = 0$ in $\mathbf{C}^3$. Choose two planes $E_0 : z = 0$ and $E_1 : z = 1$. One can see that $S' \cap E_0$ has two components $x = 0$ and $xy - 1 = 0$, while $S' \cap E_1$ is irreducible, and isomorphic to $\mathbf{C}^*$.

By Bertini's second Theorem we know that the number of irreducible components of $V(P)$ and of $V(P) \cap E$ coincide if the the 2-plane E is generic, see [1], subsection 9.1.3 for an excellent survey of this problem as well as Section 5 in [3], for relations to an effective Hilbert irreducibility theorem. In practice it is quite difficult to decide when a given plane E is generic. In the next section we explain the relation between this genericity and transversality to some Whitney regular stratifications, but this is not easy to check on explicit examples.

Moreover, once we have the factorization of P in the plane E (i.e. in a polynomial ring in two variables), it is a second difficult task to recover the factorization of P in the polynomial ring $\mathbf{C}[X_1, \ldots, X_n]$.

This shows the need of having an extension of Gao's Theorem for $n > 2$ variables, and this will be our main result below.

3. Hypersurface complements

In this section $P \in \mathsf{C}[X_1, \ldots, X_n]$ is a reduced polynomial and $P = \prod_{i=1}^s P_i$ is the factorization of P into irreducible factors in $\mathsf{C}[X_1, \ldots, X_n]$. Then the associated affine hypersurface $V(P) \subset \mathsf{C}^n$ has s irreducible components.

First we recall a basic result, relating the number s of irreducible factors to the topology of the hypersurface complement $M(P) = \mathsf{C}^n \setminus V(P)$.

PROPOSITION 3.1.
$$s = \dim H^1(M(P), \mathsf{C}).$$

PROOF. Using Corollary 1.4 on p. 103 in [2], we get $H_1(M(P), \mathsf{Z}) = \mathsf{Z}^s$. Then we use the usual identification $H^1(M(P), \mathsf{C}) = \mathrm{Hom}(H_1(M(P), \mathsf{Z}), \mathsf{C})$.

Using this result, we can give the following description of the generic 2-planes E.

Let $\overline{V(P)} \subset \mathsf{P}^n$ be the projective closure of the hypersurface $V(P)$. Then E is said to be *geometrically generic with respect to* $V(P)$ if its projective closure $\overline{E}$ is transversal to every strata of a Whitney stratification of $\overline{V(P)}$. Applying the Zariski Theorem of Lefschetz type, see for instance [2], p. 25, we get the following.

COROLLARY 3.2. *Let E be a geometrically generic affine 2-plane with respect to the affine hypersurface $V(P)$. Then $V(P)$ and $V(P) \cap E$ have the same number of irreducible components.*

PROOF. The Zariski Theorem of Lefschetz type implies that the two complements $M(P)$ and $E \setminus (V(P) \cap E)$ have isomorphic fundamental groups. Since we know that, for any path connected space X, the abelianization $\mathrm{ab}(\pi_1(X))$ of the fundamental group coincides to the integral first homology group $H_1(X, \mathsf{Z})$, the result follows using Proposition 3.1.

For any n-tuple $A = (A_1, \ldots, A_n) \in \mathsf{C}[X_1, \ldots, X_n]^n$ of polynomials, consider the rational 1-form
$$\omega(A) = \sum_{i=1}^n \frac{A_i}{P} dX_i$$

defined on the affine open set $M(P)$. Such a form $\omega(A)$ is closed by definition if
$$d\omega(A) = \sum_{i=1}^n \left[\sum_{j=1, j \neq i}^n \left(\frac{A_i}{P} \right)_{X_j} dX_j \right] \wedge dX_i = 0$$

where the subscript X_j means taking the partial derivative with respect to X_j. In other words, the following equations should be satisfied.

$$(3.1) \qquad \left(\frac{A_j}{P}\right)_{X_i} - \left(\frac{A_i}{P}\right)_{X_j} = 0$$

for all $i, j = 1, \ldots, n$ with $i < j$. Consider the vector space $F(P)$ of all solutions $A = (A_1, \ldots, A_n) \in \mathbb{C}[X_1, \ldots, X_n]^n$ of the equations (3.1) with the following multi-degree bounds

$$\text{multideg}(A_i) \leq (m_1, \ldots, m_i - 1, \ldots, m_n)$$

for all $i = 1, \ldots, n$. Here $\text{multideg}(P) = (m_1, \ldots, m_i, \ldots, m_n)$, and this obviously means that $\deg_{X_i} P = m_i$ for all $i = 1, \ldots, n$ exactly as in Definition 2.1.

Any closed form $\omega(A)$ gives rise to a cohomology class $[\omega(A)] \in H^1(M(P), \mathbb{C})$, if we work with the de Rham cohomology groups of the affine smooth variety $M(P)$.

THEOREM 3.3. *The linear map* $T : F(P) \longrightarrow H^1(M(P), \mathbb{C})$ *defined by*

$$T(A) = [\omega(A)]$$

is an isomorphism. In particular $\dim F(P) = s$.

PROOF. To prove the surjectivity of the map T, we recall that a basis for the first de Rham cohomology group $H^1(M(P), \mathbb{C})$ is given by the rational 1-forms

$$(3.2) \qquad \frac{dP_j}{P_j} = \omega(B^j)$$

for $j = 1, \ldots, s$, where $B^j = (B_1^j, \ldots, B_n^j)$ with $B_i^j = \frac{P \cdot (P_j)_{X_i}}{P_j}$ where the subscript X_i indicates the partial derivative with respect to X_i. It is clear that $B^j \in F(P)$, which yields the surjectivity of T.

To prove the injectivity of T, assume that $T(A) = 0$, i.e.

$$(3.3) \qquad \omega(A) = d\alpha$$

for some rational function $\alpha \in \Omega^0(M)$. We can restrict to the case when α is a rational function in view of Grothendieck Theorem [4] saying that for an affine smooth variety the cohomology can be computed using the regular (algebraic) de Rham complex.

It follows that α is then a regular function of the form $\alpha = \frac{Q}{P^k}$, where $k \geq 0$ and Q is not divisible by P. Then for any index $j \in \{1, 2, \ldots, s\}$, α has a pole

of order $k_j \geq 0$ along the irreducible component $V(P_j)$. Working locally in the neighborhood of a smooth point p_j of $V(P_j)$, we see that $d\alpha$ has either a pole of order zero along $V(P_j)$ if $k_j = 0$, or a pole of order $k_j + 1$ if $k_j \geq 1$. Hence in any case we do not get a pole of order 1. On the other hand, by definition, the 1-form $\omega(A)$ has poles of order at most one along any component $V(P_j)$. The equality (3.3) is possible only if these pole orders are all zero. This occurs only if the polynomial P divides all the polynomials A_j for $j = 1, \ldots, n$. But this is impossible in view of the multi-degree bounds imposed on A_j, unless all A_j are zero.

4. Finding the irreducible factors of P

In this section we explain how to find the irreducible factors of P. Our approach is similar to that of Gao explained in [1], (9.2.10)–(9.2.12), but we pay more attention to a degenerate case that may occur, which explains our next definition.

DEFINITION 4.1. We say that a polynomial $P \in \mathsf{C}[X_1, \ldots, X_n]$ is X_1-generic if the restriction of the projection $\pi_1 : \mathsf{C}^n \to \mathsf{C}^{n-1}$, $(x_1, x_2, \ldots, x_n) \mapsto (x_2, \ldots, x_n)$ to the hypersurface $V(P)$ has finite fibers.

This property, which replaces the condition $\gcd(P, P_{X_1}) = 1$ in Gao's approach in [3], can be tested by computer since we have the following obvious result.

LEMMA 4.2. *Let $P = a_0 X_1^m + a_1 X_1^{m-1} + \cdots + a_m$ where the coefficients a_j are polynomials in $\mathsf{C}[X_2, \ldots, X_n]$. Then P is X_1-generic if and only if the ideal spanned by $a_0, \ldots, a_m$ coincides to the whole ring $\mathsf{C}[X_2, \ldots, X_n]$.*

EXAMPLE 4.3. (i) If d is the total degree of P and if the monomial X_1^d occurs in P with a non-zero coefficient, then clearly the polynomial P is X_1-generic. Starting with any polynomial P, we can arrive at this situation by making a linear coordinate change $\tilde{X}_1 = X_1$, $\tilde{X}_j = X_j + c_j \cdot X_1$ for $j > 1$ and suitable constants $c_j \in \mathsf{C}$.

(ii) Let $n = 3$ and consider the polynomial $P = X^2 Y^2 Z^2 + X$. Then P is X generic, but not Y-generic.

We assume in the sequel that the polynomial P is X_1-generic and define the following two associated vector spaces. Let $E(P) = \mathrm{pr}_1(F(P))$, where

$$\mathrm{pr}_1 : \mathsf{C}[X_1, \ldots, X_n]^n \to \mathsf{C}[X_1, \ldots, X_n]$$

denotes the projection on the first factor. Let $\overline{E}(P)$ be the image of $E(P)$ under the canonical projection $p : \mathsf{C}[X_1, \ldots, X_n] \to Q(P)$, where we introduce the quotient ring $Q(P) = \mathsf{C}[X_1, \ldots, X_n]/(P)$.

PROPOSITION 4.4. *If the polynomial P is X_1-generic, then the following hold.*

(i) $\gcd(P, P_{X_1}) = 1$, *where the subscript X_1 indicates the partial derivative with respect to X_1.*

(ii) $\dim \overline{E}(P) = s$.

PROOF. To prove (i), it is enough to show that any irreducible factor P_k of P does not divide P_{X_1}. Now, with the notation from the proof of Theorem 3.3, we have

(4.1) $$P_{X_1} = \sum_{j=1,s} B_1^j.$$

In this sum, all the terms are divisible by P_k, except possibly

$$B_1^k = \frac{P \cdot (P_k)_{X_1}}{P_k}.$$

This term is divisible by the irreducible polynomial P_k exactly when $(P_k)_{X_1} = 0$ (otherwise $\deg_{X_1} P_k > \deg_{X_1}(P_k)_{X_1}$). But $(P_k)_{X_1} = 0$ implies that $P_k \in \mathsf{C}[X_2, \ldots, X_n]$ and then, for any $b \in \mathsf{C}^{n-1}$ such that $P_k(b) = 0$ (which exists since $\deg P_k > 0$), the line $\pi_1^{-1}(b)$ is contained in the hypersurface $V(P)$. This contradicts the hypothesis that P is X_1-generic, and thus proves (i).

To prove (ii), it is enough to show that the classes of the elements B_1^j for $j = 1, \ldots, s$ are linearly independent in $Q(P)$. Assume there is a relation

$$\sum_{j=1,s} c_j \cdot B_1^j = C \cdot P$$

where $c_j \in \mathsf{C}$ and $C \in \mathsf{C}[X_1, \ldots, X_n]$. Checking as above the divisibility by P_k, it follows that the coefficient c_k has to vanish, for all $k = 1, \ldots, s$.

Exactly as in the proof above, one can show that the classes of the elements

(4.2) $$C_1^j = B_1^j \cdot P_{X_1}$$

for $j = 1, 2, \ldots, s$ are linearly independent in $Q(P)$. It follows that the linear subspace

(4.3) $$\tilde{E}(P) = \{[v \cdot P_{X_1}] \mid v \in E(P)\}$$

in $Q(P)$ is s-dimensional. Let $S : \tilde{E}(P) \to \overline{E}(P)$ be the inverse of the linear isomorphism $\overline{E}(P) \to \tilde{E}(P)$ sending $[v]$ to $[v \cdot P_{X_1}]$ for $j = 1, 2, \ldots, s$.

Note that in the quotient ring $Q(P)$ one has

(4.4) $[B_1^i] \cdot [B_1^j] = 0$

for $i \neq j$ and

(4.5) $[B_1^i] \cdot [B_1^i] = [P_{X_1}] \cdot [B_1^i]$

for all $i = 1, \ldots, s$. Let $v \in E(P)$ and write $[v] = \sum_{j=1,s} \lambda_j [B_1^j]$ in $Q(P)$. Consider the linear mapping

$$\phi_v : Q(P) \to Q(P)$$

induced by the multiplication by v. Then the equations (4.2), (4.4), (4.5) imply that $\phi_v(\overline{E}(P)) \subset \tilde{E}(P)$. It follows that $\psi_v = S \circ \phi_v$ as a linear endomorphism of the s-dimensional vector space $\overline{E}(P)$. We also get

$$\psi_v([B_1^i]) = \lambda_i [B_1^i]$$

for all $i = 1, \ldots, s$.

REMARK 4.5. A key point here is that the vector space $\overline{E}(P)$ and the endomorphism $\psi_v : \overline{E}(P) \to \overline{E}(P)$ can be computed without knowing the factorization of P.

We have the following basic result.

PROPOSITION 4.6. *If the polynomial P is X_1-generic and all the eigenvalues of the endomorphism $\psi_v : \overline{E}(P) \to \overline{E}(P)$ are distinct, say $\lambda_1, \ldots, \lambda_s$, then, up-to a re-indexing of the factors, one has*

$$P_i = \gcd(P, v - \lambda_i P_{X_1})$$

for $i = 1, \ldots, s$.

PROOF. Using the above equations, we get a polynomial $C_1 \in \mathsf{C}[X_1, \ldots, X_n]$ such that

(4.6) $v - \lambda_i P_{X_1} = \sum_{j \neq i} (\lambda_j - \lambda_i)[B_1^j] + C_1 \cdot P.$

It follows that the irreducible polynomial P_i divides $v - \lambda_i P_{X_1}$. Moreover, exactly as in the proof of Proposition 4.4, we see that the irreducible polynomial P_k does not divide $v - \lambda_i P_{X_1}$ for $k \neq i$.

REFERENCES

1. Chèze, G., Galligo, A., *Four Lectures on Polynomial Absolute Factorization, Solving Polynomial Equations*, Algorithms Comput. Math. 14 (2005).
2. Dimca, A., *Singularities and Topology of Hypersurfaces*, Springer, 1992.
3. Gao, S., *Factoring multivariate polynomials via partial differential equations*, Math. Comp. 72 (2003), 801–822.
4. Grothendieck, A., *On the de Rham cohomology of algebraic varieties*, Inst. Hautes Études Sci. Publ. Math. 29 (1966), 95–103.
5. Ruppert, W., *Reduzibilität ebener Kurven*, J. Reine Angew. Math. 369 (1986), 167–191.
6. Ruppert, W., *Reducibility of polynomials $f(x, y)$ modulo p*, J. Number Theory 77 (1999), 62–70.

ABDUS SALAM SCHOOL OF MATHEMATICAL SCIENCES
GCU
68-B NEW MUSLIM TOWN
LAHORE
PAKISTAN
E-mail: hani.uet@gmail.com