https://doi.org/10.26485/0459-6854/2018/68.1/2 PL ISSN 0459-6854

B U L L E T I N

DE LA SOCIÉTÉ DES SCIENCES ET DES LETTRES DE ŁÓDŹ

2018 Vol. LXVIII

Recherches sur les déformations no. 1

pp. 27–32

Beata Hejmej

A NOTE ABOUT IRREDUCIBILITY OF A RESULTANT

Summary

We present a theorem about irreducibility of a polynomial that is the resultant of two others polynomials. The proof of this fact is based on the field theory. We also consider the converse theorem and some examples.

Keywords and phrases: Galois theory, separable extension, embedding, polynomial, irreducibility, resultant

The aim of the paper

The aim of the paper is to prove some irreducibility criterion for resultants, which are elements of the polynomial ring (Theorem 2.1). A motivation to take up this issue is irreducibility of polynomials over the ring of formal power series, which is a current problem in the algebraic geometry (see for example [4], [5], [6], [8]).

The main result of the article (Theorem 2.1) implies the following corollary.

Corollary 1. *Let k be a field and $f, g \in k[Y]$ be monic polynomials. If* $\mathrm{Res}(f-T, g)$ *is a product of some relatively prime polynomials in $k[T]$, then g is also a product of some relatively prime polynomials in $k[Y]$.*

The above fact allows to prove some generalization of the well known Hensel's Lemma (see [2]), which we outline below. Let k be an algebraically closed field of characteristic zero. We consider the formal power series ring $k[[X_1, \ldots, X_d]]$ and a fractional power series ring $k[[X_1^{1/m}, \ldots, X_d^{1/m}]]$, where m is a positive integer. For every $q = (q_1, \ldots, q_d) \in \mathbb{Q}^d_{\geq 0}$ we denote the monomial $\underline{X}^q := X_1^{q_1} \cdots X_d^{q_d}$ and we say that q is the *order* of $\underline{X}^q$. Let

$$f = Y^n + a_{n-1}Y^{n-1} + \cdots + a_0 \in k[[X_1, \ldots X_d]][Y]$$

be a monic polynomial. Such a polynomial is called *quasi-ordinary* if its discriminant equals $u\underline{X}^q$ with $u(0) \neq 0$. We say that f is a *Weierstrass polynomial* if $a_i(0) = 0$ for all $i = 0, \ldots, n-1$. The Abhyankar-Jung theorem (see [7]) says that every quasi-ordinary polynomial has its roots in the ring $k[[X_1^{1/m}, \ldots, X_d^{1/m}]]$ for some positive integer m.

Assume that $g \in k[[X_1, \ldots, X_d]][Y]$ is a Weierstrass polynomial such that

$$g(\lambda + Z\underline{X}^h) = G(Z)\underline{X}^q + \text{ terms of greater order},$$

where $\lambda \in k[[X_1^{1/m}, \ldots, X_d^{1/m}]]$ is a root of some irreducible quasi-ordinary Weierstrass polynomial $f \in k[[X_1, \ldots, X_d]][Y]$ and $G(Z) \in k[Z]$ is a nonzero polynomial such that $\deg G \cdot \deg f = \deg g$. Therefore, under suitable assumptions, if $G(Z) = G_1(Z)G_2(Z)$, where $G_1(Z), G_2(Z) \in k[Z]$ are relatively prime, then $g = g_1 g_2$ for some relatively prime polynomials $g_1, g_2 \in k[[X_1, \ldots, X_d]][Y]$ such that

$$g_1(\lambda + Z\underline{X}^h) = G_1(Z)\underline{X}^{q_1} + \text{ terms of greater order},$$
$$g_2(\lambda + Z\underline{X}^h) = G_2(Z)\underline{X}^{q_2} + \text{ terms of greater order}.$$

This generalization of Hensel's Lemma is not published yet, so we do not include the details.

1. Preliminaries

At the beginning, we recall some basic definitions and facts from the field theory.

Every nonzero homomorphism of fields is called an *embedding*. For a field extension $F < E$ and an embedding $\sigma\colon F \hookrightarrow L$, an embedding $\bar{\sigma}\colon E \hookrightarrow L$ such that $\bar{\sigma}|_F = \sigma$ is called an *extension* of σ. An extension of the identity map $F \hookrightarrow F < L$ is called an *F–embedding*.

If $\sigma\colon F \hookrightarrow E$ is an embedding and $f = a_n X^n + \cdots + a_0 \in F[X]$, then we set $f^\sigma := \sigma(a_n)X^n + \cdots + \sigma(a_0) \in E[X]$.

We say that E is a *splitting field over F* of a family $\mathcal{F} \subset F[X]$ if every polynomial $f \in \mathcal{F}$ splits over E and $E = F(S)$, where S is the set of all roots of polynomials from the family $\mathcal{F}$ (we assume that $S \subset \bar{F}$, the algebraic closure of F).

An algebraic extension $F < E$, where $E < \bar{F}$, is said to be *normal* if E is a splitting field of some family $\mathcal{F} \subset F[X]$. In this situation we also say that E is *normal over F*.

Consider a field extension $F < E$. The set $\mathrm{Gal}(E/F)$ of all F–automorphisms of E is a group under the composition of mappings, which we call the *Galois group of the extension $F < E$*.

Let f be a polynomial over a field F. We define the *Galois group of the polynomial f* as the Galois group of the extension $F < L_f$, where L_f is the splitting field of f. We denote this group by $\mathrm{Gal}(f)$. It acts on the set Z_f of all roots of f by an obvious way.

The following theorem collects some well known properties of extension of fields, all of which can be found in [3].

Theorem 1.1. *Assume that $F < E$ is an algebraic field extension and L is an algebraically closed field. Then:*

(i) *Let $\alpha \in E$ and $m_{\alpha,F}$ be the minimal polynomial of α over F. If $\sigma\colon F \hookrightarrow L$ is an embedding and $\beta \in L$ is a root of $m^{\sigma}_{\alpha,F}$, then σ can be extended to an embedding $\bar{\sigma}\colon E \hookrightarrow L$ such that $\bar{\sigma}(\alpha) = \beta$.*

(ii) *If $E < \bar{F}$, then $F < E$ is normal if and only if every F–embedding $E \hookrightarrow \bar{F}$ is an automorphism of E.*

We need a slight generalization of a well known property of the Galois group.

Theorem 1.2. *Let f be a monic polynomial over a field F, $\deg f > 0$. Then $\mathrm{Gal}(f)$ acts transitively on the set of all roots of the polynomial f if and only if f is a power of some monic irreducible polynomial.*

Proof. Assume that $\mathrm{Gal}(f)$ acts transitively on the set Z_f of all roots of the polynomial f. Let $f_1, \ldots, f_s \in F[X]$ be all distinct irreducible factors of f (all of them are monic). Take $r_i \in Z_{f_i}$, $r_j \in Z_{f_j}$. Then $r_i, r_j \in Z_f$ and according to our assumption there exists an automorphism $\sigma \in \mathrm{Gal}(f)$ such that $\sigma(r_i) = r_j$. Thus $0 = \sigma(f_i(r_i)) = f_i(r_j)$. It follows that $f_j | f_i$, so $f_i = f_j$. This implies that f is a power of a monic irreducible polynomial.

Conversely, assume that f is a power of a monic irreducible polynomial $g \in F[X]$. Then $Z_f = Z_g$ and g is the minimal polynomial of every element of Z_f. Take $r_i, r_j \in Z_f$. Since the extension $F < L_f$ is algebraic, the identity $F \hookrightarrow \overline{F}$ can be extended to an F–embedding $\sigma\colon L_f \hookrightarrow \overline{F}$ such that $\sigma(r_i) = r_j$ (Theorem 1.1(i)). According to the normality of the extension $F < L_f$, the F–embedding σ must be an element of the group $\mathrm{Gal}(f)$ (Theorem 1.1(ii)). Therefore $\mathrm{Gal}(f)$ acts transitively on the set Z_f. □

2. Main theorem

Let k be a field and $\mathrm{Res}_Y(f, g)$ denote the resultant of polynomials $f, g \in k[Y, T]$ with respect to the variable Y.

Theorem 2.1. *Let $f, g \in k[Y]$ be monic. If g is irreducible in the ring $k[Y]$ then the polynomial $h = (-1)^{\deg g}\mathrm{Res}_Y(g, f - T) \in k[T]$ is a power of some irreducible polynomial.*

Proof. Let $Z_g = \{y_1, \ldots, y_m\}$. Observe that $h = \prod_{i=1}^{m}(T - f(y_i))$, so $Z_h = \{f(y_i) : i = 1, \ldots, m\}$. Set $L_g := k(y_1, \ldots, y_m)$ and $L_h := k(f(y_1), \ldots, f(y_m))$. It is obvious that $k \subset L_h \subset L_g \subset \bar{k}$. Take $i, j \in \{1, \ldots, m\}$. Since the polynomial g is

irreducible, Theorem 1.2 implies that the action of $\mathrm{Gal}(g)$ on the set Z_g is transitive. It follows that $\sigma(y_i) = y_j$ for some $\sigma \in \mathrm{Gal}(g)$. Therefore $\sigma|_{L_h} \colon L_h \hookrightarrow \overline{k}$ is a k–embedding. The extension $k < L_h$ is normal, so according to Theorem 1.1(ii), we have that $\sigma|_{L_h}$ is a k–automorphism of L_h. Thus $\tau := \sigma|_{L_h} \in \mathrm{Gal}(h)$ and $\tau(f(y_i)) = \sigma(f(y_i)) = f(\sigma(y_i)) = f(y_j)$. It means that $\mathrm{Gal}(h)$ acts transitively on the set Z_h and by Theorem 1.2 the statement follows. □

Now, we present some examples connected with the converse theorem.

The first example shows that, in general, the converse to Theorem 2.1 does not hold.

Example 2.2. Let $f = Y^2 - X^3 \in \mathbb{C}((X))[Y]$ and $g = (Y^2 - X^3)^2 - X^7 \in \mathbb{C}((X))[Y]$. Then $h = (T^2 - X^7)^2 \in \mathbb{C}((X))[T]$ is the square of the irreducible polynomial, but g has two irreducible factors in $\mathbb{C}((X))[Y]$ (see [1]). (Here $\mathbb{C}((X))$ denotes the quotient field of the ring $\mathbb{C}[[X]]$ of formal power series.)

If we assume that h is irreducible, then the converse to Theorem 2.1 holds.

Corollary 2. *Let $f, g \in k[Y]$ be monic. If $h = (-1)^{\deg g}\mathrm{Res}_Y(g, f - T) \in k[T]$ is irreducible, then g is also irreducible.*

Proof. Assume that $g = g_1 \cdots g_s$, where $k > 1$ and $g_1, \ldots, g_s \in k[Y]$ are monic and irreducible. Then

$$h = (-1)^{\deg g}\mathrm{Res}_Y(g_1, f - T) \cdots \mathrm{Res}_Y(g_s, f - T).$$

Since $g_1, \ldots, g_s$ are monic and irreducible over k, Theorem 2.1 implies that each $\mathrm{Res}_Y(g_i, f - T)$ is a power of some irreducible polynomial. This means that h is reducible in $k[T]$. □

Consider the following example.

Example 2.3. Let $f = Y^2 - X^3$ and $g = (Y^2 - X^3)^2 - X^5Y$ be polynomials over the field $\mathbb{C}((X))$. Let $w(i, j) := 4i + 13j$ be a weight. Then the initial quasi-homogeneous part of $h = T^4 - X^{10}T - X^{13} \in \mathbb{C}[[X, T]]$ is equal to $T^4 - X^{13}$. Since the integers 4 and 13 are coprime, the polynomial $T^4 - X^{13}$ is irreducible in the ring $\mathbb{C}[X, T]$. Therefore Hensel's Lemma (see [2, Lemma A1]) implies that h is irreducible in the ring $\mathbb{C}((X))[T]$. By Corollary 2 the polynomial g is irreducible over $\mathbb{C}((X))$.

Remark 2.4. Polynomials $g_1 = (Y^2 - X^3)^2 - X^7$ and $g_2 = (Y^2 - X^3)^2 - X^5Y$ are taken from [1]. Both were proposed by Tzee-Char Kuo.

Acknowledgements

The author would like to thank Professors Evelia Rosa García Barroso, Janusz Gwoździewicz and Kamil Rusek for useful comments and helpful suggestions concerning this paper.

References

[1] S. S. Abhyankar, *Irreducibility criterion for germs of analytic functions of two complex variables*, Adv. Math. **74** (1989), 190–257.

[2] E. Artal Bartolo, I. Luengo, A. Melle-Hernndez, *High-school algebra of the theory of dicritical divisors: atypical fibers for special pencils and polynomials*, J. Algebra Appl. **14** (2015), no. 9, 1–26.

[3] S. Roman, *Field Theory*, Springer, New York, 2005.

[4] E. García Barroso, J. Gwoździewicz, *Characterization of jacobian Newton polygons of plane branches and new criteria of irreducibility,* Ann. Inst. Fourier **60** (2010), no. 2, 683–709.

[5] E. García Barroso, J. Gwoździewicz, *Quasi-Ordinary Singularities: Tree Model, Discriminant, and Irreducibility,* Int. Math. Res. Notices. Vol. **2015**, Issue 14 (2015), 5783–5805, doi:10.1093/imrn/rnu106.

[6] J. Gwoździewicz, B. Hejmej *On Abhyankar-Moh irreducibility criterion for quasi-ordinary polynomials,*, arXiv:1804.05366v1

[7] A. Parusiński, G. Rond, *The Abhyankar-Jung Theorem*, Journal of Algebra **365** (2012), 29–41.

[8] G. Rond, B. Schober, *Irreducibility criterion for power series*, Proceedings of the American Mathematical Society Volume **145**, Number 11, November 2017, 47314739, doi.org/10.1090/proc/13635

Department of Mathematics
Pedagogical University of Cracow
Podchorążych 2, PL-30-084 Kraków
Poland
E-mail: bhejmej1f@gmail.com

Presented by Andrzej Łuczak at the Session of the Mathematical-Physical Commission of the Łódź Society of Sciences and Arts on June 27, 2018.

UWAGA DOTYCZĄCA NIEROZKŁADALNOŚCI RUGOWNIKA

S t r e s z c z e n i e

W pracy przedstawiono twierdzenie dotyczące nierozkładalności wielomianu, który jest rugownikiem dwóch innych wielomianów. Dowód tego twierdzenia oparty jest na teorii ciał. Ponadto, udowodniono pewien wariant twierdzenia odwrotnego oraz zaprezentowano kilka przykładów.

Słowa kluczowe: teoria Galois, rozszerzenie rozdzielcze ciał, zanurzenie ciał, nierozkładalność wielomianu, rugownik