

SUMS OF EQUAL POWERS OF SUCCESSIVE INTEGERS

MOHAMED AYAD

RÉSUMÉ. Soit $\sigma_k(n) = \sum_{l=0}^n l^k$. On étend la définition pour obtenir le polynôme $\sigma_k(t)$. Si i et j sont des entiers positifs, il est possible, en utilisant les résultants, de calculer l'unique polynôme irréductible (à une constante multiplicative près) $P_{ij}(x, y) \in \mathbb{Q}[x, y]$ tel que $P_{ij}(\sigma_i(x), \sigma_j(y)) = 0$. Les termes dominants de ce polynôme, lorsque certains poids sont attribués à x et à y , sont explicités. De plus nous montrons que si j est pair, alors les facteurs irréductibles de $\text{Res}_y(P_{ij}(x, y), P_{jk}(y, z))$ sont $P_{ik}(x, z)$ et $S_{ik}(x, z)$. Ici $S_{ik}(x, z)$ désigne le polynôme minimal de $(\sigma_i(s), \sigma_k(t))$ le long de $\phi(x, y) = (\sigma_j(x) - \sigma_j(y))/(x - y)$. Nous démontrons que $P_{ik}(x, z)$ et $S_{ik}(x, z)$ sont distincts si $(j + 1) \nmid \text{lcm}(i + 1, k + 1)$. Nous conjecturons que cette conclusion reste vraie sans la condition imposée.

ABSTRACT. Let $\sigma_k(n) = \sum_{l=0}^n l^k$. Extend the definition to obtain the polynomial $\sigma_k(t)$. If i and j are distinct positive integers then it is possible to use resultants to compute the unique irreducible polynomial $P_{ij}(x, y) \in \mathbb{Q}[x, y]$ such that $P_{ij}(\sigma_i(x), \sigma_j(y)) = 0$. When some weights are attributed to x and y , the leading terms of this polynomial are explicitated. Moreover it is proved that if j is even, then the irreducible factors of $\text{Res}_y(P_{ij}(x, y), P_{jk}(y, z))$ are $P_{ik}(x, z)$ and $S_{ik}(x, z)$. Here $S_{ik}(x, z)$ denotes the minimal polynomial of $(\sigma_i(s), \sigma_k(t))$ along $\phi(x, y) = (\sigma_j(x) - \sigma_j(y))/(x - y)$. We conjecture that $P_{ik}(x, z)$ and $S_{ik}(x, z)$ are distinct, and prove this conjecture in the case where $(j + 1) \nmid \text{lcm}(i + 1, k + 1)$.

1. Introduction

Let k and n be natural numbers, with $n \geq 1$. Let $\sigma_k(n) = \sum_{j=0}^n j^k$. The following formula, which is due to Pascal, shows that $\sigma_k(n)$ is a polynomial in n of degree $k + 1$:

$$\begin{aligned} (n + 1)^{k+1} - 1 &= \sum_{m=1}^n \left[(m + 1)^{k+1} - m^{k+1} \right] \\ &= \sum_{m=1}^n \sum_{q=0}^k \binom{k+1}{q} m^q \\ &= \sum_{q=0}^k \binom{k+1}{q} \sigma_q(n). \end{aligned}$$

It is then possible to define the polynomials $\sigma_k(t)$. The first ones are given by:

$$\begin{cases} \sigma_0(t) = t; \\ \sigma_1(t) = t(t+1)/2 = \frac{1}{2}t^2 + \frac{1}{2}t; \\ \sigma_2(t) = t(t+1)(2t+1)/6 = \frac{1}{3}t^3 + \frac{1}{2}t^2 + \frac{1}{6}t; \\ \sigma_3(t) = (\sigma_1(t))^2 = \frac{1}{4}t^4 + \frac{1}{2}t^3 + \frac{1}{4}t^2; \\ \sigma_4(t) = \sigma_2(t)(3t^2 + 3t - 1)/5 = \frac{1}{5}t^5 + \frac{1}{2}t^4 + \frac{1}{3}t^3 - \frac{1}{30}t. \end{cases}$$

Bernoulli's numbers B_i allow to make explicit these polynomials; see [7, Chap. 18]. Let $k \geq 1$ be an integer. Then

$$(k+1)\sigma_k(t) = t^{k+1} - \binom{k+1}{1}B_1t^k + \binom{k+1}{2}B_2t^{k-1} + \dots + \binom{k+1}{k}B_kt$$

and, for $k \geq 4$,

$$(1) \quad \sigma_k(t) = t^{k+1} + \frac{1}{2}t^k + \frac{k}{12}t^{k-1} - \frac{k(k-1)(k-2)}{720}t^{k-3} + \dots$$

It is known that $\sigma_k(t) = F_k(\sigma_1(t))$ if k is odd and $\sigma_k(t) = \sigma_2(t)F_k(\sigma_1(t))$ if k is even, where F_k is a polynomial with rational coefficients of degree $(k+1)/2$ in the first case and $(k-2)/2$ in the second case; see for instance [3]. These polynomials are called *Faulhaber's polynomials* in honour of J. Faulhaber. Indeed the formula $\sigma_3(t) = (\sigma_1(t))^2$ was known to Al Karagi in the 10-11th century [5]. A. F. Beardon showed, in [3], that for any pair of integers i and j , with $i \neq j$, there exists an irreducible polynomial $P_{ij}(x, y) \in \mathbb{Z}[x, y]$ such that $P_{ij}(\sigma_i(t), \sigma_j(t)) = 0$. In fact, this is proved in a more general context in [6]. A. F. Beardon also explained in [3] that $P_{ij}(x, y)$ is a divisor of the polynomial

$$\text{Res}_t(\sigma_i(t) - x, \sigma_j(t) - y).$$

(Indeed the author suggests inopportunistically to eliminate t between $\sigma_i(t)$ and $\sigma_j(t)$.) He finally observed in the few examples he had computed when i and j are both odd that the polynomial $\text{Res}_t(\sigma_i(t) - x, \sigma_j(t) - y)$ is irreducible, hence, equal to the above polynomial $P_{ij}(x, y)$ up to multiplication by a constant. The study of these polynomials will be done in Section 2. The following result gives the complete solution to this problem.

Theorem 1. *Let i and j be distinct natural numbers.*

(1) *If one of them is even, then the polynomial*

$$R_{ij}(x, y) := \text{Res}_t(\sigma_i(t) - x, \sigma_j(t) - y)$$

is irreducible over $\mathbb{C}$.

(2) *If i and j are both odd, set $\sigma_i(t) = F_i(\sigma_1(t))$ and $\sigma_j(t) = F_j(\sigma_1(t))$. Then the polynomial*

$$R_{ij}(x, y) := \text{Res}_t(F_i(t) - x, F_j(t) - y)$$

is irreducible over $\mathbb{C}$ and we have

$$\text{Res}_t(\sigma_i(t) - x, \sigma_j(t) - y) = c[R_{ij}(x, y)]^2,$$

where c is a non-zero rational number.

The proof of this will be given in Section 3. This theorem shows that in any case $R_{ij}(x, y)$ is, up to multiplication by a rational number, equal to the irreducible polynomial $P_{ij}(x, y)$ such that $P_{ij}(\sigma_i(t), \sigma_j(t)) = 0$.

Let i, j and k be three distinct natural numbers with j even. Before stating the next result, which exhibits a relation between the polynomials $P_{ij}(x, y)$, $P_{jk}(x, y)$ and $P_{ik}(x, y)$, we make the following definition.

Let K be a field, and $u(s), v(t)$ be polynomials with coefficients in K , not both constant. Let $\phi(s, t)$ be an irreducible polynomial over K of the form

$$\phi(s, t) = as^m + \sum_{\substack{i < m \\ j < n}} a_{ij}s^i t^j + bt^n, \quad \text{with } a, b \neq 0,$$

and let S and T be such that $\phi(S, T) = 0$. We will show in Section 2 that there exists an irreducible polynomial $P(x, z) \in K[x, z]$ such that $P(u(S), v(T)) = 0$. Moreover, up to multiplication by a non-zero constant in K , this polynomial is unique. It will be called *the minimal polynomial of the pair $(u(s), v(t))$ along $\phi(s, t)$* .

An important particular case appears for $\phi(s, t) = s - t$. In this case we just say that $P(x, z)$ is *the minimal polynomial of the pair $(u(s), v(t))$ without referring to $\phi(s, t)$* . For example, the irreducible polynomial $P_{ij}(x, y)$ satisfying $P_{ij}(\sigma_i(t), \sigma_j(t)) = 0$ is the minimal polynomial of $(\sigma_i(s), \sigma_j(t))$. Because we need it for the following theorem, we will prove in Corollary 4 that the polynomial

$$\phi_j(s, t) := (\sigma_j(s) - \sigma_j(t)) / (s - t)$$

is irreducible over $\mathbb{Q}$ if j is even.

Theorem 2. *Let i, j and k be three distinct natural numbers, with j even, and let $P_{ij}(x, y)$, $P_{jk}(y, z)$ and $P_{ik}(x, z)$ be the minimal polynomials of $(\sigma_i(s), \sigma_j(t))$, $(\sigma_j(s), \sigma_k(t))$ and $(\sigma_i(s), \sigma_k(t))$ respectively. Let $S_{ik}(x, z)$ be the minimal polynomial of $(\sigma_i(s), \sigma_k(t))$ along $\phi_j(s, t)$. Then*

$$(2) \quad \text{Res}_y (P_{ij}(x, y), P_{jk}(y, z)) = \lambda [P_{ik}(x, z)]^{e_1} [S_{ik}(x, z)]^{e_2},$$

where e_1, e_2 are positive integers and λ is a non-zero rational number. Moreover we have

$$\deg_x P_{ik}(x, z) \cdot \deg_z S_{ik}(x, z) = \deg_x S_{ik}(x, z) \cdot \deg_z P_{ik}(x, z).$$

Conjecture A. The above polynomials $P_{ik}(x, z)$ and $S_{ik}(x, z)$ are distinct.

One may try to prove this conjecture by contradiction. For suppose that the above polynomials are equal, then the resultant in formula (2) is a power of $P_{ik}(x, z)$ up to multiplication by a rational number. The hope is that the contradiction will come from the comparison of the degrees in formula (2) relatively to x or z . Unfortunately this is a vain attempt.

Proposition 1. *Suppose that $(j+1) \nmid \text{lcm}(i+1, k+1)$. Then conjecture A is true.*

Remark 1. We were unable to find the analog of Theorem 2 in case j is odd.

2. Minimal polynomial

Let K be a field, and $u(s), v(t)$ be polynomials with coefficients in K , not both constant. Let $\phi(s, t)$ be an irreducible polynomial over K of the form

$$(3) \quad \phi(s, t) = as^m + \sum_{\substack{i < m \\ j < n}} a_{ij}s^i t^j + bt^n, \quad \text{with } a, b \neq 0,$$

and let S and T be such that $\phi(S, T) = 0$. Since

$$K \subset K(u(S), v(T)) \subset K(S, T)$$

it follows that $u(S)$ and $v(T)$ are algebraically dependent over K . Hence there exists an irreducible polynomial $P(x, z) \in K[x, z]$ such that $P(u(S), v(T)) = 0$. It is possible to prove the existence of this polynomial by another method which has the advantage of showing that, up to multiplication by a non-zero constant in K , this polynomial is unique.

Consider the unique K -morphism of rings $\psi : K[x, z] \rightarrow K[S, T]$ such that $\psi(x) = S$ and $\psi(z) = T$. Then $\text{Ker}(\psi)$ is a prime ideal of $K[x, z]$ of height 1, generated by an irreducible polynomial $P(x, z)$. It follows that if some polynomial $Q(x, z) \in K[x, z]$ satisfies $Q(u(S), v(T)) = 0$, then $P(x, z)$ divides $Q(x, z)$. We call this polynomial $P(x, z)$ *the minimal polynomial of the pair $(u(s), v(t))$ along ϕ* . Notice that when $\phi(s, t) = s - t$ the polynomial P is the minimal polynomial of $(u(s), v(t))$ studied in [6].

Lemma 1. *With the above hypotheses, let I be the ideal of $K[s, t, x, z]$ generated by the polynomials $u(s) - x, v(t) - z$ and $\phi(x, z)$. Then $I \cap K[x, z] = (P(x, z))$.*

Proof. It is possible that this lemma is already in the literature but we did not find it. So, we prove it completely.

Let $\theta : K[s, t, x, z] \rightarrow K[S, T]$ be the unique K -morphism of rings such that $\theta(s) = S, \theta(t) = T, \theta(x) = u(S)$ and $\theta(z) = v(T)$. Then $\text{Ker}(\theta)$ is a prime ideal of $K[s, t, x, z]$. We first show that $\text{Ker}(\theta) = I$.

It is clear that $I \subset \text{Ker}(\theta)$. For the other inclusion, let $f(s, t, x, z)$ be an element of $\text{Ker}(\theta)$. By successive euclidean divisions we obtain

$$f = (x - u(s))q_1 + r_1, \quad r_1 = (z - v(t))q_2 + r_2 \quad \text{and} \quad r_2 = \phi(s, t)q_3 + r_3,$$

where $q_1 \in K[s, t, x, z], r_1 \in K[s, t, z], q_2 \in K[s, t, z], r_2 \in K[s, t], q_3, r_3 \in K[s, t]$ and $\deg_s r_3 < \deg_s \phi$. Since $r_1, r_2, r_3 \in \text{Ker}(\theta)$, we have $r_3(S, T) = 0$, hence $\phi(s, t)$ divides $r_3(s, t)$ and then $r_3 = 0$. We deduce successively that $r_2 \in I, r_1 \in I$ and $f \in I$. Thus $\text{Ker}(\theta) \subset I$. We now have $I \cap K[x, z] = \text{Ker}(\theta) \cap K[x, z] = (P(x, z))$. $\square$

The next result allows to compute the minimal polynomial by using resultants. Before stating it, we recall the following well-known property. Let E/F be a finite extension of degree m and let $\alpha \in E$. Consider the endomorphism M_α of E such that $M_\alpha(\gamma) = \alpha\gamma$ for any $\gamma \in E$. Denote by $\text{Char}(\alpha, E/F, x)$ the polynomial $\text{Det}(M_\alpha)$ and call it the *characteristic polynomial of α over F* . It is well-known that $\text{Char}(\alpha, E/F, x) = [\text{Irr}(\alpha, F, x)]^k$, where $k = [E : F(\alpha)]$ and $\text{Irr}(\alpha, F, x)$ is the minimal polynomial of α over F .

Theorem 3. Let $\phi(s, t)$ be an irreducible polynomial over K of the form (3) and let S, T be such that $\phi(S, T) = 0$. Let $u(s)$ and $v(t)$ be polynomials over K , not both constant. Let $P(x, z)$ be the minimal polynomial of the pair $(u(s), v(t))$ along ϕ . Then there exist two non-zero elements λ and μ in K , and an irreducible polynomial $G(t, x) \in K[t, x]$, such that

$$(4) \quad \text{Res}_s (\phi(s, t), u(s) - x) = \lambda [G(t, x)]^{k_1}$$

and

$$(5) \quad \text{Res}_t (G(t, x), v(t) - z) = \mu [P(x, z)]^{k_2},$$

where, k_1, k_2 are positive integers. If we view the polynomials $G(x, z)$ and $P(x, z)$ as elements of $K(z)[x]$, (resp. $K(x)[z]$), then their leading coefficients are in K . Also,

$$(6) \quad k_1 k_2 = [K(S, T) : K(u(S), v(T))]$$

and

$$(7) \quad \deg_u \cdot \deg_t \phi(s, t) \cdot \deg_x P(x, z) = \deg_v \cdot \deg_s \phi(s, t) \cdot \deg_z P(x, z).$$

Proof. Let $l = \deg u$ and $\beta_1, \dots, \beta_m$ be the roots of $\phi(s, t)$ in $\overline{K(t)}$. Then,

$$\begin{aligned} \text{Res}_s (\phi(s, t), u(s) - x) &= a^l \prod_{i=1}^m (u(\beta_i) - x) \\ &= (-1)^m a^l \prod_{i=1}^m (x - u(\beta_i)) \\ &= (-1)^m a^l \text{Char}(u(\beta_1), K(t, \beta_1)/K(t), x) \\ &= (-1)^m a^l \text{Irr}(u(\beta_1), K(t), x)^{k_1}, \end{aligned}$$

where $k_1 = [K(t, \beta_1) : K(t, u(\beta_1))]$. Since β_1 is integral over $K[t]$, $u(\beta_1)$ is integral over $K[t]$ and $\text{Irr}(u(\beta_1), K(t), x) \in K[t, x]$. If we set $G(t, x) = \text{Irr}(u(\beta_1), K(t), x)$ and $\lambda = (-1)^m a^l$ then formula (4) is proved and it is seen that the leading term of $G(t, x)$ viewed as a polynomial in x does not depend on t .

We claim that the polynomial $G(t, x)$, viewed as a polynomial in t , has a leading term independent from x . Let u_l be the leading coefficient of $u(s)$ and let $\alpha_1, \dots, \alpha_l$ be the roots of $u(s) - x$ in $\overline{K(x)}$. Then

$$\begin{aligned} \text{Res}_s (\phi(s, t), u(s) - x) &= (-1)^{ml} u_l^m \prod_{i=1}^l \phi(\alpha_i, t) \\ &= (-1)^{ml} u_l^m \prod_{i=1}^l (bt^n + b_{n-1}(\alpha_i)t^{n-1} + \dots + b_0(\alpha_i)) \\ &= (-1)^{ml} u_l^m t^{nl} b^l + U_{nl}, \end{aligned}$$

where U_{nl} is the sum of the terms of degree in t lower than nl . This proves our claim.

Replacing in the first resultant s, t, x by t, x, z respectively, ϕ by G and u by v , we conclude that there exist a positive integer k_2 , a non-zero constant μ in K , and an irreducible polynomial $H(x, z) \in K[x, z]$ such that

$$\text{Res}_t(G(t, x), v(t) - z) = \mu[H(x, z)]^{k_2}.$$

Moreover $k_2 = [K(x, \delta_1) : K(x)]$, where δ_1 satisfies $G(\delta_1, x) = 0$. To obtain equation (5), we must verify that $H(x, z) = \gamma P(x, z)$ for some $\gamma \in K^*$, that is that H is the minimal polynomial of $(u(s), v(t))$ along ϕ .

Since the polynomials in $s, \phi(s, T)$ and $u(s) - u(S)$, have the common root $s = S$,

$$\text{Res}_s(\phi(s, T), u(s) - u(S)) = \lambda[G(T, u(S))]^{k_1} = 0.$$

Hence, $G(T, u(S)) = 0$. We also have

$$\text{Res}_t(G(t, u(S)), v(t) - v(T)) = \mu[H(u(S), v(T))]^{k_2} = 0,$$

because the polynomials for which we compute the resultant have the common root $t = T$, hence $H(x, z) = P(x, z)$. It remains to prove formulas (6) and (7). Set $t = T$ in formula (4) and obtain $\text{Res}_s(\phi(s, T), u(s) - x) = \lambda[G(T, x)]^{k_1}$. This shows that $G(T, x) = \text{Irr}(u(S), K(T), x)$. Hence,

$$\begin{aligned} k_1 &= \deg_s \phi(s, t) / \deg_x G(t, x) \\ &= [K(S, T) : K(T)] / [K(T, u(S)) : K(T)] \\ &= [K(T, S) : K(T, u(S))]. \end{aligned}$$

Set $x = u(S)$ in formula (5) and obtain

$$\text{Res}_t(G(t, u(S)), v(t) - z) = \mu[P(u(S), z)]^{k_2}.$$

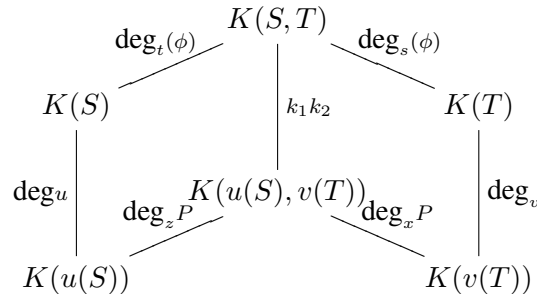
Hence, $P(u(S), z) = \text{Irr}(v(T), K(u(S)), z)$ and

$$k_2 = [K(u(S), T) : K(u(S), v(T))].$$

It follows that $k_1 k_2 = [K(S, T) : K(u(S), v(T))]$.

The following diagram shows formula (7) and implies that

$$k_1 k_2 \mid \gcd(\deg u \cdot \deg_t \phi(s, t), \deg v \cdot \deg_s \phi(s, t)).$$



□

Remark 2. Consider the curve defined by the polynomial $P(x, z)$ which is the minimal polynomial of $(u(s), v(t))$ along the polynomial $\phi(s, t)$ of the form (3). Could

it happen that this curve is unicursal? That is, could there exist two non-constant polynomials $a(s)$ and $b(s)$ such that $P(a(s), b(s)) = 0$? The answer is positive in the following cases:

(i) Suppose that $\phi(s, t)$ is an irreducible polynomial over K of the form (3) and that it defines a unicursal curve. Since $\phi(x, z)$ divides $P(u(x), v(z))$, let

$$(8) \quad P(u(x), v(z)) = \phi(x, z) \bar{P}(x, z),$$

where $\bar{P}(x, z) \in K[x, z]$. This equation implies clearly that $P(x, z)$ defines also a unicursal curve.

(ii) Suppose now that $\phi(s, t)$ is an irreducible polynomial over K of the form $\phi(s, t) = A(s) - B(t)$, where A and B are non-constant polynomials. Let $v(t)$ be any non-constant polynomial over K and let $u(s) = u_1(A(s))$, where u_1 is a non-constant polynomial over K . We have

$$0 = P(u(S), v(T)) = P(u_1(A(S)), v(T)) = P(u_1(B(T)), v(T)).$$

Hence, $P(x, z)$ defines a unicursal curve. It is clear that the same conclusion holds if $v(t) = v_1(B(t))$ and $u(t)$ is arbitrary non-constant.

Conjecture B. Suppose that $P(x, z)$ defines a unicursal curve. Then $\phi(x, z)$ defines a unicursal curve or it has the form indicated in (ii) above.

It is evident that conjecture B implies conjecture A.

Remark 3. Fix an irreducible polynomial $\phi(s, t)$ of the form (3). For any couple $(u(s), v(t))$ of non-constant polynomials over K , denote by $P_{(u,v)}(x, z)$ the minimal polynomial of (u, v) along ϕ . We want to discuss if the number of couples such that $P_{(u,v)}(u(x), v(z))$ is irreducible over K is infinite or not. Equivalently, are there infinitely many representations of $\phi(x, z)$ of the form $\phi(x, z) = P(u(x), v(z))$? If (u, v) is such a couple, then by formula (8), $\deg_u < \deg_x \phi$ and $\deg_v < \deg_y \phi$. It follows immediately that if the field K is finite, then the number of couples is finite. Suppose that K is infinite. Let $u(s) = as + b$ and $v(t) = ct + d$, with $a \neq 0$ and $b \neq 0$. Then $P_{(u,v)}(x, z) = \phi((x - b)/a, (z - d)/c)$, hence the number of couples satisfying the property is infinite.

Question 1. If the field is infinite, are there infinitely many couples (u, v) having the above property with $\deg_u \geq 2$ or $\deg_v \geq 2$?

Remark 4. Let $\phi(s, t)$ be an irreducible polynomial of the form (3), $(u(s), v(t))$ be a couple of non-constant polynomials and $P(x, z)$ be the minimal polynomial over K along ϕ . By Theorem 3, $P(x, z)$ has the form (3), so we ask: does there exist a couple $(\bar{u}(s), \bar{v}(t))$ of non-constant polynomials such that its minimal polynomial over K along P is $\phi(x, z)$? This is equivalent to say that there exists a couple $(\bar{u}(s), \bar{v}(t))$ of non-constant polynomials over K such that $\phi(x, z) \mid \phi(\bar{u}(u(x)), \bar{v}(v(z)))$. The answer is clearly positive if u and v are both of degree 1.

Here is an example of $\phi(x, z)$ where there is no couple $(u(s), v(t))$, with $\deg_u \geq 2$ or $\deg_v \geq 2$, such that the above property holds. Hereditarily irreducible polynomials over a field K are defined in [1] as follows: a polynomial $f(x, z)$ is said to be *hereditarily irreducible* if for any pair $(u(x), v(z))$ of non-constant polynomials, $f(u(x), v(z))$ is absolutely irreducible. The first example of such polynomials appeared in [8]. For

more examples, see [2]. Now let $\phi(s, t)$ be a hereditarily irreducible polynomial of the form (3). Then if $\phi(x, z) \mid \phi(\bar{u}(u(x)), \bar{v}(v(z)))$, we conclude that all the polynomials $u, v, \bar{u}$ and $\bar{v}$ are of degree 1. This example is not completely satisfactory because there is no known hereditarily irreducible polynomial of the form (3); see [2].

Question 2. Find conditions on an irreducible polynomial $\phi(s, t)$ of the form (3) so that there exist two couples $(u(s), v(t))$ and $(\bar{u}(s), \bar{v}(t))$ of polynomials, not all of degree 1, such that $\phi(x, z) \mid \phi(\bar{u}(u(x)), \bar{v}(v(z)))$.

We deduce from Theorem 3 the following result which was proved in [6] and attributed to S. S. Abhyankar.

Corollary 1. Let $u(\chi)$ and $v(\chi)$ be polynomials over K , not both constant. Then there exists a unique polynomial $P(x, z)$ (up to multiplication by a constant in K), irreducible over K such that $P(u(\chi), v(\chi)) = 0$. Moreover $P(x, z)$ is given by

$$\text{Res}_\chi(u(\chi) - x, v(\chi) - z) = \mu[P(x, z)]^k,$$

where

$$k = [K(\chi) : K((u(\chi), v(\chi)))].$$

Proof. By formula (4), $\text{Res}_s(s - \chi, u(s) - x) = u(\chi) - x$ and by formula (5), $\text{Res}_\chi(u(\chi) - x, v(\chi) - z) = \mu[P(x, z)]^k$. The formula for k is easily deduced from formula (6). $\square$

Before stating some results concerning the terms appearing in $P(x, z)$ when some weights are attributed to x and z , we prove an elementary lemma which, in the opinion of the referee, was known to Frobenius.

Lemma 2. Let $m \geq 2$ and $n \geq 2$ be integers. Then there exist integers k and l , with $1 \leq k \leq m$ and $1 \leq l \leq n$, such that $kn + lm = mn - 1$ if and only if $\gcd(m, n) = 1$. In this case, the pair (m, n) is unique, $k \equiv -n^{-1} \pmod{m}$, and $l \equiv -m^{-1} \pmod{n}$.

Proof. The necessity part is evident. Suppose that $\gcd(m, n) = 1$. It is known that there exist rational integers k and l , with $|k| < m$ and $|l| < n$, such that

$$kn + lm = mn - 1.$$

It is clear that k or l is positive. Suppose (for example) that $k > 0$ and $l < 0$. Then $1 \leq k \leq m - 1$ and $-n + 1 \leq l \leq -1$, hence

$$kn + lm = mn - 1 \leq mn - m - n < mn - 2,$$

which is impossible. It follows that k and l are positive. The rest of the proof is easy. $\square$

Let

$$(9) \quad u(\chi) = u_n \chi^n + \cdots + u_1 \chi \quad \text{and} \quad v(\chi) = v_m \chi^m + \cdots + v_1 \chi$$

be polynomials over K and let

$$(10) \quad R(x, z) = \text{Res}_\chi(u(\chi) - x, v(\chi) - z).$$

As mentioned in [6], every term in $R(x, z)$ has the same weight mn under either of the following assignments of weights, where $w(u)$ denotes the weight assigned to u :

- (i) $w(u_i) = i, w(v_j) = j$ and $w(x) = w(z) = 0$, or

(ii) $w(u_i) = n - i$, $w(v_j) = m - j$, $w(x) = n$ and $w(z) = m$.

Using the weights as defined in (ii), we observe that whenever a term $x^i z^j$ has a non-zero coefficient then $ni + mj \leq mn$. Here we are interested by the terms $x^i z^j$ such that $ni + mj = mn$ and $ni + mj = mn - 1$ respectively.

Proposition 2. Let $u(\chi)$ and $v(\chi)$ be polynomials over K given by formula (9) and let $d = \gcd(m, n)$. Let $R_{mn}(x, z)$ and $R_{mn-1}(x, z)$ be the sums of the terms $x^i z^j$ in formula (10) such that $ni + mj = mn$ and $ni + mj = mn - 1$ respectively. Then

$$(11) \quad R_{mn}(x, z) = (-1)^n \left(u_n^{m/d} z^{n/d} - v_m^{n/d} x^{m/d} \right)^d,$$

and

$$(12) \quad R_{mn-1}(x, z) = \begin{cases} 0 & \text{if } d \neq 1, \\ (pu_{n-1}v_m + qv_{m-1}u_n)u_n^{m-k-1}v_m^{n-l-1}x^k z^l & \text{if } d = 1, \end{cases}$$

where $p = (-1)^n m$, $q = (-1)^{n-1} n$, and (k, l) is the unique couple of natural numbers satisfying

$$(13) \quad 0 \leq k \leq m, \quad 0 \leq l \leq n \quad \text{and} \quad kn + lm = mn - 1.$$

Proof. Formula (11) is proved in [6, Th. 5]. For formula (12), we distinguish two cases.

If $d \neq 1$, then by Lemma 2 the equation (13) has no solutions (k, l) , hence $R_{mn-1}(x, z) = 0$ in this case. If $d = 1$, let (k, l) be the unique couple of integers satisfying equation (13). Since $R(x, z)$ is a $(m+n) \times (m+n)$ determinant, $R_{mn-1}(x, z)$ is a sum of terms of the form $\lambda x^k z^l$, where $\lambda = \epsilon u_0^{e_0} \cdots u_n^{e_n} v_0^{h_0} \cdots v_m^{h_m}$, with $\epsilon = \pm 1$, $e_0 + \cdots + e_n = m - k$ and $h_0 + \cdots + h_m = n - l$. For any of these terms the weight of λ is equal to 1, hence each term has the form

$$(14) \quad \epsilon u_{n-1} u_n^{m-k-1} v_m^{n-l} x^k z^l \quad \text{or} \quad \epsilon v_{m-1} u_n^{m-k} v_m^{n-l-1} x^k z^l,$$

where $\epsilon = \pm 1$ is the signature of a certain permutation of $\{1, \dots, n+m\}$. It follows that

$$R_{mn-1}(x, z) = \left(\left(\sum_{j=1}^r \epsilon_j \right) u_{n-1} u_n^{m-k-1} v_m^{n-l} + \left(\sum_{i=1}^s \epsilon'_i \right) v_{m-1} u_n^{m-k} v_m^{n-l-1} \right) x^k z^l$$

where $\epsilon_j = \pm 1$ and $\epsilon'_i = \pm 1$. Let $p = \sum_{j=1}^r \epsilon_j$ and $q = \sum_{i=1}^s \epsilon'_i$. Then

$$R_{mn-1}(x, z) = \left(pu_{n-1} u_n^{m-k-1} v_m^{n-l} + qv_{m-1} u_n^{m-k} v_m^{n-l-1} \right) x^k z^l.$$

We now compute p and q . It is clear from the above arguments that p and q depend on n and m , but not on the coefficients u_j and v_i nor on the field K . We may suppose that $K = \mathbb{Q}$. It follows that if we set

$$\overline{R}(x, z) = \text{Res}_t(t^n - x, t^m + t^{m-1} - z),$$

then $\overline{R}_{mn-1}(x, z) = qx^k z^l$, hence $\overline{R}_{mn-1}(x^n, x^m) = qx^{mn-1}$.

Besides this, let $H(x, z)$ be the sum of the terms of (usual) degree $mn - 1$ in $\overline{R}(x^n, z^m)$. Then $H(x, z) = qx^{kn} z^{lm}$ and if we set

$$\overline{R}(x^n, x^m) = c_{mn} x^{mn} + c_{mn-1} x^{mn-1} + \cdots + c_0,$$

then $c_{mn-1} = q$. Now we have

$$\begin{aligned}\overline{R}(x^n, x^m) &= \text{Res}_t(t^n - x^n, t^m + t^{m-1} - x^m) \\ &= \prod_{i=1}^n (\xi_i^m x^m + \xi_i^{m-1} x^{m-1} - x^m),\end{aligned}$$

where $\xi_1 = 1, \xi_2, \dots, \xi_n$ are the n -th roots of unity in $\mathbb{C}$. It follows that

$$\overline{R}(x^n, x^m) = x^{n(m-1)} \prod_{i=2}^n ((\xi_i^m - 1)x + \xi_i^{m-1}).$$

Hence,

$$q = c_{mn-1} = \prod_{i=2}^n (\xi_i^m - 1).$$

Let $A = \{\xi_2, \dots, \xi_n\}$. Since $\gcd(m, n) = 1$, for any $i = 2, \dots, n$, we have $\xi_i^m \in A$. It is clear that for any $i, j \in \{2, \dots, n\}$, $\xi_i^m = \xi_j^m$ implies $i = j$; hence,

$$A = \{\xi_2^m, \dots, \xi_n^m\}.$$

Thus $q = \prod_{i=2}^n (\xi_i - 1)$. Since $\xi_2, \dots, \xi_n$ are the roots of the polynomial

$$f(x) = (x^n - 1)/(x - 1) = x^{n-1} + \dots + x + 1,$$

it follows that $\xi_2 - 1, \dots, \xi_n - 1$ are the roots of

$$g(x) = f(x + 1) = (x + 1)^{n-1} + \dots + (x + 1) + 1.$$

Hence, $q = (\xi_2 - 1) \cdots (\xi_n - 1) = (-1)^{n-1} n$.

Let $\underline{R}(x, z) = \text{Res}_t(t^n + t^{n-1} - x, t^m - z)$. Then by formula (14)

$$\underline{R}_{mn-1}(x, z) = px^k z^l.$$

In addition, we have $\underline{R}(x, z) = (-1)^{mn} \text{Res}_t(t^m - z, t^n + t^{n-1} - x)$ and using the preceding calculations of q , we obtain $\underline{R}_{mn-1}(x, z) = (-1)^{mn} (-1)^{m-1} m x^k z^l$. Since $\gcd(m, n) = 1$,

$$p = (-1)^{mn+m-1} m = (-1)^n m$$

and the proof is complete. $\square$

Corollary 2. Let $P_{ij}(x, z)$ be the minimal polynomial of $(\sigma_i(s), \sigma_j(s))$.

(1) If i or j is even and $d := \gcd(i + 1, j + 1)$, then

$$\begin{aligned}P_{ij}(x, z) &= (-1)^{i+1} \left(\left(\frac{1}{i+1} \right)^{(j+1)/d} z^{(i+1)/d} - \left(\frac{1}{j+1} \right)^{(i+1)/d} x^{(j+1)/d} \right)^d \\ &\quad + \sum \lambda_{ab} x^a z^b,\end{aligned}$$

where the sum Σ runs over some couples (a, b) such that

$$a(i + 1) + b(j + 1) \leq (i + 1)(j + 1) - 2.$$

(2) If i and j are odd and $d := \gcd((i+1)/2, (j+1)/2) \neq 1$, then

$$P_{ij}(x, z) = (-1)^I \left(\left(\frac{2^{I-1}}{I} \right)^{J/d} z^{I/d} - \left(\frac{2^{J-1}}{J} \right)^{I/d} x^{J/d} \right)^d + \sum \lambda_{ab} x^a z^b,$$

where $I = (i+1)/2$, $J = (j+1)/2$ and the sum Σ runs over some couples (a, b) such that $aI + bJ \leq IJ - 2$.

(3) If i and j are odd and $d := \gcd((i+1)/2, (j+1)/2) = 1$, then

$$\begin{aligned} P_{ij}(x, z) &= (-1)^I \left(\left(\frac{2^{I-1}}{I} \right)^J z^I - \left(\frac{2^{J-1}}{J} \right)^I x^J \right) \\ &\quad + (-1)^I \frac{2^{I+J-4}(J-I)}{3} \left(\frac{2^{I-1}}{I} \right)^{J-k-1} \left(\frac{2^{J-1}}{J} \right)^{I-l-1} x^k z^l \\ &\quad + \sum \lambda_{ab} x^a z^b, \end{aligned}$$

where I, J and (a, b) are as in case (2), and (k, l) is the unique couple satisfying $0 \leq k \leq J, 0 \leq l \leq I$ and $kI + lJ = IJ - 1$.

(4) The polynomial P_{ij} has the form

$$P_{ij}(x, z) = (-1)^{i+1} \left(\left(\frac{1}{i+1} \right)^{j+1} z^{i+1} - \left(\frac{1}{j+1} \right)^{i+1} x^{j+1} \right) + \sum \mu_{ab} x^a z^b$$

in case (1) and

$$P_{ij}(x, z) = (-1)^I \left(\left(\frac{2^{I-1}}{I} \right)^J z^I - \left(\frac{2^{J-1}}{J} \right)^I x^J \right) \sum \mu_{ab} x^a z^b$$

in the other cases. The two sums run over some couples (a, b) such that $a < j+1$ and $b < i+1$ in the first one, and $a < J$ and $b < I$ in the second one.

Proof. The proof is straightforward. The only point which may be obscure is that when $d = 1$ in (1), why there is no term $\lambda_{ab} x^a z^b$ such that

$$a(i+1) + b(j+1) = (i+1)(j+1) - 1?$$

Indeed formula (12) gives 0 for the computation of $pu_{n-1}v_m + qv_{m-1}u_n$. $\square$

3. Proof of Theorem 1

We recall the definition of Bernoulli's polynomials $B_k(t)$ and their links with the polynomials $\sigma_k(t)$. They are defined by

$$xe^{xt}/(e^x - 1) = \sum_{k \geq 0} B_k(t) x^k / k!$$

Bernoulli's numbers B_k are given by $B_k := B_k(0)$. We will use the following formula which relates $\sigma_k(t)$ to $B_k(t)$ (see [7, Chap. 18]):

$$(15) \quad \sigma_k(t) = (B_{k+1}(t+1) - B_{k+1}) / (k+1).$$

Before proving Theorem 1, we recall some definitions and also a result from [4].

Let K be a field and let $f(t)$ be a non-constant polynomial over K . A *functional decomposition* of $f(t)$ over K is a relation of the form $f(t) = g(h(t))$, where $g(t)$ and $h(t)$ are non-constant polynomials over K . This decomposition is called *non-trivial* if $\deg g \geq 2$ and $\deg h \geq 2$. If $f(t)$ has a non-trivial decomposition then we say that $f(t)$ is *decomposable* over K . In the opposite case, we say that $f(t)$ is *indecomposable* over K . Two decompositions

$$f(t) = g_1(h_1(t)) \quad \text{and} \quad f(t) = g_2(h_2(t))$$

are called *equivalent* if there exists a polynomial $l(t) \in K[t]$ of degree 1 such that

$$g_2(t) = g_1(l(t)) \quad \text{and} \quad h_1(t) = l(h_2(t)).$$

Two proofs of this result are given in [4].

Lemma 3. *If k is odd, then $B_k(t)$ is indecomposable over $\mathbb{C}$. If k is even, then any non-trivial decomposition of $B_k(t)$ over $\mathbb{C}$ is equivalent to the decomposition $B_k(t) = \overline{B}_k((t - 1/2)^2)$, where $\overline{B}_k(t)$ is a polynomial with rational coefficients of degree $k/2$, indecomposable over $\mathbb{C}$.*

Let k be an even integer. Then from formula (15) and the above lemma, we have

$$\begin{aligned} \sigma_k(t) &= (B_{k+1}(t+1) - B_{k+1})/(k+1) \\ &= (\overline{B}_{k+1}((t+1/2)^2) - B_{k+1})/(k+1) \\ &= (\overline{B}_{k+1}(t^2 + t + 1/4) - B_{k+1})/(k+1) \\ &= (\overline{B}_{k+1}(2\sigma_1(t) + 1/4) - B_{k+1})/(k+1) \\ &= l_1(\overline{B}_{k+1}(l_2(\sigma_1(t)))) , \end{aligned}$$

where $l_1(t) = (t - B_{k+1})/(k+1)$ and $l_2(t) = 2t + 1/4$.

Hence, $\sigma_k(t) = \overline{\sigma}_k(\sigma_1(t))$, where $\overline{\sigma}_k(t) = l_1(\overline{B}_{k+1}(l_2(t)))$. It follows (see the formulas in the introduction) that $\overline{\sigma}_k(t) = F_k(t)$ and we deduce easily the following.

Corollary 3. *If k is even, then $\sigma_k(t)$ is indecomposable. If k is odd, then $F_k(t)$ is indecomposable and any non-trivial decomposition of $\sigma_k(t)$ is equivalent to the decomposition $\sigma_k(t) = F_k(\sigma_1(t))$.*

Proof of Theorem 1. (1) Suppose that i (for example) is even. By Corollary 1,

$$\text{Res}_t(\sigma_i(t) - x, \sigma_j(t) - y) = \lambda[P(x, y)]^e,$$

where λ is a non-zero rational number, $P(x, y)$ is an irreducible polynomial over $\mathbb{Q}$ and $e = [\mathbb{Q}(t) : \mathbb{Q}(\sigma_i(t), \sigma_j(t))]$. Luroth's Theorem tells us that there exists $h(t) \in \mathbb{Q}(t)$ such that $\mathbb{Q}(\sigma_i(t), \sigma_j(t)) = \mathbb{Q}(h(t))$. Moreover since the field $\mathbb{Q}(\sigma_i(t), \sigma_j(t))$ contains polynomials, we may suppose that $h(t)$ is a polynomial; see [9, Th. 4, Chap. 1.2]. Let $\sigma_i(t) = g_i(h(t))$ and $\sigma_j(t) = g_j(h(t))$, where g_i and g_j are polynomials with rational coefficients. From Corollary 3 any functional decomposition of $\sigma_i(t)$ is trivial and the one of $\sigma_j(t)$ is trivial or equivalent to $\sigma_j(t) = F_j(\sigma_1(t))$, and this last possibility occurs only if j is odd.

Suppose first that both decompositions are trivial. Then $\deg g_i = \deg g_j = 1$ or $\deg h = 1$. In the first case we deduce that there exists $l(t) \in \mathbb{Q}[t]$, with $\deg l = 1$, such that $\sigma_j(t) = l(\sigma_i(t))$. Hence $i = j$, contradicting the assumptions. So we only have to consider the second case. Here we have $\mathbb{Q}(\sigma_i(t), \sigma_j(t)) = \mathbb{Q}(h(t)) = \mathbb{Q}(t)$, hence $e = [\mathbb{Q}(t) : \mathbb{Q}(\sigma_i(t), \sigma_j(t))] = 1$. Suppose now that the decomposition of σ_i is trivial and that of σ_j is equivalent to $\sigma_j(t) = F_j(\sigma_1(t))$. Then there exists $l(t) \in \mathbb{Q}[t]$, with $\deg l = 1$, such that $\sigma_j(t) = g_j(l(t))$ and $h(t) = l(\sigma_1(t))$. Thus $\deg h = 2$. We deduce that $\deg g_i = 1$ and $\sigma_i(t) = g_i(h(t)) = g_i(l(h(t)))$. Hence, $i = 1$, which contradicts our hypothesis.

(2) Suppose that i and j are odd. Let

$$\sigma_i(t) = F_i(\sigma_1(t)) \quad \text{and} \quad \sigma_j(t) = F_j(\sigma_1(t)),$$

where F_i and F_j are the Faulhaber's polynomials which are indecomposable by Corollary 3. As in part (1) there exists a polynomial $h(t) \in \mathbb{Q}[t]$ such that

$$\mathbb{Q}(F_i(t), F_j(t)) = \mathbb{Q}(h(t)).$$

Let $F_i(t) = g_i(h(t))$ and $F_j(t) = g_j(h(t))$. Then $\deg g_i = \deg g_j = 1$ or $\deg h = 1$. In the first case, there exists $l(t) \in \mathbb{Q}[t]$, with $\deg l = 1$, such that $F_j(t) = l(F_i(t))$, hence $i = j$ contradicting the hypothesis. In the second case,

$$\mathbb{Q}(F_i(t), F_j(t)) = \mathbb{Q}(h(t)) = \mathbb{Q}(t),$$

hence $e = [\mathbb{Q}(t) : \mathbb{Q}(F_i(t), F_j(t))] = 1$. It follows that $R_{ij}(x, y)$ is irreducible over $\mathbb{Q}$ and it is the minimal polynomial of $(F_i(t), F_j(t))$. It is also clear that this polynomial is the minimal polynomial of $(\sigma_i(t), \sigma_j(t))$. Corollary 1 then implies

$$\text{Res}_t(\sigma_i(t) - x, \sigma_j(t) - y) = \mu[R_{ij}(x, y)]^{e'},$$

where $\mu \in \mathbb{Q}$ and

$$e' = [\mathbb{Q}(t) : \mathbb{Q}(\sigma_i(t), \sigma_j(t))] = [\mathbb{Q}(t) : \mathbb{Q}(\sigma_1(t))] = 2.$$

□

4. Proof of Theorem 2 and Proposition 1

Dickson's polynomials are defined recursively by the formulas:

$$D_0(x, a) = 2, \quad D_1(x, a) = x, \quad \text{and} \quad D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a).$$

The explicit expression of these polynomials for $n \geq 1$ is given by [9]:

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i},$$

where $\lfloor n/2 \rfloor$ denotes the largest integer smaller or equal than $n/2$. The following result is a particular case of [9, Th. 10, Chap. 1.5].

Lemma 4. *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $n \geq 2$. Then the following conditions are equivalent:*

(1) *The polynomial $(f(x) - f(y)) / (x - y)$ is absolutely irreducible;*

(2) $f(x)$ is indecomposable over $\mathbb{Q}$, and if n is an odd prime number, we do not have $f(x) = \alpha D_n(x + b, a) + c$ for some $\alpha, a, b, c \in \mathbb{Q}$ with $a = 0$ if $n = 3$.

Corollary 4. Let j be an even integer, with $j \geq 2$, and let

$$\phi_j(x, y) = (\sigma_j(x) - \sigma_j(y)) / (x - y).$$

Then $\phi_j(x, y)$ is absolutely irreducible.

Proof. By the formulas given in the introduction, we have

$$\begin{aligned} (\sigma_2(x) - \sigma_2(y)) / (x - y) &= (x^2 + xy + y) / 3 + (x + y) / 2 + 1/6 \\ &= \frac{1}{3}x^2 + \left(\frac{1}{3}y + \frac{1}{2}\right)x + \frac{1}{3}y^2 + \frac{1}{2}y + \frac{1}{6}. \end{aligned}$$

The discriminant of this polynomial as a polynomial in x is given by

$$\Delta(y) = -\frac{1}{3}y^2 - \frac{1}{3}y + \frac{1}{36}$$

and it is clear that this is not a square. Hence, $\phi_2(x, y)$ is absolutely irreducible. Suppose that $j \geq 4$ and $\phi_j(x, y)$ is reducible over $\mathbb{C}$. Since $\sigma_j(x)$ is indecomposable (see Corollary 3), by the preceding lemma there exists a positive integer n and rational constants α, a, b, c such that $\sigma_j(x) = \alpha D_n(x + b, a) + c$. Comparing degrees on both sides gives $n = j + 1$. Moreover, identifying the coefficients of x^{j+1} , x^j , x^{j-1} , x^{j-2} and x^{j-3} successively and using formula (1) leads to the following equations:

$$\begin{cases} \alpha = \frac{1}{j+1}; \\ nb = \frac{1}{2}; \\ \alpha \left[\frac{n(n-1)}{2}b^2 - na \right] = \frac{j}{12}; \\ \frac{n(n-1)(n-2)}{6}b^3 - n(n-2)ab = 0; \\ \alpha \left[\frac{n(n-1)(n-2)(n-3)}{4!}b^4 - \frac{n(n-1)(n-2)}{2}ab^2 + \frac{n(n-3)}{2}a^2 \right] = \frac{-j(j-1)(j-2)}{720}. \end{cases}$$

Solving the first three equations gives $\alpha = 1/(j+1)$, $b = 1/2$ and $a = j/24$. The fourth equation is satisfied with these values of a and b . The fifth equation implies that $12j = 7$ which is impossible. Hence, $\phi_j(x, y)$ is absolutely irreducible. $\square$

Proof of Theorem 2. Let $T_{ijk}(x, z) = \text{Res}_y (P_{ij}(x, y), P_{jk}(y, z))$.

Step (1). Suppose that $T_{ijk}(x, z) = 0$. Then there exists $\beta \in \overline{\mathbb{Q}(x, z)}$ such that $P_{ij}(x, \beta) = P_{jk}(\beta, z) = 0$; hence $\beta \in \overline{\mathbb{Q}(x)} \cap \overline{\mathbb{Q}(z)} = \mathbb{Q}$, which is impossible (see Corollary 2).

Step (2). We show that $P_{ik}(x, z) \mid T_{ijk}(x, z)$. Since $P_{ik}(x, z)$ is the minimal polynomial of $(\sigma_i(t), \sigma_k(t))$, it is sufficient to prove that

$$\text{Res}_y (P_{ij}(\sigma_i(t), y), P_{jk}(y, \sigma_k(t))) = 0,$$

which is the case since $y = \sigma_j(t)$ is a common root of the polynomials for which we compute the resultant.

Step (3). We show that $S_{ik}(x, z) \mid T_{ijk}(x, z)$. Since $S_{ik}(x, z)$ is the minimal polynomial of $(\sigma_i(s), \sigma_k(t))$ along $\phi_j(s, t)$, it is sufficient to prove that

$$\text{Res}_y(P_{ij}(\sigma_i(S), y), P_{jk}(y, \sigma_k(T))) = 0,$$

where S, T are transcendental elements satisfying $\phi_j(S, T) = 0$. But this is true since $y = \sigma_j(S) = \sigma_j(T)$ is a common root of the polynomials appearing in the resultant.

Step (4). For any polynomial $g(x, z) \in \mathbb{C}[x, z]$, we denote by $V(g)$ the zero set of g in $\mathbb{C}^2$. Let (x_0, z_0) be an element of $V(T_{ijk})$. Then $\text{Res}_y(P_{ij}(x_0, y), P_{jk}(y, z_0))$ is zero. Since $P_{ij}(x, y)$ and $P_{jk}(y, z)$, viewed as polynomials in y , have constant leading coefficients, there exists $y_0 \in \mathbb{C}$ such that $P_{ij}(x_0, y_0) = P_{jk}(y_0, z_0) = 0$. Thus, there exists $(s_0, t_0) \in \mathbb{C}^2$ such that $x_0 = \sigma_i(s_0)$, $y_0 = \sigma_j(s_0)$, $y_0 = \sigma_j(t_0)$, and $z_0 = \sigma_k(t_0)$. If $s_0 = t_0$, then $(x_0, y_0) \in V(P_{ik})$. If $s_0 \neq t_0$, then $(x_0, y_0) \in V(S_{ik})$. It follows that $V(T_{ijk}) \subset V(P_{ik}) \cup V(S_{ik})$. Set

$$T_{ijk}(x, z) = P_{ik}(x, z)^{e_1} S_{ik}(x, z)^{e_2} \prod_{l \in L} R_l(x, z)^{e_l},$$

where L is a finite set that may be empty and $R_l(x, z)$ is an irreducible polynomial for each l . It is known that the decomposition of $V(T_{ijk})$ into its irreducible components is given by $V(T_{ijk}) = V(P_{ik}) \cup V(S_{ik}) \cup_{l \in L} V(R_l)$. Hence, $V(R_l) = \emptyset$ and $T_{ijk}(x, z) = P_{ik}(x, z)^{e_1} S_{ik}(x, z)^{e_2}$. $\square$

Proof of Proposition 1. For polynomials $g(x, z)$ and $h(x, z)$, we write $g(x, z) \sim h(x, z)$ to mean that these polynomials are equal up to multiplication by a non-zero constant. We first claim without proof that

$$P_{ik}(x, z) \sim S_{ik}(x, z) \quad \text{if and only if} \quad \sigma_j(x) - \sigma_j(y) \mid P_{ik}(\sigma_i(x), \sigma_k(z)).$$

Suppose by contradiction that $P_{ik}(x, z) \sim S_{ik}(x, z)$, then the (usual) leading form of $\sigma_j(x) - \sigma_j(z)$ divides the leading form of $P_{ik}(\sigma_i(x), \sigma_k(z))$. The leading form of the first one is $\sim x^{j+1} - z^{j+1}$. The leading form for the second one is

$$\sim \begin{cases} x^{(i+1)(k+1)/d} - z^{(i+1)(k+1)/d} & \text{if } i \text{ or } k \text{ is even,} \\ x^{(i+1)(k+1)/2d} - z^{(i+1)(k+1)/2d} & \text{if } i \text{ and } k \text{ are odd,} \end{cases}$$

where $d = (i+1, k+1)$ or $d = ((i+1)/2, (k+1)/2)$ (see Corollary 2). It follows that $j+1 \mid (i+1)(k+1)/d$ in the first case and $j+1 \mid (i+1)(k+1)/(2d)$ in the second one. Hence, $j+1 \mid \text{lcm}(i+1, k+1)$ which contradicts our assumptions. $\square$

Acknowledgements. The author thanks the referee for suggesting corrections.

REFERENCES

- [1] S. S. Abhyankar and L. A. Rubel, *Every difference polynomial has a connected zero-set*, J. Indian Math. Soc. **43** (1979), no. 1-4, 69–78 (1980).
- [2] M. Ayad, *Irreducibility of $f(u(x), v(y))$* , J. Algebra **279** (2004), no. 1, 302–307.
- [3] A. F. Beardon, *Sums of powers of integers*, Amer. Math. Monthly **103** (1996), no. 3, 201–213.

- [4] Yu. F. Bilu, B. Brindza, P. Kirschenhofer, A. Pintér and R. Tichy, *Diophantine equations and Bernoulli polynomials*, Compositio Math. **131** (2002), no. 2, 173–188.
- [5] A. Dahan-Dalmedico and J. Peiffer, *Une histoire des mathématiques ; routes et dédales*, Points Sciences, (1986).
- [6] J. H. McKay and S. S. Wang, *An inversion formula for two polynomials in two variables*, J. Pure Appl. Algebra **40** (1986), no. 3, 245–257.
- [7] P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001. xxiv+681 pp.
- [8] L. A. Rubel, A. Schinzel, H. Tverberg, *On difference polynomials and hereditarily irreducible polynomials*, J. Number Theory **12** (1980), no. 2, 230–235.
- [9] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge University Press, Cambridge, 2000. x+558 pp.

M. AYAD, U. DU LITTORAL CÔTE D’OPALE, 50 RUE F. BUISSON, F-62228 CALAIS CEDEX, FRANCE
ayad@lmpa.univ-littoral.fr