Resultant of an equivariant polynomial system with respect to the symmetric group

Laurent Busé, Anna Karasoulou

RESULTANT OF AN EQUIVARIANT POLYNOMIAL SYSTEM WITH RESPECT TO THE SYMMETRIC GROUP

LAURENT BUSÉ AND ANNA KARASOULOU

Abstract. Given a system of $n \geqslant 2$ homogeneous polynomials in n variables which is equivariant with respect to the symmetric group of n symbols, it is proved that its resultant can be decomposed into a product of several resultants that are given in terms of some divided differences. As an application, we obtain a decomposition formula for the discriminant of a multivariate homogeneous symmetric polynomial.

1. Introduction

The analysis and solving of polynomial systems are fundamental problems in computational algebra. In many applications, polynomial systems tend to have structures and it is very useful to develop special methods in order to take them into account. In this paper, we will focus on systems of n homogeneous polynomials $f_1, \ldots, f_n$ in n variables $x_1, \ldots, x_n$ that are globally invariant under the action of the symmetric group $\mathfrak{S}_n$ of n symbols. More precisely, we will assume that for any integer $i \in \{1, 2, \ldots, n\}$ and any permutation $\sigma \in \mathfrak{S}_n$

$$\sigma(f_i) := f_i(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f_{\sigma(i)}(x_1, x_2, \ldots, x_n).$$

In the language of invariant theory these systems are called equivariant with respect to the symmetric group $\mathfrak{S}_n$, or simply $\mathfrak{S}_n$-equivariant (see for instance [13, §4] or [5, Chapter 1]). Some recent interesting developments based on Gröbner basis techniques of this kind of systems can be found in [6] where the objective is to compute the roots whose coordinates are all distinct. In this paper, we will study the resultant of $\mathfrak{S}_n$-equivariant homogeneous polynomial systems in order to reveal their structure.

There are special cases for which a decomposition of the resultant of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system is known. In the case $n = 2$, any $\mathfrak{S}_2$-equivariant homogeneous polynomial system is of the form

$$F^{\{1\}}(x_1, x_2) := a_0 x_1^d + a_1 x_1^{d-1} x_2 + \cdots + a_d x_2^d, \quad F^{\{2\}}(x_1, x_2) := F^{\{1\}}(x_2, x_1)$$

and one can show [1, Exercice 67] that there exists an irreducible polynomial $K_d \in \mathbb{Z}[a_0, \ldots, a_d]$ such that

$$\operatorname{Res}\left(F^{\{1\}}, F^{\{2\}}\right) = F^{\{1\}}(1,1)F^{\{1\}}(1,-1)K_d^2 = \left(\sum_{i=0}^{d} a_i\right)\left(\sum_{i=0}^{d} (-1)^i a_i\right) K_d^2.$$

As another example, suppose $n \geqslant 2$, $d = 1$ and set $F^{\{i\}}(x_1, \ldots, x_n) = a x_i + b e_1(x_1, \ldots, x_n)$, $i = 1, \ldots, n$. Then, since the resultant of n linear forms in n variables is the determinant of the matrix of their associated linear system, it is a straightforward computation to show that

$$\operatorname{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = a^{n-1}(a + nb).$$

The main result of this paper (Theorem 1) is to prove a general decomposition formula of the resultant of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system. This decomposition is given in terms of other resultants that are in principle easier to compute and that are expressed in terms

of the divided differences of the input polynomial system. We emphasize that the multiplicity of each factor appearing in this decomposition is also given. The appearance of divided differences is not new in the context of $\mathfrak{S}_n$-equivariant polynomial systems since they allow to produce some invariants in a natural way (e.g. [6, 11]). Another important point is that this formula is universal, that is to say that it remains valid (in particular it still has the correct geometric meaning) under any specialization of the coefficient ring of the input polynomial system. This kind of property is particularly important for applications in the fields of number theory and arithmetic geometry where the value of the resultant is as important as its vanishing.

The discriminant of a homogeneous polynomial is also a fundamental tool in the field of computer algebra. Although the discriminant of the generic homogeneous polynomial of a given degree is irreducible, for some class of polynomials it can be decomposed and this decomposition is always deeply connected to the geometric properties of this class of polynomials. The second main contribution of this paper is a decomposition of the discriminant of a homogeneous symmetric polynomial (Theorem 2). The work on this result was motivated by the unpublished note [11] by N. Perminov and S. Shakirov where a tentative formula is given without a complete proof. We emphasize that the discriminant formula is obtained as a byproduct of our first formula on the resultant of a $\mathfrak{S}_n$-equivariant polynomial system. Therefore, it inherits the same features : it allows to split the discriminant into several resultants with multiplicities and it is universal.

The paper is organized as follows. In Section 2 we state the main result of this paper, namely a decomposition formula of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system, and we also introduce the notions and notations that are needed (divided differences and partitions). The proof of this decomposition formula is provided in Section 4. The decomposition formula of the discriminant of a homogeneous symmetric polynomial is proved and discussed in Section 3.

2. The main result

In order to describe our main result, we first need to introduce some notations on divided differences and partitions. Hereafter, R denotes an arbitrary commutative ring. In addition, for any integer p the set $\{1, 2, \dots, p\}$ will be denoted by $[p]$ and given a finite set I, $|I|$ will stand for its cardinality.

2.1. **Notations.**

2.1.1. *Divided differences.* Let $P_1, ..., P_n$ be n homogeneous polynomials in $R[x_1, \dots, x_n]$ of the same degree $d > 1$. Their divided differences are recursively defined by $P^{\{i\}} := P_i$ for all $i = 1, \dots, n$ and

$$P^{\{i_1,\dots,i_k\}} := \frac{P^{\{i_1,\dots,i_{k-1}\}} - P^{\{i_1,\dots,i_{k-2},i_k\}}}{x_{i_{k-1}} - x_{i_k}}$$

for any given set of (distinct) integers $I := \{i_1, \dots, i_k\} \subset [n]$. It is well known that P^I depends on the set I and not on the order of the integers $i_1, \dots, i_k$ (for instance, as a consequence of the Newton's interpolation formula). Another important property is the following : if P^I are polynomials for all I such that $|I| = 2$, that is to say if

$$x_i - x_j \text{ divides } P^{\{i\}} - P^{\{j\}} \text{ for all } i, j \in [n], \tag{1}$$

then P^I are polynomials for all $I \subset [n]$. Indeed, for any $J \subset [n]$ and any triple of distinct integers i, j, k such that $J \cap \{i, j, k\} = \emptyset$, a straightforward application of the definition of divided differences yields the equality

$$(x_i - x_j)P^{J\cup\{i,j\}} - (x_i - x_k)P^{J\cup\{i,k\}} + (x_j - x_k)P^{J\cup\{j,k\}} = 0$$

which can be rewritten as

$$(x_i - x_k)\left(P^{J\cup\{i,j\}} - P^{J\cup\{i,k\}}\right) = (x_j - x_k)\left(P^{J\cup\{i,j\}} - P^{J\cup\{j,k\}}\right).$$

From here the claimed property follows by induction on $|I|$. In addition, we observe that P^I is an homogeneous polynomial of degree $d - |I| + 1$. In particular, $P^I = 0$ if $d + 1 < |I| \leqslant n$ and $P^I = P^J$ for all subsets I and J of $[n]$ such that $|I| = |J| = d + 1 \leqslant n$.

Example 2.1. Any polynomial system of three linear homogeneous polynomials in 3 variables satisfying (1) is of the form

$$\left\{\begin{array}{lcl} P^{\{1\}} & = & (a+d)x_1 + bx_2 + cx_3 \\ P^{\{2\}} & = & ax_1 + (b+d)x_2 + cx_3 \\ P^{\{3\}} & = & ax_1 + bx_2 + (c+d)x_3 \end{array}\right.$$

and straightforward computations show that $P^{\{1,2\}} = P^{\{1,3\}} = P^{\{2,3\}} = d$ and $P^{\{1,2,3\}} = 0$. □

2.1.2. *Partitions.* A partition is a sequence of weakly decreasing positive integers which is often written as $\lambda = (\lambda_1, \ldots, \lambda_k)$. The number k is called the length of λ and will be denoted by $l(\lambda)$. When $\sum_{i=1}^{k} \lambda_i = n$ we will say such a λ is a partition of n and write $\lambda \vdash n$.

Given a partition $\lambda \vdash n$, its associated multinomial coefficient is defined as the integer

$$\binom{n}{\lambda_1, \lambda_2, \ \ldots, \lambda_{l(\lambda)}} := \frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_{l(\lambda)}!}. \tag{2}$$

It counts the number of distributions of n distinct objects to $l(\lambda)$ distinct recipients such that the recipient i receives exactly λ_i objects. In this counting, the objects are not ordered inside the boxes, but the boxes are ordered. To avoid the count of the permutations between the boxes having the same number of objects we have to divide (2) by the number of all these permutations. If s_j denotes the number of boxes having exactly j objects, $j \in [n]$, then this number of permutations is equal to $\prod_{j=1}^{n} s_j!$. Thus, for any partition $\lambda \vdash n$ we define the integer

$$m_\lambda := \frac{1}{\prod_{j=1}^{n} s_j!}\binom{n}{\lambda_1, \lambda_2, \ \ldots, \lambda_{l(\lambda)}}. \tag{3}$$

2.1.3. $\mathfrak{S}_n$*-equivariant polynomial systems.* Consider a polynomial system of n homogeneous polynomials $F^{\{1\}}, \ldots, F^{\{n\}} \in R[x_1, \ldots, x_n]$ of the same degree $d \geqslant 1$ and assume that it is $\mathfrak{S}_n$-equivariant, that is to say that for any integer $i \in \{1, 2, \ldots, n\}$ and any permutation $\sigma \in \mathfrak{S}_n$

$$\sigma(F^{\{i\}}) := F^{\{i\}}(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = F^{\{\sigma(i)\}}(x_1, x_2, \ldots, x_n). \tag{4}$$

Equivalently, this means that for all $i = 1, \ldots, n$

$$F^{\{i\}}(x_1, \ldots, x_n) = \sum_{l=0}^{d} x_i^l S_l(x_1, \ldots, x_n)$$

where S_l is a symmetric homogeneous polynomials in $R[x_1, \ldots, x_n]$ of degree $d - l$ for all $l = 0, \ldots, d$. Suppose given in addition a partition $\lambda \vdash n$ and consider the morphism of polynomial algebras

$$\begin{array}{rcl} \rho_\lambda : R[x_1, \ldots, x_n] & \to & R[y_1, \ldots, y_{l(\lambda)}] \\ F(x_1, \ldots, x_n) & \mapsto & F(\underbrace{y_1, \ldots, y_1}_{\lambda_1}, \underbrace{y_2, \ldots, y_2}_{\lambda_2}, \ldots, \underbrace{y_{l(\lambda)}, \ldots, y_{l(\lambda)}}_{\lambda_{l(\lambda)}}) \end{array}$$

where $y_1, y_2, \ldots, y_{l(\lambda)}$ are new indeterminates. Since the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ satisfy (4), they also satisfy (1) (but this is not equivalent as shown in Example 2.1) and hence their

divided differences F^I, $I \subset [n]$, are also polynomials. Moreover, it is easy to check that for any subset $\{i_1, \dots, i_k\} \subset [n]$ and any permutation $\sigma \in \mathfrak{S}_n$

$$\sigma\left(F^{\{i_1,\dots,i_k\}}\right) = F^{\{\sigma(i_1),\dots,\sigma(i_k)\}}. \tag{5}$$

Now, observe that if $\rho_\lambda(x_i) = \rho_\lambda(x_j)$ then $\rho_\lambda(F^{\{i\}}) = \rho_\lambda(F^{\{j\}})$, so for any integer $i \in [l(\lambda)]$ we can define without ambiguity the homogeneous polynomial of degree d

$$F_\lambda^{\{i\}}(y_1, y_2, \dots, y_{l(\lambda)}) := \rho_\lambda\left(F^{\{j\}}(x_1, \dots, x_n)\right)$$

where $j \in [n]$ is such that $\rho_\lambda(x_j) = y_i$. Moreover, these polynomials also satisfy (1) and hence their divided differences are also polynomials; we will denote them by $F_\lambda^I(y_1, \dots, y_{l(\lambda)})$, where $I \subset [l(\lambda)]$. Moreover, we have the following 'lifting" property : Given $I = \{i_1, \dots, i_k\} \subset [n]$, define $J = \{j_1, \dots, j_k\} \subset [l(\lambda)]$ by the equality $\rho_\lambda(x_{i_r}) = y_{j_r}$ for all $r \in [k]$. Then, if $|J| = |I|$ we have that

$$\rho_\lambda(F^I(x_1, \dots, x_n)) = F_\lambda^J(y_1, \dots, y_{l(\lambda)}).$$

2.2. **The decomposition formula.** We are now ready to state the main result of this paper, namely a decomposition of the multivariate resultant of a $\mathfrak{S}_n$-equivariant system of homogeneous polynomials of the same degree.

Theorem 1. *Assume $n \geqslant 2$ and suppose given a $\mathfrak{S}_n$-equivariant system of homogeneous polynomials $F^{\{1\}}, \dots, F^{\{n\}} \in R[x_1, \dots, x_n]$ of the same degree $d \geqslant 1$. Then, we have that*

$$\operatorname{Res}\left(F^{\{1\}}, \dots, F^{\{n\}}\right) = R_0 \times \prod_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} \operatorname{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right)^{m_\lambda}$$

where $R_0 = 1$ if $d \geqslant n$ and $R_0 = \left(F^{\{1,\dots,d+1\}}\right)^{m_0}$ if $d < n$. In this latter case, the integer m_0 is defined by

$$m_0 = nd^{n-1} - \sum_{k=1}^{d} A_{n,k} B_{d,k}$$

where

$$A_{n,k} := \sum_{\substack{\lambda \vdash n \\ l(\lambda) = k}} m_\lambda, \quad B_{d,k} := e_{k-1}(d, d-1, d-2, \dots, d-k+1)$$

and where e_{k-1} stands for the $(k-1)$-th elementary symmetric polynomial in k variables.

Before giving the proof of this theorem which is postponed at the end of the paper, in Section 4, we make observations on some computational aspects of this theorem. First, we emphasize that the above formula is *universal*, meaning that it holds in the ring of coefficients of the polynomials system $F^{\{1\}}, \dots, F^{\{n\}}$ over $\mathbb{Z}$ and that it remains valid under any specialization of these coefficients. For that purpose, we use the formalism of the resultant as developed in [8] (see also [9, Chapter IX] and [3, Chapter 3]), in particular the resultant is normalized by setting $\operatorname{Res}(x_1, \dots, x_n) = 1$. Besides that, we will also use many computation rules and properties of the resultant in the proof of Theorem 1.

The number of resultant factors appearing in the decomposition formula is in relation with the cardinality of the set of partitions of n. This quantity has been extensively studied and we refer the interested reader to the classical book [10]. These resultant factors can be computed separately, for instance by means of the Macaulay formula, but the situation is even better : all these factors can be deduced from a very small number of resultant computations since they are actually universal with respect to the integers $\lambda_1, \lambda_2, \dots, \lambda_{l(\lambda)}$ defining a partition, providing

$l(\lambda)$ is fixed. As a consequence, all the resultant factors appearing in the decomposition formula given in Theorem 1 can be obtained as specializations of only $\min\{n, d\}$ resultant computations. The following example illustrates this property.

Example 2.2. Consider the polynomials

$$F^{\{i\}}(x_1, \ldots, x_n) = ax_i^2 + bx_i e_1(x_1, \ldots, x_n) + ce_1(x_1, \ldots, x_n)^2 + de_2(x_1, \ldots, x_n), \quad i = 1, \ldots, n.$$

The partition $\lambda = (n)$ yields the factor

$$\mathrm{Res}\left(F_\lambda^{\{1\}}\right) = a + nb + n^2c + \binom{n}{2}d$$

with multiplicity $m_\lambda = 1$. From Theorem 1 we know that the other factors come from the partitions of length 2. They are of the form $\lambda = (m, n-m)$ with $n-1 \geqslant m \geqslant n-m \geqslant 1$. The divided difference $F^{\{1,2\}}$ is equal to $a(x_1 + x_2) + be_1$ and we have

$$\rho_\lambda(e_1) = mx_1 + (n-m)x_2, \quad \rho_\lambda(e_2) = \binom{m}{2}x_1^2 + m(n-m)x_1x_2 + \binom{n-m}{2}x_2,$$

$$F_\lambda^{\{1,2\}} = \rho_\lambda\left(F^{\{1,2\}}\right) = a(x_1 + x_2) + b\rho_\lambda(e_1) = a(x_1 + x_2) + b(mx_1 + (n-m)x_2).$$

Therefore, such a partition $\lambda = (m, n-m)$ yields the factor

(6)

$$\begin{aligned}\mathrm{Res}\left(F^{\{1\}}_{(m,n-m)}, F^{\{1,2\}}_{(m,n-m)}\right) = {} & ab^2nm + 2\,dm^2ab - 1/2\,dmb^2n^2 + 1/2\,dm^2b^2n - 2\,dmna^2 - 4\,cmna^2 \\ & - 2\,dmabn + 1/2\,dn^2a^2 + 2\,dm^2a^2 + a^2bn - 1/2\,dna^2 + cn^2a^2 + 4\,cm^2a^2 - ab^2m^2 + a^3\end{aligned}$$

which is computed as the determinant of a 3×3 Sylvester matrix. To summarize, if $n = 2$ (and $d = 2$) we get

$$\mathrm{Res}(F^{\{1\}}, F^{\{2\}}) \;=\; \mathrm{Res}\left(F^{\{1\}}_{(2)}\right)\mathrm{Res}\left(F^{\{1\}}_{(1,1)}, F^{\{1,2\}}_{(1,1)}\right) \;=\; (a + 2b + 4c + d)\,(a+b)^2\,(a-d)$$

where $\mathrm{Res}\left(F^{\{1\}}_{(1,1)}, F^{\{1,2\}}_{(1,1)}\right)$ is obtained by specialization of (6). If $n > 2$ (and $d = 2$) then it is easy to check that $F^{\{1,2,3\}} = a$. Therefore, if $n = 2k+1$, k being a positive integer, then

$$\mathrm{Res}(F^{\{1\}}, F^{\{2\}}) = (a)^{m_0}\left(a + nb + n^2c + \binom{n}{2}d\right)\prod_{m=k+1}^{n-1}\mathrm{Res}\left(F^{\{1\}}_{(m,n-m)}, F^{\{1,2\}}_{(m,n-m)}\right)^{\frac{n!}{m!(n-m)!}}$$

where the resultants in this formula are again given by (6) and

$$m_0 = n2^{n-1} - 1 - 3\sum_{m=k+1}^{n-1}\frac{n!}{m!(n-m)!}$$

(for $B_{2,1} = 1$, $B_{2,2} = 3$, $A_{n,1} = 1$ and $A_{n,2} = \sum_{m=k+1}^{n-1}\frac{n!}{m!(n-m)!}$). If $n = 2k$ with $k > 1$ then

$$\begin{aligned}\mathrm{Res}(F^{\{1\}}, F^{\{2\}}) = (a)^{m_0}\left(a + nb + n^2c + \binom{n}{2}d\right)\mathrm{Res}\left(F^{\{1\}}_{(k,k)}, F^{\{1,2\}}_{(k,k)}\right)^{\frac{1}{2}\frac{n!}{(k!)^2}} \times \\ \prod_{m=k+1}^{n-1}\mathrm{Res}\left(F^{\{1\}}_{(m,n-m)}, F^{\{1,2\}}_{(m,n-m)}\right)^{\frac{n!}{m!(n-m)!}}\end{aligned}$$

where the resultants in this formula are always given by (6) and

$$m_0 = n2^{n-1} - 1 - \frac{3}{2}\frac{n!}{(k!)^2} - 3\sum_{m=k+1}^{n-1}\frac{n!}{m!(n-m)!}.$$

Before closing this example, we emphasize that the resultants appearing in Theorem 1 are not always irreducible polynomials. For instance, in the case where $n = 2k$ we have that

$$\text{Res}\left(F^{\{1\}}_{(k,k)}, F^{\{1,2\}}_{(k,k)}\right) = (a+bk)^2(a-dk). \tag{7}$$

However, we notice that $\text{Res}(F^{\{1\}}_{\lambda})$ is obviously always irreducible. □

From a geometric point of view, Theorem 1 shows that the solutions of the algebraic polynomial system

$$\{F^{\{1\}} = 0, \ldots, F^{\{n\}} = 0\} \tag{8}$$

can be decomposed into several components that correspond to the algebraic systems

$$\{F^{\{1\}}_{\lambda} = 0, \ldots, F^{\{1,\ldots,l(\lambda)\}}_{\lambda} = 0\},\ \lambda \vdash n,\ l(\lambda) \leqslant d.$$

Each component has multiplicity m_λ and it corresponds to a particular configuration of the roots of the initial system, namely the roots whose coordinates can be grouped, up to permutations, into $l(\lambda)$ blocks of identical value and of size $\lambda_1, \ldots, \lambda_{l(\lambda)}$ respectively.

The component corresponding to the partition $\lambda = (1, \ldots, 1)$ is interesting for some applications as it corresponds to solutions of (8) whose coordinates are all distinct (e.g. [6]). A usual trick for dealing with this component is to sum up all the divided differences of the same order to get symmetric polynomials. More precisely, since the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ satisfy the property (5), for any integer $k \in [n]$ the polynomials

$$\sum_{I\subset[n],\,|I|=k} F^I = \sum_{I\subset[n],\,|I|=k} F^{\sigma(I)} = \sum_{I\subset[n],\,|I|=k} \sigma(F^I) = \sigma\left(\sum_{I\subset[n],\,|I|=k} F^I\right)$$

are symmetric (i.e. invariant under the action of $\mathfrak{S}_n$). As such, they can be rewritten by using the elementary symmetric polynomials and the number of roots of the component corresponding to $\lambda = (1, \ldots, 1)$ is hence reduced by a factor $n!$. In general, the above property is no longer true if we consider F^I_λ instead of F^I, $\lambda \neq (1, 1, \ldots, 1)$. Nevertheless, it is possible to reformulate Theorem 1 by means of these sums of divided differences of the same order.

Proposition 2.3. *Using the notation of Theorem 1, let λ be a partition of n such that $l(\lambda) \leqslant d$ and for all integer $k \in [l(\lambda)]$ define the polynomial*

$$\mathcal{F}^{(k)}_\lambda := \frac{1}{\binom{l(\lambda)}{k}} \sum_{I\subset[l(\lambda)],\,|I|=k} F^I_\lambda$$

(assuming that the coefficient ring contains the rational numbers). Then, we have that

$$\text{Res}\left(F^{\{1\}}_\lambda, F^{\{1,2\}}_\lambda, \ldots, F^{\{1,2,\ldots,l(\lambda)-1\}}_\lambda, F^{\{1,2,\ldots,l(\lambda)\}}_\lambda\right) = \text{Res}\left(\mathcal{F}^{(1)}_\lambda, \mathcal{F}^{(2)}_\lambda, \ldots, \mathcal{F}^{(l(\lambda))}_\lambda\right).$$

Proof. First, we claim that for any subset $I \subset [l(\lambda)]$ such that $|I| = l(\lambda) - 1$ then

$$F^I_\lambda = F^{\{1,2,\ldots,l(\lambda)-1\}}_\lambda \mod \left(F^{\{1,2,\ldots,l(\lambda)\}}_\lambda\right). \tag{9}$$

This is a consequence of the technical Lemma 2.4 which is given after the proof of this proposition. From (9) we deduce that

$$\sum_{I\subset[l(\lambda)],\,|I|=l(\lambda)-1} F^I_\lambda = l(\lambda)\, F^{\{1,2,\ldots,l(\lambda)-1\}}_\lambda \mod \left(F^{\{1,2,\ldots,l(\lambda)\}}_\lambda\right).$$

In the same way, for any subset $I \subset [l(\lambda)]$ such that $|I| = l(\lambda) - 2$, Lemma 2.4 shows that

$$F^I_\lambda = F^{\{1,2,\ldots,l(\lambda)-2\}}_\lambda \mod \left(\left\{F^I_\lambda\right\}_{|I|=l(\lambda)-1}, F^{\{1,2,\ldots,l(\lambda)\}}_\lambda\right).$$

Using (9), this equality can be simplified to give

$$F_\lambda^I = F_\lambda^{\{1,2,\dots,l(\lambda)-2\}} \mod \left(F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right).$$

We deduce that

$$\sum_{I\subset[l(\lambda)],\,|I|=l(\lambda)-2} F_\lambda^I = \binom{l(\lambda)}{2} F_\lambda^{\{1,2,\dots,l(\lambda)-2\}} \mod \left(F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right).$$

By applying iteratively this method, we obtain for all $k = 1, \dots, l(\lambda)-1$ the equality

$$\sum_{I\subset[l(\lambda)],\,|I|=l(\lambda)-k} F_\lambda^I = \binom{l(\lambda)}{k} F_\lambda^{\{1,2,\dots,l(\lambda)-k\}} \mod \left(F_\lambda^{\{1,2,\dots,l(\lambda)-k+1\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right).$$

From these equalities, the invariance of the resultant under elementary transformations yields the claimed result (proceed from the right to the left). □

Lemma 2.4. *Using the notation of Section 2.1.1, let I and J be two subsets of $[n]$ of the same cardinality r with $1 \leqslant r \leqslant n-1$. Then, the polynomial $P^I - P^J$ belongs to the ideal of polynomials generated by the $(r+1)^{\text{th}}$ divided differences, i.e.*

$$P^I - P^J \in (\dots, P^K, \dots)_{K\subset[n],|K|=r+1}.$$

Proof. If $|I \cap J| = r-1$ then $P^I - P^J$ is a multiple of a divided difference P^K with $|K| = r+1$ by definition of divided differences (by choosing the appropriate order for the elements of I and J). Otherwise, $r \geqslant 2$, $|I \cap J| < r-1$ and hence there exist $j \in J \setminus I$ and $i \in I \setminus J$ (observe that $i \neq j$ necessarily). Now,

$$P^I - P^J = P^I - P^{(I\setminus\{i\})\cup\{j\}} + P^{(I\setminus\{i\})\cup\{j\}} - P^J$$

where the term $P^I - P^{(I\setminus\{i\})\cup\{j\}}$ is a multiple of a divided difference P^K with $|K| = r+1$ since $|I \cap ((I\setminus\{i\})\cup\{j\}))| = r-1$. So, to prove that $P^I - P^J$ belongs to the ideal generated by the $(r+1)^{\text{th}}$ divided differences amounts to prove that $P^{(I\setminus\{i\})\cup\{j\}} - P^J$ belongs to this ideal. But notice that $|J \cap ((I\setminus\{i\})\cup\{j\})| = |I\cap J|+1$. Therefore, one can repeat this operation to reach a cardinality of $r-1$ and from there the conclusion follows. □

3. Discriminant of a homogeneous symmetric polynomial

The discriminant of a homogeneous polynomial is a rather complicated object which is known to be irreducible as a polynomial in the coefficients of the input polynomial (see for instance [2, §4] and [4, 7]). In this section, we will show that it decomposes if the homogeneous polynomial is assumed to be symmetric. We will actually provide a decomposition formula (Theorem 2) that we will obtain as a particular case of our main result (Theorem 1).

Fix a positive integer $n \geqslant 2$. For any integer p we will denote by $e_p(x_1, \dots, x_n)$ the p^{th} elementary symmetric polynomial in the variables $x_1, \dots, x_n$. They satisfy the equality

$$\sum_{p\geqslant 0} e_p(x)t^p = \prod_{i=1}^{n}(1+x_it)$$

(observe that $e_0(x) = 1$ and that $e_p(x) = 0$ for all $p > n$). For any partition $\lambda = (\lambda_1 \geqslant \dots \geqslant \lambda_k)$ we also define the polynomial

$$e_\lambda(x) := e_{\lambda_1}(x)e_{\lambda_2}(x)\cdots e_{\lambda_k}(x) \in \mathbb{Z}[x_1, \dots, x_n].$$

Given a positive integer d, it is well known that the set

$$\{e_\lambda(x) \ : \ \lambda = (\lambda_1, \dots, \lambda_k) \vdash d \text{ such that } n \geqslant \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k\} \tag{10}$$

is a basis (over $\mathbb{Z}$) of the homogeneous symmetric polynomials of degree d in n variables. In other words, any homogeneous symmetric polynomial of degree d with coefficients in a commutative ring is obtained as specialization of the generic homogeneous symmetric polynomial of degree d

$$F(x_1,\dots,x_n) := \sum_{\lambda\vdash d} c_\lambda e_\lambda(x) \in \mathbb{Z}[c_\lambda : \lambda \vdash d][x_1,\dots,x_n]. \tag{11}$$

We will denote by $\mathbb{U}$ its universal ring of coefficients $\mathbb{Z}[c_\lambda : \lambda \vdash d]$. In addition, for all $i \in \{1,\dots,n\}$, we will denote the partial derivatives of F by

$$F^{\{i\}}(x_1,\dots,x_n) := \frac{\partial F}{\partial x_i}(x_1,\dots,x_n) \in \mathbb{U}[x_1,\dots,x_n]_{d-1}.$$

Finally, we recall that the discriminant of F, denoted $\mathrm{Disc}(F)$, is defined by the equality

$$d^{a(n,d)}\mathrm{Disc}(F) = \mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}\right) \in \mathbb{U} \tag{12}$$

where

$$a(n,d) := \frac{(d-1)^n - (-1)^n}{d} \in \mathbb{Z}.$$

It is an homogeneous polynomial of degree $n(d-1)^{n-1}$ in $\mathbb{U}$. The integer factor $d^{a(n,d)}$ is important to ensure that the discriminant $\mathrm{Disc}(F)$ yields the expected smoothness criterion under any specialization (especially in coefficient rings having nonzero characteristic), namely : Let S be an algebraically closed field and g be a nonzero homogeneous polynomial in $S[x_1,\dots,x_n]$, then $\mathrm{Disc}(g) = 0$ if and only if the hypersurface defined by the polynomial g in the projective space $\mathbb{P}^{n-1}_S$ is singular. For a detailed study of the discriminant and its numerous properties, mostly inherited from the ones of the resultant, we refer the reader to [2, 4, 7] and the references therein.

Lemma 3.1. *The partial derivatives $F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}$ of the symmetric polynomial F form a $\mathfrak{S}_n$-equivariant system of homogeneous polynomials of degree $d-1$.*

Proof. Since F is a polynomial in the elementary symmetric polynomials, the chain rule formula for the derivation of composed functions shows that there exist $\min\{d,n\}$ homogeneous symmetric polynomials $S_k(x_1,\dots,x_n)$ such that for all $i = 1,\dots,n$

$$F^{\{i\}} = \frac{\partial F}{\partial x_i} = \sum_{k=1}^{\min\{d,n\}} \frac{\partial e_k}{\partial x_i} S_k(x_1,\dots,x_n). \tag{13}$$

Moreover, for any pair of integers i, j we have

$$\frac{\partial e_j}{\partial x_i} = \sum_{r=0}^{j-1} (-1)^r x_i^r e_{j-1-r}. \tag{14}$$

Therefore, we deduce that $\sigma\left(F^{\{i\}}\right) = F^{\{\sigma(i)\}}$ for any $\sigma \in \mathfrak{S}_n$, as claimed. □

As a consequence of this lemma, Theorem 1 can be applied in order to decompose the resultant of the polynomials $F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}$ and hence, by (12), to decompose the discriminant of the symmetric polynomial F. We take again the notation of Theorem 1.

Theorem 2. *Assume that $n \geqslant 2$ and $d \geqslant 2$. With the above notation, we have that*

$$d^{a(n,d)}\mathrm{Disc}\,(F) = R_0 \times \prod_{\substack{\lambda\vdash n \\ l(\lambda)<d}} \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right)^{m_\lambda}$$

where $R_0 = 1$ *if* $d > n$ *and* $R_0 = \left(F^{\{1,\dots,d\}}\right)^{m_0}$ *if* $d \leqslant n$. *In this latter case,* m_0 *is defined by*

$$m_0 := n(d-1)^{n-1} - \sum_{k=1}^{d-1} A_{n,k} B_{d-1,k}$$

where

$$A_{n,k} := \sum_{\substack{\lambda \vdash n \\ l(\lambda)=k}} m_\lambda, \quad B_{d-1,k} := e_{k-1}(d-1, d-2, \dots, d-k),$$

and if F *is given explicitly by* (11) *then* $F^{\{1,\dots,d\}} = (-1)^{d-1} c_{(d)}$.

Proof. All these formulas are obtained by specialization of the formulas given in Theorem 1 with the difference that the polynomials $F^{\{i\}}$, $i = 1, \dots, n$ are of degree $d-1$ whereas they are of degree d as in Theorem 1. □

We emphasize that the formula given in this theorem is independent of the choice of basis that is used to represent F, although we have chosen the basis (10) for illustrations. We also mention that the formula given in Proposition 2.3 also applies here (this is actually the point of view used in [11]). Below, we give two examples corresponding to low degree polynomials, namely the cases $d = 2$ and $d = 3$. In these two cases the number of variables n is large compared to d and the formulas given in Theorem 2 are hence computationally very interesting since a resultant computation in n variables is replaced by several resultant computations in at most d variables.

Case $\mathbf{n \geqslant d = 2}$. The generic homogeneous polynomial of degree 2 can be written as

$$F = c_{(2)} e_2 + c_{(1,1)} e_1^2.$$

Its derivatives are

$$F^{\{i\}} = c_{(2)} \frac{\partial e_2}{\partial x_1} + 2c_{(1,1)} e_1 \frac{\partial e_1}{\partial x_1} = c_{(2)}(e_1 - x_1) + 2c_{(1,1)} e_1$$

and hence we deduce that

$$\mathrm{Res}\left(F^{\{1\}}_{(2)}\right) = (n-1)c_{(2)} + 2nc_{(1,1)}.$$

Observe that this polynomial is not irreducible over $\mathbb{Z}[c_{(2)}, c_{(1,1)}]$ if n is odd since it is divisible by 2. It is also not hard to check that $m_{(2)} = 1$ and $m_0 = n-1$ here. Finally, since $a(n,2) = 0$ if n is even and $a(n,2) = 1$ if n is odd, we get

$$\mathrm{Disc}(F) = \begin{cases} -c_{(2)}^{n-1}\left((n-1)c_{(2)} + 2nc_{(1,1)}\right) & \text{if } n \text{ is even,} \\ c_{(2)}^{n-1}\left(\frac{n-1}{2}c_{(2)} + nc_{(1,1)}\right) & \text{if } n \text{ is odd .} \end{cases}$$

Case $\mathbf{n \geqslant d = 3}$. Consider the generic homogeneous polynomial of degree 3

$$F = c_{(3)} e_3 + c_{(2,1)} e_2 e_1 + c_{(1,1,1)} e_1^3.$$

The formula given in Theorem 2 shows that

$$3^{\frac{2^n - (-1)^n}{3}} \mathrm{Disc}(F) = c_{(3)}^{m_0} \mathrm{Res}\left(F^{\{1\}}_{(n)}\right) \prod_{k=1}^{\lfloor \frac{n}{2} \rfloor} \mathrm{Res}\left(F^{\{1\}}_{(n-k,k)}, F^{\{1,2\}}_{(n-k,k)}\right)^{m_{(n-k,k)}}$$

where all the factors can be described explicitly. To begin with, from (13) and (14) we get that for all $i = 1, \dots, n$

$$F^{\{i\}} = c_{(3)}\left(e_2 - x_i e_1 + x_i^2\right) + c_{(2,1)}\left(e_2 + e_1(e_1 - x_i)\right) + 3c_{(1,1,1)} e_1^2.$$

It follows immediately that

$$\mathrm{Res}\left(F^{\{1\}}_{(n)}\right) = \binom{n-1}{2}c_{(3)} + 3\binom{n}{2}c_{(2,1)} + 3n^2c_{(1,1,1)}.$$

Now, let $(n-k,k)$ be a partition of length 2 of n. A straightforward computation shows that for any pair of distinct integers i,j we have

$$F^{\{i,j\}} = c_{(3)}\left(x_i + x_j - e_1\right) - c_{(2,1)}e_1$$

and we deduce, by means of a single (Sylvester) resultant computation that

$$\begin{aligned}\mathrm{Res}\left(F^{\{1\}}_{(n-k,k)}, F^{\{1,2\}}_{(n-k,k)}\right) &= c^2_{(3)}\left(\binom{n-1}{2}c_{(3)} + 3\binom{n}{2}c_{(2,1)} + 3n^2c_{(1,1,1)}\right)\\ &\quad - \frac{1}{2}k(n-k)\left((n-2)\,c^3_{(3)} + \left(24c_{(1,1,1)} + 3nc_{(2,1)}\right)c^2_{(3)} + (3n-6)\,c^2_{(2,1)}c_{(3)} + nc^3_{(2,1)}\right).\end{aligned}$$

The multiplicity $m_{(n-k,k)}$ are equal to the binomial $\binom{n}{k}$ for all $k = 1,\dots,\lfloor\frac{n}{2}\rfloor$ except if n is even and $k = \frac{n}{2}$ in which case $m_{(\frac{n}{2},\frac{n}{2})} = \frac{1}{2}\binom{n}{\frac{n}{2}}$. Finally, it remains to determine the integer m_0. We have

$$m_0 = n2^{n-1} - m_{(n)} - 3\sum_{\substack{\lambda\vdash n\\ l(\lambda)=2}} m_\lambda = n2^{n-1} - 1 - 3\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor} m_{(n-k,k)}.$$

But since

$$2\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor} m_{(n-k,k)} = \sum_{k=1}^{n-1}\binom{n}{k} = 2^n - 2 = 2(2^{n-1}-1),$$

we finally deduce that

$$m_0 = (n-3)2^{n-1} + 2.$$

To illustrate this general formula, we give details of the two particular cases $n=3$ and $n=4$. If $n=3$, we obtain

$$\mathrm{Disc}(F) = {c_{(3)}}^2\left(c_{(3)} + 9\,c_{(2,1)} + 27\,c_{(1,1,1)}\right)\left(-{c_{(2,1)}}^2c_{(3)} - {c_{(2,1)}}^3 + c_{(1,1,1)}{c_{(3)}}^2\right)^3$$

where

$$\mathrm{Res}\left(F^{\{1\}}_{(3)}\right) = \left(c_{(3)} + 9\,c_{(2,1)} + 27\,c_{(1,1,1)}\right),\ m_{(3)} = 1$$

and

$$\mathrm{Res}\left(F^{\{1\}}_{(2,1)}, F^{\{1,2\}}_{(2,1)}\right) = 3\left(-{c_{(2,1)}}^2c_{(3)} - {c_{(2,1)}}^3 + c_{(1,1,1)}{c_{(3)}}^2\right),\ m_{(2,1)} = 3.$$

If $n=4$ we get

$$\begin{aligned}\mathrm{Disc}(F) = -{c_{(3)}}^{10}\left(c_{(3)} + 2\,c_{(2,1)}\right)^9\left(6\,c_{(2,1)} + 16\,c_{(1,1,1)} + c_{(3)}\right)\times\\ \left(4\,c_{(1,1,1)}{c_{(3)}}^2 - 3\,{c_{(2,1)}}^2c_{(3)} - 2\,{c_{(2,1)}}^3\right)^4\end{aligned} \tag{15}$$

where

$$\mathrm{Res}\left(F^{\{1\}}_{(4)}\right) = 3\left(6\,c_{(2,1)} + 16\,c_{(1,1,1)} + c_{(3)}\right),\ m_{(4)} = 1,$$

$$\mathrm{Res}\left(F^{\{1\}}_{(3,1)}, F^{\{1,2\}}_{(3,1)}\right) = 3\left(4\,c_{(1,1,1)}{c_{(3)}}^2 - 3\,{c_{(2,1)}}^2c_{(3)} - 2\,{c_{(2,1)}}^3\right),\ m_{(3,1)} = 4$$

and

$$\mathrm{Res}\left(F^{\{1\}}_{(2,2)}, F^{\{1,2\}}_{(2,2)}\right) = -\left(c_{(3)} + 2\,c_{(2,1)}\right)^3,\ m_{(2,2)} = 3. \tag{16}$$

We notice that for the famous Clebsch surface, whose canonical equation is given by

$$h(x_1,x_2,x_3,x_4) = x_1^3 + x_2^3 + x_3^3 + x_4^3 - (x_1+x_2+x_3+x_4)^3 = 3e_3 - 3e_2e_1 = 0,$$

we recover that $h/3$ defines a smooth cubic in every characteristic except 5 (see [12, §5.4]). Indeed, (15) shows that

$$\mathrm{Disc}(h/3) = \mathrm{Disc}(e_3 - e_2e_1) = -(-1)^9(-6+1)(-3+2)^4 = -5.$$

Remark 3.2. Contrary to what was expected in [11], the resultant factors appearing in Theorem 2 are not always irreducible (see e.g. (16)). However, in all the experiments we noted that these resultant factors were always powers of irreducible polynomials (assuming the ground ring to be a field), but we do not known if this is true in general. As an illustration, we notice that the resultant (7) appearing in Example 2.2 contains two irreducible and distinct factors, but it becomes a power of a single irreducible polynomial (over a field) when specialized to get the discriminant formula in the case $n \geqslant d = 3$. Indeed, comparing the notation in these two examples we get $d = -b = c_{(3)} + c_{(2,1)}$.

4. Proof of the Main Theorem

We take again the notation of Section 2. We begin by splitting the resultant of the $F^{\{i\}}$'s into several factors by means of their divided differences. This process can be divided into steps where we increase iteratively the order of the divided differences. Thus, in the first step we make use of the first order divided differences and write

$$\begin{aligned}(17)\quad \mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) = \\ \pm \mathrm{Res}\left(F^{\{1\}}, (x_1-x_2)F^{\{1,2\}}, (x_1-x_3)F^{\{1,3\}}, \ldots, (x_1-x_n)F^{\{1,n\}}\right).\end{aligned}$$

The divided differences $F^{\{1,j\}}$ are of degree $d-1$. If $d-1=0$ then they are all equal to the same constant (see Section 2.1.1) and it is straightforward to check that we get the claimed formula in this case, that is to say

$$\mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) = \left(F^{\{1,2\}}\right)^{n-1} \mathrm{Res}\left(F^{\{1\}}_{(n)}\right) = \left(F^{\{1,2\}}\right)^{n-1} F^{\{1\}}(1,1,\ldots,1).$$

If $d-1>0$, then (17) shows that the resultant of the $F^{\{i\}}$'s splits into 2^{n-1} factors by using the multiplicativity property of the resultant : for each polynomial $(x_1-x_j)F^{\{1,j\}}$, $j=2,\ldots,n$, there is a choice between (x_1-x_j) and the divided difference $F^{\{1,j\}}$. Thus, these factors are in bijection with the subsets of $[n]$ which contain 1. If $I_1 = \{1, i_2, i_3, \ldots, i_{n-k+1}\} \subset [n]$ is such a subset, then the corresponding factor is simply

$$\pm\mathrm{Res}\left(F^{\{1\}}, F^{\{1,j_1\}}, F^{\{1,j_2\}}, \ldots, F^{\{1,j_{k-1}\}}, x_1 - x_{i_2}, x_1 - x_{i_3}, \ldots, x_1 - x_{i_{n-k+1}}\right)$$

where $\{j_1, \ldots, j_{k-1}\} = [n] \setminus I_1$. Moreover, by the specialization property of the resultant this factor is equal to

$$(18)\qquad \pm \mathrm{Res}\left(F_1^{\{1\}}, F_1^{\{1,2\}}, F_1^{\{1,3\}}, \ldots, F_1^{\{1,k\}}\right)$$

where we set $F_1^{\{1,r\}} := \rho_{I_1}(F^{\{1,j_r\}})$, ρ_{I_1} being a specialization map defined by

$$\begin{aligned}\rho_{I_1} : k[x_1,\ldots,x_n] &\to k[x_1,\ldots,x_k] \\ x_j,\ j \in I_1 &\mapsto x_1 \\ x_{j_r},\ r=1,\ldots,k-1 &\mapsto x_{r+1}.\end{aligned}$$

Roughly speaking, this amounts to put all the variables x_j, $j \in I_1$, in the "same box" and to renumber the other variables from 2 to k.

Now, one can proceed to the second step by introducing the second order divided differences. For that purpose, we start from the factor (18) obtained at the end of the previous step. If $k \leqslant 2$ the procedure stops. Otherwise, if $k > 2$ then we can proceed exactly as in the first step. Since

$$(x_2 - x_j)F_1^{\{1,2,j\}} = F_1^{\{1,2\}} - F_1^{\{1,j\}},\ j = 3, \dots, k,$$

we get

$$\begin{aligned}\operatorname{Res}\left(F_1^{\{1\}}, F_1^{\{1,2\}}, F_1^{\{1,3\}}, \dots, F_1^{\{1,k\}}\right) = \\ \pm \operatorname{Res}\left(F^{\{1\}}, F^{\{1,2\}}, (x_2 - x_3)F^{\{1,2,3\}}, (x_2 - x_4)F^{\{1,2,4\}}, \dots, (x_2 - x_k)F^{\{1,2,k\}}\right).\end{aligned}$$

So, we are exactly in the same setting as in the previous step and hence we split this factor similarly. As a result, the factors we obtain are in bijection with subsets I_2 of $[n]$ that contain 2 but not 1. After this second step is completed, then one can continue to the third step, and so on. This splitting process stops for a given factor if either it involves divided differences of distinct orders or either the order of some divided differences is higher than the degree d.

In summary, the above process shows that the resultant $\operatorname{Res}\left(F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}\right)$ splits into factors that are in bijection with ordered collections of subsets $(I_1, \dots, I_k)$ that satisfy the following three conditions :

- $1 \leqslant k \leqslant \min\{d, n\}$ and $\emptyset \neq I_j \subset [n]$ for all $j \in [k]$,
- $I_1 \coprod I_2 \coprod \dots \coprod I_k = [n]$ (disjoint union, so this is a partition of $[n]$),
- $1 = \min(I_1) < \min(I_2) < \dots < \min(I_k)$.

Definition 4.1. A collection of subsets $(I_1, \dots, I_k)$ satisfying to the three above conditions will be called an *admissible partition* (of $[n]$).

Given an admissible partition $(I_1, \dots, I_k)$, we define the specialization map

$$\begin{array}{rcl}\rho_{(I_1,\dots,I_k)} : k[x_1, \dots, x_n] & \to & k[x_1, \dots, x_k] \\ x_r, r \in I_s & \mapsto & x_s\end{array}$$

and the polynomials $F^{\{1,2,\dots,r\}}_{(I_1,\dots,I_k)} := \rho_{(I_1,\dots,I_k)}(F^{\{1,i_2,\dots,i_r\}})$, $r = 1, \dots, k$, where we set

$$i_1 := 1 = \min(I_1) < i_2 := \min(I_2) < \dots < i_k := \min(I_k).$$

Then, the factor of the resultant of the $F^{\{i\}}$'s corresponding to the admissible partition $(I_1, \dots, I_k)$ is given by

$$R_{(I_1,\dots,I_k)} := \operatorname{Res}\left(F^{\{1\}}_{(I_1,\dots,I_k)}, F^{\{1,2\}}_{(I_1,\dots,I_k)}, \dots, F^{\{1,2,\dots,k\}}_{(I_1,\dots,I_k)}\right).$$

Therefore, we proved that

$$\operatorname{Res}\left(F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}\right) = \pm\left(F^{\{1,\dots,d+1\}}\right)^{\mu} \times \prod_{(I_1,\dots,I_k)} R_{(I_1,\dots,I_k)} \tag{19}$$

where the product runs over all admissible partitions of $[n]$ and μ is an integer. Moreover, $\mu > 0$ if and only if $n > d$.

Now, we define an equivalence relation $\sim$ on the set of admissible partitions of $[n]$. Given two admissible partitions $(I_1, \dots, I_k)$ and $(J_1, \dots, J_{k'})$, we set

$$(I_1, \dots, I_k) \sim (J_1, \dots, J_{k'}) \Leftrightarrow \begin{cases} k = k' \text{ and} \\ \exists\, \sigma \in \mathfrak{S}_k \text{ such that } |I_l| = |J_{\sigma(l)}| \text{ for all } l \in [k]. \end{cases}$$

It is straightforward to check that this binary relation is reflexive, symmetric and transitive so that it defines an equivalence relation. We denote by $[(I_1,\dots,I_k)]$ its equivalence classes. Consider the admissible partitions $(L_1,\dots,L_k)$ such that

$$l_1 := |L_1| \geqslant l_2 := |L_2| \geqslant \dots l_k := |L_k| \quad \text{and} \tag{20}$$

$$L_j := \left\{ 1+\sum_{i=1}^{j-1} l_i, 2+\sum_{i=1}^{j-1} l_i, \dots, \sum_{i=1}^{j} l_i \right\} \text{ for all } j \in [k].$$

Obviously, there is exactly one such admissible partition in each equivalent class of $\sim$. Moreover, these admissible partitions are in bijection with the partitions $\lambda \vdash n$ of length k by setting $\lambda := (l_1, l_2, \dots, l_k) \vdash n$. As a consequence, we deduce that there is a bijection between the equivalence classes of $\sim$ and the partitions $\lambda \vdash n$ of length k and we write

$$[\lambda] := [(I_1,\dots,I_k)] = [(L_1,\dots,L_k)].$$

Lemma 4.2. *Let λ be a partition of n, then the cardinality of the equivalence class $[\lambda]$ is m_λ.*

Proof. Let λ be a partition of n and consider the equivalent class $[\lambda]$. The multinomial coefficient (2) counts the different ways of filling $k = l(\lambda)$ boxes $J_1,\dots,J_k$ with λ_j elements in the box J_j. These choices take into account the order between the boxes, but not inside the boxes. These boxes J_j can obviously be identified with subsets of $[n]$. Moreover, there exists a unique permutation $\sigma \in \mathfrak{S}_k$ such that

$$1 = \min(J_{\sigma(1)}) < \min(J_{\sigma(2)}) < \cdots \min(J_{\sigma(k)})$$

and hence such that the collection of subsets $(J_{\sigma(1)}, J_{\sigma(2)}, \dots, J_{\sigma(k)})$ is an admissible partition. Therefore, any choice for filling the boxes $J_1,\dots,J_k$ can be associated to a factor in the decomposition. Conversely, such a factor is associated to an admissible partition $(I_1,\dots,I_k)$, but there are possibly several choices, i.e. permutations in $\mathfrak{S}_k$, that give a way of filling the boxes $J_1,\dots,J_k$: it is possible to permute boxes that have the same cardinality. Therefore, we conclude that the cardinality of the equivalent class represented by a partition $\lambda \vdash n$ is exactly m_λ. □

The following result shows that admissible partitions that are equivalents give the same factor, up to sign, in the splitting process.

Proposition 4.3. *Let λ be a partition of n. Then, for any admissible partition $(I_1,\dots,I_k)$ such that $[\lambda] = [(I_1,\dots,I_k)]$,*

$$R_{(I_1,\dots,I_k)} = \pm \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right).$$

Proof. Let $(I_1,\dots,I_k)$ be an admissible partition and set

$$i_1 := 1 = \min(I_1) < i_2 := \min(I_2) < \cdots < i_k := \min(I_k).$$

Its corresponding factor in the splitting process is nothing but the resultant, up to sign, of the following list of n polynomials in the n variables $x_1,\dots,x_n$:

$$F^{\{1\}}, F^{\{1,i_2\}}, \dots, F^{\{1,i_2,\dots,i_k\}}, \{x_{i_1} - x_r\}_{r\in I_1\setminus\{1\}}, \dots, \{x_{i_k} - x_r\}_{r\in I_k\setminus\{i_k\}}. \tag{21}$$

Now, let $(J_1, J_2, \dots, J_k)$ be another admissible partition such that $[(I_1,\dots,I_k)] = [(J_1, J_2, \dots, J_k)]$ and set

$$j_1 := 1 = \min(J_1) < j_2 := \min(J_2) < \cdots < j_k := \min(J_k).$$

The corresponding factor of $(J_1, J_2, \dots, J_k)$ can be described similarly as the resultant, up to sign, of the polynomials

$$F^{\{1\}}, F^{\{1,j_2\}}, \dots, F^{\{1,j_2,\dots,j_k\}}, \{x_{j_1} - x_r\}_{r\in J_1\setminus\{1\}}, \dots, \{x_{j_k} - x_r\}_{r\in J_k\setminus\{j_k\}}. \tag{22}$$

First, observe that it is sufficient to prove that $R_{(I_1,\dots,I_k)} = \pm R_{(J_1,\dots,J_k)}$ by assuming that $|I_{\sigma(l)}| = |J_l|$ for all $l \in [k]$ where σ is an elementary transposition (a permutation which exchanges two successive elements and keeps all the others fixed) in $\mathfrak{S}_k$. This is because $\mathfrak{S}_k$ is generated by the elementary transpositions and because of the transitivity of $\sim$. So, let $s \in [k-1]$ and assume that

$$|I_s| = |J_{s+1}|,\ |I_{s+1}| = |J_s| \text{ and } |I_l| = |J_l| \text{ for all } l \in [k] \setminus \{s, s+1\}.$$

Let us choose a permutation $\tau \in \mathfrak{S}_n$ such that

$$\begin{cases} \tau(I_l) = J_l \text{ and } \tau(i_l) = j_l \text{ for all } l \in [k], \\ \tau(I_s) = J_{s+1} \text{ and } \tau(i_s) = j_{s+1}, \\ \tau(I_{s+1}) = J_s \text{ and } \tau(i_{s+1}) = j_s. \end{cases}$$

By the property (5), the application of τ on the list of polynomials (21) returns the following list of polynomials

$$\begin{aligned} (23)\quad & F^{\{1\}}, F^{\{1,j_2\}}, \dots, F^{\{1,j_2,\dots,j_{s-1},j_{s+1}\}}, F^{\{1,j_2,\dots,j_{s-1},j_s,j_{s+1}\}}, \dots, F^{\{1,j_2,\dots,j_k\}}, \\ & \left\{x_{j_1} - x_r\right\}_{r\in J_1\setminus\{1\}}, \dots, \left\{x_{j_{s-1}} - x_r\right\}_{r\in J_{s-1}\setminus\{j_{s-1}\}}, \left\{x_{j_{s+1}} - x_r\right\}_{r\in J_{s+1}\setminus\{j_{s+1}\}}, \\ & \left\{x_{j_s} - x_r\right\}_{r\in J_s\setminus\{j_s\}}, \dots, \left\{x_{j_k} - x_r\right\}_{r\in J_k\setminus\{j_k\}}. \end{aligned}$$

By the invariance, up to sign, of the resultant under permutations of polynomials and variables, we get that the resultant of the list of polynomials (21), i.e. $R_{(I_1,\dots,I_k)}$, is equal to the resultant of the list of polynomials (23) up to sign. Now, by definition of divided differences we have that

$$F^{\{1,j_2,\dots,j_{s-1},j_s\}} = F^{\{1,j_2,\dots,j_{s-1},j_{s+1}\}} + (x_{j_s} - x_{j_{s+1}})F^{\{1,j_2,\dots,j_{s-1},j_s,j_{s+1}\}}$$

so that the resultant of the polynomials (23) is equal, up to sign, to the resultant of the polynomials (22), i.e. $R_{(J_1,\dots,J_k)}$, by invariance of the resultant under the above elementary transformation and permutations of polynomials. Therefore, we have proved that $R_{(I_1,\dots,I_k)} = \pm R_{(J_1,\dots,J_k)}$.

Finally, to conclude the proof, let $(L_1,\dots,L_k)$ be the particular representative of the class $[\lambda] = [(I_1,\dots,I_k)]$ as defined in (20). Then, it is clear by the definitions that $\rho_{(L_1,\dots,L_k)} = \rho_\lambda$ and that

$$R_{(L_1,\dots,L_k)} = \operatorname{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right).$$

□

The comparison of (19), Lemma 4.2 and Proposition 4.3 shows that if $d \geqslant n$ then

$$(24)\qquad \operatorname{Res}\left(F^{\{1\}},\dots,F^{\{n\}}\right) = \pm \prod_{\lambda\vdash n} \operatorname{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right)^{m_\lambda}$$

and if $n > d$ then

$$\begin{aligned} (25)\quad & \operatorname{Res}\left(F^{\{1\}},\dots,F^{\{n\}}\right) = \\ & \pm \left(F^{\{1,\dots,d+1\}}\right)^\mu \prod_{\substack{\lambda\vdash n \\ l(\lambda)\leqslant d}} \operatorname{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right)^{m_\lambda}. \end{aligned}$$

To determine the integer μ, we compare the degrees with respect to the coefficients of the $F^{\{i\}}$'s. The resultant on the left side is homogeneous of degree d^{n-1} with respect to the coefficients of each polynomial $F^{\{i\}}$, so it is homogeneous of degree nd^{n-1} with respect to the coefficients of all the polynomials $F^{\{i\}}$, $i = 1,\dots,n$. Given a partition $\lambda \vdash n$, $l(\lambda) \leqslant d$, the

polynomial $F_\lambda^{\{1,2,\ldots,j\}}$, $1 \leqslant j \leqslant l(\lambda)$ is of degree $d-j+1$. Therefore, the resultant associated to this partition λ is homogeneous with respect to the coefficients of the $F^{\{i\}}$'s of degree

$$\sum_{j=1}^{l(\lambda)} \frac{d(d-1)\cdots(d-l(\lambda)+1)}{d-j+1} = e_{l(\lambda)-1}(d, d-1, \ldots, d-l(\lambda)+1).$$

Finally, since $F^{\{1,2,\ldots,d+1\}}$ is homogeneous of degree one in the coefficient of the $F^{\{i\}}$'s, we deduce that

$$\mu = nd^{n-1} - \sum_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} m_\lambda . e_{l(\lambda)-1}(d, d-1, \ldots, d-l(\lambda)+1),$$

that is to say

$$\mu = nd^{n-1} - \sum_{k=1}^{d} \sum_{\substack{\lambda \vdash n \\ l(\lambda)=k}} m_\lambda . e_{k-1}(d, d-1, \ldots, d-k+1).$$

From here we see immediately that μ is equal to the integer m_0 defined in the statement of Theorem 1.

To conclude the proof of Theorem 1, it remains to determine the signs $\pm$ that occur in the formulas (24) and (25). To this end, we examine their specialization when $F^{\{i\}} = x_i^d$, $i = 1, \ldots, n$. First, the resultant of the $F^{\{i\}}$'s is equal to 1 (normalization of the resultant). Now, given any partition $\lambda \vdash n$, it is straightforward to check that $F_\lambda^{\{1\}} = x_1^d$. Then applying iteratively the defining property of the divided differences from $j = 1$ to $j = l(\lambda)$, we get that

$$F_\lambda^{\{1,2,\ldots,j\}} = x_j^d \mod (x_1, \ldots, x_{j-1}), \quad j = 1, \ldots, l(\lambda).$$

Now, using the multiplicativity property of the resultant and its invariance under elementary transformations, we deduce that all the resultants associated to a partition λ specialize to 1. Similarly we observe that $F^{\{1,\ldots,d+1\}}$ also specializes to 1 when $n > d$, and this concludes the proof of Theorem 1.

Acknowledgments. The authors are grateful to Evelyne Hubert for useful discussions on equivariant polynomial systems and to the anonymous reviewers for their valuable comments and suggestions to improve the presentation of this paper. The second author's research has received funding from the European Union (European Social Fund) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework, Research Funding Program "ARISTEIA", Project ESPRESSO: Exploiting Structure in Polynomial Equation and System Solving with Applications in Geometric and Game Modeling. She also acknowledges the Galaad project team at INRIA Sophia-Antipolis that made possible her visit to INRIA.

References

[1] François Apéry and Jean-Pierre Jouanolou. *Élimination: le cas d'une variable*. Hermann, Collection Méthodes, 2006.

[2] Laurent Busé and Jean-Pierre Jouanolou. On the Discriminant Scheme of Homogeneous Polynomials. *Math. Comput. Sci.*, 8(2):175–234, 2014.

[3] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[4] Michel Demazure. Résultant, discriminant. *Enseign. Math. (2)*, 58(3-4):333–373, 2012.

[5] Jean A. Dieudonné and James B. Carrell. *Invariant theory, old and new*. Academic Press, New York-London, 1971.

[6] Jean-Charles Faugère and Jules Svartz. Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 170–178, New York, NY, USA, 2012. ACM.
[7] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2008. Reprint of the 1994 edition.
[8] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2):117–263, 1991.
[9] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
[10] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1995. With contributions by A. Zelevinsky, Oxford Science Publications.
[11] N. Perminov and S. Shakirov. Preprint arxiv:0910.5757v1. Discriminants of Symmetric Polynomials, 2009.
[12] Takeshi Saito. The discriminant and the determinant of a hypersurface of even dimension. *Math. Res. Lett.*, 19(4):855–871, 2012.
[13] Patrick A. Worfolk. Zeros of equivariant vector fields: algorithms for an invariant approach. *J. Symbolic Comput.*, 17(6):487–511, 1994.

Email: laurent.buse@inria.fr, INRIA Sophia Antipolis-Méditeranée, France.

Email: akarasou@di.uoa.gr, Department of Informatics & Telecommunications, National and Kapodistrian University of Athens, Greece.