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 canonical actions of the symmetric group of n symbols on the variables and on the polynomials, it is proved that its resultant can be decomposed into a product of several smaller 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 are highly structured and it is very useful to develop specific methods in order to take into account a particular structure. 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 [15, §4] or [5, Chapter 1]). Some recent interesting developments based on Gröbner basis techniques for this kind of systems can be found in [6] with applications. In this work, we will study the resultant of these systems.

The main result of this paper (Theorem 3.3) is a decomposition of the resultant of a $\mathfrak{S}_n$-equivariant polynomial system. This formula allows to split such a resultant into several 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. Another important point of our result is that it is an exact and universal formula which is valid over the universal ring of coefficients (over the integers) of the input polynomial system. Indeed, we payed attention to use a correct and universal definition of the resultant. In this way, the formula we obtain has the correct geometric meaning and stays valid over any coefficient ring by specialization. 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 computational algebra. Although the discriminant of the generic homogeneous polynomial of a given degree is irreducible, for a particular 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 4.2). This result was actually the first goal of this work that has been inspired by the unpublished (as far as we know) note [13] by N. Perminov and S. Shakirov where

a first tentative for such a formula is given without a complete proof. Another motivation was also to improve the computations of discriminants for applications in convex geometry, following a paper by J. Nie where the boundary of the cone of non-negative polynomials on an algebraic variety is studied by means of discriminants [12]. We emphasize that our formula is obtained as a byproduct of our first formula on the resultant of a $\mathfrak{S}_n$-equivariant polynomial system. Therefore, it inherits from the same features, namely it allows to split a discriminant into several resultants that are easier to compute and it is a universal formula where the multiplicities of the factors are provided. Here again, we payed attention to use a correct and universal definition of the discriminant.

The paper is organized as follows. In Section 2 we first provide some preliminaries on some material that we will need, namely multivariate divided differences, resultants and discriminants. Section 3 will be devoted to the main result of this paper (Theorem 3.3), that is to say a decomposition formula for the resultant of a polynomial system which is $\mathfrak{S}_n$-equivariant. As a corollary of this formula, a decomposition of the discriminant of a homogeneous symmetric polynomial (Theorem 4.2) is provided in Section 4.

2. Preliminaries

In this section we introduce our notation and the material we will use, namely divided differences, resultants and discriminants. We will provide proofs concerning the results on divided differences because we were not able to find the properties we needed in the literature, although these results are part of the folklore and are definitely known to the experts.

2.1. **Divided differences.** Let R be a commutative ring and denote by $R[x_1,\dots,x_n]$ the ring of polynomials in $n \geqslant 2$ variables which is graded with the usual weights: $\deg(x_i)=1$ for all $i \in \{1,\dots,n\}$. For any sequence of integers $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$ we will denote by $V(x_{i_1},x_{i_2},\dots,x_{i_k})$ the Vandermonde determinant

$$V(x_{i_1},x_{i_2},\dots,x_{i_k}) := \prod_{1\leqslant s<r\leqslant k}(x_{i_r}-x_{i_s}) = \det\begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-1} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_{i_k} & \cdots & x_{i_k}^{k-1} \end{vmatrix}.$$

It is a homogeneous polynomial in $R[x_1,\dots,x_n]$ of degree $\binom{k}{2}=\frac{k(k-1)}{2}$. For the sake of simplicity in the notation, 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.

Suppose given n homogeneous polynomials $P^{\{1\}},P^{\{2\}},\dots,P^{\{n\}}$ of the same degree $d \geqslant 1$ in $R[x_1,\dots,x_n]$ such that for all couple of integers $(i,j)\in[n]^2$ the polynomial $P^{\{i\}}-P^{\{j\}}$ is divisible by x_i-x_j:

$$P^{\{i\}}-P^{\{j\}} \in (x_i-x_j) \subset R[x_1,\dots,x_n]. \tag{1}$$

Lemma 2.1. *For any set of $k \geqslant 2$ distinct integers $\{i_1,\dots,i_k\}\subset[n]$, there exists a unique homogeneous polynomial $P^{\{i_1,\dots,i_k\}}$ in $R[x_1,\dots,x_n]$ of degree $d-k+1$ such that*

$$V(x_{i_1},x_{i_2},\dots,x_{i_k})\cdot P^{\{i_1,\dots,i_k\}}(x_1,\dots,x_n) = \det\begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-2} & P^{\{i_1\}}(x_1,\dots,x_n) \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-2} & P^{\{i_2\}}(x_1,\dots,x_n) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_k} & \cdots & x_{i_k}^{k-2} & P^{\{i_k\}}(x_1,\dots,x_n) \end{vmatrix}.$$

Proof. From the assumption (1) it is clear that $(x_i - x_j)$ divides the Vandermonde-like determinant

$$\begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-2} & P^{\{i_1\}} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-2} & P^{\{i_2\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_k} & \cdots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix}$$

and hence that $V(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ also divides it. Now, R being again an arbitrary commutative ring, the uniqueness of $P^{\{i_1,\ldots,i_k\}}$ follows from the fact that $V(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ is not a zero divisor in $R[x_1, \ldots, x_n]$, which is a consequence of the Dedekind-Mertens Lemma (see for instance [2, §2.4]). □

Definition 2.2. For all positive integer $k \leqslant n$, the polynomials $P^{\{i_1,\ldots,i_k\}}$ defined in Lemma 2.1 are called $(k-1)^{\text{th}}$ divided differences of the polynomials $P^{\{1\}}, \ldots, P^{\{n\}}$. We notice that $P^{\{i_1,\ldots,i_k\}} = 0$ if $d + 1 < k \leqslant n$.

The first divided differences $P^{\{i,j\}}$ are easily seen to satisfy the equality

$$(x_i - x_j)P^{\{i,j\}} = P^{\{i\}} - P^{\{j\}}. \tag{2}$$

This explains the terminology "divided difference". It turns out that similar equalities hold for the higher order divided differences.

Proposition 2.3. *Let $\{i_1, \ldots, i_k\}$ be a subset of $[n]$ with $k \geqslant 2$. Then, for any two distinct integers p, q in $\{i_1, \ldots, i_k\}$,*

$$(x_{i_q} - x_{i_p})P^{\{i_1,i_2,\ldots,i_k\}} = P^{\{i_1,i_2,\ldots,i_k\}\setminus\{i_p\}} - P^{\{i_1,i_2,\ldots,i_k\}\setminus\{i_q\}}.$$

Proof. We observe that it is enough to prove this result over the universal ring of coefficients of $P^{\{1\}}, P^{\{2\}}, \ldots, P^{\{n\}}$ over the integers and we proceed by induction on k. As we already noticed in (2), the claimed formula holds for $k = 2$. So, we fix an integer $k > 2$ and we assume that the claimed formula holds for any set $\{i_1, \ldots, i_r\}$ of cardinality $\leqslant k - 1$. Observe also that since $P^{\{i_1,i_2,\ldots,i_k\}}$ is independent of the order of $i_1, i_2, \ldots, i_k$, it is sufficient to prove the claimed equality for $\{p, q\} = \{1, 2\}$.

By definition (see Lemma 2.1), we have

$$V(x_{i_1}, \ldots, x_{i_k})P^{\{i_1,\ldots,i_k\}} = \begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-2} & P^{\{i_1\}} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-2} & P^{\{i_2\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_k} & \cdots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix}.$$

We denote by Δ this determinant. By subtracting the last row from all the other rows in the matrix of Δ, we get

$$\Delta = \begin{vmatrix} 0 & x_{i_1} - x_{i_k} & \cdots & x_{i_1}^{k-2} - x_{i_k}^{k-2} & P^{\{i_1\}} - P^{\{i_k\}} \\ 0 & x_{i_2} - x_{i_k} & \cdots & x_{i_2}^{k-2} - x_{i_k}^{k-2} & P^{\{i_2\}} - P^{\{i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & x_{i_{k-1}} - x_{i_k} & \cdots & x_{i_{k-1}}^{k-2} - x_{i_k}^{k-2} & P^{\{i_{k-1}\}} - P^{\{i_k\}} \\ 1 & x_{i_k} & \cdots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix} = \left(\prod_{j=1}^{k-1}(x_{i_j} - x_{i_k})\right)\tilde{\Delta}$$

where (we use (2))

$$\tilde{\Delta} = \begin{vmatrix} 0 & 1 & x_{i_1}+x_{i_k} & \sum_{r=0}^{2} x_{i_1}^r x_{i_k}^{2-r} & \cdots & \sum_{r=0}^{k-3} x_{i_1}^r x_{i_k}^{k-3-r} & P^{\{i_1,i_k\}} \\ 0 & 1 & x_{i_2}+x_{i_k} & \sum_{r=0}^{2} x_{i_2}^r x_{i_k}^{2-r} & \cdots & \sum_{r=0}^{k-3} x_{i_2}^r x_{i_k}^{k-3-r} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \\ 0 & 1 & x_{i_{k-1}}+x_{i_k} & \sum_{r=0}^{2} x_{i_{k-1}}^r x_{i_k}^{2-r} & \cdots & \sum_{r=0}^{k-3} x_{i_{k-1}}^r x_{i_k}^{k-3-r} & P^{\{i_{k-1},i_k\}} \\ 1 & x_{i_k} & x_{i_k}^2 & x_{i_k}^3 & \cdots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix}$$

$$= (-1)^{k-1} \begin{vmatrix} 1 & x_{i_1}+x_{i_k} & \sum_{r=0}^{2} x_{i_1}^r x_{i_k}^{2-r} & \cdots & \sum_{r=0}^{k-3} x_{i_1}^r x_{i_k}^{k-3-r} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2}+x_{i_k} & \sum_{r=0}^{2} x_{i_2}^r x_{i_k}^{2-r} & \cdots & \sum_{r=0}^{k-3} x_{i_2}^r x_{i_k}^{k-3-r} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots & \\ 1 & x_{i_{k-1}}+x_{i_k} & \sum_{r=0}^{2} x_{i_{k-1}}^r x_{i_k}^{2-r} & \cdots & \sum_{r=0}^{k-3} x_{i_{k-1}}^r x_{i_k}^{k-3-r} & P^{\{i_{k-1},i_k\}} \end{vmatrix}.$$

By multiplying the column $j-1$ by x_{i_k} and subtracting the result to the column j in the above matrix, for $j = k-2$ down to 2, we deduce that

$$\tilde{\Delta} = \begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-3} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-3} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} & \cdots & x_{i_{k-1}}^{k-3} & P^{\{i_{k-1},i_k\}} \end{vmatrix}.$$

Finally, we obtain

$$V(x_{i_1},\dots,x_{i_k})P^{\{i_1,\dots,i_k\}} = (x_{i_k}-x_{i_1})\cdots(x_{i_k}-x_{i_{k-1}}) \begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-3} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-3} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} & \cdots & x_{i_{k-1}}^{k-3} & P^{\{i_{k-1},i_k\}} \end{vmatrix}$$

and since $\prod_{j=1}^{k-1}(x_{i_k}-x_{i_j})$ is not a zero divisor in $R[x_1,\dots,x_n]$ (by Dedekind-Mertens Lemma), it follows that

$$V(x_{i_1},\dots,x_{i_{k-1}})P^{\{i_1,\dots,i_k\}} = \begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-3} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-3} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} & \cdots & x_{i_{k-1}}^{k-3} & P^{\{i_{k-1},i_k\}} \end{vmatrix}.$$

By repeating this process and using our inductive hypothesis (here on sets of cardinality 3), we get

$$V(x_{i_1},\dots,x_{i_{k-2}})P^{\{i_1,\dots,i_k\}} = \begin{vmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{k-4} & P^{\{i_1,i_{k-1},i_k\}} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{k-4} & P^{\{i_2,i_{k-1},i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-2}} & \cdots & x_{i_{k-1}}^{k-4} & P^{\{i_{k-2},i_{k-1},i_k\}} \end{vmatrix}.$$

Continuing this way, we end with the equality

$$(x_{i_2}-x_{i_1})P^{\{i_1,\dots,i_k\}} = V(x_{i_1},x_{i_2})P^{\{i_1,\dots,i_k\}} = \begin{vmatrix} 1 & P^{\{i_1,i_3,\dots,i_k\}} \\ 1 & P^{\{i_2,i_3,\dots,i_k\}} \end{vmatrix} = P^{\{i_2,i_3,\dots,i_k\}} - P^{\{i_1,i_3,\dots,i_k\}}$$

which concludes the proof. □

Remark 2.4. If $n \geqslant d+1$ then the d^{th} divided differences are elements in R because there are homogeneous polynomials in $R[x_1, \ldots, x_n]$ of degree 0. Then, the previous proposition shows that they are all equal : $P^I = P^J$ for all subsets I and J of $[n]$ such that $|I| = |J| = d+1 \leqslant n$.

Example 2.5. The more general system of three linear homogeneous polynomials in 3 variables satisfying (1) is of the form

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

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

The following result is another consequence of Proposition 2.3 that we record for later use.

Corollary 2.6. *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, that is to say*

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

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 Proposition 2.3. 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. □

2.2. **Resultant of homogeneous polynomials.** Suppose given an integer $n \geqslant 1$ and a sequence of positive integers $d_1, \ldots, d_n$. We consider the *generic* homogeneous polynomials in the variables $x = (x_1, \ldots, x_n)$ (all assumed to have weight 1) and of degree $d_1, \ldots, d_n$ respectively. They are of the form

$$f_i(x_1, \ldots, x_n) = \sum_{|\alpha| = d_i} u_{i,\alpha} x^\alpha, \quad i = 1, \ldots, n.$$

The ring $\mathbb{U} := \mathbb{Z}[u_{i,\alpha} : i = 1, \ldots, n, |\alpha| = d_i]$ is called the universal ring of coefficients. The polynomials $f_1, \ldots, f_n$ belong to the ring $C := \mathbb{U}[x_1, \ldots, x_n]$. Following [8], the *ideal of inertia forms* of these polynomials, i.e. the ideal $(f_1, \ldots, f_n) : (x_1, \ldots, x_n)^\infty$, is canonically graded and its degree zero part is a principal ideal of $\mathbb{U}$. The universal resultant, denoted Res, is then define as the unique generator of this principal ideal such that

$$\text{Res}(x_1^{d_1}, \ldots, x_n^{d_n}) = 1. \tag{3}$$

To define the resultant of any given n-uples of homogeneous polynomials in the variables $x_1, \ldots, x_n$ (and also to clarify (3)) one proceeds as follows. Let S be a commutative ring and for all $i = 1, \ldots, n$ suppose given a homogeneous polynomial of degree d_i

$$g_i = \sum_{|\alpha| = d_i} v_{i,\alpha} x^\alpha \in S[x_1, \ldots, x_n]_{d_i}.$$

Then, the resultant of $g_1, \ldots, g_n$ is defined as the image of the universal resultant by the specialization ring morphism $\theta : \mathbb{U} \to S : u_{j,\alpha} \mapsto v_{j,\alpha}$, that is to say

$$\text{Res}(g_1, \ldots, g_n) := \theta(\text{Res}) \in S.$$

Observe that if $S = \mathbb{U}$ and θ is the identity, then the universal resultant Res is nothing but $\mathrm{Res}(f_1, \dots, f_n)$, which is the notation we will use. If S is a field, then the resultant has the expected geometric interpretation : it vanishes if and only if the polynomials $g_1, \dots, g_n$ have a common root in the projective space $\mathbb{P}^{n-1}_{\overline{S}}$ (where $\overline{S}$ stands for the algebraic closure of S).

We now recall briefly some properties of the resultant that we will use in the sequel. For the proofs, we refer the reader to [8, §5] (see also ([9, 7, 3]). Let S be any commutative ring and suppose given $g_1, \dots, g_n$ homogeneous polynomials in the polynomial ring $S[x_1, x_2, \dots, x_n]$ of positive degree $d_1, \dots, d_n$ respectively.

Homogeneity: for all $i = 1, \dots, n$, $\mathrm{Res}(f_1, \dots, f_n)$ is homogeneous with respect to the coefficients $(u_{i,\alpha})_{|\alpha|=d_i}$ of f_i of degree $d_1 \dots d_n/d_i$.

Permutation of polynomials: $\mathrm{Res}(g_{\sigma(1)}, \dots, g_{\sigma(n)}) = (\mathcal{E}(\sigma))^{d_1 \cdots d_n} \mathrm{Res}(g_1, \dots, g_n)$ for any permutation σ of the set $\{1, \dots, n\}$ ($\mathcal{E}(\sigma)$ denotes the signature of the permutation σ).

Elementary transformations: $\mathrm{Res}(g_1, \dots, g_i + \sum_{i \neq j} h_j g_j, \dots, g_n) = \mathrm{Res}(g_1, \dots, g_n)$ for any homogeneous polynomials h_j of degree $d_i - d_j$.

Multiplicativity: $\mathrm{Res}(g_1' g_1'', g_2, \dots, g_n) = \mathrm{Res}(g_1', g_2, \dots, g_n)\mathrm{Res}(g_1'', g_2, \dots, g_n)$ for any pair of homogeneous polynomials g_1' and g_1''.

Linear change of variables: Let ϕ be a $n \times n$-matrix with entries in S and denote by $\phi(x)$ the product of the matrix ϕ with the column vector $(x_1, \dots, x_n)^t$. Then

$$\mathrm{Res}(g_1(\phi(x)), g_2(\phi(x)), \dots, g_n(\phi(x))) = \det(\phi)^{d_1 \cdots d_n} \mathrm{Res}(g_1, \dots, g_n).$$

In particular, the resultant is invariant, up to sign, under permutation of the variables $x_1, \dots, x_n$.

Finally, let us recall quickly the famous *Macaulay formula* that goes back to the work of Macaulay [10] and that is still nowadays a very powerful tool to compute exactly the resultant over a general coefficient ring (all the examples presented in this paper have been computed with this formula).

Assume we are in the generic setting over the ring $\mathbb{U}$. Set $\delta := \sum_{i=1}^n (d_i - 1)$ and denote by $\mathrm{Mon}(n; t)$ the set of all homogeneous monomials of degree t in the n variables $x_1, \dots, x_n$. if $t \geqslant \delta + 1$ then for any $x^\alpha \in \mathrm{Mon}(n; t)$ there exists $i \in \{1, \dots, n\}$ such that $x_i^{d_i}$ divides the monomial x_α. Therefore, in this case we set $i(\alpha) := \min\{i : x_i^{d_i} | x^\alpha\}$ and we define the square matrix

$$\mathbb{M}(f_1, \dots, f_n; t) = (m_{\alpha,\beta}) : \mathrm{Mon}(n; t) \times \mathrm{Mon}(n; t) \to \mathbb{U}$$

by the formula

$$\frac{x^\beta}{x_{i(\beta)}^{d_{i(\beta)}}} f_{i(\beta)} = \sum_{|\alpha|=t} m_{\alpha,\beta} x^\alpha \text{ for all } x^\beta \in \mathrm{Mon}(n; t).$$

Now, define

$$\mathrm{Dod}(n; t) := \{x^\alpha \in \mathrm{Mon}(n; t) \text{ such that } \exists i \neq j \ : \ x_i^{d_i} x_j^{d_j} | x^\alpha\} \subset \mathrm{Mon}(n; t)$$

and denote by $\mathbb{D}(f_1, \dots, f_n; t)$ the square submatrix of $\mathbb{M}(f_1, \dots, f_n; t)$ which is indexed by $\mathrm{Dod}(n; t)$. Now, for any $t \geqslant \delta + 1$ we have the Macaulay formula :

$$\det(\mathbb{M}(f_1, \dots, f_n; t)) = \mathrm{Res}(f_1, \dots, f_n) \det(\mathbb{D}(f_1, \dots, f_n; t)).$$

2.3. **Discriminant.** Consider the *generic* homogeneous polynomial of degree $d \geqslant 2$ in $n \geqslant 2$ variables

$$f(x_1, \ldots, x_n) = \sum_{|\alpha|=d} u_\alpha x^\alpha.$$

We denote its universal ring of coefficients $\mathbb{U} := \mathbb{Z}[u_\alpha : |\alpha| = d]$, so that $f \in \mathbb{U}[x_1, \ldots, x_n]$. The universal discriminant of f, denoted $\mathrm{Disc}(f)$, is defined as the unique element in $\mathbb{U}$ that satisfies the equality

$$d^{a(n,d)}\mathrm{Disc}(f) = \mathrm{Res}\left(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}\right)$$

where

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

Similarly to what we have done for the resultant, given a commutative ring S and an homogeneous polynomial of degree d

$$g = \sum_{|\alpha|=d} u_\alpha x^\alpha \in S[x_1, \ldots, x_n]_d,$$

its discriminant is denoted by $\mathrm{Disc}(g)$ and is defined as the image of the universal discriminant $\mathrm{Disc}(f)$ by the canonical specialization $\theta : \mathbb{U} \to S : u_\alpha \mapsto u_\alpha$, that is to say

$$\mathrm{Disc}(g) = \theta(\mathrm{Disc}(f)) \in S.$$

With this definition we get a smoothness criterion : If S is an algebraically closed field and $g \neq 0$, then $\mathrm{Disc}(g) = 0$ if and only if the hypersurface defined by the polynomial g in $\mathrm{Proj}(S[x_1, \ldots, x_n])$ 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. We only point out for future use that the following property : the universal discriminant is homogeneous with respect to the coefficient of f of degree $n(d-1)^{n-1}$.

3. Resultant of a $\mathfrak{S}_n$-equivariant polynomial system

In this section, we consider a polynomial system of n homogeneous equations $F^{\{1\}}, \ldots, F^{\{n\}}$ in $R[x_1, \ldots, x_n]$, R being an arbitrary commutative ring, of the same degree $d \geqslant 1$, which is equivariant (see for instance [15, §4] or [5, Chapter 1]) with respect to the canonical actions of the symmetric group $\mathfrak{S}_n$ on the variables and polynomials. More precisely, we assume that for any integer $i \in \{1, 2, \ldots, n\}$ and any permutation $\sigma \in \mathfrak{S}_n$

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

The two following examples suggest that this assumption imposes a decomposition into products of the resultant of $F^{\{1\}}, \ldots, F^{\{n\}}$.

Example 3.1. In the case $n = 2$ and $d \geqslant 1$ the polynomial system

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

over the coefficient ring $\mathbb{Z}[a_0, \ldots, a_d]$ is the universal $\mathfrak{S}_2$-equivariant polynomial system (any other equivariant system of degree d, and with $n = 2$, can be obtained as a specialization of this system). One can show (see for instance [1, Exercice 67]) that there exists an irreducible polynomial $K_d \in \mathbb{Z}[a_0, \ldots, a_d]$ such that

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

Example 3.2. Suppose $n \geqslant 2$, $d = 1$ and $F^{\{i\}}(x_1, \ldots, x_n) = ax_i + be_1(x_1, \ldots, x_n)$, $i = 1, \ldots, n$. It is clear that these polynomials satisfy (4). Moreover, since the resultant of n linear forms in n variables is the determinant of the matrix of their associated linear system, a straightforward computation shows that

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

The goal of this section is to prove a general decomposition formula (Theorem 3.3) for the resultant of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system $F^{\{1\}}, \ldots, F^{\{n\}}$. We begin this section with some observations on the specialization of divided differences with respect to a given partition of the variables.

3.1. **Divided differences and partitions.** A finite sequence $\lambda = (\lambda_1, \ldots, \lambda_k)$ of weakly decreasing integers, i.e. such that $\lambda_1 \geqslant \cdots \geqslant \lambda_k \geqslant 0$, is called a partition. When $\sum_{i=1}^{k} \lambda_i = p$ we will say such a λ is a partition of p, and write $\lambda \vdash p$. The number of nonzero λ_i's is called the length of λ, and will be denoted by $l(\lambda)$.

Given a partition $\lambda \vdash n$, we consider the morphism of polynomial algebras

$$\begin{array}{rccl} \rho_\lambda : R[x_1, \ldots, x_n] & \to & R[y_1, \ldots, y_{l(\lambda)}] \\ F(x_1, \ldots, x_n) & \mapsto & F(\underbrace{y_1, \ldots, y_1}_{\lambda_1}, \underbrace{y_2, \ldots, y_2}_{\lambda_2}, \ldots, \underbrace{y_{l(\lambda)}, \ldots, y_{l(\lambda)}}_{\lambda_{l(\lambda)}}). \end{array} \tag{5}$$

where $y_1, y_2, \ldots, y_{l(\lambda)}$ are new indeterminates. Since the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ satisfy to (4), they also satisfy to (1) (observe that Example 2.5 shows that systems satisfying (1) are strictly more general than systems satisfying (4)). Indeed, choose a pair of distinct integers $\{i, j\} \in [n]$ and let $\sigma \in \mathfrak{S}_n$ be such that $\sigma(k) = k$ if $k \notin \{i, j\}$ and $\sigma(i) = j$, then

$$F^{\{i\}} - F^{\{j\}} = F^{\{i\}} - \sigma(F^{\{i\}}) \in (x_i - x_j). \tag{6}$$

Therefore, the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ admit divided differences. In addition, from their defining equality given in Lemma 2.1 and from (4), we get that for any subset $\{i_1, \ldots, i_k\} \subset [n]$ and any permutation $\sigma \in \mathfrak{S}_n$ we have

$$\sigma\left(F^{\{i_1, \ldots, i_k\}}\right) = F^{\{\sigma(i_1), \ldots, \sigma(i_k)\}}. \tag{7}$$

Now, if $\rho_\lambda(x_i) = \rho_\lambda(x_j)$ then (6) implies that

$$\rho_\lambda(F^{\{i\}}) = \rho_\lambda(F^{\{j\}}).$$

So, for any integer $i \in [l(\lambda)]$ we can define without ambiguity the homogeneous polynomial of degree d

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

where $j \in [n]$ is such that $\rho_\lambda(x_j) = y_i$. Moreover, these polynomials also satisfy (1) and hence they also admit divided differences ; we will denote them by $F_\lambda^{\{i_1, \ldots, i_r\}}(y_1, \ldots, y_{l(\lambda)})$ with $\{i_1, \ldots, i_r\} \subset [l(\lambda)]$. From here, a straightforward application of Lemma 2.1 shows the following property : Given $I = \{i_1, \ldots, i_k\} \subset [n]$, define $J = \{j_1, \ldots, j_k\} \subset [l(\lambda)]$ by the equality $\rho_\lambda(x_{i_r}) = y_{j_r}$ for all $r \in [k]$. Then, if $|J| = |I|$ we have

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

3.2. **The decomposition formula.** Before stating the main result of this paper, we need to introduce a last notation. Given a partition $\lambda \vdash n$, its multinomial coefficient is defined as the integer

$$\binom{n}{\lambda_1, \lambda_2, \ldots, \lambda_{l(\lambda)}} := \frac{n!}{\lambda_1! \lambda_2! \cdots \lambda_{l(\lambda)}!}. \tag{8}$$

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 way of counting, the objects are not ordered inside the boxes, but the boxes are ordered. If we do not want to count the permutations between the boxes having the same number of objects, then we have to divide the above multinomial coefficient 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 $\prod_{j=1}^{n} s_j!$. Finally, for any partition $\lambda \vdash n$ we define the integer

$$m_\lambda := \frac{1}{\prod_{j=1}^{n} s_j!} \binom{n}{\lambda_1, \lambda_2, \ldots, \lambda_{l(\lambda)}}. \tag{9}$$

Theorem 3.3. *Assume that $n \geqslant 2$ and $d \geqslant 1$. With the above notation, the following equalities hold.*

- *If $d \geqslant n$ then*

$$\mathrm{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = \prod_{\lambda \vdash n} \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right)^{m_\lambda}.$$

- *If $d < n$ then*

$$\mathrm{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = \left(F^{\{1,\ldots,d+1\}}\right)^{m_0} \times \prod_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right)^{m_\lambda}$$

where

$$m_0 := nd^{n-1} - \sum_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} m_\lambda \left(\sum_{j=1}^{l(\lambda)} \frac{d(d-1)\cdots(d-l(\lambda)+1)}{(d-j+1)} \right).$$

It is immediate to check that this theorem allows to recover the formulas given in Example 3.1 and Example 3.2. Before giving its proof, we make some comments on some computational aspects.

First, we emphasize that the above formula holds over the universal ring of coefficients of the $\mathfrak{S}_n-$equivariant polynomial system $F^{\{1\}}, \ldots, F^{\{n\}}$ (over $\mathbb{Z}$) and it is hence stable under specialization. Our second comment is on the number of terms in these decompositions. It is equal to the cardinality of the set

$$\{\ \lambda = (\lambda_1, \ldots, \lambda_k) \vdash d \text{ such that } n \geqslant \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k\}$$

that has been extensively studied (we refer the reader to the classical book [11]). It is important to notice that these terms can actually be deduced from a very small number of resultant computations since these resultants are actually also universal with respect to the integers $\lambda_1, \lambda_2, \ldots, \lambda_{l(\lambda)}$ defining a partition, providing $l(\lambda)$ is fixed. Therefore, all the terms in the two decompositions given in Theorem 3.3 can be obtained as specializations of only $\min\{n, d\}$ resultant computations. The following example illustrates this property.

Example 3.4. Consider the case $d = 2$ and $n \geqslant 2$ with a polynomial system of the form $F^{\{i\}} = \sum_{i=0}^{2} x_i^k S_k$ where S_k are symmetric homogeneous polynomials in $x_1, \ldots, x_n$. More precisely, we 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

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

with multiplicity $m_\lambda = 1$. From Theorem 3.3 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

(10)

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

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

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

where $\operatorname{Res}\left(F_{(1,1)}^{\{1\}}, F_{(1,1)}^{\{1,2\}}\right)$ is obtained by specialization of (10). 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

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

where the resultants in this formula are again given by (10) and

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

If $n = 2k$ with $k > 1$ then

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

where the resultants in this formula are always given by (10) 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 3.3 are not always (geometrically) irreducible polynomials. For instance, in the case where $n = 2k$ is an even integer, we have

$$\mathrm{Res}\left(F^{\{1\}}_{(k,k)}, F^{\{1,2\}}_{(k,k)}\right) = (a+bk)^2(a-dk)^2. \tag{11}$$

However, we notice that $\mathrm{Res}(F^{\{1\}}_{\lambda})$ is obviously always irreducible (in the universal setting).

From a geometric point of view, Theorem 3.3 shows that the algebraic polynomial system

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

can be split into the smaller algebraic systems

$$\{F^{\{1\}}_{\lambda} = 0, \ldots, F^{\{1,\ldots,l(\lambda)\}}_{\lambda} = 0\},\ \lambda \vdash n,\ l(\lambda) \leqslant d \tag{12}$$

with multiplicity m_λ, respectively. For each given partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{l(\lambda)})$, the algebraic systems (12) correspond to particular configurations of the roots of the initial system, namely the roots whose coordinates can be grouped into $l(\lambda)$ blocks of size $\lambda_1, \ldots, \lambda_{l(\lambda)}$ respectively, up to permutations.

3.3. **Proof of Theorem 3.3.** 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

$$\begin{aligned}\mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) = \\ \pm\,\mathrm{Res}\left(F^{\{1\}}, (x_1-x_2)F^{\{1,2\}}, (x_1-x_3)F^{\{1,3\}}, \ldots, (x_1-x_n)F^{\{1,n\}}\right).\end{aligned} \tag{13}$$

The divided differences $F^{\{1,j\}}$ are of degree $d-1$. If $d-1=0$ then they are all equal to the same constant by Remark 2.4 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 (13) 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 $[n]$ that 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

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

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

$$\pm\,\mathrm{Res}\left(F^{\{1\}}_1, F^{\{1,2\}}_1, F^{\{1,3\}}_1, \ldots, F^{\{1,k\}}_1\right) \tag{14}$$

where we set $F^{\{1,r\}}_1 := \rho_1(F^{\{1,j_r\}})$, ρ_1 being a specialization map defined by

$$\begin{aligned}\rho_1 : k[x_1,\ldots,x_n] &\to k[x_1,\ldots,x_k]\\ x_j,\ j\in I_1 &\mapsto x_1\\ x_{j_r},\ r=1,\ldots,k-1 &\mapsto x_{r+1}.\end{aligned}$$

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 (14) obtained at the end of the previous step. If $k \leqslant 2$ then we actually do nothing and the splitting of this factor stops here. 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 3.5. 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

$$\operatorname{Res}\left(F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}\right) = \pm\left(F^{\{1,\dots,d+1\}}\right)^{\mu} \times \prod_{(I_1,\dots,I_k)} R_{(I_1,\dots,I_k)} \tag{15}$$

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

$$l_1 := |L_1| \geqslant l_2 := |L_2| \geqslant \dots l_k := |L_k| \quad \text{and} \tag{16}$$

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

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 3.6. *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 (8) 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 3.7. *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 $x_1,\dots,x_n$:

$$F^{\{1\}}, F^{\{1,i_2\}}, \dots, F^{\{1,i_2,\dots,i_k\}}, \{x_{i_1} - x_r\}_{r\in I_1\setminus\{1\}}, \dots, \{x_{i_k} - x_r\}_{r\in I_k\setminus\{i_k\}}. \tag{17}$$

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

$$F^{\{1\}}, F^{\{1,j_2\}}, \dots, F^{\{1,j_2,\dots,j_k\}}, \{x_{j_1} - x_r\}_{r\in J_1\setminus\{1\}}, \dots, \{x_{j_k} - x_r\}_{r\in J_k\setminus\{j_k\}}. \tag{18}$$

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 succesive 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 (7), the application of τ on the list of polynomials (17) returns the following list of polynomials

$$\begin{aligned} (19)\quad & F^{\{1\}}, F^{\{1,j_2\}}, \dots, F^{\{1,j_2,\dots,j_{s-1},j_{s+1}\}}, F^{\{1,j_2,\dots,j_{s-1},j_s,j_{s+1}\}}, \dots, F^{\{1,j_2,\dots,j_k\}}, \\ & \{x_{j_1} - x_r\}_{r\in J_1\setminus\{1\}}, \dots, \{x_{j_{s-1}} - x_r\}_{r\in J_{s-1}\setminus\{j_{s-1}\}}, \{x_{j_{s+1}} - x_r\}_{r\in J_{s+1}\setminus\{j_{s+1}\}}, \\ & \{x_{j_s} - x_r\}_{r\in J_s\setminus\{j_s\}}, \dots, \{x_{j_k} - x_r\}_{r\in J_k\setminus\{j_k\}}. \end{aligned}$$

By the invariance, up to sign, of the resultant under permutations of polynomials and variables (see §2.2), we get that the resultant of the list of polynomials (17), i.e. $R_{(I_1,\dots,I_k)}$, is equal to the resultant of the list of polynomials (19) up to sign. Now, by Proposition 2.3, we have

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

so that the resultant of the polynomials (19) is equal, up to sign, to the resultant of the polynomials (18), 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 (16). 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 (15), Lemma 3.6 and Proposition 3.7 shows that if $d \geqslant n$ then

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

and if $n > d$ then

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

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 $F_\lambda^{\{1,2,\dots,j\}}$, $1 \leqslant j \leqslant l(\lambda)$ is of degree $d-j+1$ by Lemma 2.1. Therefore, the resultant

associated to this partition λ is homogeneous with respect to the coefficients of the $F^{\{i\}}$'s of degree

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

Finally, since $F^{\{1,2,\ldots,d+1\}}$ is homogeneous of degree one in the coefficient of the $F^{\{i\}}$'s (see the defining equality in Lemma 2.1), we deduce that μ is equal to the integer m_0 defined in the statement of Theorem 3.3.

Remark 3.8. If we apply the above degree counting in the case $d \geqslant n$, we get the following combinatorial formula for which we do not know if it is known: if $d \geqslant n$ then

$$nd^{n-1} = \sum_{\lambda \vdash n} m_\lambda \left(\sum_{j=1}^{l(\lambda)} \frac{d(d-1)\cdots(d-l(\lambda)+1)}{d-j+1} \right).$$

To conclude the proof of Theorem 3.3, it remains to determine the sign $\pm$ that occurs in the two formulas. For that purpose, we examine the specialization of these formulas to the case where $F^{\{i\}} = x_i^d$, $i = 1, \ldots, n$. First, it follows from (3) that the resultant of the $F^{\{i\}}$'s is equal to 1. Now, given any partition $\lambda \vdash n$, it is straightforward to check that $F_\lambda^{\{1\}} = x_1^d$. Then applying iteratively Proposition 2.3 from $j = 1$ to $j = l(\lambda)$, it follows that

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

From here, 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. Finally, by Lemma 2.1 it appears that $F^{\{1,\ldots,d+1\}}$ also specializes to 1 in the case $n > d$ and this concludes the proof of Theorem 3.3.

3.4. **Averaging over the divided differences of the same order.** Since the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ satisfy to the property (7), it follows that for any integer $k \in [n]$

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

Therefore, for all $k \in [n]$, the polynomial $\sum_{I \subset [n],\, |I|=k} F^I$ is symmetric. Such a property is useful for applying various polynomial system solving methods (see e.g. [6]). In general, this property is no longer true if we consider F_λ^I instead of F^I (except for the case $\lambda = (1, 1, \ldots, 1)$ which is the case investigated in [6, §3.3]). Nevertheless, it is possible to reformulate Theorem 3.3 by means of these sums of divided differences of the same order.

Proposition 3.9. *Taking again the notation of Theorem 3.3, then for any partition $\lambda \vdash n$ such that $l(\lambda) \leqslant \min\{d, n\}$ we have*

$$\operatorname{Res}\left(\sum_{I \subset [l(\lambda)],\, |I|=1} F_\lambda^I, \sum_{I \subset [l(\lambda)],\, |I|=2} F_\lambda^I, \ldots, \sum_{I \subset [l(\lambda)],\, |I|=l(\lambda)-1} F_\lambda^I, F_\lambda^{\{1,2,\ldots,l(\lambda)\}} \right) =$$
$$\left(\prod_{k=1}^{l(\lambda)-1} \binom{l(\lambda)}{k}^{\frac{d(d-1)(d-2)\cdots(d-l(\lambda)+1)}{d-k+1}} \right) \operatorname{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}} \right).$$

Proof. For any subset $I \subset [l(\lambda)]$ such that $|I| = l(\lambda) - 1$, Corollary 2.6 shows that

$$F_\lambda^I = F_\lambda^{\{1,2,\dots,l(\lambda)-1\}} \mod \left(F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right) \tag{20}$$

from we deduce that

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

In the same way, for any subset $I \subset [l(\lambda)]$ such that $|I| = l(\lambda) - 2$, Corollary 2.6 shows that

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

Using (20), 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 equality (proceed from the right to the left)

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

Now, the claimed result follows from the multi-homogeneity of the resultant since the polynomials F_λ^I are homogeneous of degree $d - |I| + 1$. □

As a consequence of the proof of this proposition, we see that the big constant factor can be removed by taking averages in the sums of divided differences of the same order. More precisely, assume that the coefficient ring contains the rational numbers and set

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

Then, we obtain the equality

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

Example 3.10. Taking again the notation of Example 3.4, a direct computation shows that

$$\operatorname{Res}\left(F_{(m,n-m)}^{\{1\}} + F_{(m,n-m)}^{\{2\}}, F_{(m,n-m)}^{\{1,2\}}\right) = 2\operatorname{Res}\left(F_{(m,n-m)}^{\{1\}}, F_{(m,n-m)}^{\{1,2\}}\right).$$

4. Discriminant of a homogeneous symmetric polynomial

The discriminant of a homogeneous polynomial is a rather complicated object which is known to be irreducible in the universal setting over the integers (see for instance [2, §4]). The purpose of this section is to prove that when the homogeneous polynomial is symmetric then its discriminant can be decomposed into the product of several resultants that are in principle easier to compute (see Theorem 4.2). We will obtain this result by specialization of the two formulas given in Theorem 3.3.

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 to the equality

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

(observe that $e_0(x) = 1$ and that $e_p(x) = 0$ for all $p > n$). For any partition $\lambda = (\lambda_1 \geqslant \cdots \geqslant \lambda_k)$ 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

$$\{e_\lambda(x) \ : \ \lambda = (\lambda_1, \dots, \lambda_k) \vdash d \text{ such that } n \geqslant \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k\} \tag{21}$$

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

$$F(x_1, \dots, x_n) := \sum_{\lambda \vdash d} c_\lambda e_\lambda(x) \in \mathbb{Z}[c_\lambda : \lambda \vdash d][x_1, \dots, x_n]. \tag{22}$$

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 is defined by the equality (see §2.3)

$$d^{a(n,d)} \mathrm{Disc}(F) = \mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}\right) \in \mathbb{U} \tag{23}$$

and that it is homogeneous of degree $n(d-1)^{n-1}$ in $\mathbb{U}$.

Lemma 4.1. *The partial derivatives $F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}$ of the symmetric polynomial $F(x_1, \dots, x_n)$ form a $\mathfrak{S}_n$-equivariant polynomial system.*

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 $i = 1, \dots, n$

$$F^{\{i\}} = \frac{\partial F}{\partial x_i} = \sum_{k=1}^{\min\{d,n\}} \frac{\partial e_k}{\partial x_i} S_k(x_1, \dots, x_n). \tag{24}$$

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

$$\frac{\partial e_j}{\partial x_i} = \sum_{r=0}^{j-1} (-1)^r x_i^r e_{j-1-r}. \tag{25}$$

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

As a consequence of this lemma, Theorem 3.3 can be applied in order to decompose the resultant of the polynomials $F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}$ and hence, by (23), to decompose the discriminant of the symmetric polynomial F. We take again the notation of §2.1 and §3.2.

Theorem 4.2. *Assume that $n \geqslant 2$ and $d \geqslant 2$. With the above notation, the following equalities hold.*

- *If $d > n$ then*

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

- *If $d \leqslant n$ then*

$$d^{a(n,d)}\mathrm{Disc}\,(F) = \left(F^{\{1,\dots,d\}}\right)^{m_0} \prod_{\substack{\lambda\vdash n\\ l(\lambda)<d}} \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right)^{m_\lambda}$$

where

$$m_0 := n(d-1)^{n-1} - \sum_{\substack{\lambda\vdash n\\ l(\lambda)<d}} m_\lambda \left(\sum_{j=1}^{l(\lambda)} \frac{(d-1)(d-2)\cdots(d-l(\lambda))}{(d-j)}\right).$$

Moreover, if F is given by (22) then $F^{\{1,\dots,d\}} = (-1)^{d-1}c_{(d)}$ so that

$$d^{a(n,d)}\mathrm{Disc}\,(F) \;=\; (-1)^{\varepsilon}\,(c_d)^{m_0} \prod_{\substack{\lambda\vdash n\\ l(\lambda)<d}} \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\dots,l(\lambda)\}}\right)^{m_\lambda}$$

where $\varepsilon = n-1$ if $d = 2$ and $\varepsilon = 0$ if $d \geqslant 3$.

Proof. These formulas are obtained by specialization of the formulas given in Theorem 3.3 with the difference that the polynomials $F^{\{i\}}$, $i = 1, \dots, n$ are of degree $d-1$ in our setting (and not of degree d as in Theorem 3.3). Thus, the only thing we need to show is that

$$F^{\{1,\dots,d\}} = (-1)^{d-1}c_{(d)} \tag{26}$$

under the assumption $n \geqslant d$, where $c_{(d)}$ is the coefficient of F in the writing (22) that corresponds to the partition $\lambda = (d)$. Indeed, by the above second equality for m_0 we see that m_0 is even if $d \geqslant 3$, whereas the first equality shows that $m_0 = n - 1 \mod 2$ if $d = 2$.

To prove (26), observe that (24) and (25) show that there exist symmetric homogeneous polynomials $S_k(x_1, \dots, x_n)$, $k = 1, \dots, d$ of degree $d-k$ respectively, such that for all $i = 1, \dots, n$

$$F^{\{i\}} = \sum_{k=1}^{d} \frac{\partial e_k}{\partial x_i} S_k(x_1, \dots, x_n) = \sum_{k=1}^{d}\sum_{r=0}^{k-1} (-1)^r x_i^r e_{k-1-r} S_k = \sum_{r=0}^{d-1} x_i^r \left(\sum_{k=r+1}^{d} (-1)^r e_{k-1-r} S_k\right). \tag{27}$$

Now, by the defining equality of divided differences given in Lemma 2.1, we have

$$V(x_1, x_2, \dots, x_d)\cdot F^{\{1,\dots,d\}} = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{d-2} & F^{\{1\}} \\ 1 & x_2 & \cdots & x_2^{d-2} & F^{\{2\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_d & \cdots & x_d^{d-2} & F^{\{n\}} \end{vmatrix}.$$

Therefore, using (27) one can reduce, by elementary operations on columns, the last column of the above determinant to terms corresponding to the indexes $k = d, r = d-1$, that is to say

$$\begin{vmatrix} 1 & x_1 & \cdots & x_1^{d-2} & F^{\{1\}} \\ 1 & x_2 & \cdots & x_2^{d-2} & F^{\{2\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_d & \cdots & x_d^{d-2} & F^{\{n\}} \end{vmatrix} = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{d-2} & (-1)^{d-1}x_1^{d-1}S_d \\ 1 & x_2 & \cdots & x_2^{d-2} & (-1)^{d-1}x_2^{d-1}S_d \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_d & \cdots & x_d^{d-2} & (-1)^{d-1}x_1^{d-1}S_d \end{vmatrix}.$$

It follows that $F^{\{1,\dots,d\}} = (-1)^{d-1}S_d$. Finally, from the definition (22) of F, we have $S_d = c_{(d)}$ and the proof is completed. □

We emphasize that the formulas given in this theorem are universal with respect to the coefficients of F and are independent of the choice of basis that is used to represent F (for the sake of generality, we have chosen the basis (21) as an illustration). We also mention that formulas similar to the ones given in §3.4 can also be written explicitly for the discriminant of F (this is actually the point of view that has been used in [13]).

Hereafter, 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 4.2 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

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

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

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

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

$$F = c_{(3)}e_3 + c_{(2,1)}e_2e_1 + c_{(1,1,1)}e_1^3.$$

The formula given in Theorem 4.2 shows that

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

where all the factors can be described explicitly. To begin with, from (24) and (25) we get that for all $i = 1, \dots, n$

$$F^{\{i\}} = c_{(3)}\left(e_2 - x_ie_1 + x_i^2\right) + c_{(2,1)}\left(e_2 + e_1(e_1 - x_i)\right) + 3c_{(1,1,1)}e_1^2.$$

It follows immediately that

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

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

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

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 $m_{(\frac{1}{2},\frac{1}{2})} = \frac{1}{2}\binom{n}{\frac{n}{2}}$. 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 detail the two particular cases $n=3$ and $n=4$. If $n=3$, we obtain

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

where

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

and

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

If $n=4$ we get

$$\begin{aligned}\operatorname{Disc}(F) = -{c_{(3)}}^{10}\left(c_{(3)} + 2\,c_{(2,1)}\right)^9\left(6\,c_{(2,1)} + 16\,c_{(1,1,1)} + c_{(3)}\right)\times\\ \left(4\,c_{(1,1,1)}{c_{(3)}}^2 - 3\,{c_{(2,1)}}^2c_{(3)} - 2\,{c_{(2,1)}}^3\right)^4\end{aligned} \tag{28}$$

where

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

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

and

$$\operatorname{Res}\left(F^{\{1\}}_{(2,2)}, F^{\{1,2\}}_{(2,2)}\right) = -\left(c_{(3)} + 2\,c_{(2,1)}\right)^3,\ m_{(2,2)} = 3. \tag{29}$$

For instance, for the particular example of the Clebsch surface which is given by the equation

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

we recover the known fact that $h/3$ defines a smooth cubic in every characteristic except 5 (see [14, §5.4]) since (28) shows that

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

Remark 4.3. Contrary to what was expected in [13], the resultant factors appearing in Theroem 4.2 are not always irreducible (see e.g. (29)). However, we ignore if these resultant factors are geometrically irreducible (i.e. are irreducible polynomials up to a certain power) when the ground ring is assumed to be field, but this was the case in all the experiments that we have done. As an illustration, we notice that the factor (11) appearing in Example 3.4 is not geometrically irreducible, but it becomes geometrically irreducible (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 $d = -b = c_{(3)} + c_{(2,1)}$.

Acknowledgments. The authors are grateful to Evelyne Hubert for useful discussions on equivariant polynomial systems. 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] Jean-Pierre Jouanolou. Formes d'inertie et résultant: un formulaire. *Adv. Math.*, 126(2):119–250, 1997.
[10] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33):3–27, 1902.
[11] 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.
[12] Jiawang Nie. Discriminants and nonnegative polynomials. *J. Symbolic Comput.*, 47(2):167–191, 2012.
[13] N. Perminov and S. Shakirov. Preprint arxiv:0910.5757v1. Discriminants of Symmetric Polynomials, 2009.
[14] Takeshi Saito. The discriminant and the determinant of a hypersurface of even dimension. *Math. Res. Lett.*, 19(4):855–871, 2012.
[15] 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.