Efficient computation of square-free Lagrange resolvents [1]

Antoine Colin
LIX
UMR CNRS-Polytechnique 7161
Antoine.Colin@Polytechnique.fr

Marc Giusti
LIX
UMR CNRS-Polytechnique 7161
Marc.Giusti@Polytechnique.fr
École polytechnique, F-91128 Palaiseau Cedex France

[1] This work was supported in part by the French National Agency for Research (ANR-2010-BLAN-0109-04 "LEDA") and the Scientific Cooperation Foundation DIGITEO project 2009-36HD "Magix"

Abstract

We propose a general frame to compute efficiently in the algebra of polynomial invariants under a finite subgroup of the general linear group. The classical Noether normalization of this Cohen-Macaulay algebra takes a natural form when expressed with adequate data structures, based on evaluation rather than writing. This allows to compute more efficiently its multiplication tensor.

As an illustration we give a fast symbolic algorithm to compute the coefficients of the Lagrange resolvent associated to the given subgroup, either generically or specialized. We show also how to find square-free resolvents with better theoretical complexity (polynomial in the index of the subgroup after a precomputation depending only on the subgroup).

This relies on a geometric link between the discriminant of the natural Noether projection and two other discriminants related to fundamental invariants.

Contents

Dedicated to Joos Heintz
for his pioneering work

Introduction and notations

Scalars. In the whole article, k is a field of characteristic 0, $\bar{k}$ an algebraic closure. When geometry is considered (as in sections 2, 3 and 4.1), we work with the affine space $\mathbb{A}^n = \mathbb{A}^n_{\bar{k}}$. A *point* will design an element of $\mathbb{A}^n$.

When algorithmic considerations are at stake (from § 4.2), the scalars belong to k, and k is assumed to be an effective field.

Invariants. In the whole article, H is a finite subgroup of the general linear group $\mathbf{GL}_n(k)$. It has a right action on the polynomial ring $k[\mathbf{X}] = k[X_1, \ldots, X_n]$, through the map

$$(p, A) \mapsto p^A = p(A.\mathbf{X}) = p\left(a_{11}X_1 + \ldots a_{1n}X_n, \ldots, a_{n1}X_1 + \cdots + a_{nn}X_n\right)$$

where $A = (a_{i,j})$ is an element of H and p a polynomial.

The invariant polynomials under this action form the invariant algebra denoted by $k[\mathbf{X}]^H = k[X_1, \ldots, X_n]^H$, equipped with the induced graded structure inherited from $k[\mathbf{X}]$.

We consider the symmetric group $\mathfrak{S}_n$ as a subgroup of $\mathbf{GL}_n(k)$ by identifying a permutation τ with the *permutation matrix* $A_\tau = (\delta_{i,\tau(j)})$. It induces a right action of $\mathfrak{S}_n$ on $k[\mathbf{X}]$. Therefore, in the following, the case $H \subset \mathfrak{S}_n$ will be considered as a subcase of $H \subset \mathbf{GL}_n(k)$.

$\star$

A well-known theorem, which goes back to [Hochster-Eagon, 1971], says that the invariant algebra $k[\mathbf{X}]^H$ is a free module over a regular algebra. Elements of a transcendance basis of the latter are called *primary* invariants, while elements of a basis of the free module are *secondary* ones. All together, they form a set of *fundamental* invariants.

We introduce the variety $\mathcal{V}$ whose algebra of functions is the invariant algebra $k[\mathbf{X}]^H$. We have first to find an explicit embedding of $\mathcal{V}$ into a linear affine space through explicit equations. Then we consider the natural parametrization φ given by the fundamental invariants. A third step is the projection p of $\mathcal{V}$ on the n first variables (corresponding to the primary invariants). Eventually, the composition $\varpi = p \circ \varphi$ is nothing else than the map defined by the primary invariants.

The fundamental feature of this commutative triangle is the theorem

Corollary 16 *The discriminant of ϖ is the union of the discriminant of p and the image by p of the discriminant of φ.*

The discriminants of φ, p and ϖ are defined by ideals with explicit generators.

We address now the problem to compute efficiently in the invariant algebra $k[\mathbf{X}]^H$.

It turns out that the linear structure mentioned above realizes the Noether normalization lemma. Besides, M. Giusti, J. Heintz, L. M. Pardo and their collaborators showed in a sequence of papers (see *e.g.* [Giusti-Heintz, 1991], [Giusti-Heintz-Sabia, 1993], [Giusti-Heintz-Morais-Pardo, 1995], [Giusti-Hägele-Heintz-Morais-Montaña-Pardo, 1996], [Giusti-Heintz-Morais-Pardo, 1997]), that a Noether position is a good frame for fast computations in the context of multivariate polynomial algebras. The reason is that it enables to use an adequate data structure (straight-line programs) to store with better complexity the free (or transcendental) variables. In particular this explains why fast evaluation techniques work when specializing these variables. Applications of this general fact to the resolution of polynomial systems and effective Nullstellensätze can be found in *loc. cit.*

In this paper, we show that this idea has a new application in computational geometric invariant theory: considering primary invariants as free variables will allow to compute more efficiently in invariant algebras under finite groups.

As an illustration in the case of a permutation subgroup (where we chose for primary invariants the symmetric elementary polynomials) we obtain an efficient computation of Lagrange resolvents. These latter are nothing else than characteristic polynomials of primitive elements of the Noether extension, with respect to a specialization of the free variables.

In this particular case, Corollary 16 becomes

The discriminant of p (and besides the dirimant of p) coincides with the (irreducible) discriminant of the universal monic polynomial of degree n.

Eventually, we obtain the complexity theorem:

Theorem 27 *After a precomputation depending only on the permutation subgroup H, there exists an algorithm that computes the Lagrange H-resolvent of any univariate polynomial, and a square-free one if required, in polynomial time in the index of the subgroup H.*

For the general results in invariant theory used in this article, the reader can refer to [Sturmfels, 1993] and [Derksen-Kemper, 2002].

We want to thank Éric Schost for inspiring hints and corrections in sections 2 and 3.

1 The algebra of invariants

1.1 Reminder: first fundamental theorem

To the best of our knowledge, the following result was first proved by [Hochster-Eagon, 1971].

Theorem 1 *Let H be a finite subgroup of $\mathbf{GL}_n(k)$. The algebra $k[\mathbf{X}]^H$ is Cohen-Macaulay of Krull-dimension n. There exists an algebraically independent family $\mathbf{\Pi} = (\Pi_1, \ldots, \Pi_n)$ of homogeneous invariant polynomials such that*

$k[\mathbf{X}]^H$ be a finitely generated module over $k[\mathbf{\Pi}]$; and for any such choice $\mathbf{\Pi}$, $k[\mathbf{X}]^H$ is a free $k[\mathbf{\Pi}]$-module. Its rank is $r = (\prod_{i=1}^{n} \deg(\Pi_i))/|H|$.

The polynomials Π_i are called *primary invariants* of H. We note their degrees $d_i = \deg \Pi_i$. A homogeneous basis $\mathbf{\Sigma} = (\Sigma_1, \dots, \Sigma_r)$ of $k[\mathbf{X}]^H$ as a free module over $k[\mathbf{\Pi}]$ is called a family of *secondary invariants* of H. As there must be a constant polynomial among the secondary invariants, we choose conventionally for Σ_1 always the scalar 1. The degrees of the secondary invariants is bounded by $\deg \Pi_1 + \cdots + \deg \Pi_n - n$.

Together, primary and secondary invariants form a set of *fundamental invariants* generating $k[\mathbf{X}]^H$ as an algebra. To sum up we obtain the so-called *Hironaka decomposition*:

$$k[\mathbf{X}]^H = \bigoplus_{i=1}^{r} k[\mathbf{\Pi}]\Sigma_i \qquad \text{(direct sum of } k[\mathbf{\Pi}]\text{-modules)} \tag{1}$$

where the Π_i are algebraically independent over k, and the Σ_i are linearly independent algebraic integers over $k[\Pi_1, \dots, \Pi_n]$.

There are many possible choices for the primary invariants Π_i. It is easy to see that homogeneous invariant polynomials $\Pi_1, \dots, \Pi_n$ form a family of primary invariants if and only if they define the empty projective subvariety over $\bar{k}$. Indeed, this last assertion is equivalent by the projective Nullstellensatz to the finiteness of the dimension of $k[\mathbf{X}]/(\Pi_1, \dots, \Pi_n)$ as a k-vector space.

Consequently, in the case of a permutation subgroup H of $\mathfrak{S}_n$, the *elementary symmetric polynomials*, noted $\mathbf{E} = (E_1, \dots, E_n)$ from now on, are always a possible choice. The number r of secondary invariants is then $[\mathfrak{S}_n : H]$.

In the general case of a finite linear subgroup H of $\mathbf{GL}_n(k)$, an algorithm to yield a family of fundamental invariants was given by [Kemper, 1996] and implemented in `Magma`. His software can also express a given invariant in terms of the fundamental invariants.

Besides, secondary invariants can always be chosen as follows:

- the first ones, say $\Sigma_2, \dots, \Sigma_q$, are — each of them — the sum of the elements of the orbit of a monomial $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ (hence the number of terms in Σ_i divides the order of H).

- each of the last ones $\Sigma_{q+1}, \dots, \Sigma_r$ is a monomial in the first ones, *i.e.* has the form $\Sigma_2^{\nu_2} \dots \Sigma_q^{\nu_q}$.

G. Kemper's algorithm yields secondary invariants of this form, with q as low as possible. On the contrary, it is always possible to choose secondary invariants all of the first form (*i.e.* such that $q = r$). When useful in some complexity computations, we will assume that it is so.

1.2 Second fundamental theorem

In the context of the previous section, let $Y_1, \dots, Y_n, Z_1, \dots, Z_r$ be indeterminates and Ψ the k-algebra morphism from $k[\mathbf{Y}, \mathbf{Z}] = k[Y_1, \dots, Y_n, Z_1, \dots, Z_r]$ onto $k[\mathbf{X}]^H$ defined by

$$\Psi(Y_i) = \Pi_i, \ \Psi(Z_j) = \Sigma_j \ .$$

The kernel $\mathfrak{I}$ of Ψ is the ideal of $k[\mathbf{Y},\mathbf{Z}]$ of all algebraic relations among the fundamental invariants.

1.2.1 Trivial relations

We find easily polynomials in $\mathfrak{I}$ as follows. Each product $\Sigma_i\Sigma_j$, $2 \leq i \leq j \leq r$, belongs to $k[\mathbf{X}]^H$, so can be expressed in terms of the fundamental invariants $\Pi_1,\ldots,\Pi_n,\Sigma_1,\ldots,\Sigma_r$:

$$\Sigma_i\Sigma_j = \sum_{l=1}^{r} A_l^{i,j}(\Pi_1,\ldots,\Pi_n)\ \Sigma_l\ ,\ \text{ where } A_l^{i,j} \in k[\mathbf{Y}]\ . \tag{2}$$

Therefore, the polynomials $S_{i,j} = Z_iZ_j - \sum_{l=1}^{r} A_l^{i,j}(\mathbf{Y})Z_l$ ($2 \leq i \leq j \leq r$) and $S_0 = 1 - Z_1$ belong to $\mathfrak{I}$.

1.2.2 All relations

Conversely, we have:

Proposition 2 *The polynomials $S_{i,j}$, $2 \leq i \leq j \leq r$, and S_0 generate the ideal $\mathfrak{I}$ of $k[\mathbf{Y},\mathbf{Z}]$. Indeed, these polynomials form a Gröbner basis of $\mathfrak{I}$ in $k[\mathbf{Y},\mathbf{Z}]$ with respect to any monomial order $\preceq$ such that* ($\deg_Z P < \deg_Z Q \Rightarrow P \preceq Q$)*,* e.g. *a Bayer & Stillman's order.*

Proof – See [Colin Thesis, 1997, lemme 4.13]. We consider a polynomial P of $\mathfrak{I}$, and a reduced form R of P modulo all the generators $S_{i,j}$ and S_0 with respect to $\preceq$. As each product Z_iZ_j is the leading monomial of $S_{i,j}$ (with respect to $\preceq$), R must be linear in the Z_i. Now, as R belongs to $\mathfrak{I}$ and $(\Sigma_1,\ldots,\Sigma_r)$ is linearly free over $k[\mathbf{Y}]$, we deduce that $R = 0$. As a Gröbner basis generates, we are done. □

To sum up, the following exact sequence

$$0 \longrightarrow \mathfrak{I} \longrightarrow k[\mathbf{Y},\mathbf{Z}] \longrightarrow k[\mathbf{\Pi},\mathbf{\Sigma}] = k[\mathbf{X}]^H \longrightarrow 0 \tag{3}$$

allows us to identify the invariant algebra $k[\mathbf{X}]^H$ with $k[\mathbf{Y},\mathbf{Z}]/\mathfrak{I}$, with $\mathfrak{I}$ generated by S_0 and the $S_{i,j}$.

1.2.3 Computation of the generic relations: standard method

We call the previous algebraic relations "generic", in contrast with "specialized" ones, obtained by specializing the variables Y_i to scalars y_i. As the generic relations generate a prime ideal, a brute force algorithm could be any elimination process, e.g. to compute a reduced Gröbner basis $\mathcal{G}(\mathcal{I})$ of the ideal $\mathcal{I}$ generated in $k[\mathbf{X},\mathbf{Y},\mathbf{Z}]$ by the polynomials $Y_i - \Pi_i(\mathbf{X}), i \in \{1,\ldots,n\}$ and the $Z_j - \Sigma_j(\mathbf{X}), j \in \{1,\ldots,r\}$ with respect to a Bayer and Stillman order that eliminates first the block of variables $\mathbf{X}$.
Since the elements of $k[\mathbf{Y},\mathbf{Z}] \cap \mathcal{G}(\mathcal{I})$ form a Gröbner basis of the prime elimination ideal $\mathcal{I} \cap k[\mathbf{Y},\mathbf{Z}] = \mathfrak{I}$, they generate $\mathfrak{I}$.

Remark: As $k[\mathbf{X}]^H$ is a free $k[\mathbf{\Pi}]$-module, the polynomials $A_l^{i,j}$ are uniquely determined by the equations (2). The algorithm above can be interpreted in linear algebra and consists merely in inverting a linear system. For each couple (i,j) such that $2 \leq i \leq j \leq r$ we search scalars $a_{k,\boldsymbol{\alpha}}$ such that

$$\Sigma_i \Sigma_j = \sum_{k=1}^{r} \left(\sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{k,\boldsymbol{\alpha}} \prod_{l=1}^{n} \Pi_l^{\alpha_l} \right) \Sigma_k .$$

The sum on $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ is finite, since $a_{k,\boldsymbol{\alpha}} = 0$ if $\sum_{l=1}^{n} \alpha_l d_l \neq \deg \Sigma_i + \deg \Sigma_j - \deg \Sigma_k$ (homogeneity).

Now, writing this equation on the k-basis $(X_1^{i_1} \ldots X_n^{i_n})_{i_1 + \cdots + i_n = \deg \Sigma_i \Sigma_j}$ of the homogenous polynomials of degree $\deg \Sigma_i \Sigma_j$, we get a system of

$$\binom{n + \deg \Sigma_i \Sigma_j - 1}{n-1}$$

k-linear equations in the $a_{k,\boldsymbol{\alpha}}$'s, and this system has a unique solution from (1).

1.2.4 Computation of the generic relations: trace method

From [Colin Thesis, 1997, Prop. 4.11].

We recall (see [Derksen-Kemper, 2002, Lemma 3.9.6]) that $k(\mathbf{X})^H$ is the fraction field of $k[\mathbf{X}]^H$. As the field extension $k(\mathbf{X})^H : k(\mathbf{\Pi})$ is separable, it is well known that the $k(\mathbf{\Pi})$-bilinear form

$$(f,g) \longmapsto \mathrm{Tr}(fg) \tag{4}$$

induced by the trace operator Tr is non-degenerate. So, for each (i,j), the equations

$$\mathrm{Tr}(\Sigma_i \Sigma_j \Sigma_k) = \sum_{l=1}^{r} A_l^{i,j}(\mathbf{\Pi}) \mathrm{Tr}(\Sigma_l \Sigma_k), \qquad 1 \leq k \leq r \tag{5}$$

form a regular system of r linear equations in the r quantities $A_l^{i,j}$ over the field $k(\mathbf{\Pi})$. We determinate these quantities by solving the system, after having computed its coefficients if we know how by chance, as follows.

Computation of the trace: In the particular case when $k(\mathbf{\Pi})$ is itself the invariant field $k(\mathbf{X})^L$ of a finite subgroup L of $\mathbf{GL}_n(k)$ containing H, computations of traces can be done from scratch. The trace operator satisfies $\mathrm{Tr}(f) = \sum_{\tau \in L /\!\!/ H} f^{\tau}$, where $L /\!\!/ H$ is a representative system of the right cosets of H in L (of course, $[L : H] = r$).

In the even more particular case when L is $\mathfrak{S}_n$ and $\mathbf{\Pi}$ is $\mathbf{E}$, the trace of any element can be expressed easily in terms of $\mathbf{E}$ and the computation of the algebraic relations in this case was implemented in `Axiom` by the first author.

1.2.5 Computation of the specialized relations

Anticipating §4, we draw the attention of the reader on the fact that the previous method is well adapted to evaluation: instead of computing the generic coefficients $A_l^{i,j}(\mathbf{\Pi})$ (with $A_l^{i,j}$ in $k[\mathbf{Y}]$) of the relations, we can build a straight

line program that computes $A_l^{i,j}(\boldsymbol{y})$ for each $\boldsymbol{y} = (y_1, \dots, y_n) \in k^n$.
It works especially well in the particular case when $\mathbf{\Pi}$ is $\mathbf{E}$. We propose two algorithms.

Algorithm 1
Input: $(\mathbf{\Pi}, \mathbf{\Sigma}) = (\mathbf{E}, \mathbf{\Sigma})$ and a point $\boldsymbol{y} \in k^n$.
Output: the coefficients $A_k^{i,j}(\boldsymbol{y})$.

i. Precomputation: compute the products $\Sigma_i \Sigma_j \in k[\mathbf{X}]$ for $2 \leq i \leq j \leq r$ and $\Sigma_i \Sigma_j \Sigma_k \in k[\mathbf{X}]$ for $2 \leq i \leq j \leq k \leq r$

ii. Compute the specialized values $s_{i,j}$ of $\mathrm{Tr}(\Sigma_i \Sigma_j)$ and $t_{i,j,k}$ of $\mathrm{Tr}(\Sigma_i \Sigma_j \Sigma_k)$ in $\boldsymbol{y}$.

iii. For each $2 \leq i \leq j \leq r$, solve the system

$$\sum_{l=1}^{r} s_{k,l} a_l^{i,j} = t_{i,j,k} \qquad (1 \leq k \leq r)$$

and get its solution $(a_l^{i,j})_{1 \leq l \leq r}$. Then $A_l^{i,j}(\boldsymbol{y}) = a_l^{i,j}$.

Step (i) is done only once, it does not depend on the specialized value $\boldsymbol{y}$.

Step (ii) does not require an extra computation to yield the symmetric polynomials $\mathrm{Tr}(\Sigma_i \Sigma_j \Sigma_k)$ and $\mathrm{Tr}(\Sigma_i \Sigma_j)$, except a sorting algorithm, if we decide to represent a symmetric polynomial by its leading monomial (*e.g.* X_1 for $X_1 + \cdots + X_n$). With this representation, these symmetric polynomials can be specialized thanks to the algorithm of A. Valibouze [Valibouze, 1986, §5.2.1] implemented in Macsyma [Valibouze, 1989] and in AXIOM by A. Colin [Colin Thesis, 1997, Prop. 2.4].

In step (iii), the matrix of the $r(r-1)/2$ systems are the same, only the right hand side changes. Therefore, the operations to solve these systems can be saved and applied to each right hand side.

Complexity:
Each polynomial Σ_i, $2 \leq i \leq q$, has at most $|H|$ terms, of degree at most $\deg \Pi_1 + \cdots + \deg \Pi_n - n = \frac{n(n-1)}{2}$. Let us suppose $q = n$ (we can choose the secondary invariants this way). Then, each product $\Sigma_i \Sigma_j \Sigma_k$ has at most $|H|^3$ terms.

Computing the trace of one monomial with the algorithm of [Valibouze, 1986, §5.2.1] or [Colin Thesis, 1997, Prop. 2.4] has complexity $O(n!)$ (if applied to a dense polynomial, the complexity is even linear in the number of monomials, but here the polynomials $\Sigma_i \Sigma_j \Sigma_k$ are far from dense).

In fact, we needn't compute the trace of each monomial in $\Sigma_i \Sigma_j \Sigma_k$, one monomial per orbit under H is enough: that leads to $|H|^2$ monomials, and $O(|H|^2 n!)$ operations.

There are $(O(r^3))$ products $\Sigma_i \Sigma_j \Sigma_k$, so step (ii) requires $O(r^3 |H|^2 n!) = O(r(n!)^3)$ operations (as $n! = r.|H|$).

And step (iii) requires $O(r^4)$ operations : $O(r^4)$ to invert the matrix $(s_{k,l})$ without division, then $O(r^4)$ again to multiply the inverse matrix by the column $(t_{i,j,k})_{1\leq k\leq r}$ ($O(r^2)$ operations) for $2 \leq i \leq j \leq r$ ($\frac{r(r-1)}{2}$ times).

Together, the three steps require $O(r(n!)^3 + r^4)$ operations.

Remark 3 *In practise, the term $O(r(n!)^3)$ can often be improved: when each polynomial Σ_i involves only monomials in a_i inderterminates, with $a_i \ll n$. Then, each $\Sigma_i\Sigma_j\Sigma_k$ involves only monomials in $a_i + a_j + a_k$ indeterminates, and the complexity of its trace computation is reduced to $O(n^{a_i+a_j+a_k})$ (instead of $O(n!)$) for each term. The number of terms in Σ_i is bounded by $\binom{n}{a_i} = O(n^{a_i})$ so the complexity of step (ii) is $O(r^3n^{a+a'})$ where $a = \mathrm{Max}_{i<j<k}a_i + a_j + a_k$ and $a' = \mathrm{Max}_{i<j}a_i + a_j$. Note that a and a' are obviously not constant, they depend strongly on $(\mathbf{\Pi}, \mathbf{\Sigma})$.*

Cauchy modules, Ampère's relations and Algorithm 2

It is possible to specialize already in step (i), by computing in the universal decomposition algebra. For this purpose, we use Cauchy's modules (see [Machì-Valibouze, 1991]). These are the polynomials f_j in $k[X_1, \dots, X_j]$ defined for $1 \leq j \leq n$ by

$$f_j(X_1, \dots, X_j) = \sum_{i=0}^{n-j+1} (-1)^i y_i h_{j,n-j-i+1}(X_1, \dots, X_j)$$

where $y_0 = 1$ and $h_{j,p}(X_1, \dots, X_j) = \sum_{\alpha_1+\cdots+\alpha_j=p} X_1^{\alpha_1} \dots X_j^{\alpha_j}$ is the sum of all monomials of total degree p in $X_1, \dots, X_j$. From [Machì-Valibouze, 1991], $f_1, \dots, f_n$ form a Gröbner basis of the ideal $(E_1 - y_1, \dots, E_n - y_n)$ for any order refining the total degree. Besides, they can be computed recursively by Ampère's relations:

$$\begin{aligned} f_1(X_1) &= X_1^n + \sum_{l=1}^{n}(-1)^l y_l X_1^{n-l} \\ f_j(X_1, \dots, X_j) &= \frac{f(X_1, \dots, X_{j-2}, X_j) - f(X_1, \dots, X_{j-1})}{X_j - X_{j-1}} \qquad 2 \leq j \leq n. \end{aligned}$$

In steps (i) and (ii) the double and triple products are replaced by their normal form via the reduction by the Gröbner basis (so, step (i) in algorithm 2 is no longer a precomputation).

Step (iii) remains unchanged.

Complexity

For readability, we hide logarithmic factors in complexity estimates, using the notation “soft O” (noted $\widetilde{O}$), defined in [von zur Gathen-Gerhard, 2003, chapter 25.7].

The cost of an addition or multiplication in the universal decomposition algebra is $O(n!)$.

If Σ_i is irreducible, then it has at most $|H|$ terms and its degree is at most $\frac{n(n-1)}{2}$. The cost to evaluate each of its monomials in the universal decomposition algebra is $O(n!(n + n\log(n(n-1)/2))) = O(n!n\log(n)) = \widetilde{O}(n!n)$. So the cost for Σ_i is $\widetilde{O}(|H|n!n)$. As there is at most r irreducible polynomials Σ_i, the cost for all of them is $\widetilde{O}((n!)^2.n)$ (because $r|H| = n!$).

The other Σ_i's are monomials in the irreducible Σ_i's of degree at most $O(n^2)$. So, computing them involves at most r multiplications of distinct Σ_j's and r powerings (of power at most $O(n^2)$): that makes $O(r + r\log(n^2)$ multiplications in the universal decomposition algebra, which costs $\widetilde{O}(n!r)$ scalar operations for each Σ_i, and as a whole $\widetilde{O}(n!r^2)$.

Now, evaluating the $O(r^2)$ double products and the $O(r^3)$ triple products costs $O(r^3 n!)$. And from [Lebreton-Schost, 2012], their traces can then be evaluated with a complexity $O(r^3 n! \log(n!) \log\log(n!)) = O(r^3 n! n \log(n)) = \widetilde{O}(r^3 n! n)$.

Consequently, considering the $O(r^4)$ operations still needed for step (iii), the complexity of algorithm 2 is $\widetilde{O}((n!)^2 n + r^3 n! n + r^4)$.

Remark 4 *The complexity algorithm 2 is smaller than that of algorithm 1. Nonetheless, algorithm 1 is better than algorithm 2 when the degrees of the Σ_i's are small compared to n, since in this case, computing in the universal decomposition algebra is useless, wheras the precomputation of step (i) of algorithm 1 is usefull.*

Algorithm 3

X. Dahan, É. Schost and J. Wu proved in [Dahan-Schost-Wu, 2009, Theorem 1] that if a polynomial $F \in k[\mathbf{X}]$ is given by a straight-line program of size L and $\mathbf{\Pi}, \mathbf{\Sigma}$ by a straight-line program of size $L_{\mathbf{\Pi},\mathbf{\Sigma}}$, then one can construct a straigt-line program of size $O(n^4 d^4 + nd^6 + L_{\mathbf{\Pi},\mathbf{\Sigma}} nd^4 + Ld^3)$ that computes the coordinates of F in the $k[\mathbf{\Pi}]$-module basis $\mathbf{\Sigma}$, where $d = \prod_{i=1}^n \deg \Pi_i = r|H|$.

If we apply this result to each product $\Sigma_i \Sigma_j$, we get straight-line programs for all the $A_k^{i,j}$. The total complexity when (i,j) takes all possible values is $O(r^2(n^4 d^4 + nd^6 + L_{\mathbf{\Pi},\mathbf{\Sigma}} nd^4 + Ld^3))$.

Algorithm 3 can be used in the general case of a matrix group H, but is not useful in the particular case $H \subset \mathfrak{S}_n$ and $\mathbf{\Pi} = \mathbf{E}$. Indeed, in this case, $L = 1$, $L_{\mathbf{\Pi},\mathbf{\Sigma}} = O(n.(n\log n).|H| + r^2(n\log n).|H|) = \widetilde{O}(n!nr)$, $d = n!$, so that the complexity bound of algorithm 3 is $\widetilde{O}((n!)^6 nr^2 + (n!)^5 n^2 r^3)$ which is much worse than algorithm 2 and even than algorithm 1 (we remind that $r \leq n!$).

2 The geometry of invariants

In the following, if I is an ideal of $k[\mathbf{X}]$, $\mathbf{V}(I)$ denotes the algebraic subvariety defined by I in $\mathbb{A}^n$.

Usually in computer algebra, a variety is naturally embedded in a given ambient space since it is defined by equations. So its algebra of functions is a quotient of a regular algebra. On the opposite here, the invariant algebra $k[\mathbf{X}]^H$ is a subalgebra of a regular algebra. From the section above, it can be seen as the algebra of functions on the algebraic variety $\mathcal{V} = \mathbf{V}(\mathfrak{I}) \subset \mathbb{A}^{n+r}$, which is irreducible since $\mathfrak{I}$ is prime.

2.1 Reminder: the parametrization of the quotient variety

In this section, let us recall briefly classical notions and properties of quotient varieties (see e.g. [Derksen-Kemper, 2002] and [Cox-Little-O'Shea, 1992]). First, the *categorical quotient* $\mathbb{A}^n /\!\!/ H$ is the affine variety $\mathcal{V}$ corresponding to the ring $k[\mathbf{X}]^H$.

The canonical projection

$$\varphi : \left| \begin{array}{lcl} \mathbb{A}^n & \longrightarrow & \mathcal{V} \\ \boldsymbol{x} & \longmapsto & \varphi(\boldsymbol{x}) = (\boldsymbol{\Pi}(\boldsymbol{x}), \boldsymbol{\Sigma}(\boldsymbol{x})) \end{array} \right.$$

is a parametrization of $\mathcal{V}$ associated to the inclusion $\varphi^* \ : k[\mathbf{X}]^H \hookrightarrow k[\mathbf{X}]$. This extension is integral because any $P \in k[\mathbf{X}]$ is cancelled by the monic polynomial $\prod_{\tau \in H} (T - P^\tau)$ whose coefficients belong to $k[\mathbf{X}]^H$. The application φ is then finite, proper, dominant, hence onto.

On the other hand there exists a left action of the general linear group, or any of its finite subgroups, on the affine space $\mathbb{A}^n_k \simeq k^n$: for any point $\boldsymbol{x} \in k^n$, $A.\boldsymbol{x}$ is defined as the usual product of the matrix A and the column $\boldsymbol{x}$. This left action is coherent with the right action already defined on $k[\mathbf{X}]$, in the sense that $p^A(\boldsymbol{x}) = p(A.\boldsymbol{x})$.

Besides, the orbits under H are exactly the fibers of φ. First, φ maps trivially an orbit to a point, and conversely the fact that a fiber is composed of a single orbit is well known (see [Cox-Little-O'Shea, 1992, Theorem 10 p. 339]. We get also a direct proof (see [Colin Thesis, 1997]) of this fact by considering the polynomial $P = \prod_{A \in H} (A.(U_1 X_1 + \dots U_n X_n) - (U_1 x'_1 + \cdots + U_n x'_n))$, where $U_1, \dots, U_n$ are indeterminates, $\boldsymbol{x}$ and $\boldsymbol{x'}$ two points in the same fiber. Indeed, as P belongs to $k[\mathbf{X}]^H[\mathbf{U}]$, $P(\boldsymbol{x}, \mathbf{U})$ equals $P(\boldsymbol{x'}, \mathbf{U})$, which is zero, therefore one factor of $P(\boldsymbol{x}, \mathbf{U})$ is 0, which means that there exists $A \in H$ such that $\boldsymbol{x'} = A.\boldsymbol{x}$.

Thus the categorical quotient $\mathcal{V}$ is the image of φ, and coincides with the quotient set $\mathbb{A}^n/H$ defined by the orbit projection:

$$\left| \begin{array}{lcl} \mathbb{A}^n & \longrightarrow & \mathbb{A}^n/H \\ \boldsymbol{x} & \longmapsto & H\boldsymbol{x} \end{array} \right.$$

We say that the categorical quotient is also a *geometric quotient.*

2.2 The Noether projection

It is central to notice that the integral extension $k[\boldsymbol{\Pi}] \hookrightarrow k[\mathbf{X}]^H$ realizes the integral extension of a Noether normalization. Geometrically, we can identify primary invariants to free variables and secondary ones to algebraic integers over the first ones. From a computer algebra point of view, applying the ideas of Giusti, Heintz, Pardo & *al.* leads to treat differently each set of variables: classical sparse or dense representations are used for the last ones, while a polynomial in free variables is coded by a straight-line program which evaluates it at an integer point. This data structure fits particularly well elimination processes (see once more *loc. cit.*), as will be illustrated below.

The projection

$$p : \left| \begin{array}{lcl} \mathcal{V} & \longrightarrow & \mathbb{A}^n \\ (\boldsymbol{\pi}, \boldsymbol{\sigma}) & \longmapsto & \boldsymbol{\pi} \end{array} \right.$$

achieving from section 1 a Noether position w.r.t. the free variables $\mathbf{\Pi}$ is called the *Noether projection*.

2.3 The primary projection

We call *primary projection* the finite map defined from the primary invariants:

$$\varpi : \left| \begin{array}{lcl} \mathbb{A}^n & \longrightarrow & \mathbb{A}^n \\ \boldsymbol{x} & \longmapsto & \mathbf{\Pi}(\boldsymbol{x}) \end{array} \right. .$$

2.4 The fundamental diagrams

Let us call ψ the canonical embedding of $\mathcal{V}$ in $\mathbb{A}^{n+r}$. What we did up to now is summarized in the two following commutative diagrams, where the notation $\mathcal{O}$ is used for global sections of sheaves.

$$\begin{tikzcd}
\mathbb{A}^n \times \mathbb{A}^r \arrow[dr, "\mathrm{pr}_1"] & \mathcal{V} \arrow[l, "\psi"'] \arrow[d, "p"] & \mathbb{A}^n \arrow[l, "\varphi"'] \arrow[dl, "\varpi"] \\
& \mathbb{A}^n &
\end{tikzcd} \qquad (D_1)$$

All the maps in the right triangle of this diagram are finite hence proper (once more $k[\mathbf{X}]$ is integral over $k[\mathbf{X}]^H$, which is itself integral over $k[\mathbf{\Pi}]$).

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{I} \arrow[r] & k[\mathbf{Y}, \mathbf{Z}] \arrow[r] \arrow[d, equal] & k[\mathbf{Y}, \mathbf{Z}]/\mathfrak{I} \arrow[r] \arrow[d, phantom, "\wr"] & k[\mathbf{X}] \arrow[d, equal] \\
& & \mathcal{O}_{\mathbb{A}^{n+r}}(\mathbb{A}^{n+r}) \arrow[r, "\psi^* = \Psi"] & \mathcal{O}_{\mathcal{V}}(\mathcal{V}) \arrow[r, "\varphi^*"] & \mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n) \\
& & & k[\mathbf{Y}] \arrow[ul, "\mathrm{pr}_1^*"] \arrow[u, "p^*"] \arrow[ur, "\varpi^*"'] &
\end{tikzcd} \qquad (D_2)$$

2.5 Multiplication table and primitive elements

We consider an invariant Θ in $k[\mathbf{X}]^H$ and once a Hironaka decomposition is chosen, we write it

$$\Theta(\mathbf{X}) = \Xi(\mathbf{\Pi}, \mathbf{\Sigma}) = B_1(\mathbf{\Pi})\Sigma_1 + \cdots + B_r(\mathbf{\Pi})\Sigma_r \ .$$

2.5.1 Characteristic and minimal polynomial

The invariant field $k(\mathbf{X})^H$ is a $k(\mathbf{\Pi})$-vector space of dimension r. Let us call m_Θ the linear endomorphism induced on this vector space by the multiplication by this element Θ. We can define the minimal polynomial $\mu_\Theta(T)$ and the characteristic polynomial $\chi_\Theta(T)$ of m_Θ.

As $k[\mathbf{X}]^H$ is an integral extension of $k[\mathbf{\Pi}]$, there exists a monic polynomial belonging to $k[\mathbf{\Pi}][T]$ that cancels on Θ. This polynomial is a multiple of μ_Θ in $k(\mathbf{\Pi})[T]$. Since $k[\mathbf{\Pi}]$ is integrally closed, this implies that μ_Θ belongs to $k[\mathbf{\Pi}][T]$. The same is true with χ_Θ, defined as a determinant with coefficients in $k[\mathbf{\Pi}][T]$.

As $k[\mathbf{X}]^H$ is a domain, μ_Θ is irreducible and χ_Θ is a power of μ_Θ.

Important particular case. A usual case is when $H \subset \mathfrak{S}_n$ and $k[\mathbf{\Pi}] = k[\mathbf{X}]^{\mathfrak{S}_n}$ (*e.g.* when $\mathbf{\Pi} = \mathbf{E}$). This particular case can be generalized: if L is a finite reflection subgroup of $\mathbf{GL}_n(k)$, containing H, then from Chevalley's theorem, $k[\mathbf{X}]^L$ is a polynomial ring, so we can choose primary invariants such that $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$.

In the case of permutation subgroups, products of symmetric groups are the only reflection subgroups of $\mathfrak{S}_n$.

An even more general case (whose classification is known as Noether's problem) is when $k(\mathbf{\Pi}) = k(\mathbf{X})^L$.

Under this assumption, χ_Θ splits over $k(\mathbf{X})$, and can be written as follows:

$$\chi_\Theta(T) = \prod_{\tau \in L /\!\!/ H} (T - \Theta^\tau) \tag{6}$$

where $L /\!\!/ H$ is a representative set of the right cosets of H in L.

2.5.2 Primitive element

We can define three to four notions.

- **Geometry:** Θ is called a *geometric primitive element* of the Noether projection p if Ξ separates generically the fibers — in other words, if Ξ takes r distinct values on $p^{-1}(\boldsymbol{\pi})$, provided that $\boldsymbol{\pi}$ does not belong to some proper algebraic subset of $\mathbb{A}^n$.

- **Ring theory:** Θ is called an *algebraic primitive element* of the Noether extension $k[\mathbf{\Pi}] \hookrightarrow k[\mathbf{X}]^H$ iff $\mu_\Theta = \chi_\Theta$.

- **Field theory:** Θ is a *primitive element* of the field extension $k(\mathbf{\Pi}) \hookrightarrow k(\mathbf{X})^H$ iff $k(\mathbf{\Pi})[\Theta] = k(\mathbf{X})^H$.

- **Group theory:** We assume moreover that $k(\mathbf{\Pi})$ is the invariant subfield $k(\mathbf{X})^L$ of some finite subgroup L of $\mathbf{GL}_n(k)$ containing H (or more generally, with L a group of automorphisms of $k(\mathbf{X})$). Then, we say that Θ is a *primitive invariant* if its stabilizer $\mathrm{Stab}_L(\Theta) := \{\tau \in L,\ \Theta^\tau = \Theta\}$ is H.

Proposition 5 *These four notions coincide (or the three first ones, if the hypothesis used in group theory, $k(\mathbf{\Pi}) = k(\mathbf{X})^L$, is not satisfied).*

Proof – $(i) \Leftrightarrow (ii)$: postponed to the end of §3.3. $(ii) \Leftrightarrow (iii)$: is obvious, since μ_Θ and χ_Θ, defined relatively to $k[\mathbf{\Pi}] \hookrightarrow k[\mathbf{X}]^H$, are also the minimal and characteristic polynomial relative to the fraction fields. $(iii) \Leftrightarrow (iv)$: Galois' correspondance theorem proves that the condition $k(\mathbf{X})^L[\Theta] = k(\mathbf{X})^H$ is equivalent to

$$\mathrm{Stab}_L(\Theta) = H \ . \tag{7}$$

Indeed, as $k(\mathbf{X})$ is a Galois extension of $k(\mathbf{X})^L$ of Galois group L, its subextension $k(\mathbf{X})^L[\Theta]$ is the set fixed by the group $\mathrm{Stab}_L(\Theta)$. □

Remark: The hypothesis $k(\mathbf{\Pi}) = k(\mathbf{X})^L$ with L a group of automorphisms of $k(\mathbf{X})$ (equivalent to the normality of the field extension $k(\mathbf{X}) : k(\mathbf{\Pi})$) is not always satisfied. For example, with $n = 1$, $\Pi = X^3 + X$, the extension $k(X) : k(\Pi)$ is not normal. Indeed, the polynomial $T^3 + T - \Pi \in k(\Pi)[T]$ has a root X but does not split over $k(X)$.

Remark: In the particular case when $k(\mathbf{\Pi}) = k(\mathbf{X})^L$, an other proof of the equivalence of the geometric and field theory point of views results from the equalities $\chi_{\Theta,\boldsymbol{\pi}} = \prod_{\tau \in L /\!\!/ H}(T - \Theta^\tau(\boldsymbol{x})) = \prod_{\boldsymbol{\sigma} \in \mathrm{pr}_2(p^{-1}(\boldsymbol{\pi}))}(T - \Xi(\boldsymbol{\pi}, \boldsymbol{\sigma}))$. When χ_Θ is squarefree, *i.e.* when $\mathrm{Stab}_L \Theta = H$, the values $\Xi(\boldsymbol{\pi}, \boldsymbol{\sigma})$ are distinct provided $\boldsymbol{\pi}$ is not a zero of the discriminant of χ_Θ.

2.5.3 Computation of the characteristic polynomial

We address the problem to compute the characteristic polynomial χ_Θ from the components B_i of Θ in the $k[\mathbf{\Pi}]$-basis $\mathbf{\Sigma}$ and the coefficients $A_k^{i,j}$ of relations (2). It will be done through the computation of the characteristic polynomial of the matrix M_Θ of the endomorphism m_Θ in the basis $\mathbf{\Sigma}$, which is

$$M_\Theta = \sum_{i=1}^{r} B_i(\mathbf{\Pi}) M_{\Sigma_i} = \left(\sum_{i=1}^{r} B_i(\mathbf{\Pi}) A_l^{i,j}(\mathbf{\Pi}) \right)_{(l,j)\in\{1,\ldots,r\}^2} . \tag{8}$$

There exists several algorithms in the literature to perform this task. We restrict ourselves to straight line programs using only arithmetic operations without divisions, because this feature will be needed to apply Theorem 26. The complexity is polynomial with exponent say γ in the dimension r, i.e. an upper bound is $O(r^\gamma)$.

Le Verrier's method It is based on the computation of the coefficients of χ_Θ from the power sums $\mathrm{Tr}(\Theta^p)$, $1 \le p \le r$, through Newton's identities. The traces $\mathrm{Tr}(\Theta^p)$ are computed from $\mathrm{Tr}(\Sigma_i)$, $1 \le i \le r$, once Θ^p is expressed in the basis $\mathbf{\Sigma}$ thanks to the multiplication table (2). This method was implemented in `Axiom` by the first author and used in the following examples. The cost reduces to the computation of $(M_\Theta)^p = M_{\Theta^p}$, used to express Θ^p in terms of $\mathbf{\Sigma}$. Hence the exponent γ can be taken equal to $\omega + 1$, where ω is the exponent of linear algebra (the best known to our knowledge is $\omega < 2.376$).

Other methods can be found *e.g.* in the book [Abdeljaoued-Lombardi, 2004], without being exhaustive. Let us quote among others Berkowitz's. The best one in our frame is Kaltofen-Wiedemann's, with an arithmetic complexity $O(r^{\frac{\omega}{2}+2} \log r \log\log r) = \widetilde{O}(r^{\frac{\omega}{2}+2})$.

2.5.4 Examples

i. Trivial example: if $\Theta \in k[\mathbf{\Pi}]$, then $\chi_\Theta(T) = (T-\Theta)^r$ and $\mu_\Theta(T) = T-\Theta$.

ii. $n=2$, $H = \{\mathrm{Id}, A, -\mathrm{Id}, -A\} \subset \mathbf{GL}_2(k)$ where $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $r=2$.

Choose $\Pi_1 = X_1^2 + X_2^2$, $\Pi_2 = (X_1X_2)^2$, $\Sigma_2 = X_1X_2(X_1^2 - X_2^2)$. Let be $\Theta = B_1(\Pi_1,\Pi_2) + B_2(\Pi_1,\Pi_2)\Sigma_2$. We compute $\Sigma_2^2 = \Pi_1^2\Pi_2 + 4\Pi_2^2$. Then

$$M_\Theta = \begin{pmatrix} B_1 & (\Pi_1^2\Pi_2 + 4\Pi_2^2)B_2 \\ B_2 & B_1 \end{pmatrix},$$

$$\chi_\Theta(T) = (T-B_1)^2 - (\Pi_1^2\Pi_2 + 4\Pi_2^2)B_2^2 = (T-B_1)^2 - \Sigma_2^2B_2^2.$$

The polynomial Σ_2^2 is irreducible over $k[\mathbf{\Pi}]$. Therefore, Θ is a primitive element of $k(\mathbf{X})^H : k(\mathbf{\Pi})$ if and only if $B_2 \neq 0$

iii. $n=4$, $H = \langle (1234), (12)(34) \rangle \subset \mathfrak{S}_4$ (dihedral group). Choose $\Pi_1 = E_1$, $\Pi_2 = X_1X_3 + X_2X_4, \Pi_3 = E_2, \Pi_4 = E_4$, $\Sigma_1 = 1$, $\Sigma_2 = X_1^3 + X_2^3 + X_3^3 + X_4^3$, $\Theta = \Sigma_2$. Then $\chi_\Theta(T) = T^2 - ST + P$ with $S = 2\Pi_1^3 + 3\Pi_1(\Pi_2 - 2\Pi_3)$ and $P = \Pi_1^6 + 3\Pi_1^4(\Pi_2 - 2\Pi_3) - 9(\Pi_1^2\Pi_3 - \Pi_2^2 + 36\Pi_4)(\Pi_2 - \Pi_3) + 9\Pi_1^2\Pi_4$.

3 Discriminants and dirimants

In the right triangle on the diagram (D_1), we deal only with three irreducible varieties of same dimension n. The morphisms between them are finite hence proper. In this setting, let $f : W_1 \to W_2$ be such a morphism. As usual the *critical locus* $\mathcal{C}(f)$ of f is the algebraic subset formed by the critical points $\boldsymbol{x}$ at which the tangent map between the Zariski tangent spaces $d_{\boldsymbol{x}}f : T_{\boldsymbol{x}}W_1 \to T_{f(\boldsymbol{x})}W_2$ is not surjective. With our assumption on dimension of source and target, at *singular* points the Zariski tangent space is of dimension strictly larger than n. Hence the critical locus can be divided into two disjoint parts: singular points of the source, or regular points of the source at which there is a default of submersion.

The *discriminant* $\mathcal{D}(f)$ of f is the image of $\mathcal{C}(f)$ by f. This is an algebraic subset of W_2 since f is proper. It can be divided into two (not necessarily disjoint) parts: first the image of the singular locus. Second, the critical values corresponding to regular critical points. The closure of this second part is called the *dirimant* of f after [Henry-Merle-Sabbah, 1984].

3.1 Singular locus of the quotient variety

We note Sing $\mathcal{V}$ the subset of singular points of $\mathcal{V}$. The algebra of functions of $\mathcal{V}$, *i.e.* $k[\mathbf{X}]^H$, is integrally closed, since the integrally closed ring $k[\mathbf{X}]$ is integral over $k[\mathbf{X}]^H$. Consequently, the singular locus Sing $\mathcal{V}$ of the normal variety $\mathcal{V}$ has codimension at least 2 (see *e.g.* [Shafarevich, 1994, chap. II §5 Th. 3]). Note that to describe it, we can use the jacobian criterion since $\mathcal{V}$ is defined by the prime ideal $\mathfrak{I}$.

3.2 Discriminant of the parametrization of the quotient variety

We note $\mathcal{C}'(\varphi)$ the subset of $\mathbb{A}^n$ at whose points $\boldsymbol{x}$ the linear map $d_{\boldsymbol{x}}\varphi : \mathbb{A}^n \to T_{\varphi(\boldsymbol{x})}\mathcal{V}$ does not reach its maximal rank, n. As $\dim T_{\varphi(\boldsymbol{x})}\mathcal{V} \geq n$ for any point $\boldsymbol{x} \in \mathbb{A}^n$, $\mathcal{C}'(\varphi)$ characterizes the default of immersion of φ ($\boldsymbol{x}$ belongs to $\mathcal{C}'(\varphi)$ iff $d_{\boldsymbol{x}}(\psi \circ \varphi)$ is not injective), whereas $\mathcal{C}(\varphi)$ characterizes its default of submersion. We denote by $\mathcal{D}'(\varphi)$ the image of $\mathcal{C}'(\varphi)$ by φ. Both $\mathcal{C}'(\varphi)$ and $\mathcal{D}'(\varphi)$ are Zariski-closed.

Remark 6 $\mathcal{C}(\varphi) = \varphi^{-1}(\operatorname{Sing}\mathcal{V}) \cup \mathcal{C}'(\varphi)$.

Proof – First, $\varphi^{-1}(\operatorname{Sing}\mathcal{V}) \subset \mathcal{C}(\varphi)$ because if $\varphi(\boldsymbol{x})$ belongs to $\operatorname{Sing}\mathcal{V}$, then $\dim T_{\varphi(\boldsymbol{x})}\mathcal{V} > \dim \mathcal{V} = n = \dim \mathbb{A}^n$, so $d_{\boldsymbol{x}}\varphi$ is not surjective. And when $\varphi(\boldsymbol{x}) \notin \operatorname{Sing}\mathcal{V}$, the vector space $T_{\varphi(\boldsymbol{x})}\mathcal{V}$ is n-dimensional, so the points $\boldsymbol{x}$ where $d_{\boldsymbol{x}}\varphi$ is not surjective are exactly those where $d_{\boldsymbol{x}}(\psi \circ \varphi)$ is not injective. □

Lemma 7 *Let $P_1, \ldots, P_s$ be polynomials of $k[\mathbf{X}]^H$, with $s \geq n$. If a point $\boldsymbol{a} = (a_1, \ldots, a_n)$ is left invariant by an element A of H distinct of the identity, then the differential at $\boldsymbol{a}$ of the map $\boldsymbol{x} \mapsto (P_1(\boldsymbol{x}), \ldots, P_s(\boldsymbol{x}))$ is not injective.*

Proof – For any $i \in \{1, \ldots, s\}$, differentiating the identity $P_i(\mathbf{X}) = P_i^A(\mathbf{X}) = (P_i \circ A)(\mathbf{X})$, we get $d_{\mathbf{X}}P_i = d_{A\mathbf{X}}P_i \circ A$. Evaluating this identity on $\boldsymbol{a} = A.\boldsymbol{a}$, we get $d_{\boldsymbol{a}}P_i = d_{\boldsymbol{a}}P_i \circ A$. Therefore, $\operatorname{Jac}_{\boldsymbol{a}}(\mathbf{P}) = \operatorname{Jac}_{\boldsymbol{a}}(\mathbf{P})A$, where $\operatorname{Jac}_{\boldsymbol{a}}(\mathbf{P}) = \left(\frac{\partial P_i}{\partial X_j}(\boldsymbol{a})\right)_{(i,j)\in\{1,\ldots,s\}\times\{1,\ldots,n\}}$ is the jacobian matrix of $\mathbf{P} = (P_1, \ldots, P_n)$ evaluated on the point $\boldsymbol{a}$. Transposing this identity, it proves that the lines of this jacobian matrix are eigenvectors of A^t associated to the eigenvalue 1. As $A^t \neq \operatorname{Id}$, the rank over k of these line vectors is at most $n-1$. □

We thank L. Le Floch for this elementary proof of Lemma 7.

Proposition 8 *Let $\boldsymbol{x}$ be a point in $\mathbb{A}^n$. The following assertions are equivalent:*

i. There exists an element of H, different from the identity, fixing $\boldsymbol{x}$;

ii. $\boldsymbol{x} \in \mathcal{C}'(\varphi)$.

Proof – $(i) \Rightarrow (ii)$ results from Lemma 7 applied to $s = n+r$ and $(P_1, \ldots, P_s) = (\boldsymbol{\Pi}, \boldsymbol{\Sigma})$.

$(ii) \Rightarrow (i)$ is well known for a quotient variety with a Hausdorff topology (see [Greenberg-Harper, 1981, ex. 5.10 p. 25]), and could be generalized to our frame thanks to the Lefschetz principle or thanks to the étale topology. Anyway we give here an elementary proof due to Romain Lebreton.

Let $h \neq 0$ be a vector of $\bar{k}^n$ such that $d_{\boldsymbol{x}}\varphi(h)$ is zero. It implies that for all $P \in k[\mathbf{X}]^H$, $d_{\boldsymbol{x}}P(h)$ vanishes. Indeed, $\{P \in k[\mathbf{X}],\ d_{\boldsymbol{x}}P(h) = 0\}$ is a ring and contains the components of $d_{\boldsymbol{x}}\varphi$, *i.e.* generators of $k[\mathbf{X}]^H$.

Suppose that $\boldsymbol{x}$ is fixed by no element of H, except the identity of course. In order to exhibit a contradiction, we produce a polynomial $P \in k[\mathbf{X}]^H$ such that $d_{\boldsymbol{x}}P(h) \neq 0$. If Q is an element of $k[\mathbf{X}]$, then its Reynolds projection $\overline{Q} := \frac{1}{|H|}\sum_{A\in H} Q(A.\mathbf{X})$ satisfies $\overline{Q} \in k[\mathbf{X}]^H$, and $d_{\boldsymbol{x}}\overline{Q} = \frac{1}{|H|}\sum_{A\in H} d_{A.\boldsymbol{x}}Q \circ A$. So, to produce a contradiction it is sufficient to exhibit a polynomial $Q \in k[\mathbf{X}]$

such that $d_{A.\boldsymbol{x}}Q = 0$ for $A \neq \mathrm{Id}$ and $d_{\boldsymbol{x}}Q(h) \neq 0$: then $P := \overline{Q}$ will satisfy $d_{\boldsymbol{x}}P(h) = \frac{1}{|H|}d_{\boldsymbol{x}}Q(h) \neq 0$.

In the dual space $(\bar{k}^n)^*$, the set of linear forms that cancel on h is an hyperplane K, and for each $A \in H\setminus\{\mathrm{Id}\}$, the set of linear forms that cancel on $A.\boldsymbol{x}-\boldsymbol{x}$ is an hyperplane K_A. As $\bar{k}$ is an infinite field, $(\bar{k}^n)^* \setminus \left(K \cup \bigcup_{A\in H\setminus\{\mathrm{Id}\}} K_A\right)$ is non-empty. Choose v^* in this set. Without loss of generality, we can suppose that v^* is collinear to the first vector of the dual basis of the canonical basis of $\bar{k}^n$ (substitute $\varphi \circ \phi$ to φ, where ϕ is the linear automorphisme of $\overline{k}^n$ that sends $(v_1, \ldots, v_n)$ to the canonical basis of $\overline{k}^n$, where $(v_1, \ldots, v_n)$ is defined by its dual basis $(v_1^*, \ldots, v_n^*)$, built by completing $v_1^* := v^*$ in a basis of $(\overline{k}^n)^*$). So, $h_1 \neq 0$ and $x_1 - (A.\boldsymbol{x})_1 \neq 0$ for any $A \in H \setminus \{\mathrm{Id}\}$.

Consider $Q := \prod_{A\neq\mathrm{Id}}(X_1 - (A.\boldsymbol{x})_1)^2$. Then $d_{A.\boldsymbol{x}}Q = 0$ for $A \neq \mathrm{Id}$. If $d_{\boldsymbol{x}}Q(h) \neq 0$ then we have found our polynomial. Otherwise $Q' := Q(\mathbf{X}).(X_1 - x_1 + h_1)^2$ suits our requirement: $d_{\boldsymbol{x}}Q'(h) = h_1^2 d_{\boldsymbol{x}}Q(h) + 2Q(\boldsymbol{x})h_1^2 = 2Q(\boldsymbol{x})h_1^2 \neq 0$. □

Remark: As the fibers of φ are the orbits under H, Prop. 8 can be rewritten:

$$\mathcal{D}'(\varphi) = \{v \in \mathcal{V},\ \#\varphi^{-1}(v) < |H|\}, \quad \text{and} \quad \mathcal{C}'(\varphi) = \varphi^{-1}(\mathcal{D}'(\varphi)). \tag{9}$$

Then, a consequence of Remark 6 is that

$$\mathcal{D}(\varphi) = \mathcal{D}'(\varphi) \cup \operatorname{Sing}\mathcal{V} \text{ and } \mathcal{C}(\varphi) = \varphi^{-1}(\mathcal{D}(\varphi)). \tag{10}$$

Remark: Every singular point of $\mathcal{V}$ is a critical value of its parametrization φ, but the converse is false: see the first example in §3.5. (More generally, from Chevalley's theorem, reflection groups yield a family of counterexamples where $\mathcal{V}$ is smooth).

Computational point of view

From Prop. 8 and its proof, $\mathcal{C}'(\varphi)$ is a finite union of proper vector subspaces: the union when A runs through $H \setminus \{\mathrm{Id}\}$ of the eigenspaces of A associated to the eigenvalue 1. Each eigenspace is defined by the prime ideal $\mathfrak{i}_A$ generated by the components of $(A - \mathrm{Id}).\mathbf{X}$.

We set

$$\mathfrak{i} = \bigcap_{A\in H\setminus\{\mathrm{Id}\}} \mathfrak{i}_A \text{ (radical ideal of } k[\mathbf{X}]), \quad \mathfrak{h} = (\varpi^*)^{-1}(\mathfrak{i}) \text{ (radical ideal of } k[\mathbf{Y}]).$$

Then,

$$\mathcal{C}'(\varphi) = \mathbf{V}(\mathfrak{i}) \quad \text{and} \quad \mathbf{V}(\mathfrak{h}) = \varpi(\mathcal{C}'(\varphi)) = p(\mathcal{D}'(\varphi)) \tag{11}$$

(because $\varpi(\mathcal{C}'(\varphi))$ is closed). A point $\boldsymbol{\pi}$ of $\mathbb{A}^n$ is a zero of $\mathfrak{h}$ if and only if some $\boldsymbol{x}$ in the fiber $\varpi^{-1}(\boldsymbol{\pi})$ belongs to $\mathcal{C}'(\varphi)$.

Note that the assertion $\varpi(\boldsymbol{x}) \in \mathbf{V}(\mathfrak{h})$ is not equivalent to $\boldsymbol{x} \in \mathcal{C}'(\varphi)$. See for instance the example of §3.6.2, where $\mathcal{C}'(\varphi) = \mathbf{V}(X_1 - X_2)$ and $\varpi^{-1}(\varpi(\mathcal{C}'(\varphi))) = \mathbf{V}((X_1 - X_2)(X_2 - X_3)(X_3 - X_1))$.

3.3 Discriminant of the Noether projection

For each point $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_n) \in k^n$, we define the ideal of $k[Z]$

$$\mathfrak{I}_{\boldsymbol{\pi}} = (Z_1 - 1) + \left(Z_i Z_j - \sum_{l=1}^{r} A_l^{i,j}(\boldsymbol{\pi}) Z_l,\ i, j \in \{1, \ldots, r\} \right).$$

Its set of zeroes is the projection onto k^r of $p^{-1}(\boldsymbol{\pi})$, or $\mathcal{V} \cap (\{\boldsymbol{\pi}\} \times k^r)$, and then $\mathfrak{I}_{\boldsymbol{\pi}}$ is a 0-dimensional ideal because p is a finite morphism.

Observe also that if $\mathfrak{m}_{\boldsymbol{\pi}} = (\mathbf{Y} - \boldsymbol{\pi})$ denotes the maximal ideal associated to the point $\boldsymbol{\pi}$, then $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}} \simeq k[\mathbf{Y}, \mathbf{Z}]/(\mathfrak{m}_{\boldsymbol{\pi}} + \mathfrak{I}_{\boldsymbol{\pi}}) \simeq k[\mathcal{V}]/\mathfrak{m}_{\boldsymbol{\pi}} k[\mathcal{V}] \simeq k[\mathbf{X}]^H \otimes_{k[\mathbf{\Pi}]} k[\mathbf{\Pi}]/(\mathbf{\Pi} - \boldsymbol{\pi}) \simeq k[\mathbf{\Pi}]^r \otimes_{k[\mathbf{\Pi}]} k[\mathbf{\Pi}]/(\mathbf{\Pi} - \boldsymbol{\pi}) \simeq k^r$. Hence, $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$ is a k-vector space of dimension r.

We will characterize the discriminant of the Noether projection as the set of points $\boldsymbol{\pi}$ such that $\mathfrak{I}_{\boldsymbol{\pi}}$ is not radical.

Proposition 9 *For any $\boldsymbol{\pi} \in k^n$, the following assertions are equivalent:*

i. The ideal $\mathfrak{I}_{\boldsymbol{\pi}}$ of $k[\mathbf{Z}]$ is not radical;

ii. $\boldsymbol{\pi} \in \mathcal{D}(p)$.

Proof – From the jacobian criterion, the zero dimensional ideal $\mathfrak{I}_{\boldsymbol{\pi}}$ is radical if and only if for every $\boldsymbol{\sigma} \in \mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})$, the jacobian matrix $J_{\boldsymbol{\pi},\boldsymbol{\sigma}} = \left(\dfrac{\partial G_\alpha}{\partial Z_\beta}(\boldsymbol{\pi}, \boldsymbol{\sigma}) \right)_{1 \leq \alpha \leq s, 1 \leq \beta \leq r}$ has rank r, where $G_1, \ldots, G_s$ ($s = \frac{r(r-1)}{2} + 1$) are the polynomials $S_{i,j} = Z_i Z_j - \sum_{k=1}^{r} A_k^{i,j} Z_k$ ($2 \leq i \leq j \leq r$) and $S_0 = Z_1 - 1$. On the other hand, a given regular point $(\boldsymbol{\pi}, \boldsymbol{\sigma})$ of $\mathcal{V}$ is a regular point of $p = \mathrm{pr}_1 \circ \psi$ if $d_{\boldsymbol{\pi},\boldsymbol{\sigma}} p = \mathrm{pr}_1 \circ d_{\boldsymbol{\pi},\boldsymbol{\sigma}} \psi$ has rank n, which means that the tangent space $T_{\boldsymbol{\pi},\boldsymbol{\sigma}} \mathcal{V}$ is in direct sum with the kernel of pr_1 (indeed, $d_{\boldsymbol{\pi},\boldsymbol{\sigma}} \psi$ is the canonical injection from $T_{\boldsymbol{\pi},\boldsymbol{\sigma}} \mathcal{V}$ into $\bar{k}^{n+r}$). As $T_{\boldsymbol{\pi},\boldsymbol{\sigma}} \mathcal{V}$ is defined by the equations

$$\sum_{i=1}^{n} \frac{\partial G_j}{\partial Y_i}(\boldsymbol{\pi}, \boldsymbol{\sigma}) y_i + \sum_{i=1}^{r} \frac{\partial G_j}{\partial Z_i}(\boldsymbol{\pi}, \boldsymbol{\sigma}) z_i = 0 \quad (1 \leq j \leq s), \tag{12}$$

the condition is that the equations $\displaystyle\sum_{i=1}^{r} \frac{\partial G_j}{\partial Z_i}(\boldsymbol{\pi}, \boldsymbol{\sigma}) z_i = 0$ ($1 \leq j \leq s$) have only the zero solution, which means that $J_{\boldsymbol{\pi},\boldsymbol{\sigma}}$ has rank r.

Last, if $(\boldsymbol{\pi}, \boldsymbol{\sigma})$ is a singular point of $\mathcal{V}$, the rank of $J_{\boldsymbol{\pi},\boldsymbol{\sigma}}$ is still less than r (indeed, as $\dim T_{\boldsymbol{\pi},\boldsymbol{\sigma}} \mathcal{V} > n$, the rank of the $s \times (n + r)$ system (12) is at most $r - 1$ and $J_{\boldsymbol{\pi},\boldsymbol{\sigma}}$ is a submatrix of the matrix of this system), while $(\boldsymbol{\pi}, \boldsymbol{\sigma})$ is, by definition, a critical point of p.

It completes the proof, since $(\boldsymbol{\pi}, \boldsymbol{\sigma})$ runs through $p^{-1}(\boldsymbol{\pi})$ when $\boldsymbol{\sigma}$ runs through $\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})$. □

Computational point of view

In order to compute $\mathcal{D}(p)$, we introduce new indeterminates $T, \Lambda_1, \ldots, \Lambda_r$; the polynomial $\Theta_{\mathbf{\Lambda}} = \Lambda_1 \Sigma_1 + \cdots + \Lambda_r \Sigma_r$ (it belongs to $k[\mathbf{\Lambda}][\mathbf{X}]^H$); its characteristic polynomial $\chi_{\Theta_{\mathbf{\Lambda}}}(T)$ over $k[\mathbf{\Lambda}][\mathbf{\Pi}]$.

The discriminant of $\chi_{\Theta_{\mathbf{\Lambda}}}(T)$ with respect to T is a polynomial

$$\Delta(\mathbf{\Lambda}, \mathbf{\Pi}) = \mathcal{R}es_T\left(\chi_{\Theta_{\mathbf{\Lambda}}}, \frac{\partial \chi_{\Theta_{\mathbf{\Lambda}}}}{\partial T}\right) \in k[\mathbf{\Lambda}, \mathbf{\Pi}], \tag{13}$$

where Δ belongs to $k[\mathbf{\Lambda}, \mathbf{Y}]$. Let $\mathfrak{d}$ be the ideal of $k[\mathbf{Y}]$ generated by the coefficients of Δ seen as a polynomial in $\mathbf{\Lambda}$ over $k[\mathbf{Y}]$.

If $\boldsymbol{\lambda} \in k^r$ (resp. $\boldsymbol{\pi} \in k^n$) is a specialisation of $\mathbf{\Lambda}$ (resp. $\mathbf{\Pi}$), we define $\Theta_{\boldsymbol{\lambda}} = \lambda_1\Sigma_1 + \cdots + \lambda_r\Sigma_r$, its characteristic polynomial $\chi_{\Theta_{\boldsymbol{\lambda}}}(T)$ (it is also the specialisation on $\boldsymbol{\lambda}$ of $\chi_{\Theta_{\mathbf{\Lambda}}}(T)$), and its specialisation $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}}(T)$ in $\boldsymbol{\pi}$, whose discriminant is $\Delta(\boldsymbol{\lambda}, \boldsymbol{\pi})$.

Proposition 10 *For any $\boldsymbol{\pi} \in k^n$, the following assertions are equivalent.*

i. The ideal $\mathfrak{I}_{\boldsymbol{\pi}}$ of $k[\mathbf{Z}]$ is radical;

ii. $\boldsymbol{\pi} \notin \mathcal{D}(p)$;

iii. There exists $\boldsymbol{\lambda} \in k^r$ such that $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}}$ is squarefree;

iv. There exists $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_r) \in k^r$ such that $\Delta(\boldsymbol{\lambda}, \boldsymbol{\pi}) \neq 0$;

v. $\boldsymbol{\pi} \notin \mathbf{V}(\mathfrak{d})$.

Proof – The equivalence between (*i*) and (*ii*) is already proved. The condition (*iv*) is equivalent to (*iii*) because $\Delta(\boldsymbol{\lambda}, \boldsymbol{\pi})$ is the discriminant of $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}}$, and to (*v*) because k is an infinite field. A well-known result, attached to Stickelberger's name, is that

$$\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}} = \prod_{\boldsymbol{\sigma} \in \mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})} (T - (\lambda_1\sigma_1 + \cdots + \lambda_r\sigma_r))^{m_{\mathfrak{I}_{\boldsymbol{\pi}}}(\boldsymbol{\sigma})}, \tag{14}$$

where $m_{\mathfrak{I}_{\boldsymbol{\pi}}}(\boldsymbol{\sigma})$ is the multiplicity of the zero $\boldsymbol{\sigma}$ (see for instance [Elkadi-Mourrain, 2007, §4.8]). Note that

$$\sum_{\boldsymbol{\sigma} \in \mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})} m_{\mathfrak{I}_{\boldsymbol{\pi}}}(\boldsymbol{\sigma}) = \dim_k k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}} = r.$$

If $\mathfrak{I}_{\boldsymbol{\pi}}$ is not radical, there exists $\boldsymbol{\sigma} \in \mathbb{A}^r$ such that $m_{\mathfrak{I}_{\boldsymbol{\pi}}}(\boldsymbol{\sigma}) \geq 2$; so, $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}}$ is not squarefree.

Conversely, if $\mathfrak{I}_{\boldsymbol{\pi}}$ is radical, then $\#\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}}) = r$; so, as k is an infinite field, there exists $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_r) \in k^r$ such that $\lambda_1\sigma_1 + \cdots + \lambda_r\sigma_r$ take $r = \dim_k k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$ distinct values when $\boldsymbol{\sigma}$ runs through $\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})$. Indeed, we can choose $\boldsymbol{\lambda}$ in the open set defined by $\prod_{\boldsymbol{\sigma} \neq \boldsymbol{\sigma}'} ((\sigma_1 - \sigma'_1)\lambda_1 + \cdots + (\sigma_r - \sigma'_r)\lambda_r) \neq 0$, where $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ run through $\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})$. Then, $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}}$ is squarefree. Therefore, (*i*) is equivalent to (*iii*). □

Therefore,

$$\begin{aligned} \mathcal{D}(p) &= \mathbf{V}(\mathfrak{d}) & (15)\\ &= \bigcap_{\boldsymbol{\lambda} \in k^r} \mathbf{V}(\Delta(\boldsymbol{\lambda}, \mathbf{Y})). & (16) \end{aligned}$$

Proof of Prop. 5, (i) ⇔ (ii) —
Consider $m_{\boldsymbol{\pi},\Theta}$, the multiplication by $\Xi(\boldsymbol{\pi}, \mathbf{Z})$ in $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$. From (14), the characteristic polynomial $\chi_{\boldsymbol{\pi},\Theta}$ of $m_{\boldsymbol{\pi},\Theta}$ is $\prod_{\boldsymbol{\sigma} \in \mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}})} (T - \Xi(\boldsymbol{\pi}, \boldsymbol{\sigma}))$, when $\# p^{-1}(\boldsymbol{\pi}) = r$. If Θ is a geometric primitive element, then $\chi_{\boldsymbol{\pi},\Theta}$ is squarefree for some $\boldsymbol{\pi} \in \mathbb{A}^n$. Therefore, $\chi_{\boldsymbol{\pi},\Theta}$ is the minimal polynomial of $m_{\boldsymbol{\pi},\Theta}$. Now, the specialization in $\boldsymbol{\pi}$ of μ_Θ cancels on $m_{\boldsymbol{\pi},\Theta}$. Consequently, its degree is that of $\chi_{\boldsymbol{\pi},\Theta}$, r. It proves that $\mu_\Theta = \chi_\Theta$. Conversely, if Θ is an algebraic primitive element, then χ_Θ is squarefree over $k[\mathbf{\Pi}]$: it discriminant Δ is a non zero polynomial in $k[\mathbf{\Pi}]$. If $\boldsymbol{\pi}$ does not belong to the algebraic subvariety defined by Δ, then $\chi_{\boldsymbol{\pi},\Theta}$, that is the specialization of χ_Θ in $\boldsymbol{\pi}$, is squarefree. So, Θ is a geometric primitive element.

3.4 Discriminant of the primary projection

For any $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_n) \in k^n$, we define the ideal $\mathfrak{a}_{\boldsymbol{\pi}} = (\Pi_i - \pi_i,\ 1 \le i \le n)$ of the ring $k[\mathbf{X}]$ corresponding to the fiber $\varpi^{-1}(\boldsymbol{\pi})$.

Let J be the jacobian determinant of $(\Pi_1, \ldots, \Pi_n)$:

$$J = \left| \frac{\partial \Pi_i}{\partial X_j} \right| \in k[\mathbf{X}].$$

Proposition 11 *For any $\boldsymbol{\pi} \in k^n$, the two following assertions are equivalent:*

i. the ideal $\mathfrak{a}_{\boldsymbol{\pi}}$ is not radical;

ii. $\boldsymbol{\pi} \in \mathcal{D}(\varpi)$.

Proof – The set of zeroes of $\mathfrak{a}_{\boldsymbol{\pi}}$ is zero dimensional, therefore $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical if and only if $\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}}) = \varpi^{-1}(\boldsymbol{\pi})$ is smooth. From the jacobian criterion, it means that $J(\boldsymbol{x}) \neq 0$ for any $\boldsymbol{x} \in \varpi^{-1}(\boldsymbol{\pi})$. This last assertion is equivalent to $\boldsymbol{x} \notin \mathcal{C}(\varpi)$ for any $\boldsymbol{x} \in \varpi^{-1}(\boldsymbol{\pi})$, *i.e.* to $\boldsymbol{\pi} \notin \mathcal{D}(\varpi)$. □

Computational point of view

We define a discriminant δ characterizing the points $\boldsymbol{\pi}$ such that $\mathfrak{a}_{\boldsymbol{\pi}}$ is not radical.

Consider the ideal $\mathfrak{a}_{\mathbf{Y}} = (\Pi_i - Y_i,\ 1 \le i \le n)$ of the ring $k[\mathbf{X}, \mathbf{Y}]$.

Proposition 12 *The radical of $(\mathfrak{a}_{\mathbf{Y}} + (J)) \cap k[\mathbf{Y}]$ is a principal ideal of $k[\mathbf{Y}]$. Let δ be a generator. Then*

$$\mathbf{V}(\delta) = \mathcal{D}(\varpi) \tag{17}$$

Proof – The map ϖ is a finite map from $\mathbb{A}^n$ to $\mathbb{A}^n$. Its restriction to its critical locus, the hypersurface $J = 0$, is still finite, hence its set of critical values, i.e. its image described by the ideal $(\mathfrak{a}_{\mathbf{Y}} + (J)) \cap k[\mathbf{Y}]$ is of the same dimension $n - 1$. A fiber described by the ideal $\mathfrak{a}_{\boldsymbol{\pi}}$ is then smooth iff $\delta(\boldsymbol{\pi}) \neq 0$. □

This last proposition is an effective definition of δ: it enables to compute δ, by the elimination of $\mathbf{X}$ between $\mathfrak{a}_{\mathbf{Y}}$ and J. This elimination is done by any process.

3.5 Link between the 3 discriminants

Remark 13 *For every $\boldsymbol{\pi} \in k^n$, the k-algebras $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$ and $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{\pi}}^H$ are isomorphic, where $\mathfrak{a}_{\boldsymbol{\pi}}^H$ is the ideal of $k[\mathbf{X}]^H$ generated by the $\Pi_i - \pi_i$.*

Proof – The k-algebra isomorphism $k[\mathbf{Y}, \mathbf{Z}]/\mathfrak{I}$ onto $k[\mathbf{X}]^H$ (infered from the exact sequence 3) sends $Y_i - \pi_i$ to $\Pi_i - \pi_i$, then the ideal generated by the first ones is mapped bijectively onto the ideal generated by the second ones. Hence $k[\mathbf{Y}, \mathbf{Z}]/(\mathfrak{I} + (\mathbf{Y} - \boldsymbol{\pi}))$ is isomorphic to $k[\mathbf{X}]^H/(\boldsymbol{\Pi} - \boldsymbol{\pi})$. It proves the isomorphism, since $k[\mathbf{Y}, \mathbf{Z}]/(\mathfrak{I} + (\mathbf{Y} - \boldsymbol{\pi})) \simeq k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$. □

Proposition 14 *The set $\varphi^{-1}(\operatorname{Sing} \mathcal{V})$ is a subset of $\mathcal{C}(\varpi)$.*

Note that $\mathcal{C}(\varpi)$ depends on the choice of the only primary invariants, whereas $\mathcal{V}$, hence Sing $\mathcal{V}$, depend also on the secondary ones.

Proof – Consider $\boldsymbol{x} \in \mathbb{A}^n \setminus \mathcal{C}(\varpi)$ and $(\boldsymbol{\pi}, \boldsymbol{\sigma}) = \varphi(\boldsymbol{x})$. From Remark 13 (applied over $\bar{k}$), $\bar{k}[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}} \simeq \bar{k}[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{\pi}}$. As $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical from Prop. 11, $\bar{k}[\mathbf{X}]/\mathfrak{a}_{\boldsymbol{\pi}}$ is reduced, therefore its subalgebra $\bar{k}[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{\pi}}$ is reduced, $\bar{k}[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$ is reduced, $\mathfrak{I}_{\boldsymbol{\pi}}$ is radical, hence from the proof of Prop. 9, $(\boldsymbol{\pi}, \boldsymbol{\sigma}) \notin \operatorname{Sing} \mathcal{V}$. □

Theorem 15 *Let $\boldsymbol{x}$ be a point in $\mathbb{A}^n$. Then*

$$\begin{aligned} \boldsymbol{x} \in \mathcal{C}(\varpi) \quad &\Longleftrightarrow \quad (\boldsymbol{x} \in \mathcal{C}'(\varphi) \text{ or } \varphi(\boldsymbol{x}) \in \mathcal{C}(p)) &(18)\\ &\Longleftrightarrow \quad (\boldsymbol{x} \in \mathcal{C}(\varphi) \text{ or } \varphi(\boldsymbol{x}) \in \mathcal{C}(p)). &(19)\end{aligned}$$

Proof – First if $\varphi(\boldsymbol{x}) \notin \operatorname{Sing} \mathcal{V}$, then $d_{\boldsymbol{x}}\varpi = d_{\varphi(\boldsymbol{x})}p \circ d_{\boldsymbol{x}}\varphi$, where $d_{\boldsymbol{x}}\varpi$, $d_{\varphi(\boldsymbol{x})}p$ and $d_{\boldsymbol{x}}\varphi$ are all three linear maps between $\bar{k}$-vector spaces of dimension n. Consequently, $d_{\boldsymbol{x}}\varpi$ is surjective if and only if the two others are surjective (or equivalently injective).

Secondly if $\varphi(\boldsymbol{x}) \in \operatorname{Sing} \mathcal{V}$, then $\varphi(\boldsymbol{x}) \in \mathcal{C}(p)$ by definition, and $\boldsymbol{x} \in \mathcal{C}(\varpi)$ from Prop. 14. □

Corollary 16

$$\begin{aligned} \mathcal{D}(\varpi) \quad &= \quad \mathcal{D}(p) \cup p(\mathcal{D}'(\varphi)) &(20)\\ &= \quad \mathcal{D}(p) \cup p(\mathcal{D}(\varphi)). &(21)\end{aligned}$$

Remark 17 *Theorem 15 can also be proved directly as a consequence of Prop. 8, 9, 11 and the self contained following lemma (applied over $\bar{k}$), whose direct proof stresses the crushing of the orbits.*

Lemma 18 *Consider a point $\boldsymbol{\pi}$ of k^n. The following assertions*

i. The ideal $\mathfrak{a}_{\boldsymbol{\pi}}$ of $k[\mathbf{X}]$ is radical;

ii. The ideal $\mathfrak{I}_{\boldsymbol{\pi}}$ of $k[\mathbf{Z}]$ is radical;

iii. For any $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}})$ and any $A \in H \setminus \{\mathrm{Id}\}$, $A.\boldsymbol{x} \neq \boldsymbol{x}$

are linked as follows: (**i**) $\Longleftrightarrow$ ((**ii**) and (**iii**)).

Proof –

- ((**iii**) and not(**i**)) $\Longrightarrow$ not(**ii**). From (iii), each element $\boldsymbol{x} \in \mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}})$ has an orbit under H of cardinal $\#(H.\boldsymbol{x}) = |H|$. From not($i$), $\mathfrak{a}_{\boldsymbol{\pi}}$ is not radical, therefore $\#\mathbf{V}(\mathfrak{a}_{\pi}) < \dim_k k[\mathbf{X}]/\mathfrak{a}_{\boldsymbol{\pi}}$. Now, $\dim_k k[\mathbf{X}]/\mathfrak{a}_{\boldsymbol{\pi}} \leq d_1 \ldots d_n$ (in fact it is equal) where $d_i = \deg \Pi_i$. So, $\#\mathbf{V}(\mathfrak{a}_{\pi}) < r.|H|$, as $d_1 \ldots d_n = r.|H|$ from Theorem 1.

  We notice that $\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}}) = \kappa(\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}}))$ where κ is defined by $\kappa(\boldsymbol{x}) = \mathrm{pr}_2(\varphi(\boldsymbol{x})) = (\Sigma_1(\boldsymbol{x}), \ldots, \Sigma_r(\boldsymbol{x}))$.

  Now, κ is constant on the orbits of H. As all the orbits have cardinality $|H|$ and $\#\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}}) < r.|H|$, it proves that $\#\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}}) < r$. Now, $\dim_k k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}} = r$. Therefore, $\#\mathbf{V}(\mathfrak{I}_{\boldsymbol{\pi}}) < \dim k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$ and $\mathfrak{I}_{\boldsymbol{\pi}}$ is not radical in $k[\mathbf{Z}]$.

- (**i**) $\Rightarrow$ (**ii**). From Remark 13, $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}} \simeq k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{\pi}}$. As $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical, $k[\mathbf{X}]/\mathfrak{a}_{\boldsymbol{\pi}}$ is reduced, so is its subalgebra $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{\pi}}$, therefore $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}}$ is reduced and $\mathfrak{I}_{\boldsymbol{\pi}}$ is radical.

- not (**iii**) $\Rightarrow$ not (**i**). Suppose $A.\boldsymbol{x} = \boldsymbol{x}$ with $A \neq \mathrm{Id}$. From Lemma 7, $d_{\boldsymbol{x}}\varpi$ is not injective, hence not surjective as it goes from $\bar{k}^n$ to itself. We conclude with Prop.11. □

Computational point of view

The set equality (20) can be translated in terms of ideals through (11), Prop. 10, Prop. 12 and Hilbert's Nullstellensatz. Since (δ) and $\mathfrak{h}$ are radical ideals, we get:

Corollary 19

$$\mathbf{V}(\delta) = \mathbf{V}(\mathfrak{d}) \cup \mathbf{V}(\mathfrak{h}) \tag{22}$$

$$(\delta) = \sqrt{\mathfrak{d}} \cap \mathfrak{h}. \tag{23}$$

Besides, this last equality is equivalent to (20), because $\mathcal{D}(\varpi)$, $\mathcal{D}(p)$ and $p(\mathcal{D}'(\varphi))$ are Zariski-closed.

Examples:

1. $n = 1$, $H = \{1, -1\}$, $\Pi_1 = X_1^2$, $r = 1$, $\Sigma_1 = 1$. Then $\mathfrak{a}_{\mathbf{Y}} = \left(X_1^2 - Y_1\right)$, so $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical if and only if $\pi_1 \neq 0$, but $\mathfrak{I}_{\boldsymbol{\pi}} = \{0\}$ is always radical. So, $\mathrm{Sing}\,\mathcal{V} = \emptyset$, $\mathcal{D}(\varpi) = \{0\} = \mathcal{D}(\varphi)$, and $\mathcal{D}(p) = \emptyset$.

2. $n = 4$, $H = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & A \end{pmatrix} \right\rangle$ where $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $r = 2$, $k[\mathbf{X}]^H = k[X_1^2] \otimes_k (k[\Pi_2, \Pi_3, \Pi_4] \oplus k[\Pi_2, \Pi_3, \Pi_4]\Sigma_2) = k[\boldsymbol{\Pi}] \oplus k[\boldsymbol{\Pi}]\Sigma_2$, where $\Pi_1 = X_1^2$; Π_2, Π_3, Π_4 are the elementary symmetric polynomials in X_2, X_3, X_4 and $\Sigma_2 = (X_2 - X_3)(X_2 - X_4)(X_3 - X_4)$; $\Sigma_2^2 = \delta_1(\Pi_2, \Pi_3, \Pi_4)$ where $\delta_1(Y_2, Y_3, Y_4) = \mathrm{discrim}_T(T^3 - Y_2T^2 + Y_3T - Y_4)$. We compute the jacobian $J = 2X_1\Sigma_2$; therefore $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical iff $\delta(\boldsymbol{\pi}) \neq 0$, where $\delta = Y_1\delta_1$. And $\mathfrak{I}_{\boldsymbol{\pi}} = (Z_2^2 - \delta_1(\pi_2, \pi_3, \pi_4))$ is radical if and only if $\delta_1(\pi_2, \pi_3, \pi_4) \neq 0$, so $\sqrt{\mathfrak{d}} = (\delta_1)$; and $\mathcal{C}(\varphi) = \{\boldsymbol{x} \in k^4,\ x_1 = 0 \text{ or } x_2 = x_3 = x_4\}$, so $\mathfrak{h} = (Y_1\delta_1)$.

3. $n = 3$, $H = \left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, -I_3 \right\rangle$, $\Pi_i = X_i^2$, $r = 2$, $\Sigma_1 = 1$, $\Sigma_2 = X_1X_2$. Then $\mathfrak{I} = (\Sigma_1 - 1, \Sigma_2^2 - \Pi_1\Pi_2)$, $\operatorname{Sing}\mathcal{V} = \mathbf{V}(Y_1, Y_2, Z_2)$ (of codimension 2 in $\mathcal{V}$, see §3.1), $\mathfrak{a}_{\mathbf{Y}} = (X_1^2 - Y_1, X_2^2 - Y_2, X_3^2 - Y_3)$, so $\delta = Y_1Y_2Y_3$; $\chi_{\Theta_{\boldsymbol{\Lambda}}} = T^2 - 2\Lambda_1 T + \Lambda_1^2 - \Lambda_2^2\Pi_1\Pi_2$, so $\Delta_{\Theta_{\boldsymbol{\Lambda}}} = 4\Lambda_2^2\Pi_1\Pi_2$ and $\mathfrak{d} = (Y_1Y_2)$; and $\mathfrak{h} = (Y_1, Y_2).(Y_3)$.

3.6 Examples

We present here a few examples where the generic computation of the discriminants was manageable, to illustrate the separability properties studied *supra*. We begin with examples of permutation groups, considered as subgroups of $\mathfrak{S}_n$ acting on $k[X_1, \ldots, X_n]$, and we finish with an example of matrix group.

Universally separable resolvents Through these examples, we notice that in some very specific cases, it happens that there exists a r-uple $\boldsymbol{\lambda}^{(0)} \in k^r$ such that $\Delta(\boldsymbol{\lambda}^{(0)}, \boldsymbol{\pi}) \neq 0$ for any $\boldsymbol{\pi} \in k^n$ on which δ does not cancel. In these cases, we will say that $\Theta = \Theta_{\boldsymbol{\lambda}^{(0)}}$ is a *universally separating element*, and that χ_Θ is *universally separable*, as $\boldsymbol{\lambda}^{(0)}$ does not depend on $\boldsymbol{\pi}$.

If we refer to the definition of a geometric primitive invariant in §2.5.2, it means that the geometric primitive invariant Θ separates the fibers of the Noether projection p outside of a subvariety of $\mathbb{A}^n$ that is included in $\mathcal{D}(\varpi) = \mathbf{V}(\delta)$.

In the particular case of permutation groups, we shall see in §4.1 that $\mathcal{D}(p) = \mathcal{D}(\varpi)$; also, Θ being a universally separating element means that equation (16) becomes $\mathcal{D}(p) = \mathbf{V}(\Delta(\boldsymbol{\lambda}^{(0)}, \mathbf{Y}))$.

Notation If p is a polynomial of $k[\mathbf{X}]$, we denote by $\sum_H p$ the sum of the elements of the orbit p^H of p under the action of H. Observe that this notation could be misleading, since the number of terms is the index of the stabilizer of p in H, hence depends strongly on p.

3.6.1 The alternating group

We consider the case where H is the alternating group $\mathfrak{A}_n$, acting on $k[X_1, \ldots, X_n]$ as a subgroup of $\mathfrak{S}_n$, and we take for the primary invariants the elementary symmetric polynomials: $\Pi_i = E_i$ for $1 \leq i \leq n$. Then, $r = 2$, and we can choose $\Sigma_1 = 1$ and $\Sigma_2 = \prod_{1 \leq i < j \leq n}(X_j - X_i)$. We get $\Sigma_2^2 = \delta(\boldsymbol{\Pi})$. So, for any $\boldsymbol{\pi} \in k^n$, $\mathfrak{I}_{\boldsymbol{\pi}} = \big(Z_1 - 1, Z_2^2 - \delta(\pi)\big)$. It is radical if and only if $\delta(\pi) \neq 0$.

Besides, $\Delta = \delta(\mathbf{Y})\Lambda_2^2$. Therefore, χ_{Σ_2} is universally separable, and $\mathcal{D}(p) = \mathcal{D}(\varpi)$.

We compute Sing $(\mathcal{V})$ from the jacobian criterion: it consists of the common zeroes of $2Z_2 = \frac{\partial(Z_2^2 - \delta)}{\partial Z_2}$ and $\frac{\partial(Z_2^2 - \delta)}{\partial Y_i} = -\frac{\partial \delta}{\partial Y_i}$, $1 \leq i \leq n$.

As $\mathfrak{A}_n$ is generated by the 3-cycles, $\mathcal{C}'(\varphi) = \bigcup_{i<j<k} \mathbf{V}(X_i - X_j, X_i - X_k)$ and $\mathbf{V}(\mathfrak{h})$ is the primary projection of this set.

For $n = 3$, $\operatorname{Sing}\mathcal{V} = \mathbf{V}(Z_1 - 1, Z_2, 3Y_2 - Y_1^2, 27Y_3 - Y_1^3)$. We notice that $\varphi^{-1}(\operatorname{Sing}(\mathcal{V})) = \mathbf{V}(X_1 - X_2, X_1 - X_3) = \mathcal{C}'(\varphi)$, so that $\mathfrak{h} = (3Y_2 - Y_1^2, 27Y_3 - Y_1^3)$.

3.6.2 $\mathfrak{S}_2$ acting on 3 indeterminates

Let H be the subgroup of $\mathfrak{S}_3$ generated by the transposition $(1,2)$. Then,

$$k[X_1,X_2,X_3]^H = k[\mathbf{\Pi}]\Sigma_1 \oplus k[\mathbf{\Pi}]\Sigma_2 \oplus k[\mathbf{\Pi}]\Sigma_3,$$

where $\Pi_i = E_i$ $(1 \le i \le 3)$, $\Sigma_1 = 1$, $\Sigma_2 = X_3$ and $\Sigma_3 = X_3^2$. The ideal $\mathfrak{I}$ is generated by $S_0 = Z_1 - 1, S_{2,2} = Z_2^2 - Z_3$, $S_{2,3} = Z_2Z_3 - Y_3 + Y_2Z_2 - Y_1Z_3$ (we needn't $S_{3,3} = Z_3^2 - Y_1Y_3 - (Y_3 - Y_1Y_2)Z_2 - (Y_1^2 - Y_2)Z_3$, because $S_{3,3} = (Y_1 + Z_2)S_{2,3} - (Y_2 + Z_3)S_{2,2})$.

As these relations define a graph, $\mathcal{V}$ is smooth and $\operatorname{Sing}\mathcal{V} = \emptyset$.

We compute the discriminant of $\Theta_{\mathbf{\Lambda}} = \Lambda_1\Sigma_1 + \Lambda_2\Sigma_2 + \Lambda_3\Sigma_3$

$$\Delta = \delta \;.\; \left((Y_3 - Y_1\;Y_2)\;\Lambda_3^3 - \left(Y_2 + Y_1^2\right)\;\Lambda_2\;\Lambda_3^2 - 2\;Y_1\;\Lambda_2^2\;\Lambda_3 - \Lambda_2^3\right)^2,$$

where $\delta = -4\;Y_3\;Y_1^3 + Y_2^2\;Y_1^2 + 18\;Y_3\;Y_2\;Y_1 - 4\;Y_2^3 - 27\;Y_3^2$ is the discriminant of the polynomial $T^3 - Y_1T^2 + Y_2T - Y_3$.

As $\Delta(0,1,0,\mathbf{Y}) = \delta$, the polynomial χ_{Σ_2} is universally separable (not surprising, it is equal to $T^3 - Y_1T^2 + Y_2T - Y_3$), but χ_{Σ_3} is not (its discriminant cancels with $(Y_3 - Y_1Y_2)\delta$).

3.6.3 Dihedral group $\mathfrak{D}_4$ in $\mathfrak{S}_4$

We consider $H = ((1,3,2,4),(1,2))$ (subgroup of $\mathfrak{S}_4$ of order 8). The invariant algebra $k[X_1,X_2,X_3,X_4]^H$ has the following Hironaka decomposition:

$$k[\mathbf{X}]^H = k[\mathbf{\Pi}]\Sigma_1 \oplus k[\mathbf{\Pi}]\Sigma_2 \oplus k[\mathbf{\Pi}]\Sigma_3,$$

where $\Pi_i = E_i$ $(1 \le i \le 4)$, $\Sigma_1 = 1$, $\Sigma_2 = X_1X_2 + X_3X_4$ and $\Sigma_3 = \Sigma_2^2$. The ideal $\mathfrak{I}$ is generated by the relations $S_{2,2} = Z_2^2 - Z_3$ and $S_{2,3} = Z_2Z_3 - Y_2Z_3 + (Y_3Y_1 - 4Y_4)Z_2 - Y_4Y_1^2 + 4Y_4Y_2 - Y_3^2$.

From the jacobian criterion, we compute $\operatorname{Sing}(\mathcal{V}) = \mathbf{V}(8Y_3 - 4Y_1Y_2 + {Y_1}^3, 64Y_4 - 16{Y_2}^2 + 8{Y_1}^2Y_2 - {Y_1}^4, 4Z_2 - 4Y_2 + {Y_1}^2, Z_3 - Z_2^2, Z_1 - 1)$. Replacing Y_i by Π_i and Z_i by Σ_i, we compute $\varphi^{-1}(\operatorname{Sing}(\mathcal{V})) = \mathbf{V}((X_2 - X_4)(X_2 - X_3), (X_1 + X_2) - (X_3 + X_4))$.

We compute $\Delta = \delta\;\Delta'$, where $\delta = \operatorname{discrim}_T(T^4 - Y_1T^3 + Y_2T^2 - Y_3T + Y_4)$ and $\Delta' = \left(A_{0,3}(\mathbf{Y})\Lambda_3^3 + A_{1,2}(\mathbf{Y})\Lambda_2\Lambda_3^2 - 4Y_2\Lambda_2^2\Lambda_3 - \Lambda_2^3\right)^2$, with $A_{0,3} = \left(8Y_2 - Y_1^2\right)Y_4 - Y_3^2 - Y_1Y_2Y_3 - 2Y_2^3$ and $A_{1,2} = 4Y_4 - Y_1Y_3 - 5Y_2^2$.

As $\Delta'(0,1,0,\mathbf{Y}) = 1$, χ_{Σ_2} is universally separable.

And we compute $\mathcal{C}'(\varphi) = \mathbf{V}(X_1 - X_2) \cup \mathbf{V}(X_3 - X_4) \cup \varphi{-}1(\operatorname{Sing}(\mathcal{V}))$ and $\mathfrak{h} = (\delta)$.

3.6.4 The metacyclic subgroup of $\mathfrak{S}_5$

We consider $H = ((1,2,3,4,5),(2,3,5,4))$ (subgroup of $\mathfrak{S}_5$ of order 20), $\Pi_i = E_i$ $(1 \le i \le 5)$, $r = 6$, $\Sigma_1 = 1$, $\Sigma_2 = \sum_H X_1^2X_2X_3$, $\Sigma_3 = \sum_H X_1^3X_2X_3$, $\Sigma_4 = \sum_H X_1^4X_2X_3$, $\Sigma_5 = \sum_H X_1^4X_2^2X_3$, $\Sigma_6 = \Sigma_2^2$.

For $\Theta = \Lambda_1\Sigma_1 + \Lambda_2\Sigma_2 + \Lambda_3\Sigma_3$ (forgetting $\Sigma_4, \Sigma_5, \Sigma_6$), we compute

$$\Delta_\Theta = \delta_5^3\;.(\Delta'_\Theta)^2,$$

where $\delta_5 = \operatorname{discrim}_T(T^5 - Y_1T^4 + Y_2T^3 - Y_3T^2 + Y_4T - Y_5) \in k[\mathbf{Y}]$ and $\Delta'_\Theta(0,0,0,Y_4,Y_5,\Lambda_1,\Lambda_2,\Lambda_3) = (2^{15}Y_4^{10}Y_5)\Lambda_3^{15} + (2^{16}Y_4^{11})\Lambda_2\Lambda_3^{14} - (2^{12}5^3Y_4^8Y_5^2)\Lambda_2^3\Lambda_3^{12} -$

$(2^{14}5^3Y_4^9Y_5)\Lambda_2^4\Lambda_3^{11}+(2^{11}5^5Y_4^5Y_5^4+2^{15}7Y_4^{10})\Lambda_2^5\Lambda_3^{10}-(2^{10}5^5Y_4^6Y_5^3)\Lambda_2^6\Lambda_3^9+(2^{12}5^5Y_4^7Y_5^2)\Lambda_2^7\Lambda_3^8-(2^75^8Y_4^4Y_5^5+2^85^319Y_4^8Y_5)\Lambda_2^8\Lambda_3^7+(2^75^8Y_4^4Y_5^4+2^{12}5^4Y_4^9)\Lambda_2^9\Lambda_3^6+(2^55^{10}Y_5^7-2^85^519Y_4^4Y_5^3)\Lambda_2^{12}\Lambda_3^5+(-2^45^{10}Y_4Y_5^6+2^85^6Y_4^6Y_5^2)\Lambda_2^{11}\Lambda_3^4+(2^35^{10}Y_4^2Y_5^5)\Lambda_2^{12}\Lambda_3^3-(2^45^8Y_4^3Y_5^4)\Lambda_2^{13}\Lambda_3^2-(5^{10}Y_5^6)\Lambda_2^{15}$

It was proved in [Arnaudiès-Valibouze, 1993] that $\Delta'_{\Sigma_2}(\pi_1,\ldots,\pi_5)$ does not vanish when $f=T^5-\pi_1T^4+\cdots-\pi_5$ is irreducible. Therefore, χ_{Σ_2} is a *quasi-universally separable resolvent* in the sense that its specialisation in the coefficients of f is squarefree if f is irreducible. Our computation confirms this fact when f is in Bring-Jerrard's form (*i.e.* when $\pi_1=\pi_2=\pi_3=0$): indeed, $\Delta'_\Theta(0,0,0,\pi_4,\pi_5,0,\Lambda_2,0)=9765625\pi_5^6\Lambda_2^{15}$ cancels only for polynomials $f=T^5+\pi_4T-\pi_5$ that satisfy $\pi_5=0$, hence not irreducible.

3.6.5 $\mathfrak{C}_2\ltimes\mathfrak{C}_2$, subgroup of $\mathfrak{S}_4$

We consider $H=((1,2)(3,4),(1,3)(2,4))$ (subgroup of $\mathfrak{S}_4$ of order 4), and we choose $\Pi_i=E_i$ $(1\le i\le 4)$. Then $r=6$, and we can choose $\Sigma_1=1$, $\Sigma_2=X_1X_2+X_3X_4$, $\Sigma_3=X_1X_3+X_2X_4$, $\Sigma_4=\Sigma_2^2$, $\Sigma_5=\Sigma_2\Sigma_3$, $\Sigma_6=\Sigma_2^2\Sigma_3$.

The ideal $\mathfrak{I}$ is generated by the relations $S_{2,2}=-Z_2^2+Z_4$, $S_{2,3}=-Z_2Z_3+Z_5$, $S_{3,3}=-Z_3^2-Z_5-Z_4+Y_2Z_3+Y_2Z_2+4Y_4-Y_1Y_3$, $S_{2,4}=-Z_2Z_4+Y_2Z_4+(4Y_4-Y_1Y_3)Z_2+Y_3^2-4Y_2Y_4+Y_1^2Y_4$ and $S_{3,4}=-Z_3Z_4+Z_6$ (other relations $S_{i,j}$ are generated by the formers). We compute $\operatorname{Sing}(\mathcal{V})$ thanks to the jacobian criterion. It is too large to be written, but its Noether projection has simple equations: $p\,(\operatorname{Sing}(\mathcal{V}))=\mathbf{V}(8Y_3+{Y_1}^3-4Y_1Y_2,64Y_4-16Y_2^2-{Y_1}^4+8Y_2{Y_1}^2)$.

As the primary invariants are the elementary symmetric polynomials, δ is the discriminant of $T^4-Y_1T^3+Y_2T^2-Y_3T+Y_4$.

We define $\Theta=\Lambda_1\Sigma_1+\Lambda_2\Sigma_2+\Lambda_3\Sigma_3$ (we forget $\Sigma_4,\Sigma_5,\Sigma_6$).

Then we compute $\Delta_\Theta=\delta^3\Lambda_2^6\,(\Lambda_3-\Lambda_2)^6\,\Lambda_3^6\,(\Delta'_\Theta)^2$, where Δ'_Θ, over $k[\mathbf{Y}]$, is homogeneous of degree 6 in $\mathbf{\Lambda}$. It is too large to be displayed, but can be recovered from its specialisation in $y_1=0$:

$\Delta'_\Theta(0,Y_2,Y_3,Y_4)(\Lambda_1,\Lambda_2,\Lambda_3)=(256Y_4^3-128Y_2^2\,Y_4^2+(144Y_2Y_3^2+16Y_2^4)Y_4-27Y_3^4-4Y_2^3Y_3^2)\mathcal{S}^6+(-4608Y_4^3-2880Y_2^2Y_4^2+1296Y_2Y_3^2Y_4-243Y_3^4-36Y_2^3Y_3^2-4Y_2^6)\mathcal{D}^2\mathcal{S}^4+(20736Y_4^3+(3888Y_2Y_3^2+720Y_2^4)Y_4-729Y_3^4-108Y_2^3Y_3^2+8Y_2^6)\mathcal{D}^4\mathcal{S}^2+(-5184Y_2^2Y_4^2+(3888Y_2Y_3^2+288Y_2^4)Y_4-729Y_3^4-108Y_2^3Y_3^2-4Y_2^6)\mathcal{D}^6$

where $\mathcal{S}=\frac{\Lambda_2+\Lambda_3}{2}$ and $\mathcal{D}=\frac{\Lambda_2-\Lambda_3}{2}$.

Of course, if we cancel Λ_2 or Λ_3, Δ_Θ will cancel too (in fact, neither of Σ_2 and Σ_3 is a primitive invariant of H).

Now we can try to cancel $\Lambda_2+\Lambda_3$. We get:

$$\Delta'_\Theta(0,Y_2,Y_3,Y_4)(\Lambda_1,\Lambda_2,-\Lambda_2)=64\ \Lambda_2^6\ \left(72\ Y_2\ Y_4-27\ Y_3^2-2\ Y_2^3\right)^2$$

Therefore, $\chi_{\Sigma_2-\Sigma_3}$ is not universally separable. In particular, its specializations in $(y_1,y_2,y_3,y_4)=(0,0,0,a)$ or $(y_1,y_2,y_3,y_4)=(0,6,4,2)$ are not squarefree.

3.6.6 Matrix subgroup

We consider $H=\{\mathrm{Id},A,\ldots,A^5\}$ where $A=\begin{pmatrix}0&1&0\\0&0&1\\-1&0&0\end{pmatrix}$; $k[\mathbf{X}]^H=\sum_{i=1}^{4}k[\mathbf{\Pi}]\Sigma_i$ with $n=3$, $r=4$, $\Pi_1=X_3^2+X_2^2+X_1^2$, $\quad\Pi_2=(X_2-X_1)\ X_3+X_1\ X_2$, $\quad\Pi_3=X_3^6+X_2^6+X_1^6$, $\Sigma_1=1$, $\Sigma_2=X_3^4+X_2^4+X_1^4$, $\Sigma_3=-X_1\ X_3^3+X_2^3\ X_3+X_1^3\ X_2$, $\Sigma_4=-X_1\ X_3^5+X_2^5\ X_3+X_1^5\ X_2$, $\Theta=\Lambda_1\Sigma_1+\Lambda_2\Sigma_2+\Lambda_3\Sigma_3+\Lambda_4\Sigma_4$

From the jacobian criterion, we compute $\operatorname{Sing}(\mathcal{V}) = \mathbf{V}(Y_1 + Y_2, 9Y_3 - {Y_1}^3, 9Z_4 + {Y_1}^3, 3Z_3 + {Y_1}^2, 3Z_2 - {Y_1}^2, Z_1 - 1)$.

Computation of the ideal $\mathfrak{d}$ Thanks to the algorithm of §4.3, we compute the characteristic polynomial χ_Θ, then its discriminant that we factorize: we find

$$\Delta_\Theta = \frac{2^4}{3^9} f_1^2 f_2^2 f_3 f_4^2 f_5^2$$

with $f_1 = -Y_1 + 2\ Y_2$,

$f_2 = 2\ Y_1^3 - 6\ Y_2\ Y_1^2 + 3\ Y_2^2\ Y_1 + Y_3$,

$f_3 = 243\ Y_3^2 + \left(92\ Y_2^3 + 384\ Y_1\ Y_2^2 + 60\ Y_1^2\ Y_2 - 286\ Y_1^3\right) Y_3 + 12\ Y_2^6 + 48\ Y_1\ Y_2^5 + 168\ Y_1^2\ Y_2^4 + 148\ Y_1^3\ Y_2^3 - 84\ Y_1^4\ Y_2^2 - 60\ Y_1^5\ Y_2 + 43\ Y_1^6$, $f_4 = f_2\ \Lambda_4^2 + 3 f_1\ \Lambda_3^2$, and f_5 is a homogeneous polynomial in $\mathbf{\Lambda}$ of degree 4 over $k[\mathbf{Y}]$, too large to be written here. Therefore, the ideal $\mathfrak{d}$ is

$$\mathfrak{d} = f_1^2 f_2^2 f_3 . (f_1^2, f_2^2, f_1 f_2) . \mathfrak{b}^2,$$

where $\mathfrak{b}$ is the ideal of $k[\mathbf{Y}]$ generated by the coefficients of f_5 seen as an element of $k[\mathbf{Y}][\mathbf{\Lambda}]$. We compute the following Gröbner basis of $\mathfrak{b}$, with respect to the lexicographical order: $(Y_2^4 + \frac{31}{4} Y_2^2 Y_1^2 - \frac{11}{2} Y_2 Y_1^3 + \frac{3}{4} Y_1^4, Y_2^3 Y_1 - \frac{5}{2} Y_2^2 Y_1^2 + 2 Y_2 Y_1^3 - \frac{1}{2} Y_1^4, Y_3^2 - \frac{121}{1296} Y_1^6, Y_3 Y_2 - \frac{1}{2} Y_3 Y_1 - Y_2 Y_1^3 + \frac{1}{2} Y_1^4, Y_2^2 Y_1^3 - \frac{5}{6} Y_2 Y_1^4 + \frac{1}{6} Y_1^5, Y_3 Y_1^3 - \frac{11}{36} Y_1^6, Y_2 Y_1^5 - \frac{1}{2} Y_1^6, Y_1^8)$. It proves that $\mathbf{V}(\mathfrak{b}) = \{(0,0,0)\}$. Therefore, $\mathbf{V}(\mathfrak{d}) = \mathbf{V}(f_1 f_2 f_3)$.

Computation of the discriminant δ: Using a Gröbner basis with an elimination order, we compute the polynomial δ such that $k[Y_1, Y_2, Y_3] \cap (\Pi_1 - Y_1, \Pi_2 - Y_2, \Pi_3 - Y_3, J) = (\delta)$, where $J = \left|\frac{\partial \Pi_i}{\partial X_j}\right|$: we find

$$\delta = f_1 f_2 f_3.$$

This example proves that δ is not necessarily irreducible, unlike in the case of permutation groups.

Computation of the ideal $\mathfrak{h}$: 1 is not an eigenvalue of A, A^3 and A^5, but it is an eigenvalue of A^2 and A^4, with one dimensional eigenspace generated by $(1, -1, 1)$. Therefore, $\mathcal{C}'(\varphi) = \{(t, -t, t),\ t \in k\}$, $\varpi(\mathcal{C}'(\varphi)) = \{(3t^2, -3t^2, 3t^6),\ t \in k\}$. It defines the ideal $\mathfrak{h} = (Y_1 - 3T^2, Y_2 + 3T^2, Y_3 - 3T^6) \cap k[\mathbf{Y}]$, *i.e.* $\mathfrak{h} = (Y_2 + Y_1, 9Y_3 - Y_1^3)$.

Conclusion: An easy computation proves that f_3 belongs to $\mathfrak{h}$. Therefore, $\mathfrak{d}.\mathfrak{h} = \mathfrak{d}$, and $\sqrt{\mathfrak{d}} \cap \mathfrak{h} = \sqrt{\mathfrak{d}} = (f_1 f_2 f_3) = (\delta)$, as announced in Cor. 19.

Here, assertion (20) is reduced to $\mathbf{V}(\delta) = \mathbf{V}(\mathfrak{d}) \supset \mathbf{V}(\mathfrak{h})$, *i.e.* $\mathcal{D}(\varpi) = \mathcal{D}(p) \supset \mathcal{D}'(\varphi)$.

In this particular case, it proves that $\delta(\boldsymbol{y}) \neq 0$ if and only if there exists $\boldsymbol{\lambda} \in k^4$ such that $\Delta(\boldsymbol{\lambda}, \boldsymbol{y}) \neq 0$. In other words, $\mathfrak{a}_{\boldsymbol{y}}$ is radical if and only if $\mathfrak{I}_{\boldsymbol{y}}$ is radical.

4 Fast computation of Lagrange resolvents

In all that follows, we suppose that H is a subgroup of the symmetric group $\mathfrak{S}_n$ and that the primary invariants are the elementary symmetric polynomials: $\Pi_i = E_i$.

Generic Lagrange resolvent is the classical name given to the characteristic polynomial $\chi_\Theta(T)$ of an element Θ of $k[\mathbf{X}]^H$ in this particular case. Let us recall that χ_Θ is irreducible iff $\operatorname{Stab}_{\mathfrak{S}_n}\Theta = H$.

Given $\boldsymbol{\pi} \in k^n$, we call *(specialized) Lagrange resolvent* of the univariate polynomial

$$f = T^n + \sum_{i=1}^{n}(-1)^i \pi_i T^{n-i} \in k[T]$$

relatively to the invariant Θ the specialization $\chi_{\Theta,\boldsymbol{\pi}}(T)$ of $\chi_\Theta(T)$ when we substitue the scalar π_i to the elementary symmetric polynomial Π_i for $1 \leq i \leq n$. Equivalently, $\chi_{\Theta,\boldsymbol{\pi}}(T) = \chi_\Theta(x_1, \ldots, x_n, T) = \prod_{\tau \in \mathfrak{S}_n//H}(T - \Theta^\tau(\boldsymbol{x}))$ where $(x_1, \ldots, x_n)$ are the roots of f in $\bar{k}$

Lagrange resolvents (especially squarefree Lagrange resolvents) are used *e.g.* as a tool in Galois group computations (see [McKay-Soicher, 1985, Arnaudiès-Valibouze, 1993] for instance).

The basic way to compute Lagrange resolvents is to express the generic coefficients of χ_Θ in terms of the elementary symmetric polynomials $E_1, \ldots, E_n$, then to substitute π_i to E_i in order to get $\chi_{\Theta,\boldsymbol{\pi}}$. This method is expensive.

In the present section, we show (§4.2) how the Noether normalisation of $k[\mathbf{X}]^H$ enables to compute fast in this algebra, and in particular to compute fast a given Lagrange resolvent. Then we show (§4.3) that we can find with a low complexity a squarefree Lagrange resolvent. To begin with, we specify results of §3 on discriminants in the case of Lagrange resolvents.

4.1 Equality of discriminants

We specify the results of §3, showing that the last two of the three discriminants $p(\mathcal{D}'(\varphi)) = \mathbf{V}(\mathfrak{h})$, $\mathcal{D}(p) = \mathbf{V}(\mathfrak{d})$ and $\mathcal{D}(\varpi) = \mathbf{V}(\delta)$ defined in §3 happen to coincide if $H \neq \mathfrak{S}_n$, and all three if moreover H contains a transposition.

We recall that in the present case, $\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}}) = \varpi^{-1}(\boldsymbol{\pi}) = ((x_{\tau(i)})_{1 \leq i \leq n})_{\tau \in \mathfrak{S}_n})$.

Proposition 20 *In the case of Lagrange resolvents, δ (defined in Prop 12) is (up to the multiplication by a constant) the discriminant of the generic polynomial of degree n,* i.e.

$$\delta = \operatorname{discrim}_T \left(T^n + \sum_{i=1}^{n}(-1)^i Y_i T^{n-i} \right) \in k[\mathbf{Y}].$$

Consequently, δ is irreducible, and $\mathcal{D}(\varpi) = \mathbf{V}(\delta)$ is an irreducible variety.

Proof – As both δ and the generic discriminant are squarefree, from Hilbert's Nullstellensatz it is enough to prove that both polynomials have the same zeros. From Prop. 11, a point $\boldsymbol{\pi} \in \mathbb{A}^n$ is a zero of δ if and only if the cardinality of the finite set $\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}})$ is less than $\dim_k k[\mathbf{X}]/\mathfrak{a}_{\boldsymbol{\pi}} = n!$. Now, $\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}}) = \{(x_{\tau(1)}, \ldots, x_{\tau(n)}),\ \tau \in \mathfrak{S}_n\}$, where $(x_1, \ldots, x_n)$ denotes the roots in $\bar{k}$ of $f = T^n - \pi_1 T^{n-1} + \cdots + (-1)^n \pi_n$. Consequently, $\boldsymbol{\pi}$ is a zero of δ if and only if two roots of f in $\bar{k}$ are equal, *i.e.* if the generic discriminant cancels on $\boldsymbol{\pi}$. □

Remark: In the general case where H is a matrix group, δ is not necessarily irreducible, see the examples following Cor. 19, or the example of §3.6.6.

Proposition 21 *If $H \neq \mathfrak{S}_n$, then*

$$\mathcal{D}(\varpi) = \mathcal{D}(p) \supset p(\mathcal{D}'(\varphi)), \tag{24}$$

Besides, the inclusion $\mathcal{D}(p) \supset p(\mathcal{D}'(\varphi))$ is an equality if and only if H contains a transposition.

Proof – From (22), $\mathbf{V}(\delta) = \mathbf{V}(\mathfrak{d}) \cup \mathbf{V}(\mathfrak{h})$. As $\mathbf{V}(\delta)$ is irreducible, it is equal to $\mathbf{V}(\mathfrak{d})$ or to $\mathbf{V}(\mathfrak{h})$. From the description of $\mathbf{V}(\mathfrak{h})$ given by (11), we infer that if H contains no transposition, then the codimension of $\mathbf{V}(\mathfrak{h})$ in $\mathbb{A}^n$ is at least two, whereas $\mathbf{V}(\delta)$ is of codimension 1, which proves the results. And that when H contains a transposition, $\mathbf{V}(\mathfrak{h})$ is of codimension one, therefore equals $\mathbf{V}(\delta)$. We still have to prove that $\mathbf{V}(\delta) \subset \mathbf{V}(\mathfrak{d})$.

Consider $\boldsymbol{\pi} \in \mathbf{V}(\delta)$. The polynomial $f = T^n - \pi_1 T^{n-1} + \cdots + (-1)^n \pi_n$ has a multiple root in $\bar{k}$. Up to a renumbering of these roots, we can assume that $x_1 = x_2$. Now, consider $\Theta \in k[\mathbf{X}]^H$, and note $\{\tau_1, \ldots, \tau_r\}$ a representative set of the right cosets of H in $\mathfrak{S}_n$, and $\Theta_i = \Theta^{\tau_i}$. For each i, Θ_i belongs to $k[\mathbf{X}]^{\tau_i^{-1}.H.\tau_i}$. Consider the transposition $(1,2)$. If it belonged to all the groups $\tau_i^{-1}.H.\tau_i$ $(1 \leq i \leq r)$, then we would get: $\tau^{-1}.(1,2).\tau \in H$ for all $\tau \in \mathfrak{S}_n$; therefore H would contain all the transpositions (they are all conjugate to $(1,2)$), which would imply $H = \mathfrak{S}_n$, contrary to our hypothesis. Consequently, there exists $i \in \{1, \ldots, r\}$ such that $(1,2) \notin \tau_i^{-1}.H.\tau_i$. Therefore, $H.\tau_i.(1,2) \neq H.\tau_i$, so $H.\tau_i.(1,2) = H.\tau_j$ with $j \neq i$. It implies that $\Theta_i^{(1,2)} = \Theta_j$. Therefore, $\Theta_j(\boldsymbol{x}) = \Theta_i(\boldsymbol{x})$, because $x_1 = x_2$. As $i \neq j$, it implies that $\chi_{\Theta,\boldsymbol{\pi}}$ is not squarefree. As it is true for any $\Theta \in k[\mathbf{X}]^H$, it proves from Prop. 10 that $\boldsymbol{\pi} \in \mathbf{V}(\mathfrak{d})$. □

Remark: The last point of the proposition means that f not squarefree implies that the Lagrange resolvent $\chi_{\Theta,\boldsymbol{\pi}}(T)$ is not squarefree either.

Corollary 22 *When H is different from $\mathfrak{S}_n$, the dirimant and the discriminant of p coincide.*

Proof – $\mathcal{D}(p) = \mathrm{Dirimant}(p) \cup p(\mathrm{Sing}\,\mathcal{V})$, where the three sets are Zariski-closed, $\mathcal{D}(p) = \mathcal{D}(\varpi) = \mathbf{V}(\delta)$ is irreducible, codim $\mathcal{D}(p) = 1$ and codim $p(\mathrm{Sing}\,\mathcal{V}) \geq 2$. □

Corollary 23 *Suppose $H \neq \mathfrak{S}_n$. For any $\boldsymbol{\pi} \in k^n$, the following assertions are equivalent:*

i. $\delta(\boldsymbol{\pi}) \neq 0$,

ii. $\mathfrak{a}_{\boldsymbol{\pi}}$ *is radical,*

iii. $\mathfrak{I}_{\boldsymbol{\pi}}$ *is radical,*

iv. $\exists \boldsymbol{\lambda} \in k^r,\ \Delta(\boldsymbol{\lambda}, \boldsymbol{\pi}) \neq 0$, *v. There exists $\boldsymbol{\lambda}$ in k^r such that $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{\pi}}$ is squarefree.*

Corollary 24 *If $H \neq \mathfrak{S}_n$ then $\delta(\mathbf{Y})$ divides $\Delta(\mathbf{Y},\mathbf{\Lambda})$ in $k[\mathbf{Y},\mathbf{\Lambda}]$, and $(\delta) = \sqrt{\mathfrak{d}}$.*

Remark: The equivalence ($\mathfrak{a}_{\boldsymbol{\pi}}$ radical) $\iff$ ($\mathfrak{I}_{\boldsymbol{\pi}}$ radical) is obviously false if $H = \mathfrak{S}_n$. Indeed, in this case, $r = 1$, $k[\mathbf{Z}]/\mathfrak{I}_{\boldsymbol{\pi}} \simeq k[\mathbf{X}]^{\mathfrak{S}_n}/\mathfrak{a}_{\boldsymbol{\pi}} \simeq k$ is always a field, so $\mathfrak{I}_{\boldsymbol{\pi}}$ is radical (in fact it is $(Z-1)$), but $\mathfrak{a}_{\boldsymbol{\pi}}$ is not radical as soon as $\delta(\boldsymbol{\pi})$ cancels, for instance with $n = 2$, $\mathbf{\Pi} = \mathbf{E}$ and $\boldsymbol{\pi} = (2, 1)$.

4.2 The computation

4.2.1 Principle

Given a family of scalars, $\boldsymbol{y} = (y_1, \dots, y_n) \in k^n$, we adapt the algorithms of §2.5.3 to compute $\chi_{\Theta,\boldsymbol{y}}$. The idea is to specialize the $k[\mathbf{\Pi}]$-algebra structure of $k[\mathbf{X}]^H$ into a k-algebra structure of k^r: we work in $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{y}}$ instead of $k[\mathbf{X}]^H$ (we recall that $\mathfrak{a}_{\boldsymbol{y}}$ is the ideal $(\Pi_1 - y_1, \dots, \Pi_n - y_n)$). Notice that $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{y}}$ is a subalgebra of the universal decomposition algebra $k[\mathbf{X}]/\mathfrak{a}_{\boldsymbol{y}}$.

We note $\theta = \Theta + \mathfrak{a}_{\boldsymbol{y}}$ and $\sigma_l = \Sigma_l + \mathfrak{a}_{\boldsymbol{y}}$ (classes modulo $\mathfrak{a}_{\boldsymbol{y}}$).

Then, $(\sigma_1, \dots, \sigma_r)$ is a k-basis of $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{y}}$. It allows to identify $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{y}}$ to k^r. Besides, we have the following multiplication table between the basis elements (got by specializing the generic table (2)):

$$\sigma_i \sigma_j = A_1^{i,j}(\boldsymbol{y})\sigma_1 + \cdots + A_r^{i,j}(\boldsymbol{y})\sigma_r. \tag{25}$$

And $\chi_{\Theta,\boldsymbol{y}}$ is the characteristic polynomial of θ in the k-algebra $k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{y}} \simeq k^r$. So, $\chi_{\Theta,\boldsymbol{y}} = \chi_\theta$ can be computed from the multiplication table (25) by the same methods (Le Verrier or Kaltofen-Wiedemann) described in section 2.5.3 to compute χ_Θ.

The complexity of the computation using Kaltofen–Wiedemann is $\widetilde{O}(r^{2+\frac{\omega}{2}})$ additions and multiplications in k.

We can sum-up this method as follows.

4.2.2 Algorithm

Input: n, r, Σ a $k[\mathbf{\Pi}]$-basis of $k[\mathbf{X}]^H$, $\boldsymbol{y}$ a point in k^n, and Θ an invariant of H, given by its coordinates $(B_1, \dots, B_r)$ in $\mathbf{\Sigma}$: $\Theta = \sum_{i=1}^r B_i(\mathbf{\Pi})\Sigma_i$.

Alternatively, $(B_1, \dots, B_r)$ can be replaced by the point $\boldsymbol{\lambda}$ in k^r defined by $\lambda_i = B_i(\boldsymbol{y})$: indeed, the output depends only on the specialization of the coordinates of Θ (so that Θ can be assumed to be equal to $\sum_{i=1}^r \lambda_i \Sigma_i$).
Output: the characteristic polynomial $\chi_{\Theta,\boldsymbol{y}}$.

1. Compute the scalars $A_l^{i,j}(\boldsymbol{y}) = a_l^{i,j}$ thanks to Algorithm 1 or Algorithm 2 of §1.2.5 It requires the precomputation of the products $\Sigma_i\Sigma_j\Sigma_k$ in the case of Algorithm 1.

   This step does not depend on the choice of Θ.

2. Form the matrices $M_{\sigma_i} = (a_l^{i,j})_{(l,j)\in\{1,\dots,r\}^2}$, and $M_\theta = \sum_{i=1}^r \lambda_i M_{\sigma_i}$.

3. Use one of the algorithms of §2.5.3 to compute the characteristic polynomial of M_θ. This is $\chi_{\Theta,\boldsymbol{y}}$.

The first step is independent of the choice of Θ, it depends only on the choice of $\boldsymbol{y}$.

Complexity: We compute the complexity in the case of Algorithm 2.

With a view towards §4.3, we distinguish the complexity $\mathcal{P}$ of step 1, independant of Θ, and the complexity $\mathcal{Q}$ of the computation depending on Θ (steps 2 and 3).

From §1.2.5,

$$\mathcal{P}(n,r) = \widetilde{O}((n!)^2 n + n! n r^3 + r^4). \tag{26}$$

The second step costs $O(r^3)$ additions and multiplications. With a view towards §4.3, in the third step of the algorithm we distinguish according to whether divisions are authorised or not: it costs $\widetilde{O}(r^{2+\omega/2})$ using Kaltofen-Wiedesman's algorithm, or $O(r^\omega)$ if divisions in k are authorized. So, the corresponding complexities are:

$$\mathcal{Q}_{\text{no div}}(r) = \widetilde{O}(r^{2+\omega/2}), \qquad \mathcal{Q}_{\text{div}}(r) = O(r^\omega). \tag{27}$$

Implementation: The algorithm was implemented by the first author in Axiom (see [Axiom, 1992]). The same Axiom package can be used on any field of characteristic 0, either over k to get $\chi_{\Theta,\boldsymbol{y}}$, either generically over $k[\mathbf{\Pi}]$ to get χ_Θ (we just need to ask Axiom to evaluate on $\mathbf{\Pi}$ instead of $\boldsymbol{y}$).

Important remark: It is even quicker to compute $\chi_{\Theta,\boldsymbol{y}}$ through the present algorithm than to evaluate in $\boldsymbol{y}$ (*e.g.* with Horner's algorithm) the generic polynomial χ_Θ, given by the vector of its coefficients.

Thinking of it, this is not so surprising: the reason is the same, why it is quicker to compute the determinant of a square matrix from the Gauss or the KW algorithm (polynomial time in the size of the matrix) than to specialize the precomputed generic determinant in the coefficients of the matrix (exponential time).

Conclusion: Storing χ_Θ as the evaluation program defined by the present algorithm is more efficient than storing its generical coefficients (not to mention that the generical computation may be out of reach).

4.2.3 Example

We consider the case where $n = 6$, H is the subgroup of the symmetric group $\mathfrak{S}_6$ generated by the permutations $(1,3)(2,4), (1,3,4)(2,5,6), (3,4,5,6)$ (H is isomorphic to $\mathfrak{S}_5$), and the primary invariants are the elementary symmetric polynomials ($\Pi_i = E_i$). We use the following secondary invariants (given by `Magma`): $\Sigma_1 = 1$, $\Sigma_2 = \sum_H X_1^2 X_2^2 X_3 X_4$ (60 terms), $\Sigma_3 = \sum_H X_1^3 X_2^2 X_3^2 X_4$ (120 terms), $\Sigma_4 = \sum_H X_1^3 X_2^3 X_3^2 X_5$ (60 terms), $\Sigma_5 = \sum_H X_1^4 X_2^3 X_3^2 X_5$ (120 terms) and $\Sigma_6 = \Sigma_2^2$.

Precomputation: On this example, we precomputed not only the products $\Sigma_i \Sigma_j \Sigma_k$, but the generic multiplication table between the Σ_i (*i.e.* the coefficients $A_l^{i,j} \in k[\mathbf{\Pi}]$) thanks to an Axiom package (using the second method in Section 1.2.3). The result is too large to be written here, but sizeably smaller than the generic polynomial χ_Θ.

Computation of $\chi_{\Theta,\boldsymbol{y}}$: For instance, we choose $\Theta = \Sigma_2$, and we compute the resolvent of $f = T^6 + 2T^4 + 2T^3 - T^2 - 2T - 2$ relatively to Θ. So, we set $\boldsymbol{y} = (0, 2, -2, 1, -2, 2)$.

The matrix of the multiplication by θ, *i.e.* the matrix $\left(a_l^{i,2}\right)_{i,l}$, is

$$M_\theta = \begin{pmatrix} 0 & 0 & -468 & -1332 & 228 & -11640 \\ 1 & 0 & -4 & -40 & -24 & -548 \\ 0 & 0 & -\frac{24}{5} & \frac{9}{5} & -\frac{22}{5} & -\frac{398}{5} \\ 0 & 0 & \frac{54}{5} & \frac{126}{5} & -\frac{18}{5} & \frac{1008}{5} \\ 0 & 0 & -\frac{18}{5} & -\frac{27}{5} & -\frac{24}{5} & -\frac{786}{5} \\ 0 & 1 & -\frac{4}{5} & \frac{9}{5} & \frac{8}{5} & \frac{322}{5} \end{pmatrix}.$$

We compute the characteristic polynomial of M_θ, using either Le Verrier, or Gauss, or BW's algorithm. We get:

$$\chi_\theta = T^6 - 80\,T^5 + 1104\,T^4 + 19376\,T^3 + 80064\,T^2 - 72576\,T - 1259712$$

and this polynomial is also $\chi_{\Theta,\boldsymbol{y}}$. Concerning the computation time, see §5

4.3 Separability questions

The squarefreeness of Lagrange resolvents is a fundamental question: for instance in the frame of Soicher's method to compute the Galois group of a polynomial, Lagrange resolvents involved must be square-free (see [Arnaudiès-Valibouze, 1993, Théorème 6.6] for instance). We say that a primitive invariant Θ of H is *separating* for $\boldsymbol{y} = (y_1, \ldots, y_n)$ (or for $f = T^n - y_1 T^{n-1} + \cdots + (-1)^n y_n$) if the Lagrange resolvent $\chi_{\Theta,\boldsymbol{y}}$ of f is square-free.

In this section, we address the problem of finding such a separating primitive invariant of a given group H for a given polynomial f (which is a subcase of §3) and the complexity of this problem (which is new).

We look for such a Θ written as a linear combination of the secondary invariants: $\Theta_{\boldsymbol{\lambda}} = \lambda_1\Sigma_1 + \cdots + \lambda_r\Sigma_r$, where $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_r) \in k^r$. Indeed, it is equivalent to looking for a general $\Theta = \sum_{l=1}^r B_l(\boldsymbol{\Pi})\Sigma_l$ (the specialized resolvent associated to this Θ is also that of $\Theta_{\boldsymbol{\lambda}}$ with $\lambda_l = B_l(\boldsymbol{y})$).

4.3.1 Geometric problem

The following proposition completes Coro. 23.

Proposition 25 *We assume that f is squarefree (*i.e. $\delta(\boldsymbol{y}) \neq 0$*). Then, there exists an hypersurface $\mathcal{H}$ of k^r, of degree $r(r-1)$, such that $\Theta_{\boldsymbol{\lambda}}$ is a $\boldsymbol{y}$-separating primitive invariant for every $\boldsymbol{\lambda} \in k^r \setminus \mathcal{H}$.*

Proof – We consider $\Theta_\Lambda = \sum_{i=1}^r \Lambda_i\Sigma_i \in k[\boldsymbol{\Lambda}][\mathbf{X}]^H$ and call $\mathcal{H}$ the zeroes of the polynomial $\Delta(\boldsymbol{\Lambda}, \boldsymbol{y})$ of $k[\boldsymbol{\Lambda}]$. From Cor. 23, this polynomial is not zero (a self-contained proof is also given in [Colin, 1995, Propositions 8 and 9]). Therefore, $\mathcal{H}$ is a hypersurface of k^r. We note $\boldsymbol{x}$ the roots of f in $\mathbb{A}^n$. Then,

$$\chi_{\Theta_\Lambda,\boldsymbol{y}} = \prod_{\tau \in (\mathfrak{S}_n /\!\!/ H)} \left(T - \sum_{i=1}^r \Lambda_i \Sigma_i^\tau(\boldsymbol{x})\right)$$

$$\text{and } \Delta(\boldsymbol{\Lambda}, \boldsymbol{y}) = \prod_{\substack{\tau_1,\tau_2 \in (\mathfrak{S}_n /\!\!/ H) \\ \tau_1 \neq \tau_2}} \sum_{i=1}^r \Lambda_i \left(\Sigma_i^{\tau_1}(\boldsymbol{x}) - \Sigma_i^{\tau_2}(\boldsymbol{x})\right).$$

So the degree of $\Delta(\boldsymbol{\Lambda}, \boldsymbol{y})$, *i.e.* the degree of $\mathcal{H}$, is $r(r-1)$.

If $\boldsymbol{\lambda}$ does not belong to $\mathcal{H}$, then the discriminant $\Delta(\boldsymbol{\lambda}, \boldsymbol{y})$ of $\chi_{\Theta_{\boldsymbol{\lambda}}, \boldsymbol{y}}$ does not vanish. It proves that $\Delta(\boldsymbol{\lambda}, \mathbf{Y}) \neq 0$, *i.e.* that $\Theta_{\boldsymbol{\lambda}}$ is a primitive invariant of H, and that it is $\boldsymbol{y}$-separating. □

4.3.2 Complexity problem

Naive method Using the only property of $\mathcal{H}$ that its degree is $\deg(\mathcal{H}) = r(r-1)$, we need at most $(1+\deg(\mathcal{H}))^r = (r^2-r+1)^r \leq r^{2r}$ tries to find a point $\boldsymbol{\lambda}$ in $k^r \setminus \mathcal{H}$.

Using Heintz-Schnorr In our case, $\mathcal{H}$ is not any hypersurface of degree $r(r-1)$: it is defined by the polynomial $\Delta_{\Theta_{\boldsymbol{\Lambda}}, \boldsymbol{y}} = \mathcal{R}es_T(\chi_{\Theta_{\boldsymbol{\Lambda}}, \boldsymbol{y}}, \partial(\chi_{\Theta_{\boldsymbol{\Lambda}}, \boldsymbol{y}})/\partial T)$, which, as a determinant, is easier to evaluate than an arbitrary polynomial of the same degree.

Heintz-Schnorr theorem proves that a point out of $\mathcal{H}$ can be found with a number of tries polynomial in r, and hence a separable resolvent of H can be computed with a polynomial complexity in r.

We recall the Heintz-Schnorr theorem:

Theorem 26 (Heintz-Schnorr) *Let k be an effective integral domain of characteristic 0. Consider the set $P(d,p,v)$ of the polynomials in $k[X_1, \ldots, X_p]$ whose degree is at most d and that can be evaluated by a computation of length* [number of additions and multiplications on elements of k] *at most v. Let Γ be a finite subset of k of cardinal* $2v(1+d)^2$. *Then there exists a subset $\mathcal{S}(d,p,v,\Gamma)$ of Γ^p of cardinal $m := 6(v+p)(v+p+1)$ such that the only polynomial of $P(d,p,v)$ that cancels on all the points of $\mathcal{S}(d,p,v,\Gamma)$ is zero.*

Such a subset $\mathcal{S}(d,p,v,\Gamma)$ of Γ^p is called a correct test sequence. The proportion in $((\Gamma)^p)^m$ of non correct test sequences is at most $(\#\Gamma)^{-\frac{m}{6}}$.

Proof – See [Heintz-Schnorr, 1982]. □

We apply Heintz-Schnorr's theorem to the search of a point out of $\mathcal{H}$; with $p = r$, $d = r(r-1)$, and v the total evaluation length of $\Delta_{\Theta_{\boldsymbol{\Lambda}}, \boldsymbol{y}}$ in $\boldsymbol{\Lambda}$. We write $v = v_1 + v_2$, where

- v_1 is the evaluation length in $\boldsymbol{\Lambda}$ of $\chi_{\theta_{\boldsymbol{\Lambda}}} = \chi_{\Theta_{\boldsymbol{\Lambda}}, \boldsymbol{y}}$. From (27), it is $v_1 = \mathcal{Q}_{\text{no div}}(r) = \widetilde{O}(r^{2+\omega/2})$
- v_2 is the number of operations to compute the discriminant of this characteristic polynomial; so, $v_2 = \widetilde{O}(r^{2+\frac{\omega}{2}})$ by KW (a specific algorithm for resultants would yield $v_2 = O(r^2 \log r \log\log r)$, but it wouldn't change the bound on the sum $v = v_1 + v_2$).

Consequently, $v = \widetilde{O}(r^{\frac{\omega}{2}+2})$.

The statement of Heintz-Schnorr is now: given an arbitrary set $\Gamma_r \subset k$ such that $|\Gamma_r| = 2v(1+r(r-1))^2 (= \widetilde{O}(r^{\frac{\omega}{2}+6}))$, there exists a subset $\mathcal{S}_r$ of $(\Gamma_r)^r$ of cardinal $|\mathcal{S}_r| = 6(v+r)(v+r+1)$ $(= \widetilde{O}(r^{\omega+4}))$ such that $\chi_{\Theta_{\boldsymbol{\lambda}}, \boldsymbol{y}}$ is a square-free H-resolvent for some $\boldsymbol{\lambda} \in \mathcal{S}_r$.

Therefore, it is enough to compute the resolvents associated to $|\mathcal{S}_r| = \widetilde{O}(r^{\omega+4})$ values of $\boldsymbol{\lambda}$. Once a precomputation of cost $\mathcal{P}(n,r) = \widetilde{O}((n!)^2 n +$

$n!nr^3 + r^4)$ is done, the unitary cost to compute one of this resolvent (and its discriminant) is $\mathcal{Q}_{\text{div}}(r) = O(r^\omega)$. We get:

Theorem 27 *There exists an algorithm to compute a* ***square-free*** *H-resolvent of a square-free polynomial $f \in k[T]$ with a complexity $\widetilde{O}(r^{2\omega+4})$.*

It consists in computing a number $|\mathcal{S}_r| = \widetilde{O}(r^{\omega+4})$ of H-resolvents of f – with a unitary cost $\mathcal{Q}_{\text{div}}(r) = O(r^\omega)$, including the computation of their discriminants – among which one at least is square-free.

This can be done after a precomputation of complexity $\mathcal{P}(n, r) = \widetilde{O}((n!)^2n + n!nr^3 + r^4)$

INPUT:

- a system of fundamental invariants $(\Pi_1, \dots, \Pi_n, \Sigma_1, \dots, \Sigma_r)$ of an invariant algebra $k[\mathbf{X}]^H$;
- a squarefree polynomial $f = T^n - y_1T^{n-1} + \cdots + (-1)^n y_n \in k[T]$.

OUTPUT:

- scalars $\lambda_1, \dots, \lambda_r \in k$ such that $\Theta = \lambda_1\Sigma_1 + \cdots + \lambda_r\Sigma_r$ be a $\boldsymbol{y}$-separating primitive H-invariant;
- the squarefree Lagrange resolvent $\chi_{\Theta,\boldsymbol{y}} \in k[T]$.

ALGORITHM:

1. Compute the scalars $A_l^{i,j}(\boldsymbol{y}) = a_l^{i,j}$ thanks to Algorithm 1 or Algorithm 2 of §1.2.5. It requires the precomputation of the products $\Sigma_i\Sigma_j\Sigma_k$ in the case of Algorithm 1.
2. Form the matrices $M_{\sigma_i} = (a_l^{i,j})_{(l,j)\in\{1,\dots,r\}^2}$.
3. Compute a correct test sequence $\mathcal{S}$ defined by the Heintz-Schnorr theorem ($|\mathcal{S}| = 6(v+r)(v+r+1)$, $\mathcal{S} \subset \Gamma^r$ where $\Gamma \subset k$ and $|\Gamma| = 2v(r^2 - r + 1)^2$).
4. For each $\boldsymbol{\lambda} \in \mathcal{S}$, repeat: compute the characteristic polynomial $\chi_{\Theta_{\boldsymbol{\lambda}},\boldsymbol{y}}$ of the matrix $\sum_{i=1}^{r} \lambda_i M_{\sigma_i}$ whith the KW-algorithm, and its discriminant $\Delta(\boldsymbol{\lambda}, \boldsymbol{y})$ until $\Delta(\boldsymbol{\lambda}, \boldsymbol{y}) \neq 0$.

5 Future Works

Current and future implementation An old implementation in AXIOM, preliminary to our present work, already showed its efficiency compared to the classical formal computation of Lagrange resolvents [Arnaudiès-Valibouze, 1993]. In 1998, we compared the algorithm of §4.2.2 to two improvements of the classical method implemented into Maxima and SYM [Valibouze, 1989] by A. Valibouze and N. Rennert [Rennert-Valibouze, 1999]. On the example of §4.2.3, our algorithm is 910 to 30 000 times faster (0.72 s, after a precomputation time of 1h30min for the generic multiplication table, instead of 11min and 6h with the two improments of the classical method).

Now we intend to implement the same algorithm into [Mathemagix, 2002], with a view to future improvements and applications to Galois theory.

Future improvements in the computation of the multiplication table Using the fact that some secondary invariants are products of irreducible ones [King, 2013] gives an algorithm to build a minimal generating system), we notice on some examples that the $r(r-1)/2$ products $\Sigma_i\Sigma_j$ (multiplication table) can usually be deduced from a smaller number of them thanks to a straight line program. This will be the object of a future article. This noteworthy fact enables not only to decrease the complexity to build the generic multiplication table between secondary invariants, but also to decrease the computation time to evaluate this table, as the evaluation of straight line programs is faster than that of the generic table.

Application to Galois theory We intend also to apply an extension of our method to the computation of relative resolvents, following the ideas of [Colin, 1995] and [Colin Issac 1997] (rediscovered since by Fieker and Klueners in [Fiekers-Klüners, 2012]).

In [Colin Issac 1997], we showed how a symbolic computation version of Stauduhar's method could be improved by introducing what we called the "descent from uncle to nephew" in the DAG of subgroups of $\mathfrak{S}_n$, while Stauduhar's method descended from "father to son" (*i.e.* from a group to a subgroup) in this DAG.

It enables to reduce significantly the degrees of the resolvants when the index of a subgroup involved in Stauduhar's method is high.

References

[Arnaudiès-Valibouze, 1993] Arnaudiès, J.M., Valibouze, A.: Résolvantes de Lagrange. Prepublication LITP 93.63, December 1993.

[Arnaudiès-Valibouze, 1997] Arnaudiès, J.-M., Valibouze, A.: Lagrange Resolvents, (A. Cohen and M.F. Roy Eds), Journ. of Pure and Appl. Alg. **117 & 118** (1997), 23-40.

[Abdeljaoued-Lombardi, 2004] Abdeljaoued, J., Lombardi, H.: Méthodes matricielles – Introduction à la complexité algébrique. Mathématiques & applications **42**, Springer, 2004.

[Axiom, 1992] **AXIOM**, The Scientific Computation System. R.D. Jenks, R.S. Sutor. Springer-Verlag, 1992.

[Berwick, 1915] Berwick, E.H.: The condition that a quintic equation should be soluble by radicals, Proc. London Math. Soc. (1915) **2.14**, 301-307.

[Bostan-Salvy-Schost, 2003] Bostan, A., Salvy, B., Schost, É.: Fast Algorithms for Zero-Dimensional Polynomial Systems using Duality. AAECC **14**, 239-272, Springer (2003).

[Colin, 1995] Colin, A.: Formal Computation of Galois Groups with Relative Resolvents. In Cohen, G., Giusti, M. and Mora, T. editors, proc. AAECC'95, Lecture Notes in Computer Science **948**, 169-182. Springer, Berlin, 1995.

[Colin, 1996] Colin, A.: Solving a System of Algebraic Equations with Symmetries (1996). In Journ. Pure and Applied Algebra vol. 117-118 (1997) p. 195-215.

[Colin Issac 1997] Colin, A.: Relative resolvents and partition tables in Galois group computations. In Gloor, O., Proc. ISSAC'97 (1997).

[Colin Thesis, 1997] Colin, A.: Théorie des invariants effective. Applications à la théorie de Galois et à la résolution de systèmes algébriques. Implantation en AXIOM. Thèse de doctorat, École polytechnique, juin 1997.

[Cox-Little-O'Shea, 1992] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer, 1992. Springer, 1998.

[Cox-Little-O'Shea, 1998] Cox, D., Little, J., O'Shea, D.: Using Algebraic Geometry. Springer, 1998.

[Dahan-Schost-Wu, 2009] Dahan, X., Schost, É., Wu, J.: Evaluation properties of invariant polynomials, Journal of Symbolic Computation, **44**(11) (2009); 1592-1604.

[Darmon-Ford, 1989] Darmon, Ford: Computational verification of M_{11} and M_{12} as Galois groups over $\mathbb{Q}$. Comm. Algebra **17** (1989); 2941-2943.

[Derksen-Kemper, 2002] Derksen, H., Kemper, G.: Computational Invariant Theory. Springer-Verlag, Berlin, 2002.

[Eichenlaub, 1996] Eichenlaub, Y., Problèmes effectifs de théorie de Galois en degrés 8 à 11, thèse de doctorat de l'Université de Bordeaux 1, 1996.

[Elkadi-Mourrain, 2007] Elkadi, M., Mourrain, B.: Introduction à la résolution des systèmes polynomiaux, Springer, 2007.

[Fiekers-Klüners, 2012] Fieker, C., Klüners, J., "*Computational Galois theory: invariants and computations over* $\mathbb{Q}$. Preprint 2012, submitted. http://www2.math.uni-paderborn.de/fileadmin/Mathematik/AG-Klueners/publications/invar.pdf

[Geißler, 1997] Geißler, K.: Sur Berechnung von Galoisgruppen. Diplomarbeit, Technische Universität Berlin, 1997.

[Geißler-Klüners, 2000] Geißler, K., Klüners, J.: Galois Group Computation for Rational Polynomials, J. Symbolic Computation (2000) **20**, 1-23.

[Giusti-Heintz, 1991] Giusti, M., Heintz, J.: La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. Proc. Intern. Meeting on Commutative Algebra, Cortona, Cambridge University Press, 1991.

[von zur Gathen-Gerhard, 2003] von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, 2003.

[Giusti-Heintz-Sabia, 1993] Giusti, M., Heintz, J., Sabia, J.: On the efficiency of effective nullstellensätze. Comput complexity **3** (1993), 56-95.

[Giusti-Heintz-Morais-Pardo, 1995] Giusti, M., Heintz, J., Morais, J.E., Pardo, L.M.: When polynomial equations can be "solved" fast ? In Cohen, G., Giusti, M. and Mora, T. editors, proc. AAECC'95, Lecture Notes in Computer Science **948**, 169-182. Springer, Berlin, 1995.

[Giusti-Hägele-Heintz-Morais-Montaña-Pardo, 1996] Giusti, M., Hägele, K., Heintz, J., Morais, J.E., Montaña, J.L., Pardo, L.M.: Lower bounds for diophantine approximation, acts of MEGA 96, Journal of Pure and Applied Algebra 117 & 118 (1997), 277-317.
(Provisional version: `http://medicis/gage/notes/96nouvelles.html`, Note 96-08).

[Giusti-Heintz-Morais-Pardo, 1997] Giusti, M., Heintz, J. Morais, J.E., Pardo, L.M.: Le rôle des structures de données dans les problèmes d'élimination, C. R. Acad. Sci. Paris, t. 325, Série I (1997) 1223-1228.
(Provisional version `http://medicis/gage/notes/97nouvelles.html`, Note 97-01).

[Greenberg-Harper, 1981] Greenberg, M., Harper, J.R.: Algebraic Topoloy: A First Course. Benjamin Cummings, 1981.

[Heintz-Schnorr, 1982] Heintz, J., Schnorr, C.-P., Testing polynomials which are easy to compute. Logic and Algorithmic, An International Symposium held in honour of Ernst Specker, Monographie numéro 30 de l'Enseignement Mathématique, Genève, 1982.

[Henry-Merle-Sabbah, 1984] Henry, J.-P., Merle, M., Sabbah, C., Sur la condition de Thom stricte pour un morphisme analytique complexe, Ann. Sci. Éc. Norm. Sup. Sér. 417 (1984), 227–268.

[Heintz-Matera-Waissbein, 1999] Heintz, J., Matera, G., Waissbein, A.: On the time-space complexity of geometric elimination procedures AAECC (2001) **11**(4), 239-296.

[Hochster-Eagon, 1971] Hochster, M., Eagon, J.A., Cohen-Macaulay Rings, invariant theory, and the generic perfection of determinantal loci. Amer. J. Math. **93** (1971), 1020-1058.

[Kemper, 1996] Kemper, G.: Calculating Invariant Rings of Finite Groups over Arbitrary Fields (1995). Journal of Symbolic Computation **21** (1996), 351-366.

[King, 2013] King, S.A.: Minimal generating sets of non-modular invariant rings of finite groups. Journal of Symbolic Computation **48** (2013) 101-109.

[Lebreton-Schost, 2012] Lebreton, R., Schost, E.: Algorithms for the universal decomposition algebra. Proc. ISSAC 2012.

[Machì-Valibouze, 1991] Machì, A., Valibouze, A.: L'idéal des relations symétriques et l'idéal des relations. Preprint, Univ. Paris VI, 1991.

[McKay-Soicher, 1985] McKay, J., Soicher, L.: Computing Galois groups over the rationals. J. Number Theory (1985) **20**, 273-281.

[Mathemagix, 2002] van der Hoeven, J., Lecerf, G., Mourrain, B., et al. Mathemagix, 2002–2013. Software available from `http://www.mathemagix.org`.

[Rennert-Valibouze, 1999] Rennert, N., Valibouze, A.: Calcul de résolvantes avec les modules de Cauchy. Experimental Mathematics (1999) 8:4.

[Shafarevich, 1994] Shafarevich, I.R.: Basic Algebraic Geometry. Springer, 1994.

[Stanley, 1979] Stanley, R.P.: Invariants of finite groups and their applications to combinatorics. Bul. (New Series) American Math. Soc. Vol. 1 Num. 3 (1979).

[Stauduhar, 1973] Stauduhar, R.P.: The Determination of Galois Groups. Math. Comp. **27** (1973) 981-996.

[Sturmfels, 1993] Sturmfels, B.: Algorithms in Invariant Theory. Springer-Verlag, Wien, 1993.

[Valibouze, 1986] Valibouze, A.: Manipulation des fonctions symétriques, Thèse de doctorat, Université Paris VI, 1986.

[Valibouze, 1989] Valibouze, A.: **SYM**, Symbolic computation with symmetric polynomials, an extension to Macsyma, in proc. Computers and Mathematics, (MIT), Cambridge, Mass., Springer, 1989, pp. 308-320.

[Valibouze, 1996] Valibouze, A.: Modules de Cauchy, polynômes caractéristiques et résolvantes. Preprint LIP6, 1996.

[Yokoyama, 1997] Yokoyama, K.: A modular method for computing the Galois groups of polynomials, Journal of Pure and Applied Algebra (1997) **117-118**, 617-636.

[Zariski-Samuel, 1960] Zariski, O., Samuel, P., Commutative Algebra. Graduate Texts in Math., Springer, 1960.