

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

December 7, 2009

¹This work was supported in part by the French National Agency for Research (ANR “Gecko”)

Abstract

We propose a general frame to compute efficiently in the invariant algebra $k[X_1, \dots, X_n]^H$, where H is a finite subgroup of the general linear group $\mathbf{GL}_n(k)$. 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 H , either generically or specialized. We show also how to find square-free resolvents with better theoretical complexity (polynomial in the index of the group after a precomputation depending only on H).

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

Contents

1	First fundamental theorem and Noether normalisation	3
2	Second fundamental theorem	3
2.1	Trivial relations	4
2.2	All relations	4
2.3	Computation of the relations	4
3	Geometric consequences	5
4	Discriminants	7
4.1	Singular locus of the quotient variety	7
4.2	Discriminant of the parametrization of the quotient variety	7
4.3	Discriminant of the Noether projection	9
4.4	Discriminant of the primary projection	11
4.5	Link between the 3 discriminants	12
5	Multiplication tensor and primitive elements	14
6	Fast computation of the characteristic polynomial	15
6.1	Generic characteristic polynomial	16
6.2	Specialised characteristic polynomial	17
6.3	Lagrange resolvents	19
6.4	Separability in the case of Lagrange resolvents	21
7	More examples	25
7.1	The alternated group \mathfrak{A}_n , as a subgroup of \mathfrak{S}_n	25
7.2	\mathfrak{S}_2 , subgroup of \mathfrak{S}_3	25
7.3	Dihedral group \mathfrak{D}_4 , subgroup of \mathfrak{S}_4	26
7.4	The metacyclic subgroup of \mathfrak{S}_5	26
7.5	$\mathfrak{C}_2 \times \mathfrak{C}_2$, subgroup of \mathfrak{S}_4	27
7.6	Matrix subgroup	27
8	Conclusion	28

*Dedicated to Joos Heintz
for his pioneering work*

Introduction

Let k be a field of characteristic 0. In all that follows, H is a finite subgroup of the general linear group $\mathbf{GL}_n(k)$. We consider the right action of the group $\mathbf{GL}_n(k)$ on the polynomial ring $k[\mathbf{X}] = k[X_1, \dots, X_n]$, defined by the following action of the matrix $A = (a_{i,j})$ on the polynomial p :

$$(p, A) \mapsto p^A = p(A \cdot \mathbf{X}) = p(a_{11}X_1 + \dots + a_{1n}X_n, \dots, a_{n1}X_1 + \dots + a_{nn}X_n)$$

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

The general linear group has also a left action on the affine space $\mathbb{A}_k^n \simeq k^n$: for any point $\mathbf{x} \in k^n$, $A \cdot \mathbf{x}$ is defined as the usual product of the matrix A and the column \mathbf{x} . This left action is coherent with the right action on $k[\mathbf{X}]$, in the sense that $p^A(\mathbf{x}) = p(A \cdot \mathbf{x})$.

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 $H \subset \mathbf{GL}_n(k)$.

★

In this framework, a well-known theorem (see e.g. [St79]) says that the invariant algebra $k[\mathbf{X}]^H = k[X_1, \dots, X_n]^H$ is Cohen-Macaulay, and, using the Noether normalization lemma, admits a natural **Hironaka decomposition** in terms of primary and secondary invariants (see section 1 below).

On the other hand, M. Giusti, J. Heintz, L. M. Pardo and their collaborators showed in a sequence of papers (see e.g. [GiHe91], [GHS93], [GHMP95], [GHHM+96], [GHMP97]), 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 we obtain:

Theorem 28 *There exists an algorithm that computes a square-free Lagrange H -resolvent of a univariate polynomial in polynomial time in the index of the group H , after a precomputation depending only on H .*

We want to thank Éric Schost for inspiring hints and corrections in sections 3 and 4.

1 First fundamental theorem and Noether normalisation

To the best of our knowledge, the following result was first proved by Hochster and Eagon in [HoEa71].

Theorem 1 *Let H be a finite subgroup of $\mathbf{GL}_n(k)$. The algebra $k[\mathbf{X}]^H$ is Cohen-Macaulay with Krull-dimension n . There exists an algebraically free family $\mathbf{\Pi} = (\Pi_1, \dots, \Pi_n)$ of homogeneous invariant polynomials such that $k[\mathbf{X}]^H$ be a finitely generated module over $k[\mathbf{\Pi}]$; and that 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 . A homogeneous basis $\mathbf{\Sigma} = (\Sigma_1, \dots, \Sigma_r)$ of $k[\mathbf{X}]^H$ as a free module over $k[\mathbf{\Pi}] = k[\Pi_1, \dots, \Pi_n]$ 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 the scalar 1. 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*:

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

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

The inclusion $k[\mathbf{\Pi}] \hookrightarrow k[\mathbf{X}]^H$ realizes the integral extension of a Noether normalization. There are many possible choices for the primary invariants Π_i . It is easy to see that homogeneous invariant polynomials (Π_1, \dots, Π_n) form a family of primary invariants if and only if they define the empty projective subvariety over an algebraic closure of 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 G. Kemper (see [Ke96]) and implemented in `Magma`. His software can also express a given invariant in terms of the fundamental invariants.

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

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

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

2.1 Trivial relations

We find easily polynomials in \mathfrak{J} as follows. Each product $\Sigma_i \Sigma_j$, $1 \leq i \leq j \leq r$, and the scalar 1, belong to $k[\mathbf{X}]^H$, so that they can be expressed in terms of the fundamental invariants $\Pi_1, \dots, \Pi_n, \Sigma_1, \dots, \Sigma_r$: $1 = \Sigma_1$ (assumed conventionally) and

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

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

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{J} of $k[\mathbf{Y}, \mathbf{Z}]$. Furthermore, these polynomials form a Gröbner basis of \mathfrak{J} 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. Bayer & Stillman's order.*

Proof – See [Co97t, lemme 4.13]. We consider a polynomial P of \mathfrak{J} , and a reduced form R of P modulo all the generators $S_{i,j}$ and S_0 with respect to \preceq . As each product $Z_i Z_j$ is the leading monomial of a generator (with respect to \preceq), R must be linear in the Z_i . Now, as R belongs to \mathfrak{J} and $(\Sigma_1, \dots, \Sigma_r)$ is linearly free over $k[\mathbf{Y}]$, it proves that $R = 0$. Therefore: first, S_0 and the $S_{i,j}$ generate \mathfrak{J} ; second, as P can be any S -polynomial, these generators form a Gröbner basis with respect to \preceq . \square

The following exact sequence

$$0 \longrightarrow \mathfrak{J} \longrightarrow k[\mathbf{Y}, \mathbf{Z}] \longrightarrow k[\mathbf{\Pi}, \mathbf{\Sigma}] = k[\mathbf{X}]^H \longrightarrow 0 \quad (2)$$

allows us to identify the invariant algebra $k[\mathbf{X}]^H$ with $k[\mathbf{Y}, \mathbf{Z}]/\mathfrak{J}$.

2.3 Computation of the relations

As $k[\mathbf{X}]^H$ is a free $k[\mathbf{\Pi}]$ -module, the polynomials $A_l^{i,j}$ are uniquely determined by the equations (1). It was proved in [DaSc] that their evaluation complexity is polynomial in $d_1 \dots d_n$, and that a straight line program to evaluate them can be found in polynomial time too.

In the present paper, we compute them using one of the two following methods.

First method. Compute a reduced Gröbner basis $\mathcal{G}(\mathcal{I})$ of the ideal

$$\mathcal{I} = (\{Y_i - \Pi_i, i \in \{1, \dots, n\}\} \cup \{Z_i - \Sigma_i, i \in \{1, \dots, r\}\}) \subset k[\mathbf{X}, \mathbf{Y}, \mathbf{Z}]$$

with respect to the Bayer and Stillman order that eliminates the block of variables \mathbf{X} , then \mathbf{Y} . The elements of $\mathcal{G}' = k[\mathbf{Y}, \mathbf{Z}] \cap \mathcal{G}(\mathcal{I})$ form a Gröbner basis of the elimination ideal $\mathcal{I} \cap k[\mathbf{Y}, \mathbf{Z}]$, which is \mathfrak{J} . Moreover, \mathcal{G}' will be formed of the trivial algebraic relations $S_{i,j}$ and S_0 .

Second method. As the field extension $k(\mathbf{X})^H : k(\mathbf{\Pi})$ is separable, it is well known that the $k(\mathbf{\Pi})$ -bilinear form

$$(f, g) \longmapsto \text{Tr}(fg) \quad (3)$$

induced by the trace operator Tr is not degenerate. So, for each (i, j) , the equations

$$\text{Tr}(\Sigma_i \Sigma_j \Sigma_k) = \sum_{l=1}^r A_l^{i,j}(\mathbf{\Pi}) \text{Tr}(\Sigma_l \Sigma_k), \quad 1 \leq k \leq r \quad (4)$$

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.

Remains the problem of the computation of the trace. In the particular case when $k[\mathbf{\Pi}]$ is itself an invariant algebra $k[\mathbf{X}]^L$, where $H \subset L \subset \mathbf{GL}_n(k)$, the trace operator is defined by $\text{Tr}(f) = f^{\tau_1} + \dots + f^{\tau_r}$, where (τ_1, \dots, τ_r) is a right cosets representative system of $L//H$ (of course, $[L : H] = r$).

In the more particular case when $L = \mathfrak{S}_n$ and $\mathbf{\Pi} = \mathbf{E}$, 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.

3 Geometric consequences

The geometric properties considered in this section and the following need to assume that the ground field k is **algebraically closed**.

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 $\mathcal{V} = \mathbf{V}(\mathcal{J}) \subset \mathbb{A}^{n+r}$, which is irreducible ($k[\mathbf{X}]^H$ is a domain, so \mathcal{J} is prime).

Call respectively \mathbf{x} , $\mathbf{\Pi}(\mathbf{x})$ and $\mathbf{\Sigma}(\mathbf{x})$ the points (x_1, \dots, x_n) , $(\Pi_1(\mathbf{x}), \dots, \Pi_n(\mathbf{x}))$, $(\Sigma_1(\mathbf{x}), \dots, \Sigma_r(\mathbf{x}))$.

Let

$$\varphi : \begin{cases} \mathbb{A}_k^n & \longrightarrow \mathcal{V} \\ \mathbf{x} & \longmapsto \varphi(\mathbf{x}) = (\mathbf{\Pi}(\mathbf{x}), \mathbf{\Sigma}(\mathbf{x})) \end{cases}$$

We have two notions of quotient. First, the *categorical quotient* $\mathbb{A}_k^n // H$, defined as the affine variety corresponding to the ring $k[\mathbf{X}]^H$. The projection φ realizes the embedding \mathcal{V} in \mathbb{A}_k^{n+r} of this categorical quotient.

Second, the classical set quotient \mathbb{A}_k^n / H , defined as the set of orbits under H , associated to the orbit projection

$$\begin{cases} \mathbb{A}_k^n & \longrightarrow \mathbb{A}_k^n / H \\ \mathbf{x} & \longmapsto H \cdot \mathbf{x} \end{cases} .$$

The application φ is onto (see Remark 11 below, or [CLO98i, Theorem 10 p. 339]). Here is a simple proof of this fact from [DeKe02, Lemma 2.3.2]. Let (π, σ) be a point in \mathcal{V} . The preimage of this point by φ is the zero set of the ideal

of $k[\mathbf{X}]$ generated by the polynomials $\Pi_i - \pi_i$ and $\Sigma_j - \sigma_j$. If this set was empty, by Hilbert's Nullstellensatz, we could write $1 = \sum_{i=1}^n (\Pi_i - \pi_i) f_i + \sum_{i=1}^r (\Sigma_i - \sigma_i) f_{n+i}$, where the f_i 's belong to $k[\mathbf{X}]$. Applying Reynold's projection to this identity, we get a similar identity with the f_i 's in $k[X]^H$, *i.e.* the function ring of \mathcal{V} . It allows to apply this identity to the point $(\pi, \sigma) \in \mathcal{V}$ and provides $1 = 0$.

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 [CLO98i, Theorem 10 p. 339]). We get also a direct proof (see [Co97t]) of this fact by considering the polynomial $P = \prod_{A \in H} (A.(U_1 X_1 + \dots + U_n X_n) - (U_1 x'_1 + \dots + U_n x'_n))$, where U_1, \dots, U_n are indeterminates, \mathbf{x} and \mathbf{x}' two points in the same fiber. Indeed, as P belongs to $k[\mathbf{X}]^H[\mathbf{U}]$, $P(\mathbf{x}, \mathbf{U})$ equals $P(\mathbf{x}', \mathbf{U})$, which is zero, therefore one factor of $P(\mathbf{x}, \mathbf{U})$ is 0, which means that there exists $A \in H$ such that $\mathbf{x}' = A.\mathbf{x}$.

Thus the categorical quotient \mathcal{V} is the image of φ , and coincides with the quotient set \mathbb{A}_k^n/H . We say that the categorical quotient is a *geometric quotient*: the quotient map of the projection φ by the orbit projection realizes a bijection from \mathbb{A}_k^n/H onto \mathcal{V} , the embedding of the affine variety $\mathbb{A}_k^n//H$.

The projection

$$p : \begin{cases} \mathcal{V} & \longrightarrow \mathbb{A}_k^n \\ (\boldsymbol{\pi}, \boldsymbol{\sigma}) & \longmapsto \boldsymbol{\pi} \end{cases}$$

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

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

$$\varpi : \begin{cases} \mathbb{A}_k^n & \longrightarrow \mathbb{A}_k^n \\ \mathbf{x} & \longmapsto \varpi(\mathbf{x}) = \boldsymbol{\Pi}(\mathbf{x}) \end{cases} .$$

What we did up to now is summarized in the two following commutative diagrams, where ψ is the canonical injection.

$$\begin{array}{ccccc} \mathbb{A}_k^n \times \mathbb{A}_k^r & \xleftarrow{\psi} & \mathcal{V} & \xleftarrow{\varphi} & \mathbb{A}_k^n \\ & \searrow pr_1 & \downarrow p & \swarrow \varpi & \\ & & \mathbb{A}_k^n & & \end{array} \quad (D_1)$$

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

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathfrak{J} & \longrightarrow & k[\mathbf{Y}, \mathbf{Z}] & \longrightarrow & k[\mathbf{Y}, \mathbf{Z}]/\mathfrak{J} \longrightarrow k[\mathbf{X}] \\
& & & & \parallel & & \parallel \\
& & & & \mathcal{O}_{\mathbb{A}_k^{n+r}} & \xrightarrow{\psi^* = \Psi} & \mathcal{O}_{\mathcal{V}} & \xrightarrow{\varphi^*} & \mathcal{O}_{\mathbb{A}_k^n} \\
& & & & & & \uparrow p^* & & \uparrow \varpi^* \\
& & & & & & k[\mathbf{Y}] & &
\end{array} \quad (D_2)$$

Eventually 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.

4 Discriminants

In diagram (D_1) , we deal only with irreducible varieties and finite (hence proper) morphisms between them. In this setting, let $f : W_1 \rightarrow W_2$ be such a morphism. A singular point of the source or the target is characterized by the dimension of the Zariski tangent space being strictly greater than the dimension. A critical point of f is either a singular point of W_1 or a regular point \mathbf{x} at which $d_{\mathbf{x}}f : T_{\mathbf{x}}W_1 \rightarrow T_{\mathbf{x}}W_2$ is not surjective.

We call $\mathcal{C}(f)$ the algebraic subset of critical points in W_1 (critical locus of f) and $\mathcal{D}(f)$ the image of $\mathcal{C}(f)$ by f (algebraic subset of W_2 since f is proper).

4.1 Singular locus of the quotient variety

We note $\text{Sing } \mathcal{V}$ the subset of singular points of \mathcal{V} .

The algebra of functions of \mathcal{V} , *i.e.* $k[\mathbf{X}]^H$, is integrally closed: indeed, the integrally closed ring $k[\mathbf{X}]$ is integer over $k[\mathbf{X}]^H$ because any $P \in k[\mathbf{X}]$ is cancelled by the monic polynomial $\prod_{\tau \in H} (T - P^\tau)$ whose coefficients belong to $k[\mathbf{X}]^H$.

Consequently, $\text{Sing } \mathcal{V}$ is a Zariski-closed subset of \mathcal{V} that has codimension at least 2. (see *e.g.* [Sh94, chap. II §5 Th. 3]). By definition, $\text{Sing } \mathcal{V}$ is also a subset of $\mathcal{C}(p)$.

Note that to describe it, we can apply the jacobian criterion since \mathcal{V} is given by the prime ideal \mathfrak{J} .

4.2 Discriminant of the parametrization of the quotient variety

We note $\mathcal{C}'(\varphi)$ the subset of \mathbb{A}_k^n at whose points \mathbf{x} the linear map $d_{\mathbf{x}}\varphi : k^n \rightarrow T_{\varphi(\mathbf{x})}\mathcal{V}$ does not reach its maximal rank, n . As $\dim T_{\varphi(\mathbf{x})}\mathcal{V} \geq n$ for any point

$\mathbf{x} \in \mathbb{A}_k^n$, $\mathcal{C}'(\varphi)$ characterizes the default of immersion of φ (\mathbf{x} belongs to $\mathcal{C}'(\varphi)$ iff $d_{\mathbf{x}}(\psi \circ \varphi)$ 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.

Lemma 3 *Let P_1, \dots, P_s be polynomials of $k[\mathbf{X}]^H$, with $s \geq n$. If a point $\mathbf{a} = (a_1, \dots, a_n)$ is left invariant by an element A of H distinct of the identity, then the differential at \mathbf{a} of the map $\mathbf{x} \mapsto (P_1(\mathbf{x}), \dots, P_s(\mathbf{x}))$ is not injective.*

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

We thank L. Le Floch for this elementary proof of Lemma 3.

Proposition 4 *Let \mathbf{x} be a point in k^n . The following assertions are equivalent:*

- i. There exists an element of H , different from the identity, fixing \mathbf{x} ;*
- ii. $\mathbf{x} \in \mathcal{C}'(\varphi)$.*

Proof – (i) \Rightarrow (ii) results from Lemma 3 applied to $s = n + r$ and $(P_1, \dots, P_s) = (\mathbf{\Pi}, \mathbf{\Sigma})$.

(ii) \Rightarrow (i) is well known for a quotient variety with a Hausdorff topology (see [GrHa81, ex. 5.10 p. 25]), and could be generalized to our frame thanks to the Lefschetz principle or thanks to the étale topology. However, we give an elementary proof due to Romain Lebreton.

Let $h \neq 0$ be a vector of k^n such that $d_{\mathbf{x}}\varphi(h) = 0$. In the dual space $(\mathbb{A}_k^n)^*$, the set of linear forms that cancel on h is an hyperplane K , and for each $A \in H \setminus \{\text{Id}\}$, the set of linear forms that cancel on $A.\mathbf{x} - \mathbf{x}$ is an hyperplane K_A . As k is an infinite field, $(\mathbb{A}_k^n)^* \setminus \left(K \cup \bigcup_{A \in H \setminus \{\text{Id}\}} K_A \right)$ is non-empty. Choose v^* in this set, and $v \in \mathbb{A}_k^n$ such that $v^*(v) \neq 0$. Without loss of generality, we can suppose that v is collinear to the first vector of the canonical basis of k^n . So, $h_1 \neq 0$ and $x_1 - (A.\mathbf{x})_1 \neq 0$ for any $A \in H \setminus \{\text{Id}\}$.

The hypothesis $d_{\mathbf{x}}\varphi(h) = 0$ implies that for all $P \in k[\mathbf{X}]^H$, $d_{\mathbf{x}}P(h) = 0$. Indeed, $\{P \in k[\mathbf{X}], d_{\mathbf{x}}P(h) = 0\}$ is a ring and contains the components of $d_{\mathbf{x}}\varphi$, i.e. generators of $k[\mathbf{X}]^H$.

Suppose that \mathbf{x} is fixed by no element of H . In order to exhibit a contradiction, we produce a polynomial $P \in k[\mathbf{X}]^H$ such that $d_{\mathbf{x}}P(h) \neq 0$. We note $\bar{P} := \frac{1}{|H|} \sum_{A \in H} P(A.\mathbf{X})$ the Reynolds projection of $P \in K[\mathbf{X}]$. Then, $d_{\mathbf{x}}\bar{P} = \frac{1}{|H|} \sum_{A \in H} d_{A.\mathbf{x}}P \circ A$. It is sufficient to exhibit a polynomial $P \in k[\mathbf{X}]$ such that $d_{A.\mathbf{x}}P = 0$ for $A \neq \text{Id}$ and $d_{\mathbf{x}}P(h) \neq 0$. Indeed, then $d_{\mathbf{x}}\bar{P}(h) = \frac{1}{|H|} d_{\mathbf{x}}P(h) \neq 0$. Let $P := \prod_{A \neq \text{Id}} (X_1 - (A.\mathbf{x})_1)^2$. Then $d_{A.\mathbf{x}}P = 0$ for $A \neq \text{Id}$. If $d_{\mathbf{x}}P(h) \neq 0$ then we have found our polynomial. Otherwise $P' := P(\mathbf{X}).(X_1 - x_1 + h_1)^2$ suits our requirement: $d_{\mathbf{x}}P'(h) = h_1^2 d_{\mathbf{x}}P(h) + 2P(\mathbf{x})h_1^2 = 2P(\mathbf{x})h_1^2 \neq 0$. \square

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 §4.5. (More generally, from Chevalley's theorem, reflection groups yield a family of counterexamples).

Corollary 5 $\mathcal{C}(\varphi) = \varphi^{-1}(\text{Sing } \mathcal{V}) \cup \mathcal{C}'(\varphi)$, $\mathcal{D}(\varphi) = \text{Sing } \mathcal{V} \cup \{v \in \mathcal{V}, \#\varphi^{-1}(v) < |H|\}$, and $\mathcal{C}(\varphi) = \varphi^{-1}(\mathcal{D}(\varphi))$.

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

Computational point of view.

From Prop. 4, $\mathcal{C}'(\varphi)$ is a finite union of vector subspaces: the union when A runs through $H \setminus \{\text{Id}\}$ of the eigenspaces of A associated to the eigenvalue 1. Consider the (prime) ideal \mathfrak{i}_A generated by the components of $(A - \text{Id}) \cdot \mathbf{X}$, for $A \in H \setminus \{\text{Id}\}$, and the ideals

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

Then,

$$\mathcal{C}'(\varphi) = \mathbf{V}(\mathfrak{i}) \quad \text{and} \quad \mathbf{V}(\mathfrak{h}) = \varpi(\mathcal{C}'(\varphi)) = p(\mathcal{D}'(\varphi)) \quad (5)$$

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

Note that the assertion $\varpi(\mathbf{x}) \in \mathbf{V}(\mathfrak{h})$ is not equivalent to $\mathbf{x} \in \mathcal{C}'(\varphi)$. See for instance the example of §7.2, where $\mathcal{C}'(\varphi) = \mathbf{V}(X_1 - X_2)$ and $\varpi^{-1}(\varpi(\mathcal{C}'(\varphi))) = \mathbf{V}((X_1 - X_2)(X_2 - X_3)(X_3 - X_1))$.

4.3 Discriminant of the Noether projection

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

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

Its set of zeroes is the projection onto k^r of $p^{-1}(\boldsymbol{\pi})$, or $\mathcal{V} \cap (\{\boldsymbol{\pi}\} \times k^r)$. We will characterize the points $\boldsymbol{\pi}$ such that $\mathfrak{J}_{\boldsymbol{\pi}}$ is not radical.

Proposition 6 For any $\boldsymbol{\pi} \in k^n$, the following assertions are equivalent:

- i. The ideal $\mathfrak{J}_{\boldsymbol{\pi}}$ of $k[\mathbf{Z}]$ is radical;
- ii. $\boldsymbol{\pi} \notin \mathcal{D}(p)$.

Proof – From the jacobian criterion, the zero dimensional ideal \mathfrak{J}_π is radical if and only if for every $\sigma \in \mathbf{V}(\mathfrak{J}_\pi)$, the jacobian matrix $J_{\pi,\sigma} = \left(\frac{\partial G_\alpha}{\partial Z_\beta}(\pi, \sigma) \right)_{1 \leq \alpha \leq s, 1 \leq \beta \leq r}$ has rank r , where G_1, \dots, 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 (π, σ) of \mathcal{V} is a regular point of $p = pr_1 \circ \psi$ if $d_{\pi,\sigma} p = pr_1 \circ d_{\pi,\sigma} \psi$ has rank n , which means that the tangent space $T_{\pi,\sigma} \mathcal{V}$ is in direct sum with the kernel of pr_1 (indeed, $d_{\pi,\sigma} \psi$ is the canonical injection from $T_{\pi,\sigma} \mathcal{V}$ into k^{n+r}). As $T_{\pi,\sigma} \mathcal{V}$ is defined by the equations

$$\sum_{i=1}^n \frac{\partial G_j}{\partial Y_i}(\pi, \sigma) y_i + \sum_{i=1}^r \frac{\partial G_j}{\partial Z_i}(\pi, \sigma) z_i = 0 \quad (1 \leq j \leq s), \quad (6)$$

the condition is that the equations $\sum_{i=1}^r \frac{\partial G_j}{\partial Z_i}(\pi, \sigma) z_i = 0$ ($1 \leq j \leq s$) have only the zero solution, which means that $J_{\pi,\sigma}$ has rank r . Last, if (π, σ) is a singular point of \mathcal{V} , the rank of $J_{\pi,\sigma}$ is still less than r (indeed, as $\dim T_{\pi,\sigma} \mathcal{V} > n$, the rank of the $s \times (n+r)$ system (6) is at most $r-1$ and $J_{\pi,\sigma}$ is a submatrix of the matrix of this system), while (π, σ) is, by definition, a critical point of p .

It completes the proof, since (π, σ) runs through $p^{-1}(\pi)$ when σ runs through $\mathbf{V}(\mathfrak{J}_\pi)$. \square

Computational point of view.

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

The discriminant of $\chi_{\Theta_\Lambda}(T)$ with respect to T is a polynomial $\Delta(\Lambda, \mathbf{\Pi}) = \mathcal{R}es_T \left(\chi_{\Theta_\Lambda}, \frac{\partial(\chi_{\Theta_\Lambda})}{\partial T} \right) \in k[\Lambda, \mathbf{\Pi}]$, where Δ belongs to $k[\Lambda, \mathbf{Y}]$. Let \mathfrak{d} be the ideal of $k[\mathbf{Y}]$ generated by the coefficients of Δ seen as a polynomial in Λ over $k[\mathbf{Y}]$.

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

Proposition 7 *For any $\pi \in k^n$, the following assertions are equivalent.*

- i. *The ideal \mathfrak{J}_π of $k[\mathbf{Z}]$ is radical;*
- ii. *$\pi \notin \mathcal{D}(p)$;*
- iii. *There exists $\lambda \in k^r$ such that $\chi_{\Theta_\lambda, \pi}$ is squarefree;*
- iv. *There exists $\lambda = (\lambda_1, \dots, \lambda_r) \in k^r$ such that $\Delta(\lambda, \pi) \neq 0$;*
- v. *$\pi \notin \mathbf{V}(\mathfrak{d})$.*

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. Now, we can write

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

where $\mu_{\mathfrak{J}_{\boldsymbol{\pi}}}(\boldsymbol{\sigma})$ is the multiplicity of the zero $\boldsymbol{\sigma}$. Note that

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

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

Conversely, if $\mathfrak{J}_{\boldsymbol{\pi}}$ is radical, then $\#\mathbf{V}(\mathfrak{J}_{\boldsymbol{\pi}}) = r$; so, as k is an infinite field, there exists $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r) \in k^r$ such that $\lambda_1 \sigma_1 + \cdots + \lambda_r \sigma_r$ take $r = \dim_k k[\mathbf{Z}]/\mathfrak{J}_{\boldsymbol{\pi}}$ distinct values when $\boldsymbol{\sigma}$ runs through $\mathbf{V}(\mathfrak{J}_{\boldsymbol{\pi}})$. 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 $\mathbf{V}(\mathfrak{J}_{\boldsymbol{\pi}})$. Then, $\chi_{\Theta_{\boldsymbol{\lambda}, \boldsymbol{\pi}}}$ is squarefree. Therefore, (i) is equivalent to (iii). \square

4.4 Discriminant of the primary projection

For any $\boldsymbol{\pi} = (\pi_1, \dots, \pi_n) \in k^n$, we define the ideal $\mathfrak{a}_{\boldsymbol{\pi}} = (\Pi_i - \pi_i, 1 \leq i \leq n)$ of the ring $k[\mathbf{X}]$. Its set of zeroes is $\varpi^{-1}(\boldsymbol{\pi})$.

Let J be the jacobian determinant of (Π_1, \dots, Π_n) :

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

Proposition 8 *For any $\boldsymbol{\pi} \in k^n$, the two following assertions are equivalent:*

- i. the ideal $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical;
- ii. $\boldsymbol{\pi} \notin \mathcal{D}(\varpi)$.

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 $\boldsymbol{\pi} \notin \mathcal{D}(\varpi)$. \square

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

Proposition 9 *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*

$$\mathbf{V}(\delta) = \mathcal{D}(\varpi) \tag{7}$$

Proof – The map ϖ is a finite map from k^n to k^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 $(\mathfrak{a}_Y + (J)) \cap k[\mathbf{Y}]$ is of the same dimension $n - 1$. A fiber described by the ideal \mathfrak{a}_π is then smooth iff $\delta(\pi) \neq 0$. \square

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

4.5 Link between the 3 discriminants

The following lemma is a specialized version of the exact sequence (2).

Lemma 10 *For every $\pi \in \mathbb{A}_k^n$,*

$$0 \longrightarrow \mathfrak{J}_\pi \longrightarrow k[\mathbf{Z}] \xrightarrow{\Upsilon} k[\mathbf{X}]^H/\mathfrak{a}_\pi \longrightarrow 0 \quad (8)$$

is an exact sequence, where Υ is defined by $\Upsilon(P) = P(\Sigma_1, \dots, \Sigma_r) + \mathfrak{a}_\pi$.

Proof – Trivially, $\mathfrak{J}_\pi \subset \text{Ker } \Upsilon$. Conversely, let $P \in \text{Ker } \Upsilon$, and R its normal form modulo \mathfrak{J}_π with respect to any graded monomial order on $k[\mathbf{Z}]$. Then, R can be written $a_1 + a_2 Z_2 + \dots + a_r Z_r$, where the a_i belong to k . As $Q = P - R$ belongs to \mathfrak{J}_π , $Q(\Sigma)$ belongs to \mathfrak{a}_π ; so $R(\Sigma) = P(\Sigma) - Q(\Sigma)$ belongs to \mathfrak{a}_π : there exist $A_1, \dots, A_r \in k[\mathbf{X}]^H$ such that $R(\Sigma) = \sum_{i=1}^r (\Pi_i - \pi_i) A_i$. And each A_i can be written $A_i = \sum_{j=1}^r A_{i,j} \Sigma_j$, with $A_{i,j} \in k[\mathbf{\Pi}]$. Then, $R(\Sigma) = \sum_{j=1}^r (\sum_{i=1}^r (\Pi_i - \pi_i) A_{i,j}) \Sigma_j$. By uniqueness of the Hironaka decomposition, it implies $a_i = \sum_{i=1}^r A_{i,j} (\Pi_i - \pi_i)$ for each i , so $a_i \in \mathfrak{a}_\pi$. As $\mathfrak{a}_\pi \neq k[\mathbf{X}]^H$, it implies $a_i = 0$ for each i , i.e. $R = 0$ and $P \in \mathfrak{J}_\pi$. \square

Remark 11 *A consequence of Lemma 10 is that φ is onto \mathcal{V} , and more accurately, that $\mathbf{V}(\mathfrak{J}_\pi) = \kappa(\mathbf{V}(\mathfrak{a}_\pi))$ for any $\pi \in \mathbb{A}_k^n$, where the map κ from $\mathbf{V}(\mathfrak{a}_\pi)$ to $\mathbf{V}(\mathfrak{J}_\pi)$ is defined by $\kappa(\mathbf{x}) = \text{pr}_2(\varphi(\mathbf{x})) = (\Sigma_1(\mathbf{x}), \dots, \Sigma_r(\mathbf{x}))$.*

Proof – The adjoint algebra morphism κ^* is the map from $k[\mathbf{Z}]/\mathfrak{J}_\pi$ to $k[\mathbf{X}]/\mathfrak{a}_\pi$ defined by factorizing Υ . From (8), it is injective. Therefore, κ is dominant. As $\mathbf{V}(\mathfrak{J}_\pi)$ is a finite set, it implies that κ is onto: $\mathbf{V}(\mathfrak{J}_\pi) = \kappa(\mathbf{V}(\mathfrak{a}_\pi))$. Then, φ is onto because \mathcal{V} is the union of the fibers $p^{-1}(\pi) = \{\pi\} \times \mathbf{V}(\mathfrak{J}_\pi)$. \square

Proposition 12 *The set $\varphi^{-1}(\text{Sing } \mathcal{V})$ 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 $\text{Sing } \mathcal{V}$, depend also on the secondary ones.

Proof – Consider $\mathbf{x} \in \mathbb{A}_k^n \setminus \mathcal{C}(\varpi)$ and $(\pi, \sigma) = \varphi(\mathbf{x})$. From Lemma 10, $k[\mathbf{Z}]/\mathfrak{J}_\pi \simeq k[\mathbf{X}]^H/\mathfrak{a}_\pi$. As \mathfrak{a}_π is radical from Prop. 8, $k[\mathbf{X}]/\mathfrak{a}_\pi$ is reduced, therefore its subalgebra $k[\mathbf{X}]^H/\mathfrak{a}_\pi$ is reduced, $k[\mathbf{Z}]/\mathfrak{J}_\pi$ is reduced, \mathfrak{J}_π is radical, hence from the proof of Prop. 6, $(\pi, \sigma) \notin \text{Sing } \mathcal{V}$. \square

Theorem 13 *Let \mathbf{x} be a point in \mathbb{A}_k^n . Then*

$$\mathbf{x} \in \mathcal{C}(\varpi) \iff (\mathbf{x} \in \mathcal{C}'(\varphi) \text{ or } \varphi(\mathbf{x}) \in \mathcal{C}(p)) \quad (9)$$

$$\iff (\mathbf{x} \in \mathcal{C}(\varphi) \text{ or } \varphi(\mathbf{x}) \in \mathcal{C}(p)). \quad (10)$$

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

Secondly if $\varphi(\mathbf{x}) \in \text{Sing } \mathcal{V}$, then $\varphi(\mathbf{x}) \in \mathcal{C}(p)$ by definition, and $\mathbf{x} \in \mathcal{C}(\varpi)$ from Prop. 12. \square

Corollary 14

$$\mathcal{D}(\varpi) = \mathcal{D}(p) \cup p(\mathcal{D}'(\varphi)) \quad (11)$$

$$= \mathcal{D}(p) \cup p(\mathcal{D}(\varphi)). \quad (12)$$

Remark 15 *Theorem 13 can also be proved directly as a consequence of Prop. 4, 6, 8 and the self contained following lemma, whose direct proof stresses the crushing of the orbits.*

Lemma 16 *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 $\mathfrak{J}_{\boldsymbol{\pi}}$ of $k[\mathbf{Z}]$ is radical;

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

are linked as follows: (i) \iff ((ii) and (iii)).

Proof –

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

From Rem. 11, $\mathbf{V}(\mathfrak{J}_{\boldsymbol{\pi}}) = \kappa(\mathbf{V}(\mathfrak{a}_{\boldsymbol{\pi}}))$. 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 $\#\mathbf{V}(\mathfrak{J}_{\boldsymbol{\pi}}) < r$.

Now, $\dim_k k[\mathbf{Z}]/\mathfrak{J}_{\boldsymbol{\pi}} = r$, because the polynomials $S_0 = Z_1 - 1$ and $S_{i,j}(\boldsymbol{\pi}) = Z_i Z_j - \sum_{l=1}^r A_l^{i,j}(\boldsymbol{\pi}) Z_l$ make up a Gröbner basis of $\mathfrak{J}_{\boldsymbol{\pi}}$ (it follows from Prop. 2 because the leading monomials Z_1 of S_0 and $Z_i Z_j$ of $S_{i,j}$ do not cancel when we specialize $\boldsymbol{\Pi}$ in $\boldsymbol{\pi}$).

Therefore, $\#\mathbf{V}(\mathfrak{J}_{\boldsymbol{\pi}}) < \dim k[\mathbf{Z}]/\mathfrak{J}_{\boldsymbol{\pi}}$ and $\mathfrak{J}_{\boldsymbol{\pi}}$ is not radical in $k[\mathbf{Z}]$.

- (i) \implies (ii). From Lemma 10, $k[\mathbf{Z}]/\mathfrak{J}_{\boldsymbol{\pi}} \simeq k[\mathbf{X}]^H/\mathfrak{a}_{\boldsymbol{\pi}}$. 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 $k[\mathbf{Z}]/\mathfrak{J}_{\boldsymbol{\pi}}$ is reduced and $\mathfrak{J}_{\boldsymbol{\pi}}$ is radical.
- not (iii) \implies not (i). Suppose $A.\mathbf{x} = \mathbf{x}$ with $A \neq \text{Id}$. From Lemma 3, $d_{\mathbf{x}}\varpi$ is not injective, hence not surjective as it goes from k^n to itself. We conclude with Prop.8.

\square

Computational point of view.

The set equality (11) can be translated in terms of ideals through (5), Prop. 7, Prop. 9 and Hilbert's Nullstellensatz. Since (δ) and \mathfrak{h} are radical ideals, we get:

Corollary 17

$$\mathbf{V}(\delta) = \mathbf{V}(\mathfrak{d}) \cup \mathbf{V}(\mathfrak{h}) \quad (13)$$

$$(\delta) = \sqrt{\mathfrak{d}} \cap \mathfrak{h}. \quad (14)$$

Besides, this last equality is equivalent to (11), 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 $\mathfrak{a}_{\mathbf{Y}} = (X_1^2 - Y_1)$, so $\mathfrak{a}_{\boldsymbol{\pi}}$ is radical if and only if $\pi_1 \neq 0$, but $\mathcal{J}_{\boldsymbol{\pi}} = \{0\}$ is always radical. So, $\text{Sing } \mathcal{V} = \emptyset$, $\mathcal{D}(\varpi) = \{0\} = \mathcal{D}(\varphi)$, and $\mathcal{D}(p) = \emptyset$.

2. $n = 4$, $H = \left\langle \left(\begin{array}{cc} -1 & 0 \\ 0 & A \end{array} \right) \right\rangle$ 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 $\delta_1(Y_2, Y_3, Y_4) = \text{discrim}_T(T^3 - Y_2T^2 + Y_3T - Y_4)$. 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 $\mathcal{J}_{\boldsymbol{\pi}} = (Z_2^2 - \delta_1(\pi_2, \pi_3, \pi_4))$ is radical if and only if $\delta_1(\pi_2, \pi_3, \pi_4) \neq 0$, so $\sqrt{\mathfrak{d}} = (\delta_1)$; and $\mathcal{C}(\varphi) = \{\mathbf{x} \in k^4, x_1 = 0 \text{ or } x_2 = x_3 = x_4\}$, so $\mathfrak{h} = (Y_1\delta_1)$.

3. $n = 3$, $H = \left\langle \left(\begin{array}{ccc} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{array} \right), -I_3 \right\rangle$, $\Pi_i = X_i^2$, $r = 2$, $\Sigma_1 = 1$,

$\Sigma_2 = X_1X_2$. Then $\mathcal{J} = (\Sigma_1 - 1, \Sigma_2^2 - \Pi_1\Pi_2)$, $\text{Sing } \mathcal{V} = \mathbf{V}(Y_1, Y_2, Z_2)$ (of codimension 2 in \mathcal{V} , see §4.1), $\mathfrak{a}_{\mathbf{Y}} = (X_1^2 - Y_1, X_2^2 - Y_2, X_3^2 - Y_3)$, so $\delta = Y_1Y_2Y_3$; $\chi_{\Theta_{\Lambda}} = T^2 - 2\Lambda_1T + \Lambda_1^2 - \Lambda_2^2\Pi_1\Pi_2$, so $\Delta_{\Theta_{\Lambda}} = 4\Lambda_2^2\Pi_1\Pi_2$ and $\mathfrak{d} = (Y_1Y_2)$; and $\mathfrak{h} = (Y_1, Y_2).(Y_3)$.

We give more examples in Section 7.

5 Multiplication tensor and primitive elements

We consider an invariant $\Theta \in k[\mathbf{X}]^H$. We note $B_l(\boldsymbol{\Pi})$ its components in the $k[\boldsymbol{\Pi}]$ -module basis $(\Sigma_1, \dots, \Sigma_r)$:

$$\Theta = \sum_{l=1}^r B_l(\boldsymbol{\Pi})\Sigma_l, \text{ where } B_l \in k[\mathbf{Y}].$$

The matrix of the multiplication tensor by Σ_i of the $k[\boldsymbol{\Pi}]$ -module $k[\mathbf{X}]^H$ in the basis $\boldsymbol{\Sigma}$ is $M_{\Sigma_i} = (A_l^{i,j}(\boldsymbol{\Pi}))_{(l,j) \in \{1, \dots, r\}^2}$.

Then, the matrix of the multiplication by Θ is $M_\Theta = \sum_{i=1}^r B_i(\mathbf{\Pi})M_{\Sigma_i}$, so that

$$(M_\Theta)_{l,j} = \sum_{i=1}^r B_i(\mathbf{\Pi})A_i^{i,j}(\mathbf{\Pi}) \quad (l, j \in \{1, \dots, r\}). \quad (15)$$

Let $V^{(0)}$ be the one column matrix $V^{(0)} = (1, 0, \dots, 0)^t$. Then for every positive integer p , the components vector of Θ^p in the basis $(\Sigma_1, \dots, \Sigma_r)$ is $V^{(p)} = (M_\Theta)^p V^{(0)}$. Therefore, we have:

$$\Theta^p = \sum_{l=1}^r B_l^{(p)}(\mathbf{\Pi})\Sigma_l, \text{ where } (B_l^{(p)}(\mathbf{\Pi}))_{l \in \{1, \dots, r\}} = V^{(p)} = (M_\Theta)^p V^{(0)} \quad (16)$$

Primitivity The minimal polynomial $\mu_\Theta(T) \in k[\mathbf{\Pi}][T]$ (resp. the characteristic polynomial $\chi_\Theta(T) \in k[\mathbf{\Pi}][T]$) of Θ is by definition the minimal polynomial (resp. the characteristic polynomial) of the Θ multiplication endomorphism of the $k(\mathbf{\Pi})$ -vector space $k(\mathbf{X})^H$, or of the matrix M_Θ .

The definition of M_Θ can be written $(\Theta \cdot \text{Id} - M_\Theta) \cdot \Sigma = 0$. As $\Sigma \neq 0$, it proves that $0 = \det(\Theta \cdot \text{Id} - M_\Theta) = \chi_\Theta(\Theta)$ and that μ_Θ divides χ_Θ .

Of course, $\deg \chi_\Theta(T) = r$, and $\deg \mu_\Theta(T) = [k(\mathbf{\Pi})[\Theta] : k(\mathbf{\Pi})]$. Therefore, Θ is a primitive element of the field extension $k(\mathbf{X})^H : k(\mathbf{\Pi})$ if and only if one of the following equivalent conditions holds:

- $\deg_T \mu_\Theta = r$;
- $\chi_\Theta(T) = \mu_\Theta(T)$;
- $\chi_\Theta(T)$ is irreducible over $k(\mathbf{\Pi})[T]$;
- $\chi_\Theta(T)$ is irreducible over $k[\mathbf{\Pi}][T]$.

In the particular case when $k[\mathbf{\Pi}] = k[\mathbf{X}]^L$ for some finite subgroup L of $\mathbf{GL}_n(k)$, Galois' correspondance theorem proves that the condition is equivalent to

$$\text{Stab}_L(\Theta) := \{\tau \in L, \Theta^\tau = \Theta\} = H \quad (17)$$

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 $\text{Stab}_L(\Theta)$.

6 Fast computation of the characteristic polynomial

In all that follows, the real ω (with $2 \leq \omega < 3$) will be a number such that the asymptotic complexity of multiplying square matrices of size r is $O(r^\omega)$ (the best known today is $\omega < 2.377$).

We come back to the background and the notations of §5. Given an element

$\Theta = \sum_{l=1}^r B_l(\mathbf{\Pi})\Sigma_l$ of $k[\mathbf{X}]^H$, we want to compute its characteristic polynomial

χ_Θ (in §6.1), or a specialisation of χ_Θ (in §6.2).

We suppose the coefficients $A_i^{i,j}$ of the algebraic relations between secondary invariants are given (from a precomputation, see §2.3).

6.1 Generic characteristic polynomial

6.1.1 Le Verrier's method

We consider the trace function Tr as in (3). Thanks to (16), we can compute

$$\text{Tr}(\Theta^p) = \sum_{l=1}^r B_l^{(p)}(\mathbf{\Pi}) \text{Tr}(\Sigma_l) \quad (p \in \mathbb{N}). \quad (18)$$

This equation is between quantities in $k[\mathbf{\Pi}]$; the secondary invariants Σ_l no longer infer, provided we know (from a precomputation) their traces $\text{Tr}(\Sigma_l)$.

Proposition 18 $\chi_{\Theta}(T)$ is given by

$$\chi_{\Theta}(T) = T^r - \Xi_1 T^{r-1} + \dots + (-1)^r \Xi_r$$

where $\Xi_1, \dots, \Xi_r \in k[\mathbf{\Pi}]$ are defined recursively, from $\Xi_1 = \text{Tr}(\Theta)$, by:

$$k \Xi_k = \Xi_{k-1} \text{Tr}(\Theta) - \Xi_{k-2} \text{Tr}(\Theta^2) + \dots + (-1)^{k-1} \Xi_1 \text{Tr}(\Theta^{k-1}) \quad 2 \leq k \leq r. \quad (19)$$

Proof – Let Θ_i ($1 \leq i \leq r$, with $\Theta_1 = \Theta$) denote the roots of $\chi_{\Theta}(T)$ in its splitting field. The proposition arises from Newton's identities and the relations

$$\chi_{\Theta}(T) = \prod_{i=1}^r (T - \Theta_i) \quad \text{and} \quad \text{Tr}(\Theta^p) = \sum_{i=1}^r \Theta_i^p. \quad \square$$

This proposition yields an algorithm to compute $\chi_{\Theta}(T)$, known as *Le Verrier's method*. One computes $\text{Tr}(\Theta^p)$ ($1 \leq p \leq r$) thanks to (18) and then applies (19). The complexity is $O(r^\omega)$ additions or multiplications in $k[\mathbf{\Pi}]$ for each matrix product, so $O(r^{1+\omega})$ to compute the powers $(M_{\Theta})^p$ ($1 \leq p \leq r$) involved in (16). Then the computation of the elements $\text{Tr}(\Theta^p)$ thanks to (18) costs $O(r^2)$ and Newton's identities cost $O(r^2)$ additions and multiplications in $k[\mathbf{\Pi}]$ plus r divisions by scalars to compute the Ξ_k .

Therefore, the global complexity of Le Verrier's method is $O(r^{1+\omega})$ additions and multiplications over $k[\mathbf{\Pi}]$, and r divisions by scalars of k .

6.1.2 Kaltofen-Wiedemann's algorithm

>From §5, χ_{Θ} is the characteristic polynomial of the matrix M_{Θ} , whose coefficients are given by (15).

We can compute it by several algorithms, one of which will be useful in the following because it involves no division: Kaltofen-Wiedemann's algorithm (see [Ab04, §8.5]).

Lemma 19 *The determinant and the characteristic polynomial of a $r \times r$ matrix can be computed (by Kaltofen-Wiedemann's algorithm) in $O(r^{\frac{\omega}{2}+2} \log r \log \log r)$ scalar additions and multiplications.*

Proof – See [Ab04, p. 253] \square

6.1.3 Examples

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 does not depend only on H .

1. Trivial example: if $\Theta \in k[\mathbf{\Pi}]$, then $\chi_\Theta(T) = (T - \Theta)^r$ and $\mu_\Theta(T) = T - \Theta$.
2. $n = 2$, $H = \{\text{Id}, A, -\text{Id}, -A\} \subset \mathbf{GL}_2(k)$ where $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $r = 2$.

Choose $\Pi_1 = X_1^2 + X_2^2$, $\Pi_2 = (X_1 X_2)^2$, $\Sigma_2 = X_1 X_2 (X_1^2 - X_2^2)$. 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

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

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

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 $B_2 \neq 0$

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

6.2 Specialised characteristic polynomial

6.2.1 Principle

Given a family of scalars, $\boldsymbol{\pi} = (\pi_1, \dots, \pi_n) \in k^r$, we define the polynomial $\chi_{\Theta, \boldsymbol{\pi}}$ as the evaluation of χ_Θ , when we substitute π_i to each Π_i .

We can adapt the algorithm of §6.1 to compute $\chi_{\Theta, \boldsymbol{\pi}}$ very fast. 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 $k[\mathbf{X}]^H/\mathfrak{a}_\boldsymbol{\pi}$ instead of $k[\mathbf{X}]^H$, where $\mathfrak{a}_\boldsymbol{\pi}$ is the ideal $(\Pi_1 - \pi_1, \dots, \Pi_n - \pi_n)$. We note $\theta = \Theta + \mathfrak{a}_\boldsymbol{\pi}$ and $\sigma_l = \Sigma_l + \mathfrak{a}_\boldsymbol{\pi}$ (classes modulo $\mathfrak{a}_\boldsymbol{\pi}$).

Then, $(\sigma_1, \dots, \sigma_r)$ is a k -basis of $k[\mathbf{X}]^H/\mathfrak{a}_\boldsymbol{\pi}$. It allows to identify $k[\mathbf{X}]^H/\mathfrak{a}_\boldsymbol{\pi}$ to k^r . Besides, we have the following multiplication table between the basis elements (got by specializing the generic table (1)):

$$\sigma_i \sigma_j = A_1^{i,j}(\boldsymbol{\pi})\sigma_1 + \dots + A_r^{i,j}(\boldsymbol{\pi})\sigma_r. \quad (20)$$

And $\chi_{\Theta, \boldsymbol{\pi}}$ is the characteristic polynomial of θ in the k -algebra $k[\mathbf{X}]^H/\mathfrak{a}_\boldsymbol{\pi} \simeq k^r$. So, $\chi_{\Theta, \boldsymbol{\pi}} = \chi_\theta$ can be computed from the multiplication table (20) by the same methods (Le Verrier or Kaltofen-Wiedemann) described in section 6.1 to compute χ_Θ .

The complexity of the computation using KW is $O(r^{2+\frac{\omega}{2}} \log r \log \log r)$ additions and multiplications in k , from lemma 19.

We can sum-up this method in the following

Algorithm

PRECOMPUTATION : Compute the coefficients $A_k^{i,j} \in k[\mathbf{\Pi}]$ of the algebraic relations between secondary invariants.

This precomputation does not depend on the choice of Θ .

MULTIPLICATION TABLE : Given $\pi \in k^n$, compute $a_l^{i,j} = A_l^{i,j}(\pi)$; it yields the multiplication table between the basis elements of k^r : $\sigma_i \sigma_j = a_1^{i,j} \sigma_1 + \dots + a_r^{i,j} \sigma_r$.

COMPUTATION OF $\chi_{\Theta,\pi}$: Given a $\Theta \in k[\mathbf{X}]^H$, we specialize the decomposition of Θ in terms of Σ , getting $\theta = \lambda_1 \sigma_1 + \dots + \lambda_r \sigma_r$. The matrix M of the multiplication by θ in the k -basis $(\sigma_1, \dots, \sigma_r)$ is given by its coefficients $m_{i,j} = \lambda_1 a_j^{i,1} + \dots + \lambda_r a_j^{i,r}$. We compute the characteristic polynomial of M thanks to KW's algorithm. The result is $\chi_{\Theta,\pi}$.

Proposition 20 *The complexity to compute $\chi_{\Theta,\pi}$ by this algorithm is $\mathcal{A} + O(r^{2+\frac{\alpha}{2}} \log r \log \log r)$ additions and multiplications in k , where $r = \deg_T \chi_{\Theta,\pi}$ and \mathcal{A} is the evaluation length of the family $(A_k^{i,j})_{i,j,k \in \{1,\dots,r\}}$ formed by the coefficients of the relations between the secondary invariants.*

Implementation: The algorithm was implemented by the first author in Axiom (see [Ax92]). The same Axiom package can be used on any field of characteristic 0, either over k to get $\chi_{\Theta,\pi}$, either generically over $k[\mathbf{\Pi}]$ to get χ_{Θ} (we just need to ask Axiom to evaluate on $\mathbf{\Pi}$ instead of π).

Important remark: It is even quicker to compute $\chi_{\Theta,\pi}$ through the present algorithm than to evaluate in π (e.g. with Horner's algorithm) the precomputed generic polynomial χ_{Θ} .

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).

6.2.2 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: we compute the 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 2.3). The result is too large to be written here.

For instance, we choose $\Theta = \Sigma_2$ and $\pi = (0, 2, -2, 1, -2, 2)$.

COMPUTATION OF $\chi_{\Theta, \pi}$: we write the matrix of the multiplication by θ : it is the matrix $\left(A_l^{i,2}(\pi)\right)_{i,l}$. We get:

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

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 $\chi_{\Theta, \pi}$. Concerning the computation time, see §6.3.3

6.3 Lagrange resolvents

Lagrange's resolvents are used to solve the "direct problem of computational Galois theory": find the Galois group of a given polynomial $f \in k[T]$. Indeed, when the resolvents are squarefree, the degrees of their irreducible factors give information about the Galois group of f : this is known as the method of the absolute resolvent of Soicher and McKay (see [McSo85, ArVa93]).

6.3.1 Definition

Let H be a subgroup of the symmetric group \mathfrak{S}_n . We say that a polynomial Θ in $k[\mathbf{X}] = k[X_1, \dots, X_n]$ is a *primitive invariant* of H if the stabilizer of Θ in \mathfrak{S}_n is H .

As a particular case of (17), Galois' correspondance theorem proves that such a Θ is a primitive element of $k(\mathbf{X})^H$ over $k(\mathbf{X})^{\mathfrak{S}_n}$, i.e. $k(\mathbf{X})^H = k(\mathbf{X})^{\mathfrak{S}_n}[\Theta]$.

We call *generic Lagrange resolvent* by Θ , or *generic H -resolvent* by Θ , the polynomial $\mathcal{L}_\Theta = \chi_\Theta(T)$, characteristic polynomial of Θ over $k[\mathbf{X}]^{\mathfrak{S}_n}$. Then,

$$\mathcal{L}_\Theta = \prod_{\vartheta \in \Theta^{\mathfrak{S}_n}} (T - \vartheta) = \prod_{\tau \in \mathfrak{S}_n // H} (T - \Theta^\tau) \in k[\mathbf{X}]^{\mathfrak{S}_n}[T].$$

where $\Theta^{\mathfrak{S}_n}$ is the orbit of Θ under \mathfrak{S}_n and $\mathfrak{S}_n // H$ is a set of right coset representatives of H in \mathfrak{S}_n .

The coefficients of \mathcal{L}_Θ belong to $k[\mathbf{X}]^{\mathfrak{S}_n}$, hence can be expressed in terms of the elementary symmetric polynomials E_1, \dots, E_n .

Let $f = T^n + \sum_{i=1}^n (-1)^i e_i T^{n-i}$ be a polynomial of $k[T]$. We call *Lagrange resolvent of f by Θ* the polynomial $\mathcal{L}_{\Theta, f} = \chi_{\Theta, e}$. It is obtained from \mathcal{L}_Θ by specializing the family $\mathbf{E} = (E_1, \dots, E_n)$ in $\mathbf{e} = (e_1, \dots, e_n)$

If we note x_1, \dots, x_n the roots of f in an algebraic closure K of k , then $\mathcal{L}_{\Theta, f}$ is defined from $\mathcal{L}_\Theta \in k[\mathbf{X}][T]$ by specializing the family $\mathbf{X} = (X_1, \dots, X_n)$ in $\mathbf{x} = (x_1, \dots, x_n)$.

6.3.2 Classical computation

Classically, the Lagrange resolvents are computed by using the fact that their generic coefficients, as symmetric polynomials in X_1, \dots, X_n , can be expressed in terms of the elementary symmetric polynomials E_1, \dots, E_n , as follows.

We note $\Theta^{\mathfrak{S}_n} = \{\Theta_1, \dots, \Theta_r\}$ the orbit of Θ under the action of \mathfrak{S}_n , with $\Theta_1 = \Theta$. One computes the so-called *power sums* $S_i = \Theta_1^i + \dots + \Theta_r^i$, for $1 \leq i \leq r$, and expresses them in terms of the elementary symmetric polynomials E_1, \dots, E_n . Then, compute \tilde{S}_i , the specialization of S_i (we substitute e_j to E_j for each j). Then, applying Newton's identities to the specialized power sums $(\tilde{S}_1, \dots, \tilde{S}_r)$, we get the elementary symmetric polynomials in $\tilde{\Theta}_1, \dots, \tilde{\Theta}_r$, i.e. the coefficients (up to the sign) of $\mathcal{L}_{\Theta, f}$.

The problem with this method is its cost : it requires to compute symbolically Θ, \dots, Θ^r in $k[\mathbf{X}]$. Computing S_1, \dots, S_r has a null cost because the object S_i can be represented by Θ^i with the hypothesis that a monomial $M \in k[\mathbf{X}]$ represents the symmetric polynomial $\sum_{\tau \in \mathfrak{S}_n} M^\tau$. One needs then an algorithm to express each S_i (represented by Θ^i) in terms of E_1, \dots, E_n (to accelerate, we can specialize E_1, \dots, E_n in e_1, \dots, e_n at the same time). If r is big or if Θ has many monomials, then the development of Θ^r involves so many terms that this algorithm is too complex to run effectively.

Example 21 $n = 6$, $H = \langle (1, 3)(2, 4), (1, 3, 4)(2, 5, 6), (3, 4, 5, 6) \rangle \simeq \mathfrak{S}_5$; a primitive invariant of H is $\Theta = \sum_H X_1^2 X_2^2 X_3 X_4$ (example of §6.2.2). The polynomial Θ is the sum of 60 monomials. As $r = [\mathfrak{S}_n : H] = 6$, the classical computation of \mathcal{L}_Θ involves the computation of Θ^6 , which is already heavy.

6.3.3 Comparison with our algorithm

We compute Lagrange resolvents thanks to the algorithm of §6.2, since $\mathcal{L}_{\Theta, f} = \chi_{\Theta, \pi}$ if Π_1, \dots, Π_n are the elementary symmetric polynomials E_1, \dots, E_n and if $f = T^n - \pi_1 T^{n-1} + \dots + (-1)^n \pi_n$.

Consequently, once the precomputation of the relations between secondary invariants is done, $\mathcal{L}_{\Theta, f}$ can be computed symbolically, using only multiplications and additions in the field k , with a complexity $\mathcal{A} + O(r^{2+\frac{\omega}{2}} \log r \log \log r)$, where $r = [\mathfrak{S}_n : H] = \deg \mathcal{L}_{\Theta, f}$ and where \mathcal{A} is the evaluation length of the relations between secondary invariants.

Contrary to the classical computation, this algorithm avoids the heavy symbolic computation of Θ^r and the expression of its trace in terms of the elementary symmetric polynomials.

We will also show (see §6.4) how to find Θ such as to get a squarefree resolvent.

Computation time Compared to the classical symbolic computation of Lagrange resolvents, once the precomputations made, our algorithm is several orders of magnitude faster.

On the example of §6.2.2, our computation time was 0.72 s with AXIOM in 1998. The precomputation time of the generic multiplication table was 1h30min with Kemper's Magma package in 1996. The computation time of $\mathcal{L}_{\Theta, f}$ by N. Rennert and A. Valibouze with a first improvement of the classical method, implemented in Maxima and SYM, was 6h (see [ReVa99]): our algorithm is 30 000 times faster on this example. Even with a more sophisticated method

(derived from the classical method), the computation of N. Rennert and A. Valibouze still lasts 11 min, *i.e.* 910 times ours.

6.4 Separability in the case of Lagrange resolvents

In the frame of Soicher's method to compute the Galois group of a polynomial, Lagrange resolvents involved must be square-free (see [ArVa93, Théorème 6.6]). We will say that a primitive invariant Θ of H is *separating* for $\boldsymbol{\pi} = (\pi_1, \dots, \pi_n)$ (or for $f = T^n - \pi_1 T^{n-1} + \dots + (-1)^n \pi_n$) if the resolvent $\mathcal{L}_{\Theta, f}$ is square-free. In this section, we address the problem of finding such a separating invariant for a given polynomial f (which is a subcase of §4) and the complexity of this problem (which is new). We will look for such a Θ written as a linear combination of the secondary invariants: $\Theta_{\boldsymbol{\lambda}} = \lambda_1 \Sigma_1 + \dots + \lambda_r \Sigma_r$, where $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r) \in k^r$.

6.4.1 Existence problem

In this paragraph, we specify the results of §4 when H is a permutation group, subgroup of the symmetric group \mathfrak{S}_n , and the primary invariants Π_1, \dots, Π_n are the elementary symmetric polynomials E_1, \dots, E_n .

Proposition 22 *In this case, δ (defined in Prop 8) is (up to the multiplication by a constant) the discriminant of the generic polynomial of degree n , i.e.*

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

Consequently, δ is irreducible.

Proof – As both δ and the generic discriminant are squarefree, from Hilbert's Nullstellensatz it is enough to prove that, in an algebraic closure \hat{k} of k , both polynomials have the same zeros. From Prop. 8, a point $\boldsymbol{\pi} \in \hat{k}^n$ is a zero of δ if and only if the cardinality of the finite set $\mathbf{V}_{\hat{k}^n}((\Pi_1 - \pi_1, \dots, \Pi_n - \pi_n))$ is less than $\dim_k k[\mathbf{X}]/(\Pi_1 - \pi_1, \dots, \Pi_n - \pi_n) = n!$. Now, $\mathbf{V}_{\hat{k}^n}((\Pi_1 - \pi_1, \dots, \Pi_n - \pi_n)) = \{(x_{\tau(1)}, \dots, x_{\tau(n)}) \mid \tau \in \mathfrak{S}_n\}$, where (x_1, \dots, x_n) denotes the roots in \hat{k} of $f = T^n - \pi_1 T^{n-1} + \dots + (-1)^n \pi_n$, because the Π_i are the elementary symmetric polynomials. Consequently, $\boldsymbol{\pi}$ is a zero of δ if and only if two roots of f in \hat{k} are equal, *i.e.* if the generic discriminant cancels on $\boldsymbol{\pi}$. \square

REMARK: In the general case where H is a matrix group, δ is not generally irreducible, see the example following Cor. 17, or the example of §7.6.

Proposition 23 *If $H \neq \mathfrak{S}_n$, then*

$$\mathbf{V}(\delta) = \mathbf{V}(\mathfrak{d}) \supset \mathbf{V}(\mathfrak{h}). \quad (21)$$

Besides, the inclusion $\mathbf{V}(\mathfrak{h}) \subset \mathbf{V}(\mathfrak{d})$ is an equality if and only if H contains a transposition.

Proof – From (13), $\mathbf{V}(\delta) = \mathbf{V}(\mathfrak{d}) \cup \mathbf{V}(\mathfrak{h})$. As $\mathbf{V}(\delta)$ is irreducible, it is equal to $\mathbf{V}(\mathfrak{d})$ or to $\mathbf{V}(\mathfrak{h})$. If H contains no transposition, then the codimension of $\mathbf{V}(\mathfrak{h})$ in \mathbb{A}_k^n is at least two, whereas $\mathbf{V}(\delta)$ is of codimension 1, which proves the

results. 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 $f = T^n - \pi_1 T^{n-1} + \dots + (-1)^n \pi_n$ has a multiple root in \hat{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 $\{\tau_1, \dots, \tau_r\}$ 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 $k[\mathbf{X}]^{\tau_i^{-1} \cdot H \cdot \tau_i}$. Consider the transposition $(1, 2)$. If it belonged to all the groups $\tau_i^{-1} \cdot H \cdot \tau_i$ ($1 \leq i \leq r$), then we would get: $\tau^{-1} \cdot (1, 2) \cdot \tau \in H$ 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 $i \in \{1, \dots, r\}$ such that $(1, 2) \notin \tau_i^{-1} \cdot H \cdot \tau_i$. Therefore, $H \cdot \tau_i \cdot (1, 2) \neq H \cdot \tau_i$, so $H \cdot \tau_i \cdot (1, 2) = H \cdot \tau_j$ with $j \neq i$. It implies that $\Theta_i^{(1,2)} = \Theta_j$. Therefore, $\Theta_j(\mathbf{x}) = \Theta_i(\mathbf{x})$, 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. 7 that $\boldsymbol{\pi} \in \mathbf{V}(\mathfrak{d})$.

Corollary 24 *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. $\mathfrak{J}_{\boldsymbol{\pi}}$ is radical,
- iv. $\exists \boldsymbol{\lambda} \in k^r$, $\Delta(\boldsymbol{\lambda}, \boldsymbol{\pi}) \neq 0$,
- v. $\exists \boldsymbol{\lambda} \in k^r$, $\chi_{\Theta_{\boldsymbol{\lambda}}, \boldsymbol{\pi}}$ is squarefree.

Corollary 25 *If $H \neq \mathfrak{S}_n$ then $\delta(\mathbf{Y})$ divides $\Delta(\mathbf{Y}, \boldsymbol{\Lambda})$ in $k[\mathbf{Y}, \boldsymbol{\Lambda}]$, and $(\delta) = \sqrt{\mathfrak{d}}$.*

REMARK: The equivalence $(\mathfrak{a}_{\boldsymbol{\pi}} \text{ radical}) \iff (\mathfrak{J}_{\boldsymbol{\pi}} \text{ radical})$ is false if $H = \mathfrak{S}_n$. Indeed, in this case, $r = 1$, $k[\mathbf{Z}]/\mathfrak{J}_{\boldsymbol{\pi}} \simeq k[\mathbf{X}]^{\mathfrak{S}_n}/\mathfrak{a}_{\boldsymbol{\pi}} \simeq k$ is always a field, so $\mathfrak{J}_{\boldsymbol{\pi}}$ is radical (in fact it is 0), but $\delta(\boldsymbol{\pi})$ may cancel ...

REMARK: The ideal \mathfrak{h} satisfies $(\delta) \subset \mathfrak{h}$ from Cor. 17, but we can say no more. For instance, with $n = 4$, if H is the subgroup of \mathfrak{S}_4 generated by $(1, 2)(3, 4)$, then $\mathcal{C}'(\varphi) = \{(x_1, x_1, x_3, x_3), x_1, x_3 \in k\}$ and we get \mathfrak{h} by eliminating X_1, X_2, X_3, X_4 between $X_1 - X_2, X_3 - X_4$, and $Y_i - E_i(\mathbf{X})$ for $1 \leq i \leq 4$. We get: $\mathfrak{h} = (Y_1(4Y_2 - Y_1^2) - 8Y_3, (4Y_2 - Y_1^2)^2 - 64Y_4)$. It contains strictly (δ) .

6.4.2 Complexity problem

First, we need to specify Prop. 24 in order as to get a complexity bound.

Proposition 26 *We assume that f is squarefree (i.e. $\delta(\boldsymbol{\pi}) \neq 0$). Then, there exists a r -tuple $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r) \in k^r$ such that $\Delta(\boldsymbol{\lambda}, \boldsymbol{\pi}) \neq 0$ (or equivalently, such that $\Theta_{\boldsymbol{\lambda}}$ be a $\boldsymbol{\pi}$ -separating primitive invariant of H). More accurately, the set of good r -tuples $\boldsymbol{\lambda}$ is $k^r \setminus \mathcal{H}$ where \mathcal{H} is an algebraic hypersurface of k^r of degree $\deg(\mathcal{H}) = r(r-1)$.*

Proof – The following proof is inspired by those of [Co95, Propositions 8 and 9].

We note $\boldsymbol{\Lambda} = (\Lambda_1, \dots, \Lambda_r)$ new indeterminates, and $\Theta_{\boldsymbol{\Lambda}} = \sum_{i=1}^r \Lambda_i \Sigma_i \in k(\boldsymbol{\Lambda})[\mathbf{X}]^H$.

We consider $\chi_{\Theta_\Lambda, \pi} \in k(\Lambda)[T]$, the characteristic polynomial of Θ_Λ over $k(\Lambda)[\mathbf{\Pi}]$ specialized in π , and its discriminant

$$P = \mathcal{R}_{\mathcal{E}S_T} \left(\chi_{\Theta_\Lambda, \pi}, \frac{\partial(\chi_{\Theta_\Lambda, \pi})}{\partial T} \right) \in k[\Lambda].$$

Then

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

and

$$P = \prod_{\substack{\tau_1, \tau_2 \in (\mathfrak{S}_n // H) \\ \tau_1 \neq \tau_2}} \sum_{i=1}^r \Lambda_i (\Sigma_i^{\tau_1}(\mathbf{x}) - \Sigma_i^{\tau_2}(\mathbf{x})),$$

where $\mathbf{x} = (x_1, \dots, x_n)$ are the roots of f in an algebraic closure \hat{k} of k . Therefore, P is a $r(r-1)$ -homogeneous polynomial in Λ . So if $P \neq 0$, then it defines in k^r an algebraic hypersurface \mathcal{H} of degree $r(r-1)$. For each $\lambda \in k^r \setminus \mathcal{H}$, the discriminant $P(\lambda_1, \dots, \lambda_r)$ of $\chi_{\Theta_\lambda, \pi}$ is non zero. It implies two things : first that χ_{Θ_λ} itself is squarefree, so that Θ_λ is a primitive invariant of H ; and secondly that $\mathcal{L}_{\Theta_\lambda, f}$ (which is then well defined and equal to $\chi_{\Theta_\lambda, \pi}$) is squarefree.

There remains to prove that $P \in k[\Lambda]$ is non-zero. We could apply Prop. 24, based on Th. 16, but we prefer to give a self-contained proof.

It is enough to prove that there is an algebraic extension \hat{k} of k such that P is non-zero in $\hat{k} \otimes_k k[\Lambda]$, *i.e.* that there exists $\mu = (\mu_1, \dots, \mu_r) \in \hat{k}^r$ such that $P(\mu) \neq 0$.

Let us consider $\mathcal{Q} = \text{discrim}_T(\mathcal{L}_{\Theta_\Lambda}) \in k[\Lambda, \mathbf{\Pi}]$. We have

$$\mathcal{Q} = \prod_{\tau_1, \tau_2 \in (\mathfrak{S}_n // H), \tau_1 \neq \tau_2} \sum_{i=1}^r \Lambda_i (\Sigma_i^{\tau_1} - \Sigma_i^{\tau_2}),$$

and for each factor of \mathcal{Q} , as $\tau_1 \tau_2^{-1} \notin H$, there exists i such that $\Sigma_i^{\tau_1} \neq \Sigma_i^{\tau_2}$. Therefore, $\mathcal{Q} \neq 0$. As k is infinite, there exists $\lambda \in k^r$ such that $\mathcal{Q}(\lambda, \mathbf{\Pi}) \neq 0$. Therefore, Θ_λ is then a primitive invariant of H . Besides, as $\mathcal{Q}(\lambda, \mathbf{\Pi}) \neq 0$ and k is infinite, there exists $\mathbf{a} \in k^n$ such that $\mathcal{Q}(\lambda, \mathbf{a}) \neq 0$. Let $y = y_1, \dots, y_n$ denote the roots of $g = T^n - a_1 T^{n-1} + \dots + (-1)^n a_n$ in its splitting field. We note $K = k(x, y)$. As the x_i are distinct, there exists a univariate polynomial $h \in K[U]$ such that for each i , $h(x_i) = y_i$ (Lagrange interpolation). We note $\Theta \circ h = \Theta(h(X_1), \dots, h(X_n))$, where $\Theta = \Theta_\lambda$. Then, $\mathcal{L}_{\Theta, g} = \mathcal{L}_{\Theta \circ h, f}$. But $\mathcal{L}_{\Theta, g}$ is squarefree because $\mathcal{Q}(\lambda, \mathbf{a}) \neq 0$; so $\mathcal{L}_{\Theta \circ h, f}$ is squarefree too. Now, as $\Theta \circ h \in K[\mathbf{X}]^H$, it can be written $\Theta \circ h = \sum_{i=1}^r B(\mathbf{\Pi}) \Sigma_i$, with $B(\mathbf{\Pi}) \in K[\mathbf{\Pi}]$. We note $\mu_i = B_i(\pi)$. Then, $\mathcal{L}_{\Theta \circ h, f} = \mathcal{L}_{\Theta_\mu, f}$. As it is squarefree, we proved that $0 \neq \mathcal{Q}(\mu, \pi) = P(\mu)$, and therefore that $P \neq 0$. \square

Using the only property of \mathcal{H} that its degree is $\deg(\mathcal{H}) = r(r-1)$, we need at most $\binom{r+\deg \mathcal{H}}{r} = \binom{r^2}{r} \underset{+\infty}{\sim} \frac{1}{\sqrt{2\pi}} \frac{r^{2r(r-1)}}{e^{r(r-2)}} \asymp r^{(r^2)}$ tries to find a point λ in $k^r \setminus \mathcal{H}$ (it is the number of coefficients of the generic polynomial of degree $\deg(\mathcal{H})$): this is the geometric bound of the problem to find a point out of a variety. Indeed, there exists a subset A of k^r of cardinal $\binom{r+\deg \mathcal{H}}{r}$ such that no nonzero polynomial of

degree at most $\deg \mathcal{H}$ cancel on A . And this number is the minimal cardinal of such a subset A .

But in our case, \mathcal{H} is not any hypersurface of degree $r(r-1)$: it is defined by the polynomial $\Delta_{\Theta_\Lambda, \pi} = \mathcal{R}_{\text{es}_T}(\chi_{\Theta_\Lambda, \pi}, \partial(\chi_{\Theta_\Lambda, \pi})/\partial T)$, which is defined by a determinant, and consequently easier to evaluate than an arbitrary polynomial of the same degree.

Using the Heintz-Schnorr theorem, we shall prove 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 27 (Heintz-Schnorr) *Let k be an effective integral domain of characteristic 0. Consider the set $\mathcal{P}(d, p, v)$ of the polynomials in $k[X_1, \dots, X_p]$ 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 $6(v+p)(v+p+1)$ such that the only polynomial of $\mathcal{P}(d, p, v)$ that cancels on all the points of $\mathcal{S}(d, p, v, \Gamma)$ is zero.*

Proof – See [HeSc82]. \square

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 in Λ (number of scalar additions and multiplications needed to specialize Λ) of $\Delta_{\Theta_\Lambda, \pi} = \text{discrim}_T \chi_{\Theta_\Lambda, \pi} \in k[\Lambda]$. We write $v = v_1 + v_2 + v_3$, where

- v_1 is the evaluation length in Λ of $M_{\theta_\Lambda} = M_{\Theta_\Lambda, \pi} \in \mathcal{M}_r(k[\Lambda])$ (the matrix of the multiplication by Θ_Λ specialized in π). As $M_{\Theta_\Lambda, \pi} = \sum_{i=1}^r \lambda_i M_{\Sigma_i, \pi}$, each coefficient of the matrix $M_{\Theta_\Lambda, \pi}$ is a linear combination of the λ_i and requires $r-1$ additions and r multiplications, so $v_1 = r^2(2r-1)$.
- v_2 is the number of arithmetic operations to compute the characteristic polynomial of M_{θ_Λ} ; so, $v_2 = O(r^{\frac{\omega}{2}+2} \log r \log \log r)$ from Lemma 19.
- v_3 is the number of operations to compute the discriminant of this characteristic polynomial; so, $v_3 = O(r^{2+\frac{\omega}{2}} \log r \log \log r)$ by KW (in fact, a particular algorithm for resultants would give $v_3 = O(r^2 \log r \log \log r)$, but it wouldn't change the sum $v = v_1 + v_2 + v_3$).

As $\omega \geq 2$, we have $v_1 + v_3 = O(v_2)$. Consequently, $v = O(r^{\frac{\omega}{2}+2} \log r \log \log r)$.

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

To sum up:

Theorem 28 *There exists an algorithm to compute a **square-free** H -resolvent of a square-free polynomial $f \in k[T]$ with a complexity $\mathcal{A} + O(r^{\frac{3\omega}{2}+6} (\log r)^3 (\log \log r)^3)$, where \mathcal{A} is the complexity of evaluation of the precomputed multiplication table. It consists in computing a number $O(r^{\omega+4} (\log r)^2 (\log \log r)^2)$ of H -resolvents of f , among which one at least is square-free.*

INPUT:

- a system of fundamental invariants $(\Pi_1, \dots, \Pi_n, \Sigma_1, \dots, \Sigma_r)$ of an invariant algebra $k[\mathbf{X}]^H$;
- the coefficients $A_k^{i,j} \in k[\mathbf{Y}]$ ($2 \leq i \leq j \leq r$, $1 \leq k \leq r$) of the generators $S_{i,j}$ of the algebraic relations between the fundamental invariants;
- a squarefree polynomial $f = T^n - \pi_1 T^{n-1} + \dots + (-1)^n \pi_n \in k[T]$.

The inputs (i) and (ii) are given from a precomputation depending only on the group H .

OUTPUT:

- scalars $\lambda_1, \dots, \lambda_r \in k$ such that $\Theta = \lambda_1 \Sigma_1 + \dots + \lambda_r \Sigma_r$ be a π -separating primitive H -invariant;
- the squarefree Lagrange resolvent $\mathcal{L}_{\Theta, f} \in k[T]$.

Proof – The multiplication table (specialized in π , given by the coefficients of f) is computed only once (complexity \mathcal{A}): it is independent of the choice of $\lambda \in S_r$. Then, we compute characteristic polynomials, and then their discriminants, for at most $|S_r| = O(r^{\omega+4}(\log r)^2(\log \log r)^2)$ different values of λ , each one costing at most $O(r^{\frac{\omega}{2}+2} \log r \log \log r)$. \square

7 More examples

We present here a few examples to illustrate the properties of discriminants studied in §4.

7.1 The alternated group \mathfrak{A}_n , as a subgroup of \mathfrak{S}_n

We choose $\Pi_i = E_i$ for $1 \leq i \leq n$. Then, $r = 2$, and we can choose $\Sigma_1 = 1$ and $\Sigma_2 = \prod_{1 \leq i < j \leq n} (X_j - X_i)$. Then, $\Sigma_2^2 = \delta(\mathbf{\Pi})$. So, for any $\pi \in k^n$, $\mathfrak{J}_\pi = (Z_1 - 1, Z_2^2 - \delta(\pi))$. It is radical if and only if $\delta(\pi) \neq 0$. Besides, $\Delta = \delta(\mathbf{Y})\Lambda_2^2$. We say that \mathcal{L}_{Σ_2} is a *universally separable resolvent*, because for any $f = T^n - \pi_1 T^{n-1} + \dots + (-1)^n \pi_n$ in $k[T]$, $\mathcal{L}_{\Sigma_2, f}$ is squarefree from the moment that f is squarefree.

7.2 \mathfrak{S}_2 , subgroup of \mathfrak{S}_3

Let H be the subgroup of \mathfrak{S}_3 generated by the transposition $(1, 2)$. Then, the algebra invariant $k[\mathbf{X}]^H$ 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 $\Pi_i = E_i$ ($1 \leq i \leq 3$), $\Sigma_1 = 1$, $\Sigma_2 = X_3$ and $\Sigma_3 = X_3^2$. The ideal \mathfrak{J} of the algebraic relations is generated by $S_0 = Z_1 - 1, S_{2,2} = Z_2^2 - Z_3, S_{2,3} = Z_2 Z_3 - Y_3 + Y_2 Z_2 - Y_1 Z_3$ ($S_{3,3} = Z_3^2 - Y_1 Y_3 - (Y_3 - Y_1 Y_2) Z_2 - (Y_1^2 - Y_2) Z_3$ is generated by $S_{2,2}$ and $S_{2,3}$). The jacobian matrix of $(S_{2,2}, S_{2,3})$ is $\begin{pmatrix} 0 & 0 & 0 & 2Z_2 & -1 \\ -Z_3 & Z_2 & -1 & Z_3 + Y_2 & Z_2 - Y_1 \end{pmatrix}$: its rank is 2 for every specialization

of $(Y_1, Y_2, Y_3, Z_2, Z_3)$, so that the tangent space to \mathcal{V} is everywhere of dimension $5 - 2 = 3 = \dim \mathcal{V}$: we find $\text{Sing } \mathcal{V} = \emptyset$.

Then, we compute the discriminant of $\Theta_{\Lambda} = \Lambda_1 \Sigma_1 + \Lambda_2 \Sigma_2 + \Lambda_3 \Sigma_3$ (Δ is the discriminant of Θ_{Λ} in $k[\Lambda] \otimes_k k[\mathbf{Y}, \mathbf{Z}]/\mathcal{J}$ seen as a $k[\Lambda, \mathbf{Y}]$ -algebra).

$$\Delta = \delta \cdot ((Y_3 - Y_1 Y_2) \Lambda_3^3 - (Y_2 + Y_1^2) \Lambda_2 \Lambda_3^2 - 2 Y_1 \Lambda_2^2 \Lambda_3 - \Lambda_2^3)^2,$$

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 $T^3 - Y_1 T^2 + Y_2 T - Y_3$.

As $\Delta(0, 1, 0, \mathbf{Y}) = \delta$, the resolvent $\mathcal{L}_{\Sigma_2} = \chi_{\Sigma_2}(T)$ is also a universally separable resolvent (which is not surprising, as $\mathcal{L}_{\Sigma_2, f} = f$), but $\mathcal{L}_{\Sigma_3, f}$ is not.

7.3 Dihedral group \mathfrak{D}_4 , subgroup of \mathfrak{S}_4

We define $H = ((1, 3, 2, 4), (1, 2))$ (subgroup of \mathfrak{S}_4). The invariant algebra $k[\mathbf{X}]^H$ has the following Hironaka decomposition:

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

where $\Pi_i = E_i$ ($1 \leq i \leq 4$), $\Sigma_1 = 1$, $\Sigma_2 = X_1 X_2 + X_3 X_4$ and $\Sigma_3 = \Sigma_2^2$. We compute $\Delta = \delta \Delta'$, where $\delta = \text{discrim}_T(T^4 - Y_1 T^3 + Y_2 T^2 - Y_3 T + Y_4)$ and $\Delta' = (A_{0,3}(\mathbf{Y}) \Lambda_3^3 + A_{1,2}(\mathbf{Y}) \Lambda_2 \Lambda_3^2 - 4 Y_2 \Lambda_2^2 \Lambda_3 - \Lambda_2^3)^2$, with $A_{0,3} = (8 Y_2 - Y_1^2) Y_4 - Y_3^2 - Y_1 Y_2 Y_3 - 2 Y_2^3$ and $A_{1,2} = 4 Y_4 - Y_1 Y_3 - 5 Y_2^2$.

As $\Delta(0, 1, 0, \mathbf{Y}) = \delta$, the resolvent $\mathcal{L}_{\Sigma_2} = \chi_{\Sigma_2}(T)$ is a universally separable resolvent.

7.4 The metacyclic subgroup of \mathfrak{S}_5

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

For $\Theta = \Sigma_2$, we compute

$$\Delta_{\Theta} = \delta_5^3 \cdot (\Delta'_{\Theta})^2,$$

where $\delta_5 = \text{discrim}_T(T^5 - Y_1 T^4 + Y_2 T^3 - Y_3 T^2 + Y_4 T - Y_5) \in k[\mathbf{Y}]$ and $\Delta'_{\Theta}(\mathbf{Y})$ is too big to be written, but can be recovered thanks to the usual linear transformation $T \mapsto T + Y_1/5$ from $\Delta'_{\Theta}(0, Y_2, \dots, Y_5)$, with

$$\begin{aligned} \Delta'_{\Theta}(0, Y_2, \dots, Y_5) = & 9765625 Y_5^6 + ((390625 Y_3^2 + 2812500 Y_2^3) Y_4 - 1875000 Y_2^2 Y_3^2 - \\ & 928125 Y_2^5) Y_5^4 + (-1250000 Y_2^2 Y_3 Y_4^2 + (1187500 Y_2 Y_3^3 + 1012500 Y_2^4 Y_3) Y_4 - \\ & 175000 Y_3^5 - 225000 Y_2^3 Y_3^3) Y_5^3 + (250000 Y_2^4 Y_4^3 + (-15625 Y_3^4 - 850000 Y_2^3 Y_3^2 - \\ & 135000 Y_2^6) Y_4^2 + (478125 Y_2^2 Y_3^4 + 175500 Y_2^5 Y_3^2 + 18225 Y_2^8) Y_4 - 93750 Y_2 Y_3^6 - \\ & 60000 Y_2^4 Y_3^4 - 12150 Y_2^7 Y_3^2 - 729 Y_2^{10}) Y_5^2 + ((50000 Y_2^2 Y_3^3 + 60000 Y_2^5 Y_3) Y_4^3 + \\ & (-32500 Y_2 Y_3^5 - 92500 Y_2^4 Y_3^3 - 10800 Y_2^7 Y_3) Y_4^2 + (9000 Y_3^7 + 45050 Y_2^3 Y_3^5 + \\ & 9720 Y_2^6 Y_3^3 + 486 Y_2^9 Y_3) Y_4 - 5700 Y_2^2 Y_3^7 - 1584 Y_2^5 Y_3^5 - 108 Y_2^8 Y_3^3) Y_5 - \\ & 10000 Y_2^4 Y_3^2 Y_4^4 + (-625 Y_3^6 + 17500 Y_2^3 Y_3^4 + 1800 Y_2^6 Y_3^2) Y_4^3 + (-10825 Y_2^2 Y_3^6 - \\ & 2015 Y_2^5 Y_3^4 - 81 Y_2^8 Y_3^2) Y_4^2 + (2610 Y_2 Y_3^8 + 623 Y_2^4 Y_3^6 + 36 Y_2^7 Y_3^4) Y_4 - \\ & 216 Y_3^{10} - 59 Y_2^3 Y_3^8 - 4 Y_2^6 Y_3^6. \end{aligned}$$

It was proved in [ArVa93] that $\Delta'_{\Theta}(e_1, \dots, e_5) \neq 0$ when $f = T^5 - e_1 T^4 + \dots - e_5$ is irreducible. Therefore, \mathcal{L}_{Σ_2} is a *quasi-universally separable resolvent* in the sense that $\mathcal{L}_{\Sigma_2, f}$ is squarefree if f is irreducible. Our computation confirms this

fact when f is in Bring-Jerrard's form (*i.e.* when $e_1 = e_2 = e_3 = 0$): indeed, $\Delta'(0, 0, 0, e_4, e_5) = 9765625e_5^6$ cancels only for polynomials $f = T^5 + e_4T - e_5$ that satisfy $e_5 = 0$, hence not irreducible.

7.5 $\mathfrak{C}_2 \times \mathfrak{C}_2$, 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 $\Pi_i = E_i$ ($1 \leq i \leq 4$). Then $r = 6$, and we can choose $\Sigma_1 = 1$, $\Sigma_2 = X_1X_2 + X_3X_4$, $\Sigma_3 = X_1X_3 + X_2X_4$, $\Sigma_4 = \Sigma_2^2$, $\Sigma_5 = \Sigma_2\Sigma_3$, $\Sigma_6 = \Sigma_2^2\Sigma_3$. 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 Λ . It is too large to be displayed, but can be recovered (as in the former example) from its specialisation in $Y_1 = 0$:

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

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:

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

Therefore, the resolvent $\mathcal{L}_{\Sigma_2 - \Sigma_3}$ is not universally separable. In particular, $\mathcal{L}_{\Sigma_2 - \Sigma_3, f}$ is not squarefree for $f = T^4 + a$, $a \in k$, or for $f = T^4 + 6T^2 - 4T + 2$.

7.6 Matrix subgroup

We define $H = \{\text{Id}, A, \dots, A^5\}$ where $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$; $k[\mathbf{X}]^H = \sum_{i=0}^4 k[\mathbf{\Pi}] \Sigma_i$

with $n = 3$, $r = 4$, $\Pi_1 = X_3^2 + X_2^2 + X_1^2$, $\Pi_2 = (X_2 - X_1) X_3 + X_1 X_2$, $\Pi_3 = X_3^6 + X_2^6 + X_1^6$, $\Sigma_1 = 1$, $\Sigma_2 = X_3^4 + X_2^4 + X_1^4$, $\Sigma_3 = -X_1 X_3^3 + X_2^3 X_3 + X_1^3 X_2$, $\Sigma_4 = -X_1 X_3^5 + X_2^5 X_3 + X_1^5 X_2$, $\Theta = \Lambda_1 \Sigma_1 + \Lambda_2 \Sigma_2 + \Lambda_3 \Sigma_3 + \Lambda_4 \Sigma_4$

Computation of the ideal \mathfrak{d} : Thanks to the algorithm of §6.2, 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 $f_1 = -Y_1 + 2 Y_2$,

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

$f_3 = 243 Y_3^2 + (92 Y_2^3 + 384 Y_1 Y_2^2 + 60 Y_1^2 Y_2 - 286 Y_1^3) Y_3 + 12 Y_2^6 + 48 Y_1 Y_2^5 +$

$168 Y_1^2 Y_2^4 + 148 Y_1^3 Y_2^3 - 84 Y_1^4 Y_2^2 - 60 Y_1^5 Y_2 + 43 Y_1^6$, $f_4 = f_2 \Lambda_4^2 + 3 f_1 \Lambda_3^2$,

and f_5 is a homogeneous polynomial in Λ of degree 4 over $k[\mathbf{Y}]$, too big to be written here. Therefore, the ideal \mathfrak{d} is

$$\mathfrak{d} = f_1 f_2 f_3 \cdot (f_1, f_2) \cdot \mathfrak{b},$$

where \mathfrak{b} is the ideal of $k[\mathbf{Y}]$ generated by the coefficients of f_5 seen as an element of $k[\mathbf{Y}][\mathbf{A}]$. We compute the following Gröbner basis of \mathfrak{b} , with respect to the lexicographical order: $(Y_2^4 + \frac{31}{4}Y_2^2Y_1^2 - \frac{11}{2}Y_2Y_1^3 + \frac{3}{4}Y_1^4, Y_2^3Y_1 - \frac{5}{2}Y_2^2Y_1^2 + 2Y_2Y_1^3 - \frac{1}{2}Y_1^4, Y_3^2 - \frac{121}{1296}Y_1^6, Y_3Y_2 - \frac{1}{2}Y_3Y_1 - Y_2Y_1^3 + \frac{1}{2}Y_1^4, Y_2^2Y_1^3 - \frac{5}{6}Y_2Y_1^4 + \frac{1}{6}Y_1^5, Y_3Y_1^3 - \frac{11}{36}Y_1^6, Y_2Y_1^5 - \frac{1}{2}Y_1^6, Y_1^8)$. 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, contrary to what happens 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 eigenspace $k \cdot (1, -1, 1)$. 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, $\mathfrak{d} \cdot \mathfrak{h} = \mathfrak{d}$, and $\sqrt{\mathfrak{d}} \cap \mathfrak{h} = \sqrt{\mathfrak{d}} = (f_1 f_2 f_3) = (\delta)$, as announced in Cor. 17. Here, the property (11) 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 $\delta(\boldsymbol{\pi}) \neq 0$ if and only if there exists $\boldsymbol{\lambda} \in k^4$ such that $\Delta(\boldsymbol{\lambda}, \boldsymbol{\pi}) \neq 0$. In other words, $\mathfrak{a}_\boldsymbol{\pi}$ is radical if and only if $\mathfrak{J}_\boldsymbol{\pi}$ is radical.

8 Conclusion

We described a fast method to compute among invariants, illustrated by a fast computation of Lagrange resolvents. The reason of the great velocity of the method is the structure of the data, represented by evaluation programs (straight line programs) thanks to a geometric Noether position. This high velocity has a price: it requires a precomputation of the Noether position and of the related multiplication table, which is done for the moment by a classical representation of the data (“rewriting”).

We hope in the future to be able to do this precomputation thanks to a straight line program too.

We intend also to apply an extension of our method to the computation of relative resolvents, following the ideas of [Co95] and [Co97i].

Another hope is to apply this data structure to the resolution of system of polynomial equations with symmetries.

References

[ArVa93] Arnaudiès, J.M., Valibouze, A.: Résolvantes de Lagrange. Prepublication LITP 93.63, December 1993.

- [ArVa97] 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.
- [Ab04] Abdeljaoued, J., Lombardi, H.: Méthodes matricielles – Introduction à la complexité algébrique. Mathématiques & applications **42**, Springer, 2004.
- [Ax92] **AXIOM**, The Scientific Computation System. R.D. Jenks, R.S. Sutor. Springer-Verlag, 1992.
- [Be15] Berwick, E.H.: The condition that a quintic equation should be soluble by radicals, Proc. London Math. Soc. (1915) **2.14**, 301-307.
- [Co95] Colin, A.: Formal Computation of Galois Groups with Relative Resolvents. In Cohen, G., Giusti, M. and Mora, T. editors, proc. AAEECC'95, Lecture Notes in Computer Science **948**, 169-182. Springer, Berlin, 1995.
- [Co96] Colin, A.: Solving a System of Algebraic Equations with Symmetries (1996). In Journ. Pure and Applied Algebra vol. 117-118 (1997) p. 195-215.
- [Co97i] Colin, A.: Relative resolvents and partition tables in Galois group computations. In Gloor, O., Proc. ISSAC'97 (1997).
- [Co97t] 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.
- [CLO98i] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer, 1992. Springer, 1998.
- [CLO98u] Cox, D., Little, J., O'Shea, D.: Using Algebraic Geometry. Springer, 1998.
- [DaSc] Dahan, X., Schost, É., Wu, J.: Evaluation properties of invariant polynomials, Journal of Symbolic Computation, to appear.
- [DaFo89] Darmon, Ford: Computational verification of M_{11} and M_{12} as Galois groups over \mathbb{Q} . Comm. Algebra **17** (1989); 2941-2943.
- [DeKe02] Derksen, H., Kemper, G.: Computational Invariant Theory. Springer-Verlag, Berlin, 2002.
- [Ei96] Eichenlaub, Y., Problèmes effectifs de théorie de Galois en degrés 8 à 11, thèse de doctorat de l'Université de Bordeaux 1, 1996.
- [Ge97] Geißler, K.: Sur Berechnung von Galoisgruppen. Diplomarbeit, Technische Universität Berlin, 1997.
- [GeKl00] Geißler, K., Klüners, J.: Galois Group Computation for Rational Polynomials, J. Symbolic Computation (2000) **20**, 1-23.
- [GiHe91] 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.

- [GHS93] Giusti, M., Heintz, J., Sabia, J.: On the efficiency of effective nullstellensätze. *Comput complexity* **3** (1993), 56-95.
- [GHMP95] 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.
- [GHHM+96] 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).
- [GHMP97] 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).
- [GrHa81] Greenberg, M., Harper, J.R.: *Algebraic Topology: A First Course*. Benjamin Cummings, 1981.
- [HeSc82] 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.
- [HMW99] Heintz, J., Matera, G., Waissbein, A.: On the time-space complexity of geometric elimination procedures. Manuscript of Universidad Favaloro, Buenos Aires, Argentina, 1999.
- [HoEa71] Hochster, M., Eagon, J.A., Cohen-Macaulay Rings, invariant theory, and the generic perfection of determinantal loci. *Amer. J. Math.* **93** (1971), 1020-1058.
- [Ke96] Kemper, G.: Calculating Invariant Rings of Finite Groups over Arbitrary Fields (1995). *Journal of Symbolic Computation* (1996) **21**, 351-366.
- [McSo85] McKay, J., Soicher, L.: Computing Galois groups over the rationals. *J. Number Theory* (1985) **20**, 273-281.
- [ReVa99] Rennert, N., Valibouze, A.: Calcul de résultantes avec les modules de Cauchy. *Experimental Mathematics* (1999) 8:4.
- [Sh94] Shafarevich, I.R.: *Basic Algebraic Geometry*. Springer, 1994.
- [St79] Stanley, R.P.: Invariants of finite groups and their applications to combinatorics. *Bul. (New Series) American Math. Soc.* Vol. 1 Num. 3 (1979).
- [St73] Stauduhar, R.P.: The Determination of Galois Groups. *Math. Comp.* **27** (1973) 981-996.
- [St93] Sturmfels, B.: *Algorithms in Invariant Theory*. Springer-Verlag, Wien, 1993.

- [Yo97] Yokoyama, K.: A modular method for computing the Galois groups of polynomials, *Journal of Pure and Applied Algebra* (1997) **117-118**, 617-636.
- [ZaSa60] Zariski, O., Samuel, P., *Commutative Algebra*. Graduate Texts in Math., Springer, 1960.